

وزارة التعليم العالي والبحث العلمي

جامعة يحيى فارس المدينة

كلية العلوم الإنسانية والاجتماعية

فرقة مشروع البحث التكويني الجامعي P.R.F.U

الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها



أعمال الملتقى الوطني الافتراضي

أعمال الملتقى الوطني الافتراضي



Ministry of Higher Education and Scientific Research

University of Medea

Faculty of Humanities and Social Sciences

The University's Formative Research Project Team-PRFU
Cybercrimes in the Algerian society, their effects and how to confront them

Code : I05L02UN260120190001

Proceedings of the Virtual National Forum

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني

15 مارس 2022

إعداد وتحرير:
د. رقية محمودي
د. نور الهدى قدوح

تصميم الغلاف: فؤاد حلوان

هيئة النشر العلمي:
جامعة يحيى فارس المدينة

الجرائم الإلكترونية في المجتمع الجزائري

CYBERCRIME IN ALGERIAN SOCIETY

Diagnosing reality and cybersecurity challenges

Preparation and editing:

Dr. Mahmoudi Reguia

Dr. Guedouh Nour El Houa

March, 15th 2022

Cover Design : Fouad Hallouane

Scientific Publishing Authority:
Yahya Fares Medea University

ISBN : 978-9931-9892-0-2



9 789931 989202



أعمال الملتقى
الوطني الافتراضي

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني

© groupe de chercheurs, 2022
ISBN : 978-9931-9892-0-2
Dépôt Légal : juillet 2022

© مجموعة من الباحثين ، 2022
ISBN : 978-9931-9892-0-2
الإيداع القانوني : جويلية 2022

اعداد وتحرير:

د. رقية محمودي

د. قدوح نور الهدى

الطبعة الأولى: 2022

البحوث الواردة في هذا الكتاب محكمة ، ولا تعبر الا على رأي أصحابها

جميع الحقوق محفوظة © Copy Right

2022

جميع الحقوق محفوظة ، ولا يسمح بطبع أو نسخ أو إعادة نشر هذا الكتاب أو أي جزء منه أو تخزينه في اطار استعادة المعلومات ، بأي شكل من الأشكال ، دون اذن خطي مسبق من الناشر
All rights reserved. NO part of this book may be reproduced, stored in retrieval system, or transmitted in any form means, without prior permission in writing of the publisher

هيئة النشر العلمي، جامعة يحيى فارس المدية
العنوان: جامعة يحيى فارس المدية، الطريق الوطني رقم 18، القطب الحضري، المدية 26000

أعمال الملتقى الوطني الافتراضي

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني

15 مارس 2022

الإيداع القانوني : جويلية 2022

إعداد وتحرير :
د. رقية محمودي
د. نور الهدى قدوح

تصميم الغلاف :
فؤاد حلوان

أعضاء اللجنة العلمية

أ.د / مزاري توفيق عبد الصمد.....جامعة يحيى فارس المدينة
أ.د جمال معتوق.....جامعة علي لونيبي البلدية 02
أ.د / حوييتي أحمد.....جامعة الجزائر 02
أ.د / سواكري الطاهر.....جامعة علي لونيبي البلدية 02
مقدم دقيش عبد الغني

المعهد الوطني للأدلة الجنائية وعلم الاجرام الدرك الوطني

حماني سمير.....نائب رئيس مجلس قضاء المدينة
دكاني نبيل.....نائب عام مساعد أول - مجلس قضاء المدينة
تاكروست علي.....عميد قضاة التحقيق بمحكمة المدينة
أ.د / منادلي محمد.....جامعة يحيى فارس المدينة
أ.د / عمور محمد.....جامعة يحيى فارس المدينة
أ.د / بن قطاف محمد.....جامعة يحيى فارس المدينة
أ.د / بوحية وسيلة.....المركز الجامعي مرسلبي عبد الله تيبازة
أ.د / بوشياوي اسمهان.....جامعة وهران 02
د / لدرع نبيلة.....المركز الجامعي مرسلبي عبد الله تيبازة
أ.د / رامي حليم.....جامعة البلدية 02
أ.د / بيبمون كلثوم.....جامعة الحاج لخضر باتنة 01
د / عمير عبد القادر.....جامعة البلدية 02
د / قنيبي يوسف.....جامعة يحيى فارس المدينة
د / بضياف عادل.....جامعة يحيى فارس المدينة
د / محمودي رقية.....جامعة يحيى فارس المدينة
د / بن عائشة نبيلة.....جامعة يحيى فارس المدينة
د / ولد قويل خليفة.....جامعة اكلي محند الحاج البويرة
د / معطاوي موسى.....جامعة اكلي محند الحاج البويرة
د / لدرم أحمد.....جامعة يحيى فارس المدينة
د / رتيبي أسماء.....جامعة يحيى فارس المدينة
د / قاسم سعاد.....المركز الجامعي أفلو
د / غوالم أمينة.....جامعة يحيى فارس المدينة
د / بلقاسم عادل.....جامعة يحيى فارس المدينة
د / سنوسي حياة.....جامعة يحيى فارس المدينة
د / لكحل صليحة.....المركز الجامعي تيسمسيلت



جامعة يحيى فارس المدينة
كلية العلوم الإنسانية والاجتماعية
فرقة مشروع البحث التكويني الجامعي P.R.F.U
الجرائم الإلكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها



الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني

15 مارس 2022

هيئة الملتقى

الرئيس الشرفي للملتقى: أ.د. جعفر بوعروزي، مدير جامعة يحيى فارس المدينة
المدير الشرفي للملتقى: أ.د. موسى هيصام، عميد كلية العلوم الإنسانية والاجتماعية
رئيسة الملتقى: د. محمودي رقية
التنسيق والإشراف: د. جاب الله يوسف
رئيس اللجنة العلمية: د. حاج الله مصطفى
رئيس اللجنة التنظيمية: د. بناول محمد

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني

محاور الملتقى:

البعد القانوني:

- المحور 01: فلسفة التشريع الجنائي الرقمي
- المحور 02: واقع وتحديات التشريعات القانونية في مواجهة الجرائم السيبرانية.
- المحور 03: إشكاليات قانونية تتعلق بطرق التحري والاثبات للدليل الرقمي

البعد الأمني:

- المحور 01: واقع الجرائم الإلكترونية في المجتمع الجزائري "قياس الجريمة الإلكترونية"
- المحور 02: التهديدات السيبرانية وانعكاساتها على الأمن المجتمعي.
- المحور 03: تحديات الأمن السيبراني في مواجهة مخاطر الجرائم الإلكترونية.

البعد السوسولوجي:

- المحور 01: إشكالية انتقال الفعل الإجرامي من الواقع المادي الى الواقع الافتراضي.
- المحور 02: السلوك الإجرامي الرقمي عبر المنصات الإلكترونية
- المحور 03: تحليل أبعاد السلوك الإجرامي الرقمي وانعكاساته على المستوى الفردي والمجتمعي.



بالانترنت OnLine Connectivity وتزايد نسب الاجرام السيبراني ، وهذا ما تعكسه الصورة العالمية للموصولة بالانترنت، والصورة العالمية للجريمة الالكترونية وتكاليف الأمن السيبراني.

والجزائر- كغيرها من دول العالم- تشهد نموا متزايدا في نسب الاجرام المعلوماتي وهذا ما تعكسه الإحصاءات الجنائية المسجلة على مستوى المؤسسات الأمنية والقضائية ، والتي تعكس صورة واقع ودلالات الاجرام السيبراني وعلاقته بالفضاء الرقمي، والذي يفرض بذاته أبعادا وتحديات جديدة ومتداخلة على المستويين التشريعي والأمني، في مجال تحديد العلاقة التكاملية للكشف عن سياقات الفعل الإجرامي الرقمي ضمن فلسفة تشريعية رقمية توائم خصوصيته من خلال تحديد ماهيته وتحديد وسائل الإثبات والتحري "حجية الدليل الرقمي"، ومن جانب الأمني فواقع الفعل الإجرامي تمخض عنه جملة من تحديات الأمن السيبراني في مجال مواجهة الجريمة الإلكترونية.

وعليه تتمحور إشكاليتنا في منطلقات التشخيص الواقع للإجرام السيبراني وتحديات الأمن السيبراني في المجتمع الجزائري وانعكاساته على الفرد والمجتمع.

أهداف الملتقى:

1. تشخيص واقع الإجرام السيبراني في المجتمع الجزائري.
2. تحديد مضامين ودلالات الاجرام السيبراني "الجرائم الالكترونية" وعلاقتها بالفضاء الرقمي وانعكاساته على الفرد والمجتمع.
3. الكشف عن أبعاد جديدة متداخلة مع الجانب التشريعي والأمني اللذان يحددان العلاقة التكاملية للكشف عن سياقات الفعل الإجرامي الرقمي.
4. بيان تحديات الأمن السيبراني في مكافحة الجريمة الالكترونية في المجتمع الجزائري.

الديباجة:

الجريمة الالكترونية cyber crime جريمة مستحدثة مستجدة، كانت نتاج تطور تكنولوجيا المعلومات والاتصال وما أفرزته الثورة الرقمية المعلوماتية، اذ انتقلت من مفهوم الضيق المتعلق بجرائم الحاسوب، الغش المعلوماتي، إلى جرائم الانترنت، إلى الجرائم المتعلقة بالمعالجة الآلية للمعطيات، وهذا باعتبار الحاسوب بيئة الكترونية لارتكاب الجريمة، أو وسيلة تنفذ من خلالها جرائم مستحدثة أخرى كالاختيال الالكتروني، أو أن تكون هدفا للجريمة في البيئة الافتراضية الالكترونية التي تمخض عنها جرائم مستحدثة القاسم المشترك بينها استعمال التقنية والمعلوماتية في تنفيذ جرائم عديدة.

ومما لاشك فيه أن الجرائم الإلكترونية تختلف في مضمونها وجوهرها، فكل جريمة تعكس طابعها الخاص بها، ووسائلها وأساليبها الخاصة بها أيضا كما توحى بوجود سهولة الهدف والفرصة السانحة لارتكاب مثل هذه الجرائم المختلفة، التي تأخذ صورا عديدة داخل بوتقة المعلوماتية التي تضمن جانباً من السرية في ادائها على المستوى الاقليمي أو الدولي وتتنافس وفق نوعها ونوع المستهدف، ونوع الجاني ومستوى تنفيذه (فردى /مجتمعي/كوني).

وتتعد أنماط الإجرام المعلوماتي، وسمات الفعل الإجرامي والمجرم في الفضاء السيبراني، مبرزة بذلك فجوة التباين بين ملامح الواقع المادي للفعل الإجرامي التقليدي، والواقع الافتراضي للفعل الإجرامي الرقمي المستحدث، كما تتباين تحليلات المقاربات النظرية في تحديد العوامل الكامنة لارتكاب السلوك الإجرامي المعلوماتي وسمات المجرم المعلوماتي من عوامل مرتبطة بالفضاء السيبراني "التعلم الاجتماعي الجنائي"، والضغط العامة "و" العوامل الاقتصادية والاجتماعية"، مبرزة بذلك صلة الموصولة

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني

كلمة السيد : أ.د جعفر بعروري
مدير جامعة يحيى فارس المدية
الرئيس الشرفي للملتقى

الجرائم الالكترونية في المجتمع الجزائري: تشخيص الواقع وتحديات الأمن السيبراني 15 مارس 2022 قاعة المحاضرات بالمصالح المشتركة بالقطب الجامعي ، جامعة المدية.

بسم الله الرحمن الرحيم

السلام عليكم ورحمة الله وبركاته

- السادة ممثلي مجلس قضاء المدية .
- السيد ممثل عن المصلحة المركزية لمكافحة الاجرام السيبراني الدرك الوطني.
- السادة الأفاضل عن أمن ولاية المدية "فرقة مكافحة الجريمة المعلوماتية، والمصلحة الولائية للتكوين، خلية الاتصال والعلاقات العامة ".
- السادة نواب مدير جامعة يحيى فارس كل باسمه ومقامه.
- السيد عميد كلية العلوم الإنسانية والاجتماعية و السادة عمداء الكليات.
- السادة نواب عميد كلية العلوم الإنسانية والاجتماعية .
- الاسرة الإعلامية عن التلفزيون الجزائري وإذاعة المدية الجهوية.
- السادة الحضور والمشاركون في الملتقى الوطني الافتراضي.

أن التطور التقني في مجال تكنولوجيا الاعلام والاتصال والاعتماد على نظم المعلومات وشبكة الحواسيب والانترنت " ومن خلال إساءة استخدام نظم المعلومات الالية استحدث بدوره أنماط إجرامية جديدة " الجريمة المعلوماتية" ، هذا النمط الاجرامي الذي اتخذ منحى تصاعديا لاسيما فيما يتعلق بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال ، منها جرائم المساس بالأشخاص وجرائم المساس بالأنظمة المعلوماتية على وجه الخصوص كما تعكسه الإحصاءات الأمنية والقضائية.

وعليه كان هذا الملتقى الوطني الافتراضي الموسوم ب : " الجرائم الالكترونية في المجتمع الجزائري:

تشخيص الواقع وتحديات الأمن السيبراني" المنظم من طرف فرقة بحث المشروع التكويني الجامعي PRFU " الجرائم الالكترونية في المجتمع الجزائري انعكاساتها وسبل مواجهتها" بقسم العلوم الاجتماعية " كلية الإنسانية والاجتماعية، بجامعة المدية ، والذي تشرف بمشاركة جهات أمنية وقضائية والممثلة في مجلس

قضاء المدية، بالإضافة الى المصلحة المركزية لمكافحة الاجرام السيبراني للدرك الوطني، وفرقة مكافحة الجريمة المعلوماتية الى جانب مصلحة التكوين الولائي لأمن ولاية المدية.

وهذا قصد الإحاطة بإشكالية الملتقى وأهدافه المتمثلة في تشخيص واقع الاجرام السيبراني في المجتمع الجزائري وآليات مكافحته، من منظور ثلاثي الأبعاد ينطلق من تأصيل تشريعي للإجرام الرقمي، وبعد أمني من خلال قياس الجريمة الالكترونية وتحديات الأمن السيبراني، من أجل فهم وتحليل أبعاد الفعل الاجرامي الرقمي وانعكاساته على المستوى الفردي والمجمعي، وهذا ما تجلّى من خلال محاور الملتقى.

هذا الملتقى الذي تضمن برنامجه مداخلات علمية قيمة من طرف باحثين أكاديميين من مختلف الجامعات الجزائرية المشاركة، نأمل من خلالها تشخيص الظاهرة الاجرامية الرقمية، وتقديم إضافة علمية وعلمية للجهات القضائية والأمنية .

أهلا بكم في جامعة يحيى فارس المدية ، وتمنياتي لكل بالتوفيق والنجاح.

السيد : أ.د جعفر بوعروزي

مدير جامعة يحيى فارس المدية

كلمة الكتاب

"الجرائم الالكترونية في المجتمع الجزائري: تشخيص الواقع وتحديات الأمن السيبراني" ملتقى وطني ضمن نشاط فرقة البحث التكويني الجامعي PRFU "الجرائم الالكترونية في المجتمع الجزائري: انعكاساتها وسبل مواجهتها"، المعتمد بتاريخ 2019/01/1، تمحورت اشكاليته حول منطلقات التشخيص الواقعي للإجرام السيبراني وتحديات الأمن السيبراني في المجتمع الجزائري وانعكاساته على الفرد والمجتمع، بهدف تشخيص واقع الاجرام السيبراني في المجتمع الجزائري. وتحديد مضامين ودلالات الاجرام السيبراني "الجرائم الالكترونية" وعلاقتها بالفضاء الرقمي وانعكاساته على الفرد والمجتمع، مع الكشف عن أبعاد جديدة متداخلة مع الجانب التشريعي والأمني اللذان يحددان العلاقة التكاملية للكشف عن سياقات الفعل الاجرامي.

وبناء عليه فقد تم الإحاطة النظرية بالظاهرة الاجرامية الرقمية بأبعادها الثلاث: "القانوني، الأمني، السوسولوجي"، ضمن محاور الملتقى، لاسيما من خلال الكشف عن التحديات التشريعية في مواجهة الجرائم السيبرانية، وكذا تحديات الأمن السيبراني في مواجهة مخاطر الجرائم الالكترونية، وذلك لفهم وتحليل إشكالية سياق الفعل الاجرامي الرقمي.

1. الملتقى الوطني... بالأرقام

تضمن كتاب الملتقى¹ 35 مداخلة علمية منها 17 مداخلة فردية بنسبة 48.57 %، و 18 مداخلة ثنائية بنسبة 51.42 %، شملت الأبعاد الثلاث للملتقى بكل محاوره على النحو الآتي:

البعد	المحور	عدد المداخلات	%
البعد القانوني 11 مداخلة 31.42%	فلسفة التشريع الجنائي الرقمي	06	34.28
	واقع وتحديات التشيعات القانونية في مواجهة الجرائم السيبرانية	03	33.33
	إشكاليات قانونية تتعلق بطرق التحري والاثبات للدليل الرقمي	02	16.16
البعد الأمني 10 مداخلات 28.53 %	واقع الجرائم الالكترونية في المجتمع الجزائري "قياس الجريمة الالكترونية"	06	60
	التحديات السيبرانية وانعكاساتها على الأمن المجتمعي	03	30
	تحديات الأمن السيبراني في مواجهة مخاطر الجرائم الالكترونية	01	10
البعد	إشكالية انتقال الفعل الاجرامي من الواقع المادي الى الواقع	06	42.57

¹ تتعلق فقط بالمداخلات المقبولة للنشر في الكتاب

		الافتراضي	السوسيولوجي
28.57	04	تحليل أبعاد السلوك الاجرامي الرقمي وانعكاساته على المستوى الفردي والمجتمعي	14مداخلة %40
28.57	04	السلوك الاجرامي الرقمي عبر المنصات الالكترونية	
35 مداخلة		09 محاور	3 أبعاد

وهذا بمشاركة 54 أستاذ باحث وطالب دكتوراه من كلا الجنسين بنسبة 53.7 اناث، و46.29 ذكور ، منهم أربع 4 أساتذة رتبة أستاذ تعليم عالي ، وتسعة عشر 19 أستاذ برتبة أستاذ محاضر أ ، وأربعة 4 أساتذة برتبة أستاذ محاضر ب، إضافة الى وأربعة 4 أساتذة بصفة أستاذ مؤقت، بالإضافة الى ثلاث وعشرون 23 طالب في طور الدكتوراه والذين جل مداخلاتهم هي مداخلات ثنائية بمعية آساتذهم المشرفين. المشاركون يمثلون 23 مؤسسة جامعية على المستوى الوطني ، وبمشاركة مجلس قضاء المدية.

2. الملتقى الوطني ... من حيث المحتوى

أ. البعد القانوني:

من خلال المقالات المتعلقة بالبعد القانوني للجريمة الالكترونية والمتنقة للنشر، تم طرح ومعالجة الإشكاليات القانونية الآتية:

- التحديات التي واجهت المشرع الجزائري في عملية سن القوانين لمواجهة الجريمة السيبرانية، و مدى توفيقه في كبح جماح مرتكبيها.
- مدى فعالية القطب الجزائري الوطني في الحد من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- الجريمة الالكترونية ومدى معالجتها ومكافحتها دوليا ووطنيا.
- مدى فعالية السياسة الجنائية المتبعة من قبل المشرع الجزائري في مجال التحري والكشف ومكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات
- التطرق الى علم اللسانيات الجنائية الذي يعتبر نمط جديد لكشف الجريمة وتحقيق العدالة، من خلال تحديد ماهيته، نشأته وتطوره، أهميته في مجال التحقيق والاثبات الجنائي.
- التطرق الى جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني في حماية التوقيع الإلكتروني

- التطرق الى حجية الدليل الرقمي في اكتشاف الجرائم الإلكترونية، من خلال بيان السلطة التقديرية للقاضي الجنائي في تقدير الدليل الرقمي والمقصود بمبدأ الاقتناع الشخصي للقاضي الجنائي في تقدير الدليل الرقمي وتوضيح ضوابط الاقتناع الشخصي للقاضي الجنائي.
 - الضمانات القانونية الموضوعية والشكلية والاجرائية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية التي أوردها المشرع الجزائري في القانون 04/09 لحماية حقوق وحرية الأفراد
- ب. البعد الأمني:**

- من خلال المقالات المتعلقة بالبعد الأمني للجريمة الالكترونية تم تسليط الضوء على النقاط التالية:
- ماهية الجرائم الالكترونية، دوافع واسباب ارتكابها، تهديداتها للأمن المجتمعي وسبل مواجهتها والحد منها.
 - مفهوم الاجرام السيبراني، طرق مواجهته وسبل تحقيق الأمن السيبراني.
 - واقع الجريمة الالكترونية في المجتمع الجزائري وتطورها، والاليات المسخرة لمواجهة تحدياتها.
 - التعريف بالأجهزة الأمنية المكلفة بالتصدي ومحاربة الجريمة الالكترونية.
 - دور الأجهزة الأمنية في الحد من الجريمة الالكترونية في المجتمع الجزائري.
 - عرض بعض الاحصائيات والتجارب الخاصة بالمؤسسات الأمنية في التصدي لهذه الظاهرة.
 - تحليل الاحصائيات والأرقام المتعلقة بهذا النمط من الجرائم على المستوى المحلي والوطني.
 - مقارنة النتائج المتوصل اليها من خلال الدراسات والبحوث المتعلقة بالظاهرة.
 - الخروج بمجموعة من التوصيات التي من شأنها الاسهام في مواجهة الظاهرة.

ج. البعد الاجتماعي

لقد أفرز تزايد استعمال شبكات الاتصال الحديثة والأنظمة المعلوماتية إشكالات سوسيولوجية هامة اتفقت مع محتوى المداخلات في العديد من الجوانب الاجتماعية للفعل الاجرامي الرقمي وآثاره على الفرد والمجتمع، وذلك من خلال تحليل ماكرو و ميكروسوسيولوجي لأهم أنواعه و عوامله و التي أظهرت تواجد مزيج متشابه و متداخل من العوامل سواء عوامل فردية أو عوامل بيئية اجتماعية اقتصادية أو سياسية تدفع بالأفراد او الجماعات الى مخالفة القواعد التي تنظم السلوك بصفة عامة في المجتمع من جهة و من جهة اخرى انتشار اضرار و سلبيات مبطنة تحت ما يسمى بالمحتوى الرقمي والتي تهدد تماسك النظم و الأبنية الاجتماعية على المدى القريب و المتوسط و البعيد.

فمن أبرز جرائم الفعل الرقمي نجد المخدرات الرقمية، المحتوى الرقمي الموجه للأطفال، التنمر السيبراني وغيرها، والتي تعتبر مخرجات متطورة للجريمة الالكترونية و هذا ما يعكس تماما دور العولمة الرقمية لعولمة الجرائم السيبرانية جراء التطور الهائل لتكنولوجيات الاعلام والاتصال ، المنصات الرقمية و مواقع التواصل الاجتماعي .
و عليه أبرزت واتفقت جميع آراء الباحثين و المختصين على تبني فكرة نشر ثقافة المواطنة الرقمية في الجزائر كاتجاه وأسلوب فعال لمواجهة أخطار و سلبات الجرائم السيبرانية، وأيضا على مدى أهمية و فاعلية مؤسسات التنشئة الاجتماعية بمختلف مستوياتها وكذلك السلطات و الهيئات المختصة بمختلف أنواعها على نشر التوعية و انشاء خطط و برامج شاملة وجادة على المستوى الاجتماعي، الثقافي، الاقتصادي، السياسي و القانوني من شأنها القضاء على العوامل المؤدية الى الفعل الاجرامي الرقمي .

كل الشكر والتقدير والعرفان للهيئة المشرفة على الملتقى الوطني وعلى رأسها الرئيس الشرفي للملتقى الأستاذ الدكتور **جعفر بوعروري** ، مدير جامعة يحيى فارس المدية ، و المدير الشرفي للملتقى الأستاذ الدكتور **موسى هيصام**، عميد كلية العلوم الإنسانية و الاجتماعية ، و مسؤول هيئة النشر العلمي بجامعة المدية الأستاذ الدكتور **شبوطي حكيم** ، و الهيئات الأمنية والقضائية المشاركة، و كل الأساتذة والطلبة المشاركين من مختلف المؤسسات الجامعية.

كل الشكر والتقدير والعرفان لأعضاء اللجنة العلمية، كل باسمه ومقامه و الذين لم يدخروا أي جهد علمي في تقييم و تحكيم المداخلات العلمية بكل جدية و أمانة علمية، وكذا أعضاء اللجنة التنظيمية ونخص بالذكر كل من طلبة الدكتوراه* **مرازية عادل**، **خبزاي مراد** الذين سهروا على تنظيم وتنسيق هذه الأعمال البحثية - تحت اشراف رئيسة الملتقى - والتي احتوت هذا المنتج العلمي الذي نأمل أن يرقى لمستوى التطلعات العلمية.
وفي الأخير نأمل اننا وفقنا في الإحاطة بإشكالية الملتقى الوطني: "الجرائم الالكترونية في المجتمع الجزائري : تشخيص الواقع وتحديات الأمن السيبراني، بأبعاده الثلاث. من خلال المساهمات النوعية لمختلف المشاركين الباحثين.

رئيسة الملتقى

د. رقية محمودي، جامعة يحيى فارس المدية

* طلبة دكتوراه علم الاجتماع بجامعة المدية

تقديم الكتاب

الحمد لله رب العالمين والصلاة والسلام على عبده ورسوله الأمين محمد ابن عبد الله وعلى آله الطاهرين الطيبين وأصحابه اجمعين.

اما بعد

يعد موضوع الجرائم السيبرانية او المسماة تارة بالجرائم الالكترونية من المشكلات الاجتماعية الأكثر تهديدا للمجتمعات الحديثة وهذا لما لهذه الظاهرة من خصائص تجعلها تتحدى جل وسائل الضبط الاجتماعي ومؤسساته الضبطية والردعية.

وكغيرها من المشكلات الاجتماعية، تتميز الجرائم السيبرانية حسب وصف العالم "اميل دوركايم" بالقهر والتسلط والخروج عن إرادة الافراد، أي انها موجودة ودائمة الانتشار والاستمرارية عبري الزمان والمكان. كما تعرف: " بالجرائم الحديثة والمعاصرة التي تختلف كلياً عن الجرائم التقليدية والكلاسيكية من خلال خصائص الجاني، الجريمة وطبيعتها، موضوع الجريمة، والوسائل او الادوات المستعملة في تنفيذها". وقد قال بعض المختصين في شان الجرائم السيبرانية او الالكترونية: "الجرائم التي يتحها الفضاء السيبراني هي، من ناحية أخرى، جرائم يسهلها التزايد المطرد في قدراتنا التكنولوجية (مثل الاحتيال الالكتروني والتجارة الالكترونية في سلع غير مشروعة، مثل المخدرات او الأسلحة النارية، واستغلال الأطفال والتعدي عليهم جنسيا من خلال الانترنت."

كما ان هذا النوع من الجرائم لا يعرف حدود جغرافية ولا يخص مجتمع دون الاخر، بل انه ينتشر في كافة بقاع المعمورة، ولكن بنسب ومستويات متباينة، وهذا حسب درجة التطور التكنولوجي واستخدام الحاسوب ووسائل التواصل الحديثة، بالإضافة الى ظهور مجرمين مختصين في المجال الالكتروني.

والجزائر كغيرها من بلدان العالم لا تخلو من هذه الظاهرة التي أصبحت تشكل هاجسا وتهديدا لأمن وسلامة البلاد والعباد. وكون هذه الجريمة، كما سبق الإشارة اليه، عابرة للحدود، ولا تميز بين بلد واخر، فان الجزائر بدورها عرفت ولا تزال تعرف ارتفاعا كبيرا في عدد الجرائم السيبرانية حسب ما أكدته التقارير الأمنية والاكاديمية، الامر الذي دفع بالمشروع الى سن العديد من القوانين ووضع الخطط والاستراتيجيات للحد من هذه المشكلة.

وفي ظل هذا الوضع تأتي الجهود التي بذلتها جامعة "يحيى فارس ومن خلالها كل من كلية العلوم الإنسانية والاجتماعية وبالخصوص فرقة مشروع البحث التكويني الجامعي، جاءت اعمال هذا الملتقى العلمي وفق إشكالية

دقيقة وهادفة، كمحاولة للتنقيب والبحث في ظاهرة الجريمة السيبرانية في الجزائر، تحت عنوان "الجرائم الالكترونية في المجتمع الجزائري. تشخيص والواقع وتحديات الامن السيبراني"، وهذا بتاريخ 15 مارس 2022. ومن بين الأهداف التي سطرها هذا الملتقى وسعى لتحقيقها من خلال مداخلات الخبراء والأساتذة الباحثين نذكر:

- تشخيص واقع الاجرام السيبراني في المجتمع الجزائري.
- تحديد مضامين ودلالات الاجرام السيبراني "الجرائم الالكترونية" وعلاقتها بالفضاء الرقمي وانعكاساته على الفرد والمجتمع.
- الكشف عن ابعاد جديدة متداخلة مع الجانب التشريعي والأمني اللذان يحددان العلاقة التكاملية للكشف عن سياقات الفعل الاجرامي الرقمي.
- بيان تحديات الامن السيبراني في مكافحة الجريمة الالكترونية في المجتمع الجزائري.

ولتحقيق هذه الأهداف قسمت اعمال هذا الملتقى العلمي الى ثلاثة ابعاد وهي: البعد القانوني، البعد الأمني والبعد السوسولوجي. حيث حاولت اللجنة العلمية لهذه التظاهرة حصر ظاهرة "الجرائم الالكترونية" من جميع جوانبها، وذلك لفهم طبيعتها، اليات نشاطها وخصوصيتها وسبل مواجهتها. أي ان الملتقى من خلال هذه الكيفيات في التعامل مع المشكلة حاول الانطلاق من النظرية الشمولية او المسماة بنظرية العوامل المتعددة لتحليل وفهم هذه الظاهرة.

فيما يخص محاور هذا الملتقى جاءت منسجمة مع الابعاد السابقة الذكر، حيث اعطي لكل بعد ثلاثة محاور. بالنسبة للبعد القانوني نجد المحاور:

- المحور 01: فلسفة التشريع الجنائي الرقمي.
 - المحور 02: واقع وتحديات التشريعات القانونية في مواجهة الجرائم السيبرانية.
 - المحور 03: إشكاليات قانونية تتعلق بطرق التحري و الاثبات للدليل الرقمي.
- بالنسبة للبعد الأمني نجد المحاور الآتية:

- المحور 01: واقع الجرائم الالكترونية في المجتمع الجزائري "قياس الجريمة الالكترونية".
 - المحور 02: التهديدات السيبرانية و انعكاساتها على الامن المجتمعي.
 - المحور 03: تحديات الامن السيبراني في مواجهة مخاطر الجرائم الالكترونية.
- وأخيرا البعد السوسولوجي او الاجتماعي والذي خصصت له المحاور التالية:

المحور 01: إشكالية انتقال الفعل الاجرامي من الواقع المادي الى الواقع الافتراضي.

المحور 02: السلوك الاجرامي الرقمي عبر المنصات الالكترونية.

المحور 03: تحليل ابعاد السلوك الاجرامي الرقمي وانعكاساته على المستوى الفردي والمجتمعي.

من الملاحظات التي نسجلها ونشير اليها هنا، ان جل اعمال الملتقى التي تم قبولها من طرف أعضاء اللجنة العلمية للملتقى وهذا بعد عملية تقييم صارمة ساهت في ضمان جودة ونجاح فعاليات هذه التظاهرة العلمية. كما لا يفوتنا هنا الإشارة الى السهر الدؤوب والمجهودات المضاعفة التي بذلتها الدكتورة رقية محمودي بصفتها رئيسة الملتقى وهذا منذ الوهلة الأولى، أي عند كان هذا الملتقى مجرد فكرة الى يوم تنظيمه والخروج بالتوصيات. دون ان ننسى رئيس الملتقى الشرفي و المتمثل في الأستاذ الدكتور جعفر بوعرووي ، مدير جامعة يحيى فارس المدنية و المدير الشرفي للملتقى الأستاذ الدكتور موسى هيصام ، عميد كلية العلوم الإنسانية و الاجتماعية. كما لا يفوتنا ان نشكر المقدم دقيش عبد الغني بالمعهد الوطني للأدلة الجنائية وعلم الاجرام الدرك الوطني، ونائب رئيس مجلس القضاء بالمدينة، ونائب عام مساعد اول لمجلس القضاء المدنية، عميد قضاة التحقيق بمحكمة المدينة، وكل اعضاء فرقة البحث، وأعضاء اللجنة التنظيمية للملتقى والأساتذة الذين ساهموا في إنجاح هذا الملتقى الوطني الأول من نوعه بكلية العلوم الإنسانية والاجتماعية بجامعة يحيى فارس المدنية. في الختام نتمنى المزيد من النجاح والتألق لأعضاء فرقة مشروع البحث التكويني الجامعي 'الجرائم الالكترونية في المجتمع الجزائري، وانعكاساتها، وسبل مواجهتها'، في أعمالهم المستقبلية وان تسلط المزيد من الأضواء على ظاهرة الجرائم الالكترونية وهذا للحد منها ولما لا الوصول الى التنبؤ بحجمها وابعادها مستقبلا. وفقنا الله في خدمة العلم والنهوض بالجامعة الجزائرية.

البروفيسور جمال معتوق

جامعة البليدة 2، مدير مخبر الجريمة والانحراف بين الثقافة والتمثيلات الاجتماعية

الجلسة الافتتاحية

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني



مقدمات في الجريمة السيبرانية

البروفيسور معتوق جمال

مدير مخبر الجريمة والانحراف بين الثقافة والتمثلات الاجتماعية ، جامعة علي لونيبي البليدة2

مقدمة:

تعد الجريمة بأنواعها المختلفة من الظواهر الاجتماعية التي أرهقت المشتغلين بمسائل الأمن وسلامة الأفراد والمجتمعات من جهة وعلماء الاجتماع والإجرام والنفس وغيرها من العلوم الأخرى الاجتماعية وذلك لما لها من مخاطر على حياة الأفراد والمجتمعات الإنسانية من جهة أخرى.

كما كانت ولا تزال من أخطر المشكلات الاجتماعية التي تواجهها المجتمعات باختلاف درجة تقدمها ونموها، إذ أصبحت تنتشر بقوة وسرعة في كافة البلدان.

هذا وقد ارتبطت الجريمة بكل من التغير الاجتماعي والضبط الاجتماعي وذلك لما لها من خصائص ومميزات تجعلها تتكاثر بسرعة.

وفي هذا العمل سوف نسلط الضوء على أحد أنواع الجرائم المستحدثة والمتمثلة في الجرائم السيبرانية أو الإلكترونية، والتي تعد اليوم بمثابة أكبر تهديد تعيشه المجتمعات الإنسانية. ولما كانت الجريمة من ميزات التنوع والتطور والتكاثر عبر الزمان والمكان، فالجريمة السيبرانية كانت وليدة هذا التغير الاجتماعي والثقافي والاقتصادي الذي عرفته و لا تزال تعرفه المجتمعات الإنسانية.

إن الجريمة السيبرانية عكس الجرائم الكلاسيكية، تتميز بعدة خصائص تجعلها صعبة المنال وتتطلب آليات ووسائل جديدة للمواجهة، عكس الجرائم الكلاسيكية. وعليه نسعى من وراء هذا العمل عرض بعض الأفكار التي نراها بالأساسية حول هذا النوع من الجرائم وذلك حتى يتسنى للباحثين الوقوف على هذه المشكلة الاجتماعية الحديثة.

1. مصطلح " جريمة سيبرانية Cyber-Criminalité :

مصطلح دخيل على القاموس اللغوي العربي وهو تسمية أطلقت في الدول الغربية للإشارة إلى الجرائم التي ترتكب عن طريق استعمال أو توظيف جهاز الكمبيوتر -الحاسب الآلي- وبالتالي هي ترجمة حرفية للتسمية التي أطلقت عليها في الدول الغربية ويمكن القول بأنها: "Une Transcription" أي نسخ للكلمة كما أطلق عليها في بيئتها الأصلية.

وعليه فمصطلح الجرائم السيبرانية هو مصطلح حديث ومعاصر بالنسبة للمجتمعات العربية عامة والجزائر خاصة، إلا أن استعماله وتداوله بين مختلف الأوساط الاجتماعية وليس الأصلية فقط أصبح جد منتشرا.

هذا ولما ارتبط مفهوم السيبرانية (Cyber) بالجريمة وجب علينا أولا تحديد معنى الجريمة (Crime) فنقول: ورد في لسان العرب أن جرم بمعنى جنى جريمة، وجرم إذا عظم جرمه أي ذنبه (ابن منظور، 1990).

أصل كلمة جريمة من جرم بمعنى كسب وقطع، ويظهر أن هذه الكلمة خصصت من القديم للكسب المكروه وغير المستحسن، ولذلك كانت كلمة جرم يراد منها الحمل على فعل حصل آثم (الهاشمي، 2005، صفحة 15).

وتطلق كلمة جريمة على ارتكاب كل ما هو مخالف للحق والعدل والطريق المستقيم، واشتقت من ذلك كلمة إجرام وأجرموا، فقد قال الله تعالى: " إن الذين أجرموا كانوا من الذين آمنوا يضحكون " (سورة المطففين، الآية 29). وقوله: "كلوا وتمتعوا قليلا إنكم مجرمون" (سورة المرسلات، الآية 46). وقوله تعالى: " إن المجرمين في ضلل وسعر " (سورة القمر، الآية 47).



نستنتج من هذه الآيات وغيرها من الآيات الأخرى التي تطرقت إلى الجريمة على أن هذا الفعل أو السلوك:

- فعل نهي الله عنه.
- شكل من أشكال العصيان لما أمر الله به.
- الانحراف والابتعاد عن الطريق المستقيم.

والجرم هو التعدي وهو الذنب والجمع أحزم والمجرم هو المذنب والكافر، وقد وردت مشتقات الفعل (جرم) 66 مرة في القرآن الكريم.

وعليه نستطيع أن نقول:

أن الجريمة فعل ما نهي الله عنه وعصيان ما أمر الله به، أو عبارة أعم هي عصيان ما أمر الله به بحكم الشرع الشريف، وأن تعريف الجريمة على هذا النوع يكون مرادفا لتعريف الفقهاء لها بأنها إتيان فعل محرم معاقلة على فعله، أو ترك فعل مأمور به معاقب على تركه، وذلك لأن الله تعالى قرر عقابا لكل من يخالف أوامره ونواهيه، وهو إما أن يكون عقابا دنيويا ينفذه الحاكم، وإما أن يكون تكليفا يكفر به عما ارتكب في جنب الله، وإما أن يكون عقابا أخرويا يتولى تنفيذه الحاكم الديان، وهو خير الفاصلين (الامام محمد، 1998، صفحة 19)

وهذا وللإشارة فإن كل الديانات السماوية منها وغير السماوية قد وقفت موقفا مناهضا ورافضا للسلوك الإجرامي، بل حرمة وحاربه في آن واحد، وهذا لما لهذا السلوك أو الفعل من انعكاسات وتهديدات للبناء الاجتماعي. بعد تعريف الجريمة لغة وفقها من المنظور الديني الإسلامي نقدم لها بعض التعاريف السوسولوجية حتى يتسنى لنا الوقوف على أبعادها ودلالاتها الاجتماعية.

أول ملاحظة يجب الإشارة إليها هنا هو أن التعريف القانوني كان دائما هو السباق وكذلك المهيم على كافة أعمال علماء الاجتماع من جهة الاقتراب السوسولوجي للظاهرة.

ومن بين التعاريف القانونية نذكر أن الجريمة هي: "ذلك الفعل الذي يعاقب عليه بموجب القانون" (عثمان الصديق و اخرون، 2002، صفحة 235)

وبمعنى آخر هي: "ذلك الفعل أو الامتناع الذي نص القانون على تجريمه، ووضع عقوبة جزاء على ارتكابه" (عثمان الصديق و اخرون، 2002، صفحة 35).

أما سوسولوجيا فنقول:

تعرف الجريمة اجتماعيا بأنها رد فعل يخالف الشعور العام للجماعة، وأنها أي فعل فردي أو جماعي يشكل خرقا للقواعد الضبط الاجتماعي التي أقرها المجتمع، والذي يمكن التعبير عنه بمجموعة القيم والتقاليد والأعراف السائدة في المجتمع. " (اسماعيل عبيد، 1993، صفحة 97)

وعند إميل دور كايم الجريمة هي "كل فعل أو امتناع يتعارض مع القيم والأفكار التي استقرت في وجدان الجماعة." (Durkheim , 1977, p. 67)



ومن التعريف السابق نستنتج أن مثالا بالنسبة لموضوع الجريمة السيبرانية هي فعل يسلكه فرد أو جماعة من الأفراد باستعمال الوسائل التكنولوجية الحديثة والمتمثلة في الكمبيوتر -الحاسب- أو الهاتف الخليوي وغيرها من الوسائل لنشر الفيروسات عبر الأجهزة التابعة للبنوك أو المؤسسات الخدمانية أو أي قطاع من قطاعات الدولة بهدف تعطيله، أو تخريبه، أو سرقة البيانات والمعلومات.

وعليه تكون الجريمة الإلكترونية أو السيبرانية نشاط إجرامي إما يستهدف أو يستخدم -يوظف- جهاز الكمبيوتر أو شبكة كمبيوتر أو جهاز متصل بالشبكة العنكبوتية، معظم الجرائم السيبرانية وليس كلها ترتكب من طرف مجرمين سيبرانيين (Cybercriminals) أو قراصنة (Pirates) في الإعلام الآلي.

ويمكن أن يكون المغزى من وراء هذه الجرائم هو:

- الحصول على الأموال.
 - الفدية من طرف الإرهابيين.
 - التجسس.
 - الحروب الإلكترونية بين المؤسسات والأنظمة.
- من جهته حدد جيمس ديفير الجريمة قائلا هي كل سلوك ينحرف عن معايير المجتمع السياسي، ويقصد به المجتمع الذي تحكمه القوانين التي تشرف على صياغتها وتقود عملية تنفيذها سلطة منظمة معترف بها اجتماعيا ورسميا، وبالتالي فإن الجريمة هي كل فعل يعاقب عليه القانون" (Davis , 1970, p. 193)
- هذا وللإشارة أنه لا يوجد اتفاق بين علماء الاجتماع فيما يخص تعريف شامل وكامل للجريمة، إلا أنهم إتفقوا على ثلاثة عناصر أساسية لهذا المفهوم وهي: (احمد محمد، 1959، صفحة 110).
- الضرر الاجتماعي الذي ينطوي عليه الفعل الإجرامي من تهديد للمجتمع في كيانه.
 - أفعال وسلوكيات مخالفة للشعور العام ولقواعد الضبط الاجتماعي الرسمي (القوانين والأنظمة) أو غير الرسمي (العادات والتقاليد والأعراف والقيم والمعايير الاجتماعية) ..
 - إن الجريمة ليس فعلا بحد ذاته بماديته، بل بصفته بنظر المجتمع، فإذا لم تصل جماعة إلى حد الاعتقاد بأن فعلا معيناً يخل بمصلحة اجتماعية فإنما لا تعده جريمة.

2. تعريف الجريمة السيبرانية:

إن الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، فجرائم الانترنت، إلى آخر المصطلحات الجرائم السيبرانية (آل جار الله،، 2007، صفحة 70)

كما تعرف الجرائم السيبرانية بأنها: "هي التي تتم بواسطة الكمبيوتر أو أحد الوسائل التقنية الحديثة على كمبيوتر آخر أو أحد الوسائل التقنية الحديثة مع ضرورة توفر شبكة الاتصال فيما بينها (مهمل، 2018، صفحة 9).



هذا وقد عرفت كذلك بأنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود." (القرعان، 2017، صفحة 19) وعليه يمكن القول بأن الجريمة السيبرانية أو الإلكترونية هي من الجرائم الممكن تسميتها بـ:

- الحادثة.

- العابرة للحدود.
- التي توظف الوسائل الإلكترونية كالحاسوب أو الهواتف الخلوية.
- تهدف إلى إلحاق الضرر والأموال.
- في تطور مستمر وهذا التطور الهائل الذي تعرفه الوسائل الإلكترونية ومختلف أجيالها.

وعليه يمكن القول أن هناك العديد من المحاولات سعى أصحابها تعريف الجريمة الإلكترونية أو السيبرانية من خلالها، وفي ها المبحث سنحاول عرض بعضها.

تعتبر الجريمة الإلكترونية من الظواهر الحديثة لارتباطها بالتكنولوجيا الحديثة، ولقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، حيث لم يتفق الفقه على تعريف محدد بل إذ بعض الفقهاء ذهب إلى ترجيح عدم وضع تعريف بحجة أن مثل هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني (ممدوح، 2008، صفحة 17) ومنه نقول بأنه مثل باقي المفاهيم والمصطلحات الخاصة بالظواهر الاجتماعية، تعرف هذه الظاهرة -الجريمة الإلكترونية- صعوبة التحديد أو التعريف وهذا راجع إلى خصائصها من جهة وإلى الانتماءات الإيديولوجية للمشتغلين بالعلوم الاجتماعية ومن جهة أخرى وتعدد المدارس الاجتماعية.

كذلك البحث عن تعريف شامل وكامل ومانع في الحقيقة ما إلا هو ضرب من الخيال والمثالية وعليه لا يوجد في نظرنا تعريف شامل وكامل.

في تسمية الجريمة الإلكترونية:

نشير هنا إلى الجريمة الإلكترونية عدة تسميات، ومنها نذكر:

- الجرائم السيبرانية.
- الجرائم المعلوماتية.
- جرائم الحاسوب والانترنت.
- جرائم التقنية العالية.
- جرائم الباقات البيضاء.

هذا التنوع في التسميات راجع إلى الوسائل المستعملة في ارتكاب الجريمة من طرف المجرمين السيبرانيين تارة والمساس أو ارتكاب الجريمة من خلال الهجمات على هذه الوسائل كالحاسوب والهواتف الجدة متطورة وغيرها من وسائل الاتصال والإعلام.



كذلك للإشارة هنا أن المجرمين السيبرانيين يختلفون جذريا عن المجرمين الكلاسيكيين، حيث يرتكبون جرائمهم دون استعمال القوة الجسدية أو الأسلحة المعروفة البيضاء أو النارية، بل يلجئون إلى توظيف العقل والذكاء الإلكتروني في القيام بالقرصنة أو التخريب أو السطو على المعلومات والبيانات... إلخ.

3. مميزات وخصائص الجرائم السيبرانية:

الكلام عن الجرائم السيبرانية يجرنا إلى التطرق بشيء من الإيجاز إلى خصائص هذه الظاهرة التي أصبحت اليوم تنتشر في كافة بلدان العالم بدرجات متباينة.

ومن بين هذه المميزات والخصائص نذكر:

1.3 ترتكب بواسطة الأجهزة الإلكترونية:

تتميز هذه الجريمة كونها تنفرد في خصوصياتها من حيث أنها يعتمد في ارتكابها على الوسائل والأجهزة الإلكترونية كالمبيوتر، الهواتف الخلوية والانترنت بصفة عامة.

كما أنها تعد من الجرائم المستحدثة: أي حديثة العهد ولها أدواتها الإجرامية الخاصة مقارنة بالجرائم الكلاسيكية.

2.3 جرائم خفية أو غير مرئية:

ليس من السهولة اكتشافها لضعف القدرة الفنية للضحية وذلك مقارنة للضحية، وربما أيضا لمهارات المجرم الفنية والعلمية المتقدمة لقدرته على إخفائها، أو لخوف الضحية من الإبلاغ عن الجريمة تجنباً للإساءة إلى السمعة (القرعان، 2017، صفحة 39).

تعد كذلك من الجرائم الافتراضية، الأمر الذي يزيد في تعقيدها وصعوبة الوقوف عليها أو رؤيتها وعليه فهي جرائم خفية Invisible يصعب على الضحية اكتشافها نظراً لما تتميز به هذه الجريمة من مميزات خاصة.

3.3 السرعة في التنفيذ:

تتميز هذه الجريمة المستحدثة في كونها ترتكب في وقت جد قياسي مقارنة بالمدة الزمانية التي ترتكب فيها الجرائم الكلاسيكية، فهي جرائم سريعة التنفيذ والوقوع وهذا لاعتمادها على الانترنت أو الوسائط الافتراضية.

4.3 ترتكب عن بعد:

كذلك من خصائص هذا النوع من الجرائم هو أنها ترتكب عن بعد يمكن للمجرم تنفيذ جرمته وهو في بلد أو مكان آخر يبعد مئات الكيلومترات عن مكان وقوع الجريمة.

5.3 عابرة للحدود:

فهي تمارس من بلد أو جهة نحو بلد أو جهة جغرافية ما، فهي تعبر الحدود دون تنقل الجاني، حيث يستطيع هذا الأخير دون التنقل من بلده أو الجهة التي يتواجد فيها إلحاق الضرر بالضحية المتواجدة في بلد أو جهة تختلف تماماً عن موطنه.

6.3 لا يتم التبليغ عنها:

جرائم لا يتم في أغلب الأحيان التبليغ عنها، خاصة إذا تعلق الأمر بالمؤسسات والشركات التجارية، تجنباً للسمعة أو اهتزاز ثقة العملاء (متعب الأسدي، 2015، صفحة 25).

نشير كذلك أن هذا النوع من الجرائم إذا مس مثلاً "قضايا الشرف" فغالبا ما تسعى العائلات في المجتمعات المحافظة كالجائز إلى التستر عليها وعدم التبليغ عنها، وهذا فيما يخص أخذ الصور للفتيات والسيدات في وضعيات محرجة واستعمالها كورقة تهديد وابتزاز.



7.3 جرائم غامضة: ويرجع هذا لغياب الركن المادي للجريمة، كون هذه الأخيرة لا تترك ورائها آثار مادية تسمح للشرطة والمحققين الوقوف عليها.

8.3 جرائم نعيمة: تتميز باللاعنف المادي نظرا لكون مرتكبيها لا يستعمل القوة الجسدية (الفيزيائية) لتحقيق أغراضه وأهدافه.

9.3 لا يمكن لأي كان القيام بمثل هذا النوع من الجرائم (السيبرانية) كونها تتطلب مهارات خاصة كالتحكم في تقنيات الإعلام الآلي والحاسوب.

تضاف للنقطة الخاصة بالخصوصية:

تتميز الجريمة السيبرانية بقلة عدد الحالات التي تم اكتشافها بالفعل إذا ما قارنا ذلك على ضوء ما يتم اكتشافه من الجرائم التقليدية، ويرى البعض أن من بين الأسباب وراء صعوبة اكتشاف هذه الجرائم يرجع إلى تميزها بأنه لا يشوب ارتكابها أي عمل من أعمال العنف، كما أنها لا تترك آثارا، وإنما يتمثل مظهرها في تغيير أو محو الأرقام والبيانات الموجودة بأنظمة الحسابات الآلية، ولا تترك آثارا خارجيا مرئيا أو ملموسا (رستم، 1994، صفحة 41).

يرى البعض صعوبة قبول هذا الرأي المتقدم على إطلاقه، فمن ناحية لا يقتصر أثر جرائم المعلوماتية على تغيير أو محو الأرقام والبيانات من الملفات المخزنة في ذاكرة الحاسب الآلي حتى في هذه الحالة فمجرد تغيير أو محو هذه البيانات يعد أثر على ارتكاب الفعل، فصعوبة اكتشافها وإثباتها يرجع إلى عدة أسباب من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضيف عليها الكثير من التعقيد، بالإضافة إلى الأحجام عن الإبلاغ عنها في حالة اكتشافها لحشية المجني عليهم من فقد ثقة عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن ثانية واحدة. (رستم، 1994، صفحة 42).

فعلا نحن نشاطر الرأي الثاني والذي يذهب بعيدا حيث لا يمكن حصر أو اقتصار أثر الجرائم السيبرانية على محو البيانات والمعلومات من الملفات المخزنة في ذاكرة الحاسب الآلي بل تكمن خصوصية وتمييز هذه الجريمة عن باقي الجرائم الأخرى في درجة تعقيدها، والسكوت عنها من طرف الضحايا وعدم الإبلاغ عنها، بالإضافة إلى .

4. القانون الجزائري والجريمة السيبرانية:

عملت العديد من الدول المتقدمة والسائرة في طريق النمو، ومنها الجزائري على تحديد وتعريف الجريمة السيبرانية وهذا نظرا لانتشارها في هذه المجتمعات، لقد أصبحت الجريمة السيبرانية حقيقية لا مفر منها بل هاجس يهدد أمن كافة المجتمعات ومنها الجزائر، وفي هذا المطلب سنحاول عرض نظرة المشرع الجزائري لهذه الجريمة المستحدثة.

عرف المشرع الجزائري الجرائم السيبرانية وأطلق عليها تسمية الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال، وعرفها بموجب الفقرة (أ) المادة 02 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على أنها : " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.



ولمواجهة هذا النوع من الجرائم فقد أمضت الجزائر العديد من الاتفاقيات مع العديد من الدول وذلك لتصنيف على المجرمين السيبرانيين من جهة والحد من مخاطر هذه الظاهرة من جهة أخرى.

كما أحدثت الجزائر ما يسمى بالمنظومة الوطنية لأمن الأنظمة المعلوماتية، حيث نجد أن المشرع الجزائري قد تبنى إستراتيجية جديدة لمكافحة الجرائم المعلوماتية، والتي استفحلت في السنوات الأخيرة، إذ قام بإنشاء منظومة وطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 والمتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

5. أنواع الجرائم الإلكترونية:

تحدد أنواع وأشكال الجرائم السيبرانية (الإلكترونية) مع تنوع تطلعات وغايات المجرمين السيبرانيين، وأصبحت تشكل إحدى المشكلات الاجتماعية المهددة للكيانات الاجتماعية.

ونظرا لتنوعها نحاول في هذا العمل ذكر البعض منها:

1.5 أمثلة عن بعض الجرائم السيبرانية:

- سرقة بيانات الشركات والمؤسسات الاقتصادية، التجارية وحتى وزارات الدولة بكل أنواعها.
- سرقة البيانات الشخصية للأفراد واستعمالها وهذا في إطار جرائم تزوير الهويات.
- الاحتيال عبر البريد الإلكتروني.
- السطو والسرقة للبيانات المالية وبطاقات الدفع.
- الابتزاز الإلكتروني والمساومة.
- التجسس الإلكتروني.
- الإرهاب الإلكتروني.
- التسول الإلكتروني.
- تعطيل وتخريب الأجهزة الإلكترونية من خلال نشر الفيروسات.
- تعطيل الخدمات المختلفة كالبنكية، تسيير الطرقات، الطيران.... الخ.
- الترويج للمعلومات الكاذبة.
- نشر البرامج الضارة في الأجهزة الإلكترونية.
- حجب الخدمة وشلها.
- بيع السلع غير المشروعة أو المزورة وغير الصالحة عبر الانترنت.
- الترويج للإباحية واستغلال القاصرين سنا.

2.5 شدة الاحترافية لدى الجاني ونوعية الوسائل المستعملة في الجريمة :

هذا وتشير إلى أنه رغم الائتلاف الواسع حول كون هذه الظاهرة لا تتسم بالعنف إلا أننا نرى بأن فعل الائتلاف والتخريب للمعلومات والبيانات هو عنف رمزي لا يقل درجة عن باقي الممارسات العنيفة الأخرى.



ومحو المعلومات والبيانات من أنظمة الحاسبات الآلية هو بمثابة غسل الأدمغة للضحايا، وعليه يمكن أن نطلق على جريمة السيرانية تسمية غسل ذاكرة (mémoire) أنظمة الحاسبات الآلية.

كما تعد هذه الجريمة من جرائم الياقات البيضاء، كون أن في أغلب الحالات ترتكب من طرف أشخاص متعلمين وذوي انتماءات طبقية محترمة، بل من طرف أصحاب مناصب وظيفية محترمة ومتعلمين، عكس الجرائم الكلاسيكية التي ترتكب من طرف أفراد أميين في أغلب الأحيان.

من جهة أخرى تعد مخاطر وانعكاسات الفعل الإجرامي السيبراني من اخطر الممارسات عواقب حيث ينجر عليه تعطيل نشاط الأجهزة الإلكترونية والخدمات التي تعتمد على هذه الأجهزة بل تهدد كل مظاهر الحياة الاجتماعية والاقتصادية.

3.5 الجرائم السيبرانية والجنس:

إن الإقبال على هذا النوع من الجرائم لا يخص أو يقتصر على نوع أو جنس بعينه دون الآخر، بل نجد عكس الجرائم الكلاسيكية أن الولوج إلى عالم الجرائم السيبرانية يخص الجنسين معا، حيث نجد من أطراف الجانحين أو المجرمين كل من الذكور والإناث وهذا لكون هذا الفعل لا يتطلب مثلا جهد عضلي معتبر يستحيل للمرأة - الأنثى - القيام به، بل بالعكس هو جرم متاح لكلا الجنسين دون أي تمييز.

هذا وقد أشارت النظريات الراديكالية الأنثوية في تناولها للجريمة السيبرانية، أن هذه الأخيرة بينت عبقرية الأنثى في إقبالها على الجريمة والتي كان البعض يرى بأنها خاصة بالرجال دون النساء.

ومنه يظهر جليا أن أغلب النظريات المفسرة للجريمة أصبحت اليوم قاصرة وغير قادرة على تفسير هذا النوع من الجرائم وهذا للأسباب الآتية:

- نظريات من إنتاج الذكور.
- نظريات تعمل على تكريس اللامساواة في ممارسة الجريمة بين الجنسين كما بينته أعمال مثلا الباحثة ريتا سيمون (Rita Simous) ومسير شميدت (Messerschmidt) وهاجان (Hagan) وتشني-ليند (Chesny-Lind) وغيرهم.

حيث تذهب جل هذه النظريات أن المرأة شأنها شأن الرجل قادرة على ممارسة أي جريمة مثل الذكور ولا يشكل الجانب الفيزيولوجي بالنسبة لها عائقا (معتوق، 2017).

إلا أن هذا لا ينفي وجود جرائم خاصة بالمرأة كإلجهاض، وقتل الأطفال الرضع، ووضع السم للأزواج، والدعارة... الخ، كما بينته أعمال العديد من العلماء الاجتماع وعلى رأسهم إميل دوركايم، أوتو بولاك (Otto Pollak)، وويليام إسحاق توماس (William Issac Thomas) وغيرهم من علماء الاجتماع الجنائي وعلم الإجرام.

6. طرق الجريمة الإلكترونية:

وقد لخصتها لنا الباحثة في النقاط الآتية:

1.6 تخريب المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات، تمزيق الكتب، تخريف المعلومات،

تخريف السجلات الرسمية... الخ.



- 2.6** سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني أو الصناعي أو العسكري أو تخريبها أو تدميرها... الخ.
- 3.6** تزوير المعلومات ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتخريفها، مثل تغيير علامات الطلاب.
- 4.6** تزيف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مضل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.
- 5.6** انتهاك الخصوصية ويشمل نشر المعلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر المعلومات عنهم أو وضع معلومات تخص تاريخ الأفراد ونشرها.
- 6.6** التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.
- 7.6** التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
- 8.6** التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.
- 9.6** السرقة العلمية، الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.
- 10.6** سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.
- 11.6** الدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.
- 12.6** قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.
- 13.6** قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمة الدخول وكلمة السر.
- 14.6** خلاعة الأطفال وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة، ولإلانات على الشبكات بشكل عام ونشر الجنس التخليبي.
- 15.6** القنال البريدية وتشمل إرسال الفيروسات لتدمير البيانات من خلال رسالة إلكترونية.
- 16.6** إفشاء الأسرار وتشمل الحصول على معلومات خاصة جدا ونشرها على الشبكة.
- 17.6** الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسويق أو المالية أو الهاتف... الخ.
- 18.6** سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.
- 19.6** التحرش الجنسي ويقصد به المضايقة من الذكور للإلانات أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة أو الملامسة.
- 20.6** المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإلانات أو العكس والتتبع بقصد فرض إقامة علاقة ما وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.



21.6 الإرهاب الإلكتروني ويشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرض الإرهاب ومصادرة هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.

وكتعليق على هذه النقاط نرى بأن هناك تنوع وكم هائل من الطرق الإجرامية الإلكترونية وهي في تزايد وتنوع مستمر نظرا لظهور فئات من الشباب خاصة المتحكمين في التكنولوجيا الحديثة للمعلومات (رشاد مرعي، 2016).

إلا أن هذا لا ينفي أن حتى فئة الكهول لها باع في إنتشار هذه الظاهرة.

وعليه نقول بأن الجريمة السيبرانية هي من أخطر الظواهر الاجتماعية المهددة للإستقرار والامن الاقتصادي والاجتماعي والسياسي للمجتمعات الانسانية اليوم. كما أنها من الجرائم المستحدثة والتي لا تتوقف عن النمو والتطور الأمر الذي يزيد من صعوبة مواجهتها. إلا أن هذا لا ينفي وجود جهود دولية ومحلية تعمل جاهدة على التصدي لهذه المشكلة بحزم وصرامة.

خاتمة:

بعد عرضنا هذا الوجيز لما أستخدم على تسميته بالجريمة السيبرانية أو المسماة كذلك بالجريمة الإلكترونية، تبين لنا أن هذه الظاهرة قد أصبحت اليوم ترهق كافة المجتمعات الإنسانية سواء منها المتقدمة أو السائرة في طريق النمو، كما أصبحت تشكل أكبر تهديد للإستقرار هذه المجتمعات وذلك لما تنفرد به من خصائص تجعل مواجهتها والحد منها من الأعمال الصعبة المنال. هذا وقد توصلنا إلى أن هذه الجريمة في تنوع وتزايد مستمر نظرا لتطور وسائل الاتصال والتكنولوجيا المعلوماتية. يجب انتظار تدفق هائل لأجيال من المجرمين السيبرانيين متحكمين في النظم المعلوماتية ومختلف تكنولوجيا الاتصال نظرا لإنفراد هؤلاء المجرمين بخصائص تجعلهم بعيدين عن قبضة العدالة.... إن الباقات البيضاء المهددة لأمن واستقرار الدول. وعليه أصبح من الضروري والملح تضافر جهود كافة الدول للحد من انتشار هذه المشكلة.

قائمة المراجع:

- إسراء جبريل رشاد مرعي. (9 أغسطس، 2016). الجرائم الإلكترونية: الأهداف-الأسباب-طرق الجريمة ومعالجتها. لمركز الديمقراطي العربي. democraticac.de.
- Durkheim , E. (1977). *les règles de la méthode sociologique*, édition P.U.F, Paris, 1977, p67. PARIS: édition P.U.F.
- Davis , J. (1970). *Social problem*. NEW.YORK: free press.
- بيروت. (Vol. 12) *سان العرب*. (1990). ابن منظور.
- ابو زهرة الامام محمد. (1998). ، *الجريمة والعقوبة في الفقه الإسلامي*، . القاهرة مصر: دار الفكر العربي.
- أسامة مهمل. (2018). *الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، . الجزائر: جامعة محمد بوضياف*.
- سورة المطففين. (الاية 29).
- سورة المرسلات. (الاية 46).
- سورة القمر. (الاية 47).
- جمال معنوق. (2017). *المرأة والجريمة، النظريات المفسرة للجرائم النسوية*. القاهرة، مصر: دار الكتاب الحديث.
- حسن اسماعيل عبيد. (1993). *سوسيولوجيا الجريمة*. لندن: شركة ميدلات المحدودة.
- خالد ممدوح. (2008). *أمن الجريمة الإلكترونية، الدار الجامعية الإلكترونية، الإسكندرية، مصر، 2008، ص 41*. الإسكندرية، مصر: الدار الجامعية الإلكترونية.
- خليفة احمد محمد. (1959). *النظرية العامة للتجريم*. القاهرة مصر: دار المعارف.
- سلوى عثمان الصديق، و اخرون. (2002). *إنحراف الصغار وجرائم الكبار*. الاسكندرية مصر: المكتب الجامعي الحديث.



عبد العزيز بن غرم الله آل جار الله، (2007). جرائم الأنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي، دراسة مقارنة. الرياض: دار الكتاب الجامعي.
لينا محمد متعب الأسدي. (2015). مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية. عمان، الأردن: دار الحامد للنشر والتوزيع.
محمد الهاشمي. (2005). موسوعة جرائم النساء العالمية والعربية. عمان، الأردن: دار أسامة للنشر والتوزيع.
محمود أحمد القرعان. (2017). الجرائم الإلكترونية، (المجلد 1). عمان: دار وائل للنشر والتوزيع.
هشام فريد رستم. (1994). قانون العقوبات ومخاطر تقنية المعلومات. أسبوط، مصر: مكتبة الآلات الحديثة.

التحديات القانونية لمواجهة الجرائم السيبرانية *

The Legal challenges to confronting cybercrime

د/ حمالي سمير نائب رئيس مجلس قضاء المدينة ، رئيس غرفة الاتهام

مقدمة:

لقد شكل التطور التكنولوجي و انتشار وسائل الاتصال مرتع جديد لظهور أشكال جديدة من الإجرام اصطلح عليه بالجريمة الإلكترونية أو الجريمة السيبرانية أو جرائم الانترنت أو الجريمة المعلوماتية , إذ من الطبيعي أن يصاحب التطور التقني ظهور أشكال من السلوكيات و أفعال تهدد أمن و استقرار المجتمع وتضر بمصالح الأشخاص ، الأمر الذي دفع بالمشرع في بعض الدول إلى تجريمها و تقرير عقوبات على

* مداخلة ألقيت ضمن المحور الأول المعنون " البعد القانوني " من الملتقى الوطني الافتراضي بتقنية التحاضر عن بعد حول "الجرائم الالكترونية في المجتمع الجزائري: تشخيص الواقع و تحديات الامن السيبراني " و المنظم من قبل كلية العلوم الانسانية و الاجتماعية بجامعة يحي فارس بالمدينة بالشراكة مع المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني ومجلس قضاء المدينة بتاريخ 15-03-2022
ب- أول نص قانوني في مجال جرائم المعلوماتية أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات صدر سنة 1988 في فرنسا بموجب القانون رقم 88-19 الصادر في 05 جانفي 1988 والمتعلق بالغش المعلوماتي ، و عدل هذا القانون بموجب القانون رقم 2004-575 الصادر في 21 جوان 2004، المتعلق بالثقة في الاقتصاد المعلوماتي والمعدل والمتمم في 11 جويلية 2011، بينما في الجزائر فإن أول نص تشريعي جزائري في مجال الإجرام المعلوماتي صدر في 26 جويلية 2001 بموجب القانون 01-09 في المواد 144 مكرر و 146 و 144 مكرر 1 و 144 مكرر 2 و 146 من قانون العقوبات الجزائري والمتعلق بجريمة القذف والسب إزاء رئيس الجمهورية أو فيما يخص دين الإسلام ، أو ضد الهيئات العمومية، حيث أدرج المشرع فيها لأول مصطلح وسيلة الكترونية أو معلوماتية وبعدها جاء القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 في الفصل السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر الى المواد 394 مكرر 7 ، ولقد تم تعديل هذا القانون بموجب القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها



مرتكبيها إذ أن التطور الحاصل في تكنولوجيا الإعلام والاتصال، وظهور شبكة الانترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام، لأنه بقدر ما أحدث آثار إيجابية وغير نمط حياة المجتمعات وساهم في التطور والرقى في جميع المجالات ولاسيما المعاملات الالكترونية، بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول، كل هذا تجلّى في تطويع الانترنت والوسائل الالكترونية لتكون عالما من عوالم الجريمة، وهكذا ظهرت إلى الوجود الجرائم الالكترونية بشتى أنواعها

هذا النوع من الجرائم ظهر نتيجة إساءة استخدام الأنظمة المعلوماتية أو استغلالها على نحو غير شرعي قصد الأضرار بمصالح الأفراد أو الجماعات وبذلك يتبين لنا أن جرائم "السيبرانية" هي جريمة مرتبطة أساسا بالتطور التقني العالي ظهرت بظهوره وتطور بتطوره ومن هنا كان لزاما على المشرع الجزائري مواكبة هذا التطور على غرار باقي الدول بسن تشريعات تعنى بمحاربة هذا النوع من الجريمة⁽¹⁾ وهو في الحقيقة تحدي وضع فيه المشرع الجزائري نتيجة التطور التكنولوجي في مجال الإعلام والاتصال و التجارة الالكترونية و بذلك يتضح جليا مدى اتساع رقعة التاثير التشريعي لهذا المجال سواء من حيث تاثير النشاطات المدرجة في هذا المجال او في مكافحة الجرائم المرتبطة به ، وحتى يتسنى لنا معرفة وضبط النشاطات المرتبطة بتكنولوجيا الإعلام والاتصال التي عكف المشرع الجزائري على تاطيرها بموجب قوانين ومن ثمة سن قوانين لمكافحة الجرائم المرتبطة بها كان لزاما علينا ضمن هذه الدراسة ضبط اهم التحديات التي واجهت المشرع الجزائري لمواجهة الجرائم السيبرانية وتحديد مدى توفيقه في كبح جماح مرتكبيها ، وعليه نطرح الإشكالية القانونية التالية:

ما هي التحديات التي واجهت المشرع الجزائري في عملية سن القوانين لمواجهة الجريمة السيبرانية ؟

وما مدى توفيقه في كبح جماح مرتكبيها ؟

وللوقوف على الإجابة القانونية للإشكالية المطروحة حصرت التحديات ضمن محورين هي:

أولا: مفهوم الجريمة السيبرانية

ثانيا: مواجهة الجريمة السيبرانية

1/ مفهوم الجريمة السيبرانية

1.1/ تعريف و أنواع الجريمة السيبرانية

1.1.1. تعريف الجريمة السيبرانية

تتكون الجريمة السيبرانية cyber crimes من مقطعين هما:

- الجريمة crime و هي السلوكيات والأفعال الخارجة على القانون.



- الإلكترونية cyber و يستخدم مصطلح الإلكترونيّة لوصف فكرة جزء من الحاسب أو عصر المعلومات.

و للجريمة السيبرانية عدة مسميات فمنهم من يسميها بالجرائم الالكترونية ومنهم من ينعتهها بجرائم الحاسوب ومنهم من ينعتهها بجرائم الانترنت، ومنهم من ينعتهها بجرائم التقنية العالية ومنهم من ينعتهها بجرائم المعلوماتية، ومع تعدد المسميات تتعدد التعاريف فمنهم من يعطيها تعريفا ضيقا ومنهم من يعطيها تعريفا موسعا و من التعريفين يظهر التحدي الأول للمشرع الجزائري في تبني تعريف يتماشى و التطور التكنولوجي من جهة وواقع المجتمع الجزائري من جهة ثانية .

2.1.1 الاتجاه المضيق لمفهوم الجرائم السيبرانية : هذا الاتجاه يعتمد على تعريف الجريمة الإلكترونية أو السيبرانية من الجانب الفني و الذي بدوره يجعل من المنظومة المادية المعلوماتية حقل للجريمة⁽¹⁾ و هي الهدف المباشر للمجرمين والجريمة الالكترونية ضمن هذا التعريف هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي و بالتالي فالجريمة السيبرانية هي:

- كل سلوك غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية قدر كبير لارتكابه من ناحية وملاحقته من ناحية أخرى (ححو رمزي . 2014 : ص 42)

- فعل ضار يستخدم الفاعل، الذي يفترض أن لديه معرفة بتقنية الحاسوب، نظاماً حاسوبياً أو شبكة حاسوبية للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة . و بالتالي كخلاصة ضمن هذا الاتجاه نستنتج :

- إن الجريمة السيبرانية هي جريمة ذات طابع مادي و تتمثل في كل فعل أو سلوك غير مشروع، تستعمل فيه الوسائط الإلكترونية و حيث تتسبب في تحميل أو إمكانية تحميل المجني عليه خسارة و حصول أو إمكانية حصول مرتكبه على أي مكسب، وتهدف إلى الوصول غير المشروع لبيانات سرية غير مسموح بالاطلاع عليها ونقلها ونسخها أو حذفها ، أو تهديد وابتزاز الأشخاص والجهات المعنية بتلك المعلومات، أو تدمير بيانات وحواسيب الغير .

- ان هذا الاتجاه يعطي تعريف جامع مانع من الناحية الفنية للجريمة الالكترونية حيث انه لارتكاب الجريمة يتطلب وجود أجهزة ووسائل تقنية زيادة على ربطها بشبكة معلوماتية ضخمة

أ- أحصت وزارة العدل عدد الجرائم المنصبة على المنظومة المعلوماتية سنة 2018 - 149 جريمة و سنة 2019 - 140 جريمة و سنة 2020 - 178 جريمة



إن هذا الاتجاه يعطي تعريف ضيق للجريمة السيبرانية إذ يقتصر هدف المجرم فيه على ذلك الفعل الغير المشروع الذي يرتكبه بواسطة وسائل تكنولوجيا المعلومات و يكون هدفه البرامج و المعطيات الالكترونية المرتبطة بهذه الوسائل .

3.1.1 الاتجاه الموسع لمفهوم الجرائم السيبرانية :

هذا الاتجاه يعتمد على تعريف الجريمة الإلكترونية من الجانب القانوني و الذي بدوره يجعل من المنظومة المادية المعلوماتية حقل ووسيلة وهدف للجريمة في ان واحد وضمن هذا الإطار الجرائم السيبرانية هي :

- كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب (ححو رمزي , 2014 : ص 40)
- هي جميع المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (ذياب البدائية , 2014 : بدون ص) ، إذن ضمن هذا الاتجاه يتسع مفهوم الجريمة السيبرانية فيشمل الأفعال الغير مشروعة التي يكون هدفها المنظومة المادية لوسائل الاتصال المعلوماتية وكذا الأفعال الغير مشروعة التي تخضع في تعريفها و تحديد أركانها للقانون العام أو الخاص مع إضافة أنها جريمة ترتكب باستخدام وسائل الكترونية .

4.1.1 / تعريف المشرع الجزائري للجريمة السيبرانية :

لقد عكف المشرع الجزائري على تسمية الجرائم السيبرانية بالجرائم الالكترونية وضبط مفهومها على أساس أنها تلك الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، و قد عرفها ضمن محطتين هما:

1/ **المحطة الأولى :** التعريف الذي وضعه المشرع بموجب المادة 02 من القانون 04-09 المؤرخ في 05 غشت 2009، أين عرفها على أساس أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.⁽¹⁾ و إذ يلاحظ على هذا التعريف ما يلي : (بوضياف اسمهان , 2018 : ص 352) .

- أن المشرع الجزائري قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكترونية، وثانيها معيار موضوع الجريمة وهو المساس بأنظمة المعالجة الآلية

أ- المادة 02 من القانون رقم 04-09 المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا

الاعلام و الاتصال ومكافحتها الجريدة الرسمية عدد 47 الصادرة بتاريخ 16-08-2009 ص 5

ب- أحصت وزارة العدل عدد مثل هذه الجرائم سنة 2018 - 422 جريمة و سنة 2019 - 608 جريمة و سنة 2020 - 785 جريمة

ج- المادة 211 مكرر 22 من الامر رقم 11-21 المؤرخ في 25-08-2021 المعدل و المتمم لقانون الاجراءات الجزائية الجريدة الرسمية

عدد 65 الصادرة بتاريخ 26-08-2021 ص 8



للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص
عليها في قانون العقوبات .

- اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة الالكترونية، كونه أقر أن الجريمة الالكترونية
ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه ⁽¹⁾ ، وهذا ما يوسع من نطاق مجال الجرائم الالكترونية
في القانون الجزائري.

ومن هذا التعريف ضمن المخطط الأولى يتبين لنا إن المشرع الجزائري اخذ بالمفهوم الموسع للجريمة السيبرانية إذ انه
اعتبر من جهة أن الأفعال الغير المشروعة التي تستهدف وتمس بأنظمة المعالجة الآلية للمعطيات من الجرائم
المعلوماتية و أشار إليها بوضوح ضمن الجزء الأول من التعريف "جرائم المساس بأنظمة المعالجة الآلية
للمعطيات الآلية المحددة في قانون العقوبات" كما اعتبر من جهة ثانية أن كل الأفعال الغير المشروعة التي
ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية .

2/ المخطط الثانية : التعريف الذي وضعه المشرع الجزائري بمناسبة إنشائه القطب الجزائري الوطني لمكافحة الجرائم
المتصلة بتكنولوجيات الإعلام و الاتصال أين عرف الجريمة الالكترونية على أنها: " أي جريمة ترتكب أو
يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية
ذات صلة بتكنولوجيات الإعلام و الاتصال " ⁽²⁾

و الملاحظ على هذا التعريف ما يلي:

- أن المشرع الجزائري لم يشر إلى "جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون
العقوبات" كما كان يشير إليها ضمن القانون رقم 09-04 المؤرخ في 05 غشت 2009، المتضمن
القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها -إن المشرع الجزائري
وسع من تعريف الوسائل التكنولوجية التي بواسطتها ترتكب الجرائم الالكترونية بنصه "....أو أي وسيلة
أخرى أو آلية ذات صلة بتكنولوجيات الإعلام و الاتصال" وهذا توسيع منطقي لتوسع نطاق تكنولوجيا
نقل المعلومات و الأخبار .

2/ أنواع الجريمة السيبرانية :

معرفة الجريمة السيبرانية هو تحدي ولكن معرفة أنواعها هو تحدي آخر للمشرع الجزائري للتحكم في العقوبات
المقررة لها وهذا التحدي يظهر من خلال حلقتين هما :



- هناك مجالات كثيرة مؤطرة قانونا بقوانين خاصة لا يمكن إضافة قوانين أخرى تضع عقوبات أخرى عليها مما يجعل من احتمال تناقضها على محك من جهة ومن جهة ثانية خلق تضخم تشريعي في ذات المجال ومن جهة أخرى زعزعة الأمن القانوني المنصوص عليه دستوريا⁽¹⁾
- تحديد القانون الواجب التطبيق عند ظهور هذه الجرائم وتمييز الجريمة المعلوماتية من الجريمة التقليدية فالنصب يمكن أن يكون جريمة معلوماتية وجريمة تقليدية في أن واحد فما هو القانون الواجب التطبيق في حالة تعدد النصوص القانونية التي تجرمه .

وانطلاقا مما سبق ذكره و بالاعتماد على التعريفات التقنية و القانونية و الخصائص التي تميز الجرائم السيبرانية يمكن لنا حصر أنواع الجرائم المعلوماتية فمنها من يستمد تجريمه من القانون العام ولكن الوسيلة المرتكبة تكون بواسطة تكنولوجيا المعلومات ومنها من يستمد تجريمه من القانون الخاص ولكن الوسيلة المرتكبة تكون بواسطة تكنولوجيا المعلومات ومنها من تكون الأنظمة المعلوماتية هي الهدف المعتدى عليه. وكخلاصة يمكن أن يكون النظام المعلوماتي هو نفسه موضوع أو محل الجريمة الالكترونية ومن ناحية أخرى، قد يكون النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها .

1.2/ الجرائم الواقعة بواسطة النظام المعلوماتي:

- يعد النظام المعلوماتي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حد ذاته أو براجمه كوسيلة لتنفيذ الجريمة (دبش سورية , 2018 : ص 241) فجرائم القانون العام المرتكبة بواسطة تكنولوجيا المعلومات مثلا هي جرائم في الأصل يعاقب عليها القانون العام و بذلك تخضع هذه الجرائم في تعريفها وتحديد عناصرها و أركانها والعقوبة المقررة لها للقواعد العامة المنصوص عليها في قانون العقوبات، فهي في الحقيقة أعمال غير مشروعة ترتكب ضد الأشخاص أو الأموال أو كلاهما معا بواسطة وبمساعدة تكنولوجيا المعلوماتية مثل : جرائم القذف و النصب و السب والإشادة بالأعمال الإرهابية . كما أن جرائم القانون الخاص المرتكبة ضمن تكنولوجيا المعلوماتية هي جرائم في الأصل تعاقب عليها بعض القوانين الخاصة وهي أفعال مرتبطة ارتباطا وثيقا بتكنولوجيا المعلومات، وهي بذلك تكون مدرجة ضمن الحقل المعلوماتي مثل :
- الجرائم الماسة بحقوق المؤلف و الحقوق المجاورة كجرائم الاعتداء على أنظمة الإعلام الآلي ومواقع الانترنت⁽²⁾

أ- الأمن القانوني أصبح مبدأ دستوري نص عليه المشرع الجزائري ضمن المادة 4/34 من الدستور الجزائري

أ- انظر المواد 152 الى 156 من الأمر رقم 05/03 المؤرخ في 19-07-2003 يتعلق بحقوق المؤلف و الحقوق المجاورة الجريدة الرسمية الجزائرية عدد 44.



-الجرائم الماسة بالعلامات التجارية (1)

-الجرائم الماسة بتسميات المنشأ (2)

-الجرائم الماسة بالرسوم و النماذج الصناعية (3)

وتنقسم هذه الجرائم على العموم إلى:

2.2/ الجرائم الواقعة على الأشخاص⁽⁴⁾: ظهرت عدة أنواع خاصة من الجرائم الالكترونية الواقعة على الأشخاص

كجريمة التهديد والمضايقة والملاحقة، خاصة عن طريق البريد الالكتروني بإرسال رسالة خاصة للترويع والتهديد أو عن طريق وسائل الحوارات المختلفة على شبكة الانترنت: كالفيسبوك، والفايبر و الواتساب وكذلك جريمة القذف والسب وتشويه السمعة للمساس بشرف الغير وكرامتهم واعتبارهم عن طريق وسائل الاتصال المباشر أو الكتابة أو عن طريق المطبوعات أو المبادلات الالكترونية (بريد الكتروني) صفحات الويب، غرف المحادثة (ديش سورية , 2018 : ص 243) . كما تعتبر من أهم الجرائم الالكترونية الواقعة على الأشخاص صناعة ونشر الإباحة والجنس سواء للبالغين والأطفال خاصة، حيث يتعرض الأطفال للاستغلال الجنسي على الانترنت بأشكال متعددة انطلاقا من الصور إلى التسجيلات المرئية للجرائم الجنسية العنيفة، حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنت.

ويضاف إلى الجرائم الالكترونية الشخصية جرائم انتحال الشخصية والتغريب والاستدراج باستخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحياته أو تتخذ هذه الجريمة وجهان: انتحال شخصية الفرد وانتحال شخصية المواقع .

3.2/ الجرائم الواقعة على الأموال: في خضم هذه التداول المالي عبر الإنترنت ظهرت عدة جرائم الكترونية على

الأموال مثل: السطو والسرقعة، والتحويل الالكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة، حيث أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريقة الغير المشروعة ممكنة عبر قنوات شبكة الانترنت . كما ظهرت جريمة القمار وغسيل الأموال عبر الانترنت بظهور الكازينوهات الافتراضية أو أندية القمار الافتراضية التي أصبحت فيما بعد مسرحا كذلك لجريمة غسيل الأموال، حيث ساعدت

ب- المواد 32 و 33 من الأمر رقم 06/03 المؤرخ في 19-07-2003، يتعلق بالعلامات. الجريدة الرسمية الجزائرية عدد44

ج- انظر المواد 28 الى 30 من الأمر رقم 65/76 المؤرخ في 16-07-1976 يتعلق بتسميات المنشأ الجريدة الرسمية الجزائرية رقم 59.

د- انظر المادة 23 من الأمر رقم 77/66 المؤرخ في 28-04-1966 المتعلق بالرسوم و النماذج الجريدة الرسمية الجزائرية رقم 35.

هـ- احصت وزارة العدل عدد مثل هذه الجرائم سنة 2018 -25 جريمة و سنة 2019 -47 جريمة و سنة 2020 -36 جريمة



الشبكة العنكبوتية في انتشارها وتطورها بنقل هذه الجريمة من دولة إلى دولة أخرى لاستثمارها في مجالات مشروعة .

ومن أهم الجرائم الإلكترونية على الأموال , نذكر جريمة المخدرات على الانترنت حيث تتخذ المواقع الإلكترونية للترويج للمخدرات وتسويقها للناشئ لاستخدامها، وتعليمه كيفية صناعتها بكافة أصنافها وأنواعها .

4.2/ الجرائم الواقعة على أمن الدولة : تعد هذه الجرائم من أخطر الجرائم الإلكترونية خاصة الإرهاب المعلوماتي والجريمة المنظمة المعلوماتية، حيث أتاحت الانترنت للكثير من المنظمات الإرهابية الترويج لأفكارها ومعتقداتها، وأدت إلى ظهور جريمة أخرى أخطر منها وهي جريمة التجسس الإلكتروني على الدول بالاطلاع على مختلف الأسرار العسكرية والاقتصادية بين الدول المتصارعة، كما تعطى الشبكة العنكبوتية فرصا للتأثير على المعتقدات الدينية وتقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة والمساس بأمنها الداخلي وبنظامها العام .

5.2/ الجرائم الواقعة على النظام المعلوماتي : الجرائم الواقعة على الأنظمة المعلوماتية هي تلك الأفعال الغير مشروعة التي تجعل من الدعاية المادية للأنظمة المعلوماتية أو الأنظمة المعلوماتية هدفا لها مثل جرائم المساس بأنظمة المعالجة الآلية للمعطيات وهذا من خلال عملية اختراقها باستعمال الفيروسات . ويمكن أن تكون لهذه الأفعال الغير مشروعة التي تجعل من الدعاية المادية للأنظمة المعلوماتية أو الأنظمة المعلوماتية هدفا لها تجريم خاص ضمن بعض المجالات إذا ما ارتبطت بالتقليد كتقليد الاختراعات ⁽¹⁾ أو التصاميم الشكلية للدوائر المتكاملة ⁽²⁾

أو برامج الحاسوب ⁽³⁾

والجرائم الواقعة على النظام المعلوماتي تنقسم إلى ماييلي :

6.2/ الجرائم الواقعة على المكونات المادية للنظام المعلوماتي: يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل للسرقة وخيانة الأمانة أو الإتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، مما يترتب عليها خسائر كبيرة (ديش سورية , 2018 : ص 246) .

7.2/ الجرائم الواقعة على البرامج الإلكترونية: تنقسم هذه الجرائم بدورها إلى الجرائم الواقعة على البرامج التطبيقية، عن طريق تحديد البرنامج أولا ثم التلاعب به أو تعديله، أو الجرائم الواقعة على برنامج التشغيل وهي البرامج

أ- انظر المادة 61 و 62 من الأمر رقم 07/03 المؤرخ في 19-07-2003، يتعلق ببراءة الاختراع الجديدة الرسمية الجزائرية عدد 44.

ب- انظر المادة 35 الى 39 من الأمر رقم 08/03 المؤرخ في 19-07-2003 يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة الجديدة الرسمية الجزائرية عدد 44.

ج- انظر المادة 04 من الأمر رقم 05/03 المؤرخ في 19-07-2003 يتعلق بحقوق المؤلف و الحقوق المجاورة الجديدة الرسمية الجزائرية عدد 44.



المسؤولة عن عمل النظام المعلوماتي، ومن حيث قيامها بضبط ترتيب العمليات الخاصة بالنظام، وتقوم هذه الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشيفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام المعلوماتي ومثالها: جريمة تصميم برنامج وهمي من خلاله تنفذ الجريمة .

8.2/ الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي: تعد المعلومة المعالجة آليا ذات أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي، لما لها من قيمة اقتصادية، وتتم الجرائم عليها من خلال التلاعب فيها بصفة مباشرة أو غير مباشرة إذ لم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار أمن الموانئ، التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة أو الإرهابيين أو حتى الدول المعادية .

3 / خصائص الجريمة السيبرانية :

تتميز الجريمة السيبرانية بخصائص وصفات تميزها عن غيرها من الجرائم الأخرى التقليدية وهذا ما يشكل تحدي تشريعي آخر للمشرع الجزائري فلا يمكن لنا تصور وجود نصوص قانونية ناجعة على المستوى العملي التطبيقي دون ان تكون للمشرع نظرة على الخصائص التي تميز هذا النوع من الجرائم عن الجرائم التقليدية ومن خلال معرفته بخصائصها تمكنه من وضع اليات قانونية موضوعية واجرائية لمكافحةها ومن بين أهم هذه الخصائص ما يلي:

1.3/ الجريمة الالكترونية جريمة عالمية عابرة للحدود الجغرافية : (معاشي سميرة , 2018 :ص 411)

من أهم الخصائص التي تميز الجريمة الالكترونية أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الانترنت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد بسبب السرعة الهائلة في تنفيذها وحجم الأموال والأشخاص المستهدفة خاصة بعد ارتباط آثارها بالمعاملات الالكترونية على شبكة الانترنت كتقليد عناصر الملكية الفكرية أو ظهور آثار سلبية لها تتخطى الحدود الجغرافية للدول كقضية اللعبة الالكترونية التي كان مجالها حقل الانترنت وكانت تستهدف الأطفال و التي عرفت في السنوات الماضية بقضية " الحوت الأزرق".

وتثير خاصة عالمية الحدود للجريمة الالكترونية ضمن هذا الإطار تحدي للمشرع الجزائري و أشار إلى هذا التحدي ضمينا بموجب القانون 09 – 04 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بسنه أحكام خاصة بالتعاون والمساعدة القضائية والدولية المتبادلة في مجال محاربة الجريمة الالكترونية (1)

أ- انظر المواد 16 و 17 و 18 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

* مادة 13 و 14 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال



2.3/ مرتكبو الجريمة الالكترونية ذوو صفات خاصة: مرتكب الجريمة الإلكترونية في الغالب شخص

يتميز بالذكاء والدهاء (بوضياف اسمهان , 2018 : ص 356) . و ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها ، و عو بذلك يتميز عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامي النمطي بعدة خصائص منها -انه مجرم متخصص ومحترف في تنفيذ جريمته الالكترونية، حيث إن ارتكابها يتطلب التغلب على تقنيات حماية أنظمة الكمبيوتر.

- انه لا يلجأ إلى العنف في تنفيذ جرائمه، فهو مجرم ذكي يتمتع بالمهارة والمعرفة وبدرجة عالية من الثقافة (حوحو رمزي , 2014 : ص 48)

وبذلك كان لزاما على المشرع سن قواعد تقنية إجرائية تسمح بإنشاء هيئة متخصصة يناط بها مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذا النوع من الجرائم ⁽¹⁾ و إلزام كل المتعاملين و مقدمي خدمات الاتصالات الالكترونية بتقديم يد المساعدة لها ⁽²⁾

3.3/ الجريمة الالكترونية جريمة صعبة الإثبات : (معاشي سميرة , 2018 : ص 412) .

من أهم خصائص الجريمة الالكترونية أنها صعبة الإثبات لأسباب ترجع إلى الجاني أو إلى المجني عليه، وإلى وسيلة تنفيذها، حيث تتم هذه الجريمة بشكل منظم من إقليم دولة واحدة باستخدام الانترنت، أضف إلى أن الجاني المجرم المعلوماتي كما أسلفنا الذكر مجرم محترف ذكي مثقف لا يترك آثارا جانبية خارجية للجريمة مما يصعب إثباتها، فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية وهذا ما جعل وسائل الإثبات التقليدية غير كافية، وهو تحدي آخر للمشرع الجزائري أدى به إلى البحث عن طرق جديدة و فعالة لجمع الأدلة لإثباتها، كاستخراج البصمات الصوتية أو استعمال شبكية العين ومضاهاتها باستخدام وسائل آلية سريعة

4.3/ أسلوب ارتكاب الجريمة :

تبرز خصوصية الجريمة المعلوماتية بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي فان الجريمة المعلوماتية لا تحتاج إلى أي مجهود ماعدا الفكري وهو

* المادة 02/15 من المرسوم الرئاسي رقم 21-439 المؤرخ في 7-11-2021 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها الجريدة الرسمية رقم 86 الصادرة بتاريخ 11-11-2021 ص رقم 8

أ- المادة 13 و 14 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال
ب- المادة 02/15 من المرسوم الرئاسي رقم 21-439 المؤرخ في 7-11-2021 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها الجريدة الرسمية رقم 86 الصادرة بتاريخ 11-11-2021 ص رقم 8



القدرة على التعامل مع التكنولوجيا المعلوماتية وبذلك فهي جريمة ناعمة، أي أنه لا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطيرة كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار، تنفذ بسرعة أي أنها تتميز بإمكانية تنفيذها بسرعة فأغلب الجرائم المعلوماتية ترتكب في وقت قصير جداً قد لا يتجاوز الثانية الواحدة، وهذا تحدي آخر للمشرع الجزائري أين قام بوضع قواعد قانونية تسمح باللجوء إلى مراقبة الاتصالات الالكترونية وتفتيش المنظومة المعلوماتية وحجز المعطيات المعلوماتية أو الحجز عن طريق الوصول إلى المعطيات و إلزام مقدمي الخدمات بمساعدة السلطات ⁽¹⁾ و اقر ضدهم عقوبات تحت عنوان جنحة عرقلة حسن سير التحريات القضائية ⁽²⁾

5.3/ المجاذبية:

نظرا لما تمثله التجارة الالكترونية من ثروة كبيرة لارتباطها بالبضائع التي يتم الاتجار بها من جهة و الإشهار الالكتروني المرتبط بها من جهة ثانية بسوق كبيرة مرتبطة هي الأخرى أساسا بشبكة الإنترنت ، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن من الدخول إلى الشبكات المعلوماتية وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات... الخ وهنا يكمن التحدي الآخر للمشرع الجزائري من خلال قدرته على سن أكبر قدر من القوانين لتأطير كل مجال أصبح مرتبط بتكنولوجيا المعلومات بعد اتجاهاه إلى إنشاء ما أصبح يصطلح عليه بالحكومة الالكترونية (نافع زينب , 2020 : ص780) و هذا ما سنتحدث عنه عند الحديث عن الآليات القانونية التي وضعها المشرع الجزائري لمكافحة الجرائم الالكترونية .

6.3/ امتناع المجني عليهم عن التبليغ:

أن المجني عليهم في الجرائم السيبرانية وهم غالبا مؤسسات عامة أو خاصة يحجمون عن الإبلاغ عنها تجنباً للإساءة إلى السمعة وهز الثقة ، إذ أن مثل هذه الجرائم عادة ما يتم اكتشافها بمحض الصدفة خاصة و إنما لا تترك أي اثر خارجي بصورة مرئية ، ففي غالب الأحيان لا يتم الإبلاغ عن الجرائم الإلكترونية إما لعدم اكتشاف الضحية لها و إما خشية من التشهير الذي قد يطاله ، لذا نجد أن معظم الجرائم في هذا المجال تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها وهو تحدي آخر للمشرع الجزائري قام

أ- انظر المواد من 04 الى 10 من القانون رقم 09-04 (مرجع سابق)

ب- وقد حدد المشرع الجزائري عقوبة بالحبس من 06 اشهر الى 5 سنوات وبغرامة من 50000 دج الى 500000 دج للشخص الطبيعي

و بغرامة وفقا للقواعد المقررة في قانون العقوبات بالنسبة للشخص المعنوي انظر المادة 11/الاخيرة من القانون رقم 09-04

ج- المادة 11 من القانون رقم 09-04 (مرجع سابق)



بتأطيره من خلال من خلال إلزام مقدمي الخدمات الالكترونية بحفظ المعطيات التي

تسمح بالتعرف على مستعملي الخدمة و الخصائص التقنية وكذا تاريخ و وقت ومدة كل اتصال⁽¹⁾

ثانيا : مواجهة الجريمة السيبرانية في ظل القوانين :

يمكن التحدي الثاني الذي يواجه المشرع الجزائري في مواجهة الجرائم السيبرانية هي في مدى توفيقه في وضع الآليات الموضوعية و الإجرائية لمواجهة الجرائم السيبرانية , فالخصوصيات التي تتسم بها هذه الجرائم عن الجرائم التقليدية تجعل من التحدي أكثر جدية , فمن خلال الاطلاع على النصوص التشريعية الجزائرية نجد أن الدولة وضعت عدة آليات لمواجهة الجرائم السيبرانية على غرار ما هو موجود في عدد من الدول , وبذلك عكفت الدولة من خلال مشرعها على إصدار العديد من القوانين التي تعنى بمكافحة الجرائم السيبرانية كما اهتمت بإنشاء هيئات خاصة عهد إليها مكافحتها , وبذلك ساعمد ضمن هذا المحور إلى تبيان ما يلي:

أ- القواعد الموضوعية المدرجة في القوانين الداخلية التي سنّها المشرع الجزائري لمواجهة الجرائم السيبرانية

ب- القواعد الإجرائية المدرجة في القوانين الداخلية التي سنّها المشرع الجزائري لمواجهة الجرائم السيبرانية

1/ القواعد الموضوعية في مواجهة الجريمة السيبرانية :

القواعد الموضوعية ضمن هذه الدراسة هي تلك القواعد التي رسمها المشرع الجزائري ضمن العديد من القوانين وهي أحكام موضوعية تتضمن بيان الحقوق التي يتمتع بها الأفراد و الواجبات المفروضة عليهم و العلاقات التي تربطهم بها ومن ذلك سأحاول ضبط كل القوانين التي سنّها المشرع الجزائري ومن ثمة تبيان صلتها بالجرائم السيبرانية.

1.1/ مواجهة الجريمة السيبرانية على ضوء القوانين ذات الصلة بالمعاملات الالكترونية : المعاملات الإلكترونية هي

معاملات يتم إبرامها أو تنفيذها بشكل كلي أو جزئي بواسطة وسائل أو سجلات إلكترونية. و هي شكل من أشكال الاستخدام المتكامل لكل تقنيات المعلومات، وتكنولوجيا الاتصالات على أن يكون الغرض من هذا التجميع تسهيل وتسريع التعاملات ، مع ضمانة الدقة العالية وهذه المعاملات مؤطرة بموجب قوانين تعنى بهذا المجال لها علاقة بالجرائم الالكترونية و يمكن حصرها :.

1.1.1/ القانون رقم 83-11 المتعلق بالتأمينات الاجتماعية⁽²⁾

عقب استحداث الدولة الجزائرية لبطاقة الكترونية للتأمين الاجتماعي "الشفاء" سنة 2008 وجعلها وسيلة لإثبات صفة المؤمن له اجتماعيا وربطها تقنيا بقاعدة معطيات وطنية تنبأ المشرع الجزائري آنذاك باحتمال

أ- القانون رقم 08-01 المؤرخ في 2008/07/23 المعدل و المتمم للقانون رقم 83-11 المتعلق بالتأمينات الاجتماعية ج ر عدد 04 لسنة 2008



الاعتداء على هذه الوسيلة الكترونيا أين قام بوضع بنود ضمن المادة 93 مكرر 03

ومكرر 04 تجرم بعض الأفعال والتي يمكن إدراجها ضمن الجرائم الالكترونية وهي :

- القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية و/أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة.

- الإعداد أو التعديل أو النسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة.

- القيام بنسخ أو صنع أو حيازة أو توزيع بطريقة غير مشروعة البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة.

وقد اقر المشرع الجزائري عقوبة حبس تتراوح بين عامين و خمس سنوات حبس نافذ وغرامة مالية تصل إلى 05 مليون دينار جزائري وافر عقوبة للشخص المعنوي تقدر ب خمسة أضعاف المبلغ الأقصى للغرامة المقررة قانونا

2.1.1/ قانون رقم 18-5 المؤرخ في 01 مايو سنة 2018 يتعلق بالتجارة الإلكترونية (الجريدة الرسمية , 2018 : ص

04) يحدد هذا القانون القواعد العامة المتعلقة بالتجارة الإلكترونية للسلع والخدمات فنجده يطبق في مجمل المعاملات التجارية الإلكترونية في حالة ما إذا كان أحد أطراف العقد الإلكتروني :

— متمتعاً بالجنسية الجزائرية، أو مقيماً إقامة شرعية في الجزائر، أو شخصاً معنوياً خاضعاً للقانون الجزائري ، أو كان العقد محل إبرام أو تنفيذ في الجزائر .

وقد أدرج المشرع عقوبات تقدر بغرامة من 200000 دج إلى 100000 دج كل من يعرض للبيع، أو يبيع عن طريق الاتصال الإلكتروني، المنتجات أو الخدمات التالية :

- لعب القمار والرهان واليانصيب .

- المشروبات الكحولية والتبغ .

- المنتجات الصيدلانية .

- المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية .

- كل سلعة أو خدمة محظورة بموجب التشريع المعمول به .

- كل سلعة أو خدمة تستوجب إعداد عقد رسمي

و يمكن القاضي أن يأمر بغلق الموقع الإلكتروني لمدة تتراوح من شهر إلى ستة أشهر.



كما اقر عقوبة غرامة من 500000 إلى 2000000 دج على كل معاملة عن طريق الاتصالات الإلكترونية تستهدف ما يلي :

- العتاد والتجهيزات والمنتجات الحساسة المحددة عن طريق التنظيم المعمول به، وكذا كل المنتجات .
- الخدمات الأخرى التي من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي .
- و يمكن القاضي أن يأمر بغلق الموقع الإلكتروني والشطب من السجل التجاري .

3.1.1/ قانون رقم 04-18 المؤرخ في 01-05-2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية (الجريدة الرسمية , 2018 : ص 3) يحدد هذا القانون القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية و يهدف على وجه الخصوص، إلى ما يأتي:

- تحديد الشروط التي من شأنها تطوير وتقديم خدمات البريد والاتصالات الإلكترونية ذات نوعية مضمونة في ظروف موضوعية وشفافة وغير تمييزية في مناخ تنافسي مع ضمان المصلحة العامة،
 - ترقية تطوير الاتصالات الإلكترونية واستعمالها
 - تحديد الشروط العامة لاستغلال نشاطات البريد والاتصالات الإلكترونية من طرف المتعاملين .
 - تحديد إطار و كفاءات ضبط النشاطات ذات الصلة بالبريد والاتصالات الإلكترونية .
 - تحديد الإطار المؤسسي لسلطة ضبط مستقلة .
 - ضمان توفير الخدمة الشاملة.
- ويطبق هذا القانون على نشاطات البريد والاتصالات الإلكترونية ، بما فيها البث التلفزيوني والإذاعي في مجال

الإرسال والبث والاستقبال ، باستثناء محتوى النشاطات السمعية البصرية ووسائل الإعلام الإلكترونية، الذي يخضع لأحكام القانون العضوي رقم 05-12 المؤرخ في 12 يناير سنة 2012 والمتعلق بالإعلام .

وقد اقر المشرع الجزائري عقوبة الحبس من سنة إلى خمس سنوات وبغرامة من 500000 دج إلى 100000 دج ، لكل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها .

كما عاقب بالحبس من سنة إلى ثلاث سنوات و بغرامة من 1000000 دج إلى 5000000 دج أو بإحدى هاتين العقوبتين، كل من ينشئ أو يستغل شبكة اتصالات إلكترونية مفتوحة للجمهور دون رخصة أو مواصلة ممارسة النشاط خرقا لقرار التعليق أو سحب هذه الرخصة .

4.1.1/ قانون رقم 21-15 المؤرخ في 28 ديسمبر سنة 2021 يتعلق بمكافحة المضاربة غير المشروعة (الجريدة الرسمية , 2021 : ص 06) يهدف هذا القانون إلى مكافحة المضاربة غير المشروعة و التي يقصد بها كل تخزين أو



إخفاء للسلع أو البضائع بهدف إحداث ندرة في السوق واضطراب في التموين، وكل رفع أو خفض مصطنع في أسعار السلع أو البضائع أو الأوراق المالية بطريق مباشر أو غير مباشر أو عن طريق وسيط أو استعمال الوسائل الإلكترونية أو أي طرق أو وسائل احتيالية أخرى .
وقد أدرج المشرع لهذا النوع من الجرائم وكل من يحرض عليها باستعمال أي وسيلة إلى أن تصل إلى حد السجن المؤقت من 20 إلى 30 سنة وبغرامة من 10000000 دج إلى 20000000 دج .

2.1 : مواجهة الجريمة السيبرانية على ضوء القوانين ذات الصلة بالملكية الفكرية :

إن المستهلك يرتبط بحقوق الملكية الفكرية من خلال إيجاره على الشبكة الرقمية حيث إن هذه الأخيرة تحتوي على الكثير من المصنفات و الابتكارات و الرسوم و النماذج و العلامات المحمية , و تعمل على جذب المستهلك إليها . سواء لتصفحها , أو الاطلاع عليها , أو اقتنائها . و في هذا الشأن حاولت مختلف التشريعات تطويع قوانين الملكية الفكرية لتستوعب التكنولوجيا الحديثة التي أطلت علينا مع ظهور الشبكة الرقمية و التي أصبح يعبر عنها البعض بالملكية الرقمية . و التي تشمل حقوق الملكية الفكرية على الانترنت .

و بظهور الشبكة الرقمية أصبح أصحاب حقوق التأليف و حقوق الملكية الصناعية يستغلون منتجاتهم الإبداعية على الانترنت نظرا لما يوفره النشر الالكتروني لها من مزايا لهم ، إذ إن النشر يكون بأقل التكاليف و أوسع مجال بحيث يشمل جل أرجاء العالم. و في هذا ساهمت شبكة الانترنت في إحداث تغيير عميق بين المنتجين و المستهلكين عن طريق إقامة خط اتصال مباشر بينهم . فأصبح هذا التنوع التكنولوجي بمثابة مفتاح جديد للمستهلكين للوصول إلى المعرفة بطريقة تكون شبه مجانية . (حمالي سمير ، 2015 : ص 41) .

- الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة

جاء الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة بعد أن أردت الجزائر الدخول إلى المنظمة العالمية للتجارة ، و أصبحت المنظمة العالمية للملكية الفكرية تتمتع بالأشراف على تنفيذ جميع الاتفاقيات الدولية الخاصة بحماية حقوق الملكية الفكرية و هذا ابتداء من سنة 1995 و أصبحت العضوية في المنظمة العالمية للتجارة لا تتم إلا بالتوقيع على كافة اتفاقيات الجات و منها ما يخص الملكية الفكرية " اتفاقية تريپس " .

ويظهر اعتناء المشرع الجزائري بالمصنفات المحمية بموجب حقوق المؤلف و التي لها ارتباط بالجرائم الالكترونية من خلال ما يلي :

1.2.1 / حماية المصنفات على شبكة الانترنت (المصنف الرقمي) : و الذي هو احد مفرزات التكنولوجيا الحديثة

فهو لا يختلف في المبدأ أي المحتوى والتسمية عن المصنفات التقليدية كالكتاب والدورية والقطعة الموسيقية واللوحة الزيتية ، غير انه يختلف فقط في الحامل فبدل الحامل الورقي الذي تخط عليه كلمات أصبح



الحامل رقميا منذ نشأته كان نكتب فقرة من خلال لوحة مفاتيح الحاسوب ونحفظها في ذاكرته يكون الناتج ملف او نص الكتروني يحفظه ويسترجه الحاسوب من خلال تحويل كلماته المدخلة باللغة الطبيعية إلى لغة تفهمها الآلة وهي اللغة الثنائية و توجد على الشبكة العالمية العديد من المصنفات الرقمية المختلفة غير انه سنحصر هذه المصنفات في الأصناف الرقمية التي يحميها القانون بموجب حقوق المؤلف ، ونشير انه هناك مصنفات محمية بموجب قوانين الملكية الصناعية والتجارية وهذه المصنفات لا منا في بحثنا هذا وإجمالاً المصنفات المعنية بالحماية هي : برامج الحاسوب ، البرمجيات ، قواعد البيانات ، والدوائر المتكاملة ، بالإضافة إلى الملفات الرقمية لمصادر المعلومات التقليدية من الكتب الرقمية والدوريات والموسوعات وغيرها المتاحة عبر الشبكة في شكل رقمي حديث .

2.2.1/ اعتبار البرامج والبرمجيات مصنفات : والتي تعتبر الفكر المحرك لجسم الحاسوب من قبيل المصنفات فبرامج الكمبيوتر من أهم المصنفات التي يرتبط بها المستهلك في العصر الحالي .وهي عبارة عن نتاج أدبي للمبرمج يمكن أن يظهر بصورة مباشرة بالكتابة كما في الصورة الأولية له ، أو بعد أن يترجم إلى لغة لا تفهمها إلا الآلة .و هي الصورة المنقوشة التي تقوم الآلة بنقل الأفكار الموجودة فيها إلى الحس الإنساني . و هذه البرامج سواء بالصورة المنقوشة على وحدة العمل المركزي ، أو وحدات الذاكرة الثابتة ، أو في اللوحات المنقولة ما هي إلا ترجمة للأفكار الموجودة في الصورة الأولية . وبرامج الكمبيوتر هي في حقيقتها طرق للتعبير عن الأفكار التي يرتبط بها المستهلك ، فالمبرمج يتناول أفكارا معينة مبتكرة أو متداولة ، و يعبر عنها وفقا لطريقته تعبيرا أصيلا باستخدام التكنولوجيا الحديثة . فكما في المصنفات الأخرى فان برامج الكمبيوتر ليست إلا تعبيرات للتخاطب مع مستعمل الكمبيوتر ، و من خلال الكمبيوتر ، فهو يعد البرنامج كتابة بأحد لغات البرمجة التي تقرا إنسانيا في صورة أولية ، ثم يتم تحويله بعدها إلى لغة الآلة بالصورة المنقوشة التي يستطيع الكمبيوتر قراءتها ، و من ثم إخراجها إلى المستعمل المستهلك للاستفادة منها . (حمالي سمي ، 2015 : ص 88) . و الحماية المقررة قانونا لهذه المصنفات لا تشمل إلا برامج الحاسوب ،و ليس سنده المادي الذي يستفيد هو الآخر من الحماية المقررة على ضوء براءة الاختراع متى توافرت شروطها فيه أما شكل البرنامج الذي يظهر على الشاشة فحمايته كقاعدة عامة تخضع لنظام الرسوم و النماذج و ليس هناك فرق في مفهوم الحماية القانونية بين برامج التشغيل والبرامج التطبيقية فكلاهما تتمتع بالحماية القانونية (حصاص صونية ، 2012 : بدون ص) .

وهناك العديد من القوانين التي تعنى بالملكية الفكرية ولها ارتباط وثيق بالجرائم السيبرانية وهي :

- الأمر رقم 07/03 المؤرخ في 19-07-2003، يتعلق ببراءة الاختراع
- الأمر رقم 65/76 المؤرخ في 16-07-1976 يتعلق بتسميات المنشأ
- الأمر رقم 77/66 المؤرخ في 28-04-1966 المتعلق بالرسوم و النماذج



- الأمر رقم 08/03 المؤرخ في 19-07-2003 يتعلق بحماية التصميم الشكلى للدوائر المتكاملة

- الأمر رقم 06/03 المؤرخ في 19-07-2003، يتعلق بالعلامات.

1.3.1/ مواجهة الجريمة السيبرانية على ضوء القوانين ذات الصلة بالمرفق العام :

المرفق العام هو كل نشاط تضطلع به الإدارة بنفسها أو بواسطة أفراد عاديين تحت إشرافها وتوجيهها بقصد إشباع الحاجات العامة، ويقصد بذلك أن الدولة هي التي تقدر اعتبار نشاط ما مرفقا عاما فتقدر إخضاعه للمرافق العامة بناء على قانون معين، وليس من اللازم أن يكون كل مشروع تحدته الدولة أن تتولى هي مباشرة إدارته، فكثيرا ما تعهد الإدارة إلى الأفراد أو شركة خاصة بأداء خدمة عامة تحت إشرافها ولكن تحت غطاء قانوني يرتبط أحيانا بقوانين لها ارتباط بتكنولوجيا الإعلام و الاتصال ومن ثمة يجعلها عرضة للجرائم السيبرانية .

1.3.1/ قانون رقم 7-18 المؤرخ في 1 يونيو سنة 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة

المعطيات ذات الطابع الشخصي (الجريدة الرسمية ، لم تذكر السنة : ص 11) ، يطبق هذا القانون على المعالجة الآلية

الكلية أو الجزئية للمعطيات ذات الطابع الشخصي وكذا على المعالجة غير الآلية للمعطيات ذات الطابع

الشخصي الواردة أو التي يمكن ورودها في ملفات يدوية. ويطبق على معالجة المعطيات ذات الطابع الشخصي

التي تقوم بها الهيئات العمومية أو الخواص و التي يمكن أن تكون محل جرائم معلوماتية وهذا :

— عندما تتم من طرف شخص طبيعي أو معنوي يكون المسؤول عنها مقيما على التراب الوطني أو فوق تراب

دولة لها تشريع معادل للتشريع الوطني في مجال المعالجة الآلية للمعطيات ذات الطابع الشخصي.

يعتبر مقيما بالجزائر، المسؤول عن المعالجة الذي يمارس نشاطا بالتراب الجزائري في إطار منشأة .

— عندما يكون المسؤول عنها غير مقيم على التراب الوطني و يلجأ بغرض معالجة معطيات ذات طابع شخصي إلى

وسائل آلية أو غير آلية توجد فوق التراب الوطني ، باستثناء المعالجات التي تستعمل لأغراض العبور فوق التراب

الوطني ففي هذه الحالة، يجب على المسؤول عن المعالجة ، دون الإخلال بمسؤوليته الشخصية ، أن يبلغ السلطة

الوطنية بهوية ممثلة المقيم بالجزائر الذي يحل محله في جميع حقوقه والتزاماته الناتجة عن أحكام هذا القانون ونصوصه

التطبيقية .

و تخضع لأحكام هذا القانون أيضا المعالجات الآلية للمعطيات ذات الطابع الشخصي المتعلقة بالصحة ، التي يكون

الغرض منها بحث ودراسة وتقييم وتحليل المعطيات المرتبطة بنشاطات العلاج أو الوقاية ، باستثناء :

— معالجة المعطيات ذات الطابع الشخصي التي يكون الغرض منها المتابعة العلاجية أو الطبية الفردية للمرضى .

— المعالجة التي تسمح بإجراء دراسات .

— المعالجات التي يكون الغرض منها التعويض أو الرقابة من قبل الهيئات المكلفة بالتأمين على المرض .

— المعالجات التي تتم داخل مؤسسات الصحة من قبل الأطباء المسؤولين عن المعلومة الطبية .



وقد اقر المشرع ضمن هذا الإطار عقوبة لمرتكبيها وهي الحبس من سنة إلى ثلاث سنوات وبغرامة من 100000 دج إلى 300000 دج أو بإحدى هاتين العقوبتين فقط، كل من يلج، دون أن يكون مؤهلا لذلك إلى السجل الوطني الخاص بحماية المعطيات ذات الطابع الشخصي الممسوك من طرف السلطة الوطنية، و المقيدة فيه :

- الملفات التي تكون السلطات العمومية مسؤولة عن معالجتها .
- الملفات التي يكون الخواص مسؤولين عن معالجتها .
- مراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة إحداث ملفات عمومية .
- التصريحات المقدمة للسلطة الوطنية والتراخيص التي تسلمها .
- المعطيات المتعلقة بالملفات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم المنصوص عليها في هذا القانون .

كما اقر عقوبة الحبس من سنة إلى ثلاث سنوات وبغرامة من 100000 دج إلى 300000 دج أو بإحدى هاتين العقوبتين فقط، مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية .

2.3.1/ قانون رقم 15-03 المؤرخ في 01 فبراير سنة 2015 يتعلق بعصرنة العدالة (الجريدة الرسمية ، لم تذكر

السنة : ص 04) ، لقد احدث المشرع الجزائري منظومة معلوماتية مركزية للمعالجة الآلية للمعطيات تتعلق بنشاط وزارة العدل والمؤسسات التابعة لها وكذا الجهات القضائية للنظام القضائي العادي والنظام القضائي الإداري ومحكمة التنازع و تضمن الحماية التقنية للمعطيات المذكورة قراءة وكتابة بواسطة برنامج إلكتروني يرخص باستعمال معطيات المنظومة المركزية .

وقد عاقب المشرع الجزائري ضمن هذا النحو كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر بالحبس من سنة إلى خمس سنوات وبغرامة تتراوح بـ 100.000 دج إلى 500.000 دج .

كما عاقب كل شخص حائز شهادة إلكترونية يواصل استعمالها رغم علمه بانتهاء مدة صلاحيتها أو إلغائها بالحبس من سنة إلى خمس سنوات وبغرامة تتراوح بـ 100.000 دج إلى 500.000 دج .

3.3.1/ قانون رقم 15-04 المؤرخ في 01-02-2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق

الإلكتروني (الجريدة الرسمية ، 2021 : ص 09) ، يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني والتصديق الإلكتروني هو شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية :



- أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني طبقا لسياسة التصديق الإلكتروني الموافق عليها
- أن تمنح للموقع دون سواء .
وقد يكون التوقيع الإلكتروني أو شهادة التصديق الإلكتروني محل جريمة الكترونية طالما أن استعمالها ومجال نشاطهم مرتبط بحالة التقنية

و قد عاقب المشرع كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من مليون دينار 1.000.000 دج إلى خمسة ملايين دينار 5.000.000 دج أو بإحدى هاتين العقوبتين فقط .

4.3.1/ الأمر رقم 21-9 المؤرخ في 8 يونيو سنة 2021 يتعلق بحماية المعلومات والوثائق الإدارية (الجريدة الرسمية ، 2015 : ص 06) ، تكتسي المحررات و المراسلات و كذا المعلومات و المحادثات بين مختلف الادارات المشكلة للسلطة العمومية أهمية بالغة من خلالها تقوم الإدارة بتجسيد سلطتها وتكريس قاعدة خدمتها للمرفق العام على ان هذه المراسلات و المحادثات تحتوي في العديد من الأحيان على معلومات في غاية السرية يلحق إفشاؤها إضرارا بالأمن العام ومساسا داخليا وخارجيا بمصالح وسيادة الدولة لذلك عمد المشرع إلى سن قواعد تعنى إلى تأمين المراسلات و الوثائق التي تصدها الإدارة وقد تجسد ذلك في الأمر رقم 21-9 المؤرخ في 8 يونيو سنة 2021 يتعلق بحماية المعلومات والوثائق الإدارية (بن فردية محمد ، 2021 : ص 117) .

و تخضع قانونا لأحكام هذا الأمر المعلومات والوثائق المصنفة المتعلقة بالدولة ومؤسساتها وهيئاتها التشريعية والقضائية والتنفيذية والإدارات العمومية والجماعات المحلية وكل مؤسسة تملك الدولة كل أو بعض رأسمالها وكل مؤسسة تقدم خدمة عمومية .

وقد اقر المشرع ضمن هذا الأمر عقوبة لكل من يدخل دون ترخيص إلى منظومة معلوماتية أو موقع إلكتروني أو شبكة إلكترونية أو أي وسيلة أخرى من وسائل تكنولوجيايات الإعلام والاتصال للسلطات المعنية .

بقصد الحصول بغير وجه حق على معلومات أو وثائق مصنفة بالحبس من خمس سنوات إلى عشر سنوات وبغرامة من 500000 دج إلى 1000000 دج .

و تضاعف العقوبة في حال نشر هذه المعلومات أو الوثائق المصنفة قصد الإضرار بالسلطات المعنية أو الحصول على منافع مباشرة أو غير مباشرة .
كما اقر المشرع عقوبة لكل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني أو برنامج معلوماتي يستعمل لنشر المعلومات أو الوثائق المصنفة أو محتواها كلياً أو جزئياً وهي الحبس من خمس سنوات إلى عشر سنوات وبغرامة من 500000 دج إلى

1000000 دج ويعاقب بنفس العقوبة كل من ينشر المعلومات و الوثائق المصنفة أو محتواها كلياً أو جزئياً على شبكة إلكترونية أو بإحدى وسائل تكنولوجيايات الإعــــــــــــــلام.

كما اقر المشروع عقوبة لكل من يقوم عمدا بنشر أو بث، عن طريق الاتصالات الإلكترونية أو منظومة معلوماتية، معلومة أو وثيقة مصنفة ، بغرض المساس بالنظام العام والسكينة العمومية بالحبس من عشر سنوات إلى خمس عشرة سنة وبغرامة من 1000000دج إلى 1500000دج .

4/ مواجهة الجريمة السيبرانية على ضوء قانون العقوبات (الجريدة الرسمية ، 2004 : ص 08) ، لقد تعرض المشرع الجزائري إلى

الجرائم السيبرانية من خلال تجريمه مايلي :

عند تجريمه الأفعال الماسة بأنظمة الحاسب الآلي وهذا ضمن التعديل الذي أحدثته في قانون العقوبات بموجب القانون رقم 15/04 أين أحدث القسم السابع مكرر و أعطى له عنوان “المساس بأنظمة المعالجة الآلية للمعطيات” و يتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 8 .

و في عام 2006 أدرج المشرع تعديل آخر على قانون العقوبات بموجب القانون رقم 23/06 حيث مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و قد تم تشديد العقوبة المقررة لهذه الأفعال و يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى . وتجدر الإشارة إلى أن المشرع قد قام بتعديل قانون العقوبات في سنة 2016 ، مستحدثا بذلك نصا جديدا وهو المادة 87 مكرر 12 والتي أحدثت لنا جريمة جديدة وهي جناية تجنيد الأشخاص لصالح إرهابي أو منظومة إرهابية بإستخدام وسائل تكنولوجيا الإعلام و الإتصال .

أما بالنسبة لأنواع الجرائم الإلكترونية المنصوص عليها في هذه المواد من قانون العقوبات يمكن حصرها فيما يلي (قسمية محمد ، خضري حمزة ، : ص 127) .

- الدخول أو البقاء عن طريق الغش أو الشروع فيه ، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات.

- إدخال أو تعديل أو حذف أو تغيير عن طريق الغش لمعطيات تتضمنها المنظومة للمعالجة الآلية للمعطيات

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإلتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية.

- حيازة أو إفشاء أو نشر أو إستعمال المعطيات المتحصل عليها من الجرائم المذكورة أعلاه .



-تضاعف العقوبات المقررة للجرائم المذكورة أعلاه إذا استهدفت الدفاع الوطني أو المؤسساتا
و الهيئات الخاضعة للقانون العام .

- عند تجريمه بعض الأفعال لارتباطها بتكنولوجيا المعلومات كجرح التهديد و القذف و النصب
5/ القانون رقم 20-05 المؤرخ في 28 أبريل 2020 يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها (
الجريدة الرسمية ، 2020 : ص 04) ، يهدف هذا القانون إلى الوقاية من التمييز وخطاب الكراهية ومكافحتها و
يقصد، في مفهوم هذا القانون مايلي :

- بخطاب الكراهية جميع أشكال التعبير التي تنشر أو تشجع أو تبرر التمييز، وكذا تلك التي تتضمن
أسلوب الإزدراء أو الإهانة أو العداء أو البغض أو العنف الموجهة إلى شخص أو مجموعة أشخاص على
أساس الجنس أو العرق أو اللون أو النسب أو الأصل القومي أو الإثني أو اللغة أو الانتماء الجغرافي أو
الإعاقة أو الحالة الصحية .

- التمييز كل تفرقة أو استثناء أو تقييد أو تفضيل يقوم على أساس الجنس أو العرق أو اللون أو النسب أو
الأصل القومي أو الإثني أو اللغة أو الانتماء الجغرافي أو الإعاقة أو الحالة الصحية، يستهدف أو يستتبع
تعطيل أو عرقلة الاعتراف بحقوق الإنسان والحريات الأساسية .

وقد اقر المشرع عقوبة على التمييز وخطاب الكراهية بالحبس من ستة أشهر إلى ثلاث سنوات
وبغرامة من 600000 دج إلى 300000 دج وعاقب أيضا كل من يقوم علنا بالتحريض على ارتكاب
الجرائم المنصوص عليها في هذه المادة أو ينظم أو يشيد أو يقوم بأعمال دعائية من أجل ذلك، ما لم
يشكل الفعل جريمة يعاقب عليها القانون بعقوبة أشد، بالحبس من سنة إلى ثلاث سنوات وبغرامة من
100000 دج إلى 300000 دج

و عاقب على التمييز وخطاب الكراهية بالحبس من سنتين إلى خمس سنوات وبغرامة من :50000 دج
إلى 200000

— إذا كانت الضحية طفلا أو سّ هل ارتكاب الجريمة حالة الضحية الناتجة عن مرضها أو إعاقتها أو عجزها
البدني أو العقلي .

— إذا كان لمرتكب الفعل سلطة قانونية أو فعلية على الضحية أو استغل نفوذ وظيفته في ارتكاب
الجريمة .

— إذا صدر الفعل عن مجموعة أشخاص سواء كفاعلين أصليين أو كمشاركين .

— إذا ارتكبت الجريمة باستعمال تكنولوجيات الإعلام والاتصال .



وقد اقر المشرع عقوبة لكل من يشيد أو يشجع أو يمول بأي وسيلة الأنشطة أو الجمعيات أو التنظيمات أو الجماعات التي تدعو إلى التمييز والكراهية بالحبس من سنتين إلى خمس سنوات وبغرامة من 500000 دج إلى 1000000 دج .

كما اقر عقوبة لكل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني يخصص لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز والكراهية في المجتمع بالحبس من خمس سنوات إلى عشر سنوات وبغرامة من 5000000 دج إلى 10000000 دج .

6/ القانون عضوي رقم 12 - 05 المؤرخ 12 يناير سنة 2012 يتعلق بالإعلام (الجريدة الرسمية ، 2012 : ص 21)

(. يهدف هذا القانون العضوي إلى تحديد المبادئ والقواعد التي تحكم ممارسة الحق في الإعلام وحرية الصحافة إذ يمارس نشاط الإعلام بحرية في إطار أحكام هذا القانون العضوي والتشريع والتنظيم المعمول بهما وفي ظل احترام :

- الدستور وقوانين الجمهورية
- الدين الإسلامي وباقي الأديان
- الهوية الوطنية والقيم الثقافية للمجتمع
- السيادة الوطنية والوحدة الوطنية
- متطلبات أمن الدولة والدفاع الوطني
- متطلبات النظام العام
- المصالح الاقتصادية للبلاد
- مهام والتزامات الخدمة العمومية
- حق المواطن في إعلام كامل وموضوعي
- سرية التحقيق القضائي
- الطابع التعددي للآراء والأفكار
- كرامة الإنسان والحريات الفردية والجماعية

كما يقصد بأنشطة الإعلام في مفهوم هذا القانون العضوي كل نشر أو بث لوقائع أحداث أو رسائل أو آراء أو أفكار أو معارف عبر أية وسيلة مكتوبة أو مسموعة أو متلفزة أو إلكترونية وتكون موجهة للجمهور أو لفئة منه وهنا ترتبط القواعد الموضوعية ضمن هذا القانون بالجرائم السيبرانية.



وقد عاقب المشرع كل من نشر أو بث بإحدى وسائل الإعلام المنصوص

عليها في هذا القانون العضوي أي خبر أو وثيقة تلحق ضررا بسر التحقيق الابتدائي في الجرائم بغرامة من خمسين ألف دينار (50.000 دج) إلى مائة ألف دينار 100.000 (دج) كما عاقب المشرع كل من نشر أو بث بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي فحوى مناقشات الجهات القضائية التي تصدر الحكم إذا كانت جلساتها سرية. بغرامة من مائة ألف دينار 100.000 (دج) إلى مائتي ألف دينار 200.000 (دج)

وقد عاقب المشرع كل من نشر أو بث بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي تقارير عن المرافعات التي تتعلق بحالة الأشخاص والإجهاض بغرامة من خمسين ألف دينار (50.000 دج) إلى مائتي ألف دينار 200.000 (دج) .

7/ القانون رقم 14 - 04 المؤرخ في 24 فبراير سنة 2014 يتعلق بالنشاط السمعي البصري (الجريدة الرسمية ،

2014 : ص 06) ، يهدف هذا القانون إلى تحديد القواعد المتعلقة بممارسة النشاط السمعي البصري وتنظيمه و الاتصال السمعي البصري هو كل ما يقدم للجمهور من خدمات إذاعية أو تلفزيونية مهما كانت كفاءات بثها بواسطة الهيرتز أو الكابل أو الساتل .

وقد أشار هذا القانون إلى أن مجال السمعي البصري ينصرف إلى أي اتصال موجه للجمهور بوسيلة إلكترونية و الذي عرف على أساس انه وضع كل ما لا يحمل صفة مراسلة خاصة مهما كانت طبيعتها من إشارات أو علامات أو كتابات أو صور أو أصوات أو رسائل تحت تصرف الجمهور أو فئات منه عن طريق وسيلة اتصال إلكتروني .

وقد تطرق المشرع الجزائري إلى في مجال العقوبات و قرر عقاب بالعقوبات المنصوص عليها في المادة 153 من الأمر رقم 03-05 المؤرخ في 19 يوليو سنة 2003 و المتعلق بحقوق المؤلف والحقوق المجاورة كل شخص معنوي مرخص له باستغلال خدمة الاتصال السمعي البصري ينشر أعمالا فنية ما يخالف حقوق المؤلف والحقوق المجاورة

ب : القواعد الإجرائية في مواجهة الجريمة السيبرانية :

ضمن أحكام القانون الجزائري بوجه عام كما أن هناك قواعد موضوعية كما سبق الإشارة إليها هناك قواعد إجرائية جزائية تحدد كيفية التحري عن الجرائم والتحقيق فيها و وتوقيف مرتكبيها وإحالتهم إلى المحاكم المختصة لمحاكمتهم وإصدار الأحكام بحقهم كما أن ذات القواعد تحدد طرق الطعن في الأحكام و القرارات و الأوامر الجزائية وتنفيذها والسلطات المختصة بذلك .



و بمعنى آخر القواعد الإجرائي و الجزائية المقصودة ضمن هذه الدراسة هي وسيلة لتطبيق قانون العقوبات و القوانين العقابية الخاصة و المعبر عنها في هذه الدراسة بالقواعد الموضوعية لمكافحة الجرائم السيبرانية ، وهي مقرر في التشريع الجزائري وتنحصر في قانونين يستند إليهما في مواجهة الجرائم السيبرانية هما :

- القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها
- قانون الإجراءات الجزائية .

1 : مواجهة الجريمة السيبرانية في ظل القانون رقم 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها (الجريدة الرسمية ، 2009 : بدون ص) .
كتجربة أولى للجزائر لمواجهة الجريمة الالكترونية بطريقة مباشرة صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 غشت 2009 ، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلا أن تجسيد بنوده على أرض الواقع لا يزال ضعيف إلى حد الساعة ، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها .
و يتضمن هذا القانون 19 مادة موزعة على 6 فصول، فيه أحكاما خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية وعددت الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية .

و نص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم .
كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل وقد خول هذا القانون بعض الإجراءات التي تطبق على الجرائم الإلكترونية من :
- مراقبة الاتصالات الإلكترونية :

استحدثت المشرع الجزائري إجراءات المراقبة الإلكترونية بموجب المادة 04 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حينما أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إظهار هذا النوع من الجرائم اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها ،³ غير أن المشرع الجزائري لم يتطرق إلى



تحديد المقصود بمراقبة الاتصالات الإلكترونية واكتفى بتحديد مفهوم الاتصالات الإلكترونية وذلك في الفقرة "و" من المادة الأولى من نفس القانون . من الواضح أن المشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الإلكتروني فقط بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية . و وفقا للقواعد المنصوص عليها في القانون فقد وضع المشرع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية" وقد اعتبر المشرع الجزائري المراقبة التقنية للاتصالات وسيلة إجرائية للحصول على الدليل في مجال الجريمة الإلكترونية بمجموعة من الشروط أهمها:

- أن يتم تنفيذ هذا الإجراء تحت سلطة القضاء وبإذن منه، وهو ما أكدته المادة 04 من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بنصها على أنه : " لا يجوز إجراء عملية المراقبة إلا بإذن من السلطة القضائية المختصة " - أن تكون هناك ضرورة تتطلب هذا الإجراء، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء إلى المراقبة الإلكترونية ، وهو ما أكد عليه المشرع في المادة 04 الفقرة "ج" من القانون المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها .

- تفتيش المنظومة المعلوماتية (بوزنون سعيد، 2019 : ص51) يجوز للسلطات القضائية وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى :

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية .

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية مسبقا بذلك. إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.



يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها .

- حجز المعطيات المعلوماتية : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية. و يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية. غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

- الحجز عن طريق منع الوصول إلى المعطيات : نص المشرع في حالة ما إذا استحال إجراء حجز المعطيات المعلوماتية لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية - إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال عهد المشرع الجزائري في المادة 13 من القانون رقم 09-04 الى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (الجريدة الرسمية ، 2021 : ص 05) مكافحة الجرائم السيبرانية و في هذا المجال تتولى المهام التالية :

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

- مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات.

- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

وقد بينت المادة 04 من المرسوم الرئاسي 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المهام الأساسية التي تكلف بها الهيئة وهي على سبيل الحصر، الهدف منها هو الوقاية من الجرائم الإلكترونية ومكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث



- والتحقيق ومد يد العون لمصالح الشرطة القضائية وابرز مهام هذه الهيئة هي :
- تحديد عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال
- تنشيط وتنسيق عمليات الوقاية عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها .
- مساعدة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدنها بالمعلومات والخبرات القضائية .
- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماساة بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها .
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.

- المساهمة في تحديث المعايير القانونية في مجال اختصاصها

وقد رتب المشرع جزاء وحيد ضمن هذا القانون و يتعلق بترتيب المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية وهو عقاب الشخص الطبيعي بالحبس من ستة 6 أشهر إلى خمس 5 سنوات وبغرامة من 50.000 دج إلى 500.000 دج وعقاب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات .

2/ مواجهة الجريمة السيبرانية في ظل قانون الإجراءات الجزائية :

لقد مرت مواجهة الجريمة السيبرانية في ظل قانون الإجراءات الجزائية بعدة مراحل منها:

1.2/ القانون رقم 04-14 المؤرخ في 10-11-2004 المتضمن تعديل قانون الإجراءات الجزائية (الجريدة

الرسمية، 2004 : بدون ص) . لقد وضع المشرع ضمن هذا التعديل بموجب المواد 37 و 40 و 329 منه قواعد خاصة بمكافحة الجريمة السيبرانية بمفهومها الضيق و المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إذ أجاز تمديد الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق والمحاكم إلى محاكم أخرى إذا تعلق الأمر بمكافحة مثل هذه الجرائم

2.2/ القانون رقم 06-22 المؤرخ في 20-12-2006 المتضمن تعديل قانون الإجراءات الجزائية (الجريدة

الرسمية ، 2004 : بدون ص) ، لقد مدد المشرع ضمن هذا التعديل بموجب المادة 16 / 07 منه الاختصاص



الإقليمي لضباط الشرطة القضائية لكل التراب الوطني إذا تعلق الأمر بالبحث ومعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، كما أجاز المشرع لضباط الشرطة القضائية بموجب المادة 03/47 القيام بإجراء التفتيش و المعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات , كما أجاز ذات التعديل بموجب الفصل الرابع لضباط الشرطة القضائية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور إذا اقتضت ضرورات التحري في مثل هذه الجرائم بموجب إذن مسبق من السيد وكيل الجمهورية أو قاضي التحقيق وتحت مراقبتهما المباشرة.

3.2/ الأمر رقم 11-21 المؤرخ في 2021/07/08 المتضمن تعديل قانون الإجراءات الجزائية (الجريدة

الرسمية ، 2021 : بدون ص) .لقد وضع المشرع الجزائري ضمن قانون الإجراءات الجزائية عدة ترتيبات تخص مكافحة الجرائم المعلوماتية خاصة بموجب تعديل قانون الإجراءات الجزائية بموجب الأمر رقم 11-21 المؤرخ في 2021/07/08 المعدل و المتمم للقانون رقم 66-156 والمتضمن قانون الإجراءات الجزائية أحكام وقواعد إجرائية و آليات خاصة لمكافحة الجريمة السيبرانية منها:

- إنشاء القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال :
تم إنشاء القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على مستوى محكمة مقر مجلس قضاء الجزائر، وهو قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا .

- إعطاء صلاحية لوكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب لممارسة مهامهم في كامل الإقليم الوطني وهذا ضمن مايلي:

- صلاحيات حصريّة بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها :

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني .
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.

- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية .



- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية .

- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين .

- جرائم التمييز وخطاب الكراهية .

- صلاحيات حصريّة بالمراقبة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها (1)

- إعطاء لوكيل الجمهورية للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، وكذا قاضي التحقيق ورئيس ذات القطب اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد 37 و 40 و 329 من قانون الإجراءات الجزائية بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.

- إنشاء القطب الجزائي الاقتصادي والمالي .

- تم إنشاء القطب الجزائي الاقتصادي والمالي بموجب مادة 112 مكرر من قانون الإجراءات الجزائية ضمن تعديل سنة 2020 (2) على مستوى محكمة مقر مجلس قضاء الجزائر وهو متخصص، لمكافحة الجريمة الاقتصادية والمالية ويتداخل اختصاص هذا القطب مع القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في حالة ارتباط الجرائم ببعضها وقد أعطى القانون حلول إجرائية لذلك منها:

- منح الاختصاص للقطب الاقتصادي والمالي إذا تزامن اختصاصه مع اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

- منح الاختصاص لمحكمة مقر مجلس قضاء الجزائر إذا تزامن اختصاصها مع اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

- الإثبات في الجريمة الإلكترونية :

أ- يقصد بالجريمة المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا، بمفهوم هذا القانون، الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامتها آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي .

ب- أمر رقم 04-20 المؤرخ في 30-08-2020 المعدل و المتمم لقانون الإجراءات الجزائية الجريدة الرسمية عدد 51 لسنة 2020 ص 05



يختلف الوسط الذي ترتكب فيه الجريمة المعلوماتية من وسط مادي إلى وسط معنوي (الوسط الافتراضي)، مما أدى إلى ظهور أدلة جنائية خاصة يمكن الاعتماد عليها في الإثبات، بحيث تكون من ذات الطبيعة التقنية الناجمة عن النشاط الإلكتروني التي تنتج منها في حالة الاعتداء عليها، وتتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الرقمية أو الإلكترونية حسب ما عبرت عنها الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية. وليس للدليل الرقمي صورة واحدة بل يوجد له العديد من الصور والأشكال نذكر منها على سبيل المثال:

- الصورة الرقمية :

هي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية والصورة الرقمية تمثل تكنولوجيا بديل للصورة التقليدية .

- النصوص المكتوبة :

وتشمل الأوراق التحضيرية التي يتم إعدادها بخط اليد كمسودة أو تصور العملية التي يتم برمجتها، وكذلك نصوص أساسية وقانونية محفوظة في الملفات العادية وتكون لها علاقة بالجريمة .

- التسجيلات الصوتية :

وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية ، وتشمل المحادثات الصوتية على .

- التسرب في مجال الجريمة المعلوماتية:

يمكن تصور عملية التسرب في نطاق الجرائم الإلكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي، وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها أو اشتراكه في محادثات في غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم، والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات هيئات مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام المخترق للمواقع، أو كيفية ارتكاب الجرائم وحتى المشاركة معهم في ارتكابها لتجميع كل ما يمكن جمعه من الأدلة .

- اعتراض المراسلات السلكية واللاسلكية :

استحدثت المشرع الجزائري بموجب تعديل قانون الإجراءات الجزائية سنة 2006 (السابق ذكره) من خلال المادة 65 مكرر 05 إلى 65 مكرر 10 منه، إجراء جديد يتعلق بمكافحة الجرائم السيبرانية وهو "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور إذ أجاز المشرع في حالة ما إذا اقتضت ضرورات التحري في مثل هذه الجرائم لضباط الشرطة القضائية الحصول على إذن سواء من السيد وكيل الجمهورية أو قاضي التحقيق للقيام بما يلي:

-اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.



- وضع الترتيبات التقنية دون موافقة المعني من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

-الدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن. وضمن هذا الإطار يجب أن يتضمن الإذن المذكور أعلاه كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها و يسلم الإذن مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية و يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينييه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات وعند نهاية العملية يحضر ضابط الشرطة القضائية محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري و يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها و يصف أو ينسخ ضابط الشرطة القضائية المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف و تنسخ وترجم المكالمات التي تتم باللغات الأجنبية .

خاتمة :

إن التطورات الهائلة التي عرفت التكنولوجيا الحديثة للإعلام والاتصال، ورغم ما وفرته من تسهيلات في أمور حياتنا، إلا أنها في المقابل فتحت الباب على مصراعيها لتطور أدوات ووسائل وسبل تنفيذ الجرائم الالكترونية، وجعلتها أكثر تعقيدا وصارت مكافحتها تبدو صعبة المنال إذا لم تتضافر جهود جميع الأطراف الفاعلة في الساحة المعلوماتية، وأمام هذا الوضع بات لزاما على حكومات الدول الإسراع في اتخاذ الإجراءات اللازمة لتطوير آليات التصدي لمثل هذه الجرائم وتعزيز التعاون الدولي في هذا المجال ، و الملاحظ أن المشرع الجزائري واكب من حيث التشريع المتطور الذي وصلت إليه الجريمة ولكن هذا لا يتأني إلا بالتطور الفقهي و الاجتهاد القضائي الذي يمكن من خلاله تفسير النصوص القانونية .



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل

مواجهتها

رمز I05L02UN260120190001

ضحايا الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال في الوسط الجامعي من وجهة نظر الطلبة الجامعيين
دراسة ميدانية على عينة من الطلبة الجامعيين

**Offences relating to information and communication technologies in university
settings from the standpoint of university students**

1- د. محمودي رقية
mahmoudi.rokaia@gmail.com

2- ط د خيزاوي مراد
khabzaoui.mourad@univ-medea.dz

مقدمة

تعيش مجتمعاتنا الحديثة تقدما رقميا كبيرا ، يتسم بتطور التكنولوجيات الجديدة والتسهيلات التي تقدمها الانترنت والتي تعتبر تقدما تكنولوجيا واجتماعيا فعليا ، بالرغم من أن الصعوبات والمخاطر التي تجلبها تمثل تحديات في الحاضر والمستقبل القريب.

ان التطور الحاصل في الجريمة وامتداد مجاله إلى التكنولوجيات الحديثة يستدعي متابعة مستجداتها عبر مجتمعاتنا بالتعرف على الجرائم الحديثة وخصائصها وانماطها وصولا إلى تشخيص اسبابها بهدف الوقاية منها وحماية الافراد من مخاطرها. ان المتتبع لتطور الجريمة المتعلقة بتكنولوجيات الاعلام والاتصال يجد أنها تسجل ارقاما كبيرة تفسر الانتشار الواسع لها في جميع اوساط المجتمع التي لم يسلم منها الوسط الجامعي الذي يشهد تناميا ملحوظا في ضحايا هذا النوع من الجرائم ضمن فئة الطلبة الجامعيين لذلك وجب علينا تسليط الضوء لمعرفة نمطية الجريمة في أوساط الطلبة وأهم الاسباب التي تجعل الطالب الجامعي يقع ضحية لهذا النمط من الجرائم.



1. مشكلة الدراسة:

لقد جاءت الدراسات المتعلقة بالجرائم الماسة بالأشخاص والممتلكات في صورتها التقليدية دون أن يكون للتقنية الحديثة دور فيها، ومع التطور الحاصل والمستمر في تكنولوجيا الاتصال صارت الجريمة ترتكب عبرها مما خلق مشكلات عديدة إذا أسئى استخدامها في ارتكاب الجريمة حيث نلاحظ تفشي ظاهرة الجريمة الواقعة ضد الأشخاص والمتصلة بتكنولوجيات الإعلام والاتصال لا سيما جرائم التهديد والشتم والسب إضافة إلى جرائم النصب والاحتيال والقرصنة وغيرها، وما ينجم عن هذه الجرائم من آثار سلبية تؤثر على المنظومة الاجتماعية والحياة الأمنية .

وبما أن جرائم الشتم والسب تعد من الجرائم الماسة بجرمة وشرف الإنسان المنصوص عليهما في التشريعات العقابية، أصبحت في الوقت الحاضر مع التطور السريع في نظم الاتصال والإعلام ترتكب عبر شبكة الانترنت وغيرها، إذ يساء استخدامها في الاعتداء على الأفراد في شرفهم وأموالهم والتشهير بهم بما يتم إرساله للجمهور عن طريق الأجهزة التقنية و الشبكة العنكبوتية العالمية ، أو عبر المواقع الاجتماعية المفتوحة للجمهور، ولما كان محيط الجامعة والطالب الجامعي ضحية لهذا الصنف من الجرائم وجب علينا التساؤل عن أسباب وقوع الطالب الجامعي ضحية للجريمة المتعلقة بتكنولوجيات الاعلام والاتصال وكذا العوامل المؤدية لمثل هذه الجرائم في أوساط الطلبة الجامعيين؟.

2. أسئلة الدراسة:

- ما هو سبب وقوع الطالب ضحية لجرائم السب والشتم عبر مواقع الانترنت؟.
- بما نفسر تعرض الطالب الجامعي للقرصنة وسرقة البيانات والمعلومات الشخصية؟.
- لماذا يتعرض الطالب الجامعي للتشهير والابتزاز عبر مواقع الأنترنت؟.
- ما سبب تعرض الطالب الجامعي لجريمة النصب والاحتيال الالكتروني؟

3. فرضيات الدراسة

الفرضية العامة: يقع الطالب الجامعي ضحية للجرائم المتعلقة بتكنولوجيات الاعلام والاتصال عبر الفضاء السيبراني بسبب اخلاله بإحدى قواعد الاستخدام السليم لهذا الفضاء، من وجهة نظر الطلبة الجامعيين.

الفرضيات الفرعية:

- يقع الطالب الجامعي ضحية لجرائم السب والشتم بسبب سوء استخدامه لمواقع التواصل وشبكة الانترنت.
- يتعرض الطالب الجامعي للقرصنة وسرقة بياناته الشخصية بسبب ضعف ادراكه لأساليب حماية معطياته الشخصية عبر شبكة الانترنت.
- يرجع تعرض الطالب الجامعي لجريمة التشهير والابتزاز عبر مواقع الانترنت إلى نشر خصوصياته عبر شبكة الانترنت.
- يكون الطالب الجامعي ضحية لجريمة النصب والاحتيال الالكتروني نتيجة جهله للمستعملين دون وعي .

4. أهداف الدراسة: تهدف الدراسة إلى:

- التعرف على مفهوم الجريمة المتعلقة بتكنولوجيات الاعلام والاتصال



- معرفة العوامل المؤدية إلى وقوع الطالب الجامعي ضحية في جرائم المتعلقة بتكنولوجيات الاعلام والاتصال
 - تبيان مدى وجود علاقة ذات دلالة احصائية بين نوع الجريمة التي وقع الطالب الجامعي ضحية لها ومتغيرات الدراسة.
5. أهمية الدراسة :
- ستمد البحث أهميته من التغيرات والتطورات التي يشهدها عالم الإجرام اليوم وتطور أساليب ارتكابه مع دخول تكنولوجيا الاعلام والاتصال الحديثة في حياتنا اليومية والتي أدت إلى وقوع الأفعال الإجرامية التقليدية في صورة الجرائم الحديثة.
 - تناول ظاهرة إجرامية " سلوكات انحرافيه مجرمة قانونيا " جديدة وهي جريمة مستحدثة متمثلة في الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال.
 - تبحث في أسباب وقوع الطالب الجامعي ضحية للجرائم المتعلقة بتكنولوجيات الاعلام والاتصال.
 - تشمل الدراسة مختلف الجامعات والمدارس والمعاهد الجزائرية مما يعطيها القدرة على تعميم النتائج المتحصل عليها.
 - تعمل على تحليل نتائج ومعطيات متحصل عليها لعينة من الشباب الجامعي باعتبارهم ضحايا لهذا النمط من الجرائم

6. حدود الدراسة:

- 1.6 الحدود المكانية: تشمل الحدود المكانية للدراسة كل المؤسسات الجامعية الجزائرية (54 مؤسسة جامعية جزائرية منها 46 جامعة" الوسط:14، الشرق:20، الغرب:12"، 04 مراكز جامعية و04 مدارس عليا) .
- 2.6 الحدود البشرية: تتكون الحدود البشرية للدراسة من 280 طالب جامعي ينتمون إلى إحدى المؤسسات الجامعية الجزائرية و الذين يدرسون في مختلف الأطوار (ليسانس ، ماستر، دكتوراه) .
- 3.6 الحدود الزمانية: الفترة الممتدة من 2022.01.24 إلى غاية 2022.02.12 .
- 4.6 الحدود المنهجية:

المنهج المستخدم: تم خلال الدراسة استخدام المنهج الوصفي التحليلي الذي يعرفه أنه المنهج الذي يتناول الوضع القائم للظواهر والعلاقات المتبادلة بينها، كما يهتم أيضا بالتغيرات التي تحدث نتيجة لمرور الزمن وذلك بوصف المتغيرات في تطورها عبر فترة زمنية. (خناجة، 2002، ص 101)

التقنية البحثية المستخدمة: تم استخدام الاستبيان كتقنية للبحث والتي يعرفها موريس أنجرس أنها تقنية مباشرة لطرح الأسئلة على الأفراد وبطريقة موجهة لأن أجابات الأسئلة تحدد مسبقا وهذا مايسمح بمعالجة كمية بهدف اكتشاف علاقات رياضية واقامة مقارنات كمية. (انجرس، 2006، ص 204) حيث تم صياغة استبيان مكونة من 18 سؤالا مقسمة على ثلاثة محاور (المحور الاولتعلق بالبيانات العامة- 05 أسئلة- ، المحور الثاني متعلقة ببيانات اسعمال الطلبة لشبكة الانترنت-08 أسئلة-، المحور الثالث بيانات متعلقة بالضحية في الجرائم-04أسئلة-)، وقد تم توزيعه الكترونيا عبر منصات التواصل الاجتماعي " المجموعات الخاصة، المجموعات المتخصصة".

7. تحديد المفاهيم:



1.7 تعريف الجريمة : تعرف الجريمة عموما، في نطاق القانون الجنائي بأنها "فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازا " لا جريمة ولا عقوبة أو تدبير أمن إلا بنص " (الأمر رقم 66-156 المتضمن قانون العقوبات، 08 يونيو 1966، ص 02) .

2.7 تعريف الجريمة المتعلقة بتكنولوجيات الاعلام والاتصال: لقد صاغ الفقهاء والدارسون لها عددا ليس بالقليل من التعريفات، تتمايز وتباین تبعا لموضع العلم المنتمية إليه وتبعاً لمعيار التعريف ذاته ، فاختلقت بين أولئك الباحثين في الظاهرة الإجرامية ، وتعددت حسب ما إذا كانت الدراسة متعلقة بالقانون الجنائي أم متصلة بالحياة الخاصة أم متعلقة بحقوق الملكية الفكرية غير أنها اجتمعت كلها في تحديد الجريمة التقنية الحديثة أنها سلوك غير مشروع معاقب عليه قانونا صادر عن ارادة اجرامية محله معطيات تقنية أو باستعمال تكنولوجيات حديثة . ويعرفها القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال ومكافحتها أنها مجموع الجرائم المتعلقة بالمعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

- **تعريف جرائم المساس بحرمة الحياة الخاصة للأفراد:** هي الجرائم المعلوماتية التي تستهدف الأفراد وتقضي الحصول بطريقة غير شرعية على هويتهم الالكترونية وكلمات السر الخاصة بهم ، كما تتم عبر هذه الجريمة عمليات سرقة الصور الشخصية والملفات المهمة من أجهزة الضحايا والمساس بحرمة الاشخاص مثل السب والشتم ، القذف ، الابتزاز ، فهذا النوع من الجرائم هو الأكثر انتشارا لأنه يستهدف الافراد في حد ذاتهم (مجلة الشرطة العلمية والتقنية، 2019 ص 10).

- **تعريف جرائم الانظمة المعلوماتية:** يعرفها القانون 09-04 في المادة الثانية الفقرة 2 على أنها الجرائم التي تمس كل نظام منفصل أو مجموعة الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

- **تعريف السب و الشتم:** تنص المادة 297 من قانون العقوبات الجزائري على أنه يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على اسناد أية واقعة ، ويقصد بالسب كل خدش للشرف والاعتبار وقد تناول المشرع الجزائري جريمة السب والشتم تحت عنوان الاعتداء على شرف واعتبار الاشخاص في المواد 297، 298 مكرر و 299 من قانون العقوبات. وتتعدد صور السب والشتم بتنوع الغرض من استخدامه وطريقته وجاهيا عبر خطوط الاتصال المباشر "هاتفيا" ، وقد يكون كتابيا وقد يكون غيبيا ، او قد يكون بواسطة المطبوعات ، وجميعها ترتكب عن طريق التقنية الحديثة من خلال المبادلات الالكترونية الكتابية أو الصوتية أو الفيديوية " البريد الالكتروني، الأنترنت، مجموعات الاخبار، غرف المحادثات والدرشة" (جعفر، 2013، ص 364)

- **تعريف القرصنة:** هي تلك الافعال الاجرامية المتعلقة بالولوج غير المشروع أو غير المسموح به لنظم المعلومات وتتم عن طريق اختراق شبكات المعلومات، الولوج والاستيلاء على المعلومات الموجودة في قواعد البيانات، التجسس على البيانات ، مع الإشارة الى أنه الاختراق يتم بمجرد الدخول الى نظام الحاسوب او عن بعد في العالم الافتراض ، ويختلف الاختراق عن الدخول غير المصرح به ، كون أنه بعد الاختراق يقوم بالإضافة او بالتعديل أو الاضرار بنظام الحاسوب أو تخريبه أو انتهاك الحق في خصوصية البيانات) سليم، 2012(ص 205، اذ يتم استغلال البيانات المتحصل عليها بالقرصنة وسرقة المعطيات في جرائم النصب والاحتيال والتشهير والابتزاز خاصة .



- تعريف التشهير والابتزاز: تعتبر جنحة في القانون الجزائري ، وقد حدد لها عقوبة ضمن المادة 303

مكرر ، تمس الحياة الخاصة من خلال التقاط صور او تسجيل او نقل مكالمات او احاديث خاصة او نشره دون اذن صاحبه او رضاه ، وكذا التقاط صور او تسجيل صورة لشخص ما في مكان خاص ، كما تنص المادة 303 مكرر " كل من احتفظ أو وضع أو سمح بان توضع في متناول الجمهور او الغير او استخدام أي وسيلة كانت التسجيلات أو الصور او الوثائق المتحصل عليها، وينطبق ذلك على استغلال الملفات الالكترونية من خلال التبادلات الالكترونية بغرض نشر والإساءة والتشهير بالضحايا، أما الابتزاز يعني تهديد شخص وحمله على القيام بفعل أو الامتناع عنه لدافع مادي أو أخلاقي أو الانتقام ، وذلك من خلال استغلال عرض محتوى التبادلات الالكترونية .

تعريف النصب والاحتيال عبر شبكة الأنترنت: يعرف النصب والاحتيال على أنه سلب أو الاستيلاء على ثروة الغير أو البعض منها أو الشروع فيها بالاحتيال ، إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي أو بإحداث الأمل بالفوز بالشيء ويكون برضا المالك تحت تأثير التدليس الجنائي وتحت تأثير الوسائل الاحتيالية (مجلة الشرطة العلمية والتقنية، 2019، ص46).

التعريف الاجرائي للضحية: هو من ارتكب جرما ضده من طرف فاعل ضمن المجال الرقمي أي باستخدام تكنولوجيا الاعلام والاتصال، سواء اتم قرصنة حسابه الشخصي وسرقة بياناته ، او تعرض للنصب والاحتيال او التشهير والابتزاز أو السب والشتيم.

المقاربة السوسيولوجية:

نظرية النشاط الاعتيادي RAT Routine Activity Theory

تدرس نظرية النشاط الروتيني الجريمة كحدث ، وتربط الجريمة ارتباطاً وثيقاً ببيئتها وتؤكد على عملياتها البيئية ، وبالتالي تشتت الانتباه الأكاديمي بعيداً عن المجرمين، وتستند نظرية النشاط الروتيني إلى البيئة البشرية و نظرية الاختيار العقلاني وقد تم استخدام النظرية على نطاق واسع لدراسة الجرائم الجنسية والسرقة والجرائم الإلكترونية).

فرضية نظرية النشاط الروتيني هي أن الجريمة لا تتأثر نسبياً بالأسباب الاجتماعية النشاط الاجرامي السيرياني كنشاط اعتيادي أو روتيني هو من الأنشطة الالكترونية التي افزتها تقنيات نظم المعلومات والتكنولوجيات الرقمية والتي تعكس المخاطر والتهديدات الالكترونية التي يشهدها المجتمع المعلوماتي. (https://emirate2.wiki/wiki/Routine_activity_theory)

تفترض النظرية أن مخاطر احتمال حدوث جريمة يزداد عندما تجتمع عدة عوامل:

- مجرم معلوماتي " SKRAM لديه دافع لارتكاب الجريمة.
- البيانات هي هدف ملائم.
- غياب الرقابة القوية. " تجاوز صلابة ومناعة الجهاز والنظام المعلوماتي"

في الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال يمكن للجناة أن يصلوا إلى العديد من الأهداف " جرائم متعددة" من خلال معرفتهم العلمية ومهارتهم الالكترونية والتقنية من خلال التلاعب بالبيانات والبرامج المعلوماتية وغير ذلك من الأساليب التي تستهدف الولوج إلى الانظمة المعلوماتية ، بهدف تحقيق غاية أو ربح مادي غير مشروع فوجود البيانات والقدرة على التلاعب



بها و التلاعب بالبرمجيات تعتبر فرصة سهلة قليلة المخاطر واحتمالية الكشف عنها في حينها او بعد مدة ضئيلة لا سيما أن كان الفاعل متخصصا أو ضمن جماعة إجرامية ، وباستعمال البرمجيات الحديثة والتقنية العالية لاستهداف النظام المعلوماتي، لاسيما مع تطور التقنيات الحديثة ، وكذا تطور البرمجيات الخبيثة المستخدمة في الجرائم المعلوماتية. وبالنسبة للضحايا من فئة الطلبة الجامعيين فبالنظر الى الخدمات التي تقدمها شبكة الانترنت ،مثل البحوث الجامعية، الخدمات المصرفية، والتسوق الالكتروني، وشبكات التواصل الاجتماعي، والتشارك في الملفات، الأمر الذي يجعل الطلبة متصلين بصفة روتينية ودائمة بشبكة الانترنت اضافة إلى فتح حسابات الكترونية وهذا يؤدي إلى جعلهم عرضة لهجمات اجرامية الكترونية مثل النصب و الاحتيال، التشهير والابتزاز، السب والشتم، القرصنة ... وغيرها كما توفر مواقع التواصل الاجتماعي من الفيس بوك، تويتر... وغيرها اطارا جاهزا للضحايا المحتملين من فئة الطلبة يستغلها المجرمون المعلوماتيون للقيام بنشاطهم الاجرامي.

الاطار النظري:

1- ضحايا الجرائم:

لقد أجمع العلماء أن علم الضحايا يندرج ضمن علم الإجرام و أن مجال الدراسة هذا يعد مناظرا لما يسمى تصميم صفحة المجرم النفسية، ولقد ورد في قاموس علم النفس أن علم الضحايا هو : "العلم الذي يعنى بدراسة شخصية الأفراد ضحية جنحة أو إجرام و مراكزهم الاجتماعية و علاقاتهم العاطفية بالمعتدي " و على الرغم من أن هذا التعريف محدد إلا أنه يتطرق إلى الإشكالية التي كان لرواد هذا العلم أن عالجوها ، إذ انصب اهتمامهم على دراسة العوامل التي بإمكانها أن تهيب الشخص ليصبح ضحية أو كخاصية فريدة (<https://criminologie-victimo.forumactif.org/t26-17->) (2009).

يتضح من خلال هذا التعريف أن علم الضحايا يدرس الضحية انطلاقا من نقطتين :

- الأولى : ستجيب عن مجموع الأفراد المعرضين للخطر ، أي الأفراد الذين يصبحون ضحية على لهذا الفعل الإجرامي أو ذاك
 - الثانية : لتوضيح العوامل الاجتماعية النفسية و النفس- مرضية التي تميز أفرادا سبق أن كانوا ضحية .
- كما يعرف علم الضحايا بأنه يهتم بالعلاقة بين الضحية والجاني أي التفاعل بين الضحايا و نظام العدالة إضافة إلى العلاقة بين الضحايا و الجماعات و المؤسسات مثل وسائل الاعلام و رجال الأعمال و الحركات الاجتماعية .
- يعرف إعلان الأمم المتحدة بشأن المبادئ لتوفير العدالة لضحايا الجريمة و إساءة استعمال السلطة ضحايا الجريمة على النحو التالي:

- يقصد بمصطلح "الضحايا" الأشخاص الذين أصيبوا بضرر فردي أو جماعي بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة من التمتع بحقوقهم الأساسية عن طريق أفعال أو حالات إهمال تشكل انتهاكا للقوانين الجنائية النافذة في الدول الأعضاء بما فيها القوانين التي تحرم الإساءة الجنائية لاستعمال السلطة .
- يمكن اعتبار شخص ما ضحية بمقتضى هذا الإعلان بصرف النظر عما إذا كان مرتكب الفعل قد عرف أو القي عليه القبض أو قوضي أو أدين، و بصرف النظر عن العلاقة الأسرية بينه و بين الضحية. ويشمل مصطلح "الضحية" أيضا ،



حسب الاقتضاء العائلة المباشرة للضحية الأصلية أو معاليها المباشرين والأشخاص الذين أصيبوا بضرر

من جراء التدخل لمساعدة الضحايا في محتهم أو لمنع الإيذاء.

- تطبق الأحكام الواردة هنا على المجتمع دون تمييز من أي نوع بسبب العرق و اللون و الجنس والسن و اللغة و الدين و الجنسية و الرأي السياسي أو غيره و المعتقدات أو الممارسات الثقافية و الملكية و المولد أو المركز الأسري و الأصل العرقي أو الاجتماعي و العجز.

(البشري، 2005، ص 70 ص71)

أما التعريف الذي تعتمد الأكاديمية القومية لمساعدة الضحايا ، فقد توسع أكثر من التعريف الوارد في إعلان الأمم المتحدة بشأن المبادئ الأساسية لعدالة ضحايا الجريمة وإساءة استخدام السلطة و ذلك على النحو التالي :

* تستخدم عبارة ضحايا الجريمة لتشمل شخصا، جماعة أو كيانات تعاني من أذى أو خسارة بسبب نشاط غير مشروع. وقد يكون الإيذاء بدنيا أو نفسا أو اقتصاديا، ويشمل هذا ضحايا الغش أو المشاريع المالية، الأعمال و حتى الحكومة.

كما يشمل تعريف الضحايا مايلي :

* الشخص الذي عانى مباشرة او تعرض لتهديد مادي ،عاطفي او كنتيجة لارتكاب جريمة وهذا بالنظر إلى طبيعة الضحية

أي الحالة القانونية للضحية (قاصر، أعزب)

أو عبارة عن شخص معنوي (مؤسسة ، دولة ...) ، أو عبارة عن متضرر مباشر أو عبارة عن ذوي الحقوق (البشري، 2005، ص72).

ان الضرر من الجريمة يخلف آثار اجتماعية واقتصادية غير محدودة ويصعب حصرها وتقييمها بسبب تجدد أنماط الجرائم وتشعب طبيعة الخسائر الأضرار التي تلحق بالأشخاص و الأموال ، علاوة على التعقيدات التي تصاحب كل تلك الحسابات .

2- الضحايا في الجرائم المستحدثة

هناك عدة ضحايا لم يكن العالم في وقت ليس ببعيد يعرفها منها :

ضحايا الجرائم الإرهابية : رغم الاختلاف الموجود حول التعريف الحديث والموحد للإرهاب إلا إن الإرهاب هو كل عمل وحشي وعنفي منظم يرمي إلى خلق الرعب وإلى أهداف أخرى سياسية ولكن ضحايا الإرهاب لم يعد مقتصر على فئة معينة من دون غيرها وحتى دولة معينة .

ضحايا الجرائم ضد الإنسانية : هي مجمل الجرائم التي ترتكبها في الغالب قوات نظامية ضد البشر، والضحايا هنا تكون عبارة عن قبائل وأسر بأكملها تخضع لأبشع أنواع التنكيل و الإبادة و الأعمال الوحشية و التعذيب و تستعمل فيها أبشع أساليب الفتك والدمار ، ورغم أن هذه الأنواع من الجرائم والضحايا ضد الإنسانية كانت منذ القديم إلا أن صحو المجتمع الدولي كانت معاصرة من خلال سن مجموعة من الاتفاقيات الدولية مثل : ميثاق الأمم المتحدة ، الإعلان العالمي لحقوق الإنسان . وفي الغالب هذه الجرائم لا تخلف ضحايا يمكن تقديم يد المساعدة إليهم لأنه تقضي عليهم نهائيا.

ضحايا جرائم التقنية العالية : تعتبر جرائم التقنية العالية نتائج طبيعية لبيئة التقنية العالية التي يعيش فيها الإنسان ويعتبر الكمبيوتر محورا لها بحيث على الرغم من انه تم صناعته منذ أكثر من نصف قرن إلا انه اليوم أصبح اليوم أكثر سرعة وتطورا .

أما استخداماته أصبح اليوم في مختلف مجالات الحياة العملية في الطب و الجراحة و التجارة و بطاقات الصرف

المجالات الأمنية....الخ



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل

مواجهتها

رمز I05L02UN260120190001

أصبحت جرائم القرصنة و سرقة المعلومات أكثر الجرائم المعلوماتية انتشارا في العالم، وجرائم التقنية العالية يمكن تقديم بعض أنماطها كالعبث بالحاسوب والإخلال بأمن الحاسوب وسرقة المعلومات والمساس بأنظمة معالجة المعلومات الخاصة بالكمبيوتر. أما ضحايا جرائم التقنية العالية ومختلفة ومتنوعة ومعقدة فقد تشمل الدول والمؤسسات العالمية وصولا إلى الحواسيب الشخصية للأفراد .

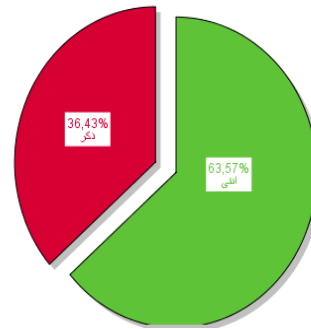
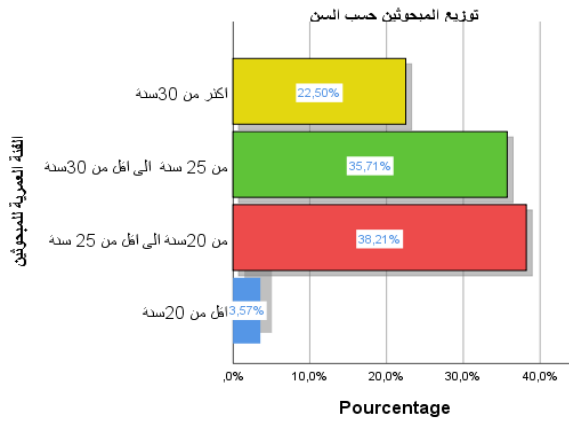
الجانب الميداني

عرض وتحليل النتائج ومناقشتها:

المحور الأول: الخصائص السوسيوديموغرافية للعينة

توزيع المبحوثين حسب الجنس

جنس المبحوث
الأنثى
الذكر



الشكل رقم (02) : توزيع المبحوثين حسب السن

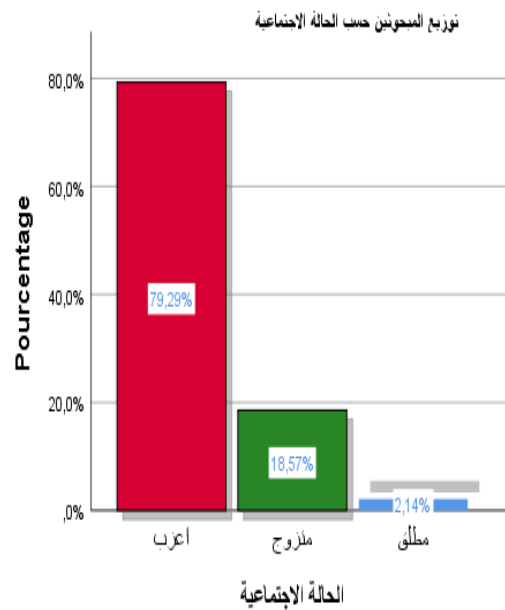
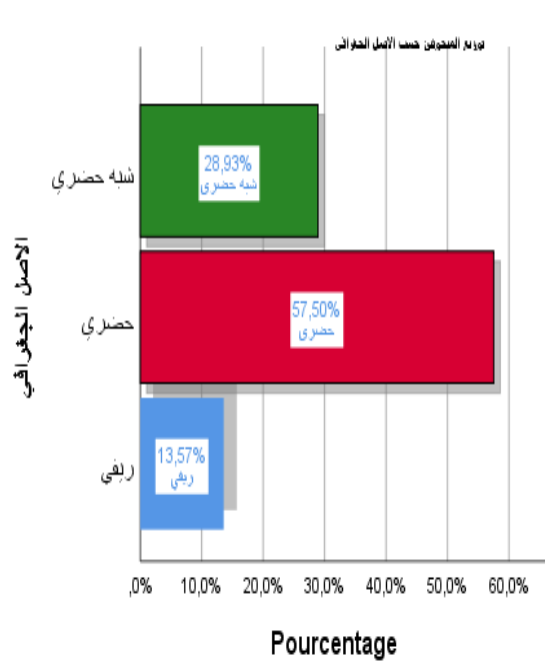
الشكل رقم (01) : توزيع المبحوثين حسب الجنس



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل

مواجهتها

رمز I05L02UN260120190001



الشكل رقم (03) : توزيع المبحوثين

حسب الحالة الاجتماعية

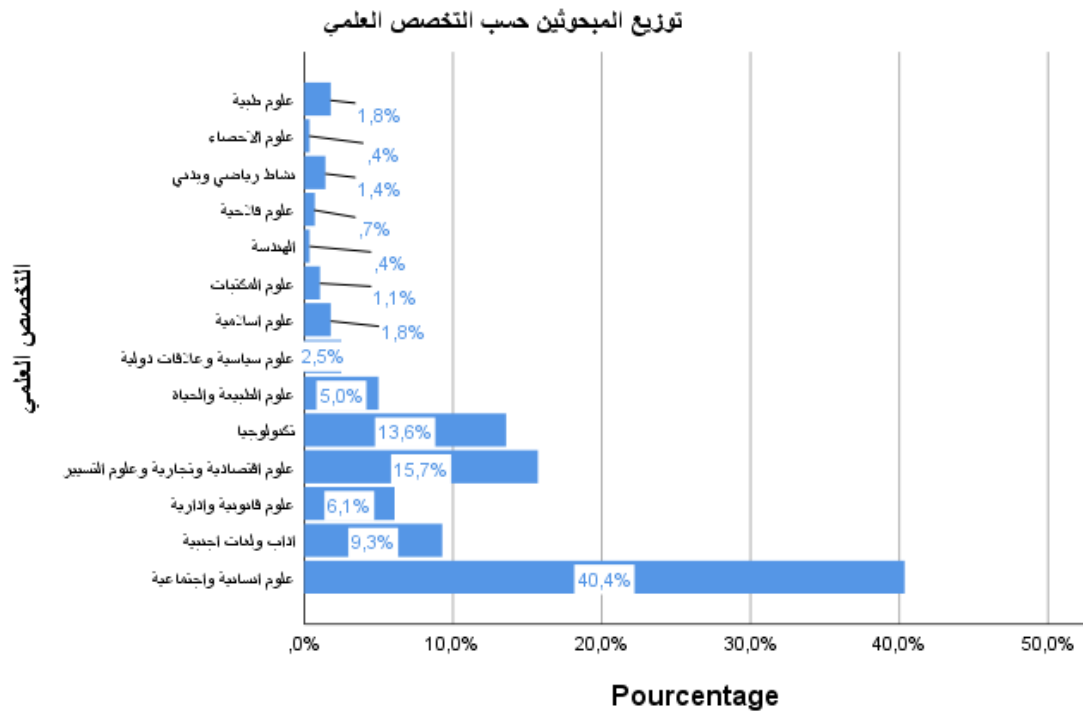
الشكل رقم (04) : توزيع المبحوثين

حسب الأصل الجغرافي

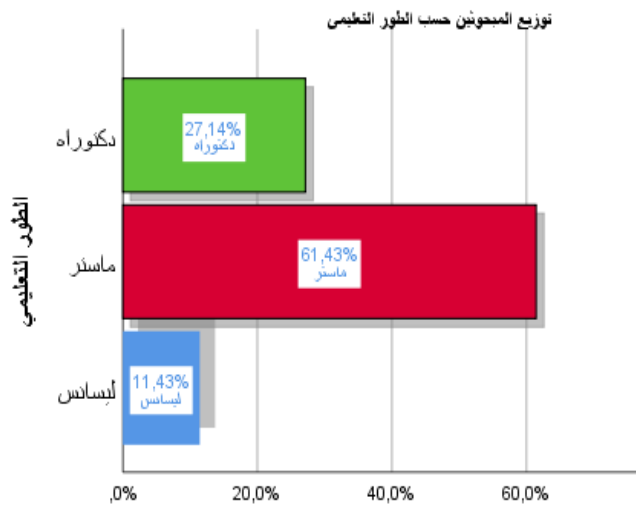


فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها

رمز I05L02UN260120190001



الشكل رقم (06) : توزيع المبحوثين حسب التخصص العلمي



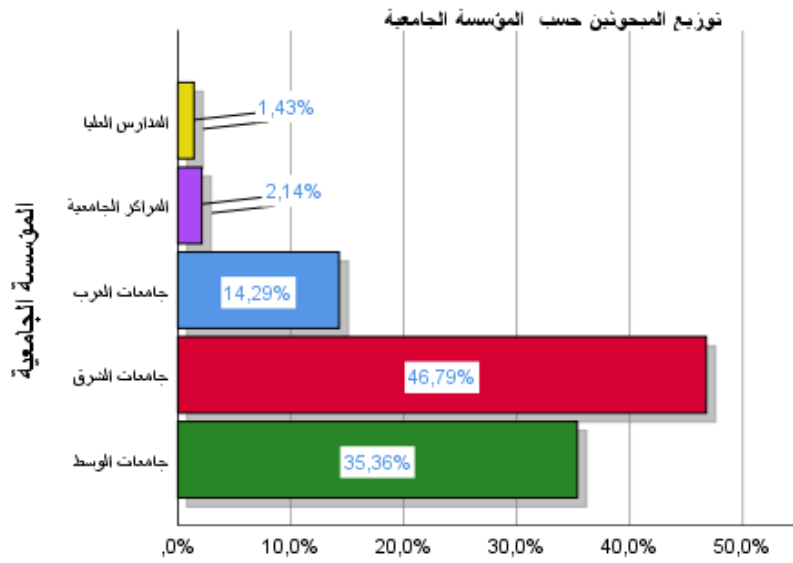
الشكل رقم (05) : توزيع المبحوثين حسب الطور التعليمي



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل

مواجهتها

رمز I05L02UN260120190001



الشكل رقم (07) : توزيع المبحوثين حسب المؤسسة الجامعية

تمثلت عينة البحث في 86.25، الحالة الاجتماعية اعزب بنسبة 79.29 من أصل حضري بنسبة 57.5 مقابل شبه حضري بنسبة 28.93،

يزالون دراستهم في طور الماستر بنسبة 61.43%، مقابل 27.14% طور الثالث دكتوراه ل م د ، ونسبة 11.43% في طور الليسانس، شملت مختلف التخصصات العلمية خاصة العلوم الإنسانية والاجتماعية بنسبة 40% ، وعلوم اقتصادية وتجارية وعلوم التسيير بنسبة 15.7%، و13% تكنولوجيا إضافة الى الطب والهندسة والاحصاء والفلاحة وغيرها. ممثلة 54 مؤسسة جامعية بنسبة 46.70% ناحية الشرق، 35.36% ناحية الوسط، 14.29% ناحية الغرب ، بالإضافة الى المدارس العليا والمراكز الجامعية بنسبة 1.43% و2.14%

المحور الثاني : عادات استهلاك الطلبة لشبكة الانترنت.



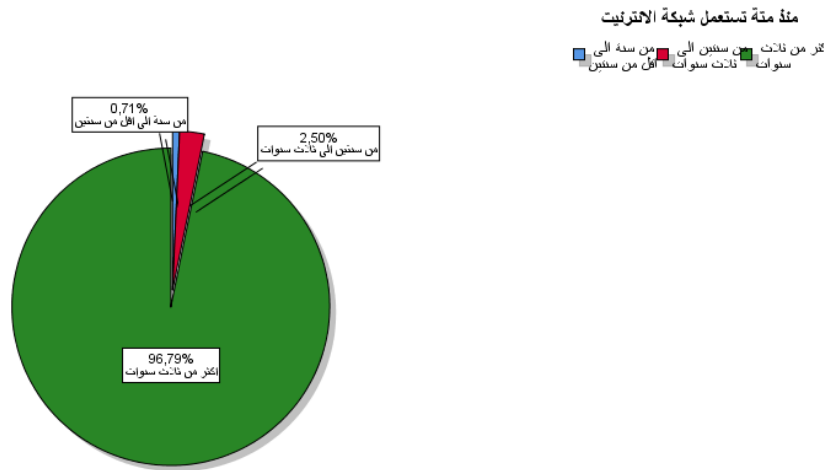
فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل

مواجهتها

رمز I05L02UN260120190001

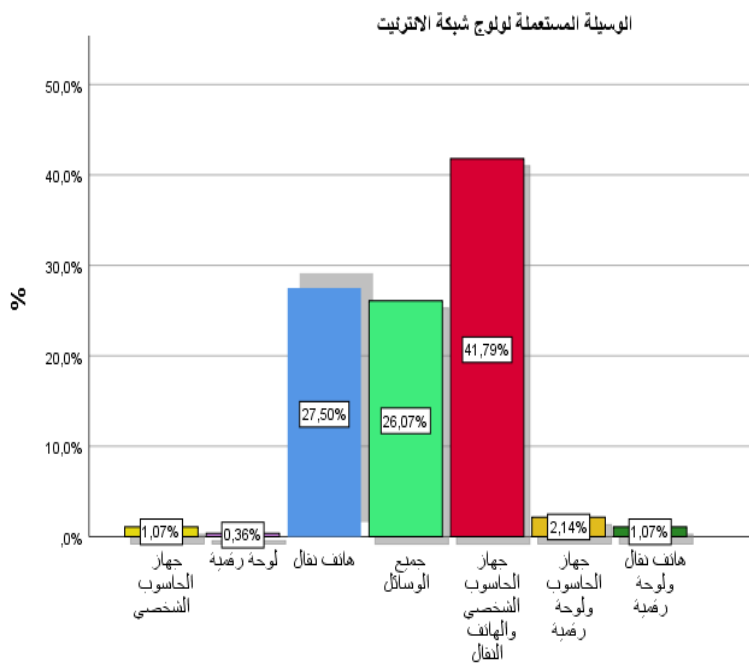
1- استعمال الطلبة لشبكة الانترنت

من متى تستعمل الانترنت



الشكل رقم (08) : استعمال المبحوثين لشبكة

2- الوسيلة المستعملة في ولوج شبكة الانترنت



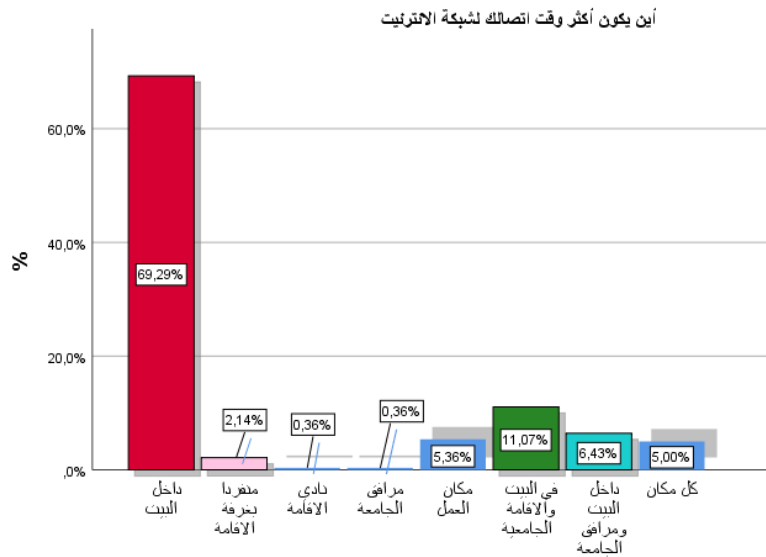
الشكل رقم (09) : الوسيلة المستعملة في الاتصال بشبكة الانترنت لدى



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل

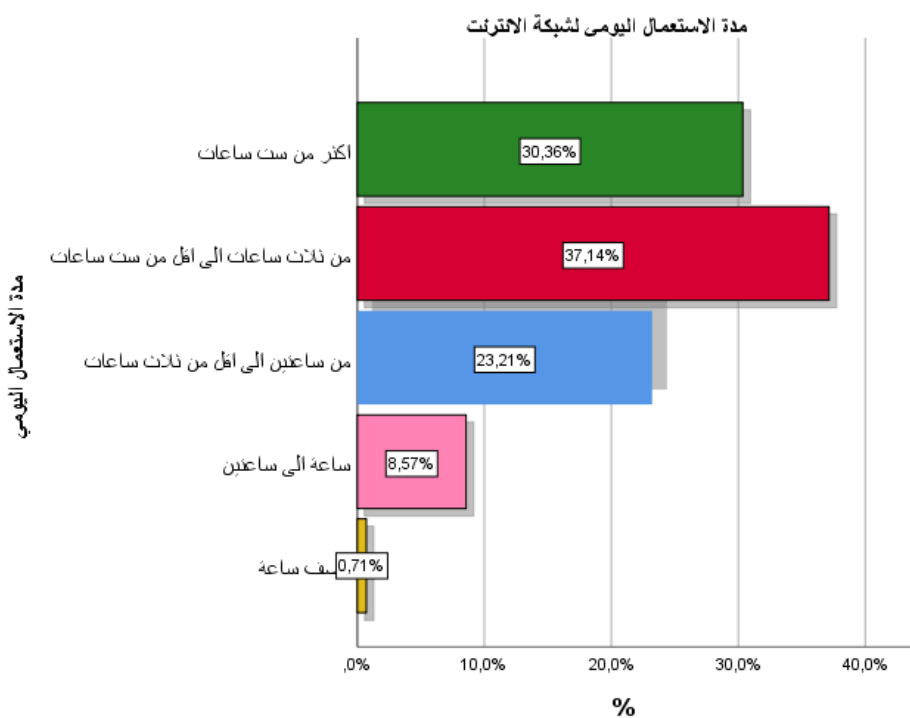
مواجهتها

رمز I05L02UN260120190001



الشكل رقم (10) : المكان الذي يكون فيه أكثر وقت للاتصال بشبكة

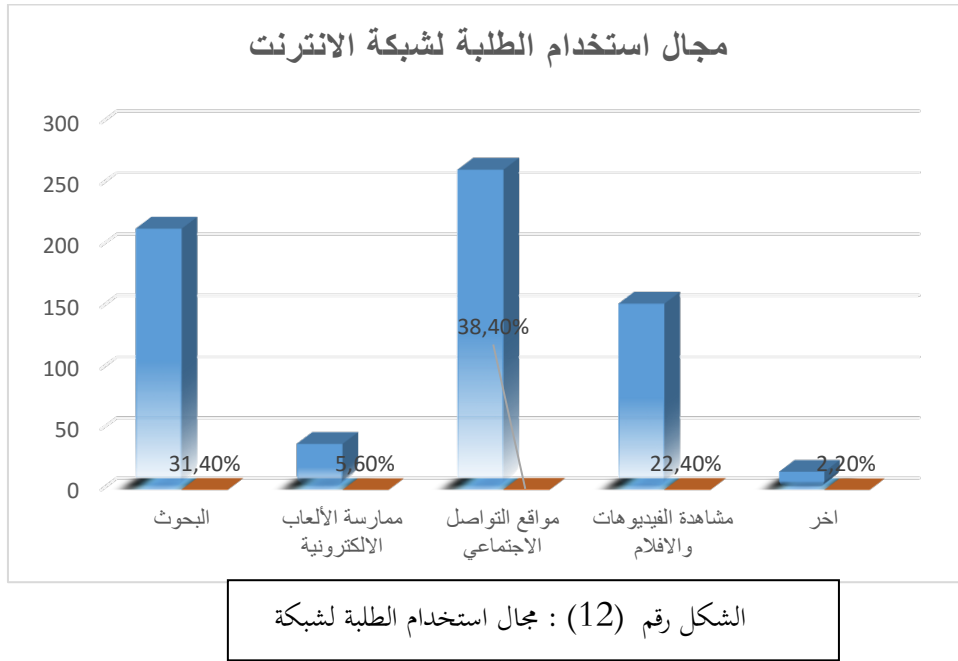
3- مدة الاستعمال اليومي لشبكة الانترنت.



الشكل رقم (11) : مدة الاستعمال اليومي لشبكة



4- مجال استخدام الطلبة لشبكة الانترنت



2. عادات استهلاك الطالب الجامعي لشبكة الانترنت :

يستخدم معظم أفراد العينة الانترنت منذ أكثر من 3 سنوات بنسبة 96.79 %، على مختلف الأجهزة الالكترونية بنسبة 20.07 %، لا سيما الحاسوب الشخصي " 41.79% " و الهواتف الذكية " 27.50% "، في البيت بنسبة 69.29% بالموازاة في أماكن أخرى " الإقامة الجامعية ومرافقها والمرافق الجامعية". ضمن حجم ساعي يتجاوز ساعتين الى أكثر من ست ساعات بنسبة اجمالية تقدر ب 91.71 %، وذلك قصد ولوج مواقع التواصل الاجتماعي بنسبة 38.40%، واعداد البحوث الجامعية بنسبة 31.40%، ومشاهدة الفيديوهات والأفلام بنسبة 22.40%.

مع وجود فروق دالة احصائية في وقوع الطالب ضحية الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومدة الاستعمال اليومي .



5- تحكم الطالب في التكنولوجيات الحديثة حسب متغير الجنس

جدول رقم (01): يبين مدى تحكم الطالب في التكنولوجيات الحديثة

الجنس		ذكر		انثى		المجموع
تحكم الطالب في التكنولوجيات الحديثة	ك	%	ك	%	ك	%
غير متحكم	05	04.9	09	05.1	14	05
متوسط	35	34.3	75	42.1	110	39.3
متحكم	42	41.2	76	42.7	118	42.1
ماهر	06.4	19.6	18	10.1	38	13.6
المجموع	102	100	178	100	280	100
كا ² =5.356	درجة الحرية 03		الدلالة الاحصائية (0.05=α)=0.147		القرار الاحصائي: غير دال احصائيا	

من خلال معطيات الجدول نلاحظ أن ما نسبته 5% من الطلبة فقط غير متحكمين في التكنولوجيات الحديثة (5% من الذكور و 5.1% من الإناث) مقابل 13.6% من الطلبة متحكمين في التكنولوجيات الحديثة بدرجة ماهر يمثلها مجموع 10.1% من الاناث و 6.4% من الذكور ، وبذلك نجد أن أغلبية الطلبة (81.4%) بين متوسط ومتحكم إلى حد ما، وهذا يعني قدرة الطلبة الجامعيين على الاستخدام السليم للتكنولوجيات الحديثة. كما نجد من خلال الجدول عدم وجود فروق ذات دلالة احصائية حسب الجنس تفسر التحكم في التكنولوجيات الحديثة.



7. درجة وعي الطالب بالأمن السيبراني عبر شبكة الانترنت حسب الجنس

جدول رقم (02): يبين وعي الطالب في التكنولوجيات الحديثة

الجنس وعى الطالب بالأمن السيبراني		ذكر		انثى		المجموع	
ك	%	ك	%	ك	%	ك	%
04	03.9	11	06.2	15	05.4		
07	06.9	24	13.5	31	11.1		
40	39.2	92	51.7	132	47.1		
27	26.5	38	21.3	65	23.2		
24	23.5	13	07.3	37	13.2		
102	100	178	100	280	100		
كا ² =18.975		درجة الحرية 04		الدلالة الاحصائية α(=)=0.000 (0.01		القرار الاحصائي: دال احصائيا	
توجد فروق دالة احصائيا في درجة وعى الطلبة بالأمن السيبراني حسب متغير الجنس							

من خلال نتائج الجدول نلاحظ نجد أن نسبة عدم الوعي بالامن السيبراني عند المبحوثين تقدر بـ 16.5% مقابل 83.5% من المبحوثين الواعين موزعين بنسبة 47.1% واعين إلى حد ما و 23.2% واعين و 13.2% واعين جدا. كما نخلص من الجدول إلى وجود فروق دالة احصائية بين متغيري الجنس ودرجة الوعي بالأمن السيبراني .



المحور الثالث : الطالب الجامعي ضحية الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

1. الطالب الجامعي ضحية جريمة الكترونية

جدول رقم (03): يبين وقوع الطالب ضحية للجريمة الالكترونية

المجموع		انثى		ذكر		الجنس الطاب ضحية جريمة الالكترونية
%	ك	%	ك	%	ك	
32.1	90	62.4	53	36.3	37	نعم
60	168	29.8	111	55.9	57	لا
07.9	22	07.9	14	07.8	02	لا اذكر
100	280	100	178	100	102	المجموع

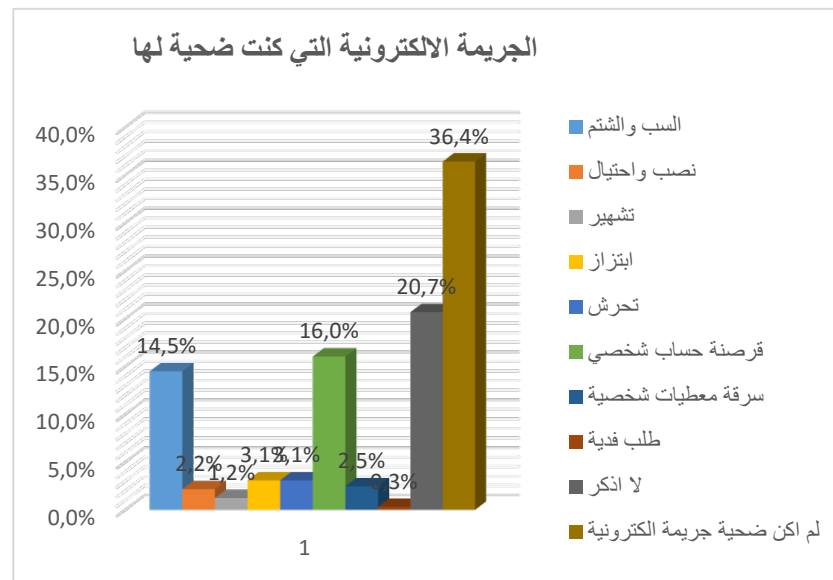
من خلال قراءتنا لمعطيات الجدول نجد أن ما نسبته 60 % من المبحوثين لم يكونوا ضحية لجريمة الكترونية ممثلين من مجموع

55.9 % من الذكور و 29.8 % من الاناث مقابل 32.1 % من المبحوثين لم يتعرضوا لجريمة منهم ما نسبته

36.3 % من الذكور إضافة إلى 62.2 % من الاناث ، أما بقية المبحوثين المقدّر نسبتهم بـ 7.9 % لا يذكرون

تعرضهم للجريمة الالكترونية من عدمه .

2. الجريمة الالكترونية التي كان الطالب ضحية لها



الشكل رقم (13): الجريمة الالكترونية التي تعرض لها المبحوثين



جدول رقم (04): يبين نوع الجريمة التي تعرض لها المبحوثين

الجنس		ذكر		انثى		المجموع	
نوع الجرائم الالكترونية التي كنت ضحية لها		ك	%	ك	%	ك	%
السب والشتيم		15	12.5	32	15.7	47	14.5
نصب واحتيال		02	01.7	05	02.5	07	02.2
تشهير		03	02.5	01	0.5	04	1.2
ابتزاز		04	03.3	06	02.9	10	03.1
تحرش		04	03.3	06	02.9	010	03.1
قرصنة حساب شخصي		22	18.3	30	14.7	52	16
سرقة معطيات شخصية		05	02.5	05	02.5	08	02.5
طلب فدية		01	0.8	-	-	01	03
لا اذكر		23	19.2	44	21.6	67	20.7
لم اكن ضحية جريمة الكترونية		43	35.8	75	36.8	118	36.4
المجموع*		120	100	204	100	324	100

من خلال قراءتنا لمعطيات الجدول نجد ان 36.4% من المبحوثين لم يتعرضو لجريمة الكترونية بينما تراوحت اجابات

المبحوثين ضحية الجريمة الالكترونية بنسبة 16% لجرائم القرصنة تليها جرائم السب والشتيم بنسبة 14.5% تليها جرائم النصب

والاحتيال ، جرائم التحرش الابتزاز والتشهير بنسب تقل عن 5%.

كما نجد أنه لا توجد فروقات كبيرة بين نسب تعرض الذكور لجريمة ما مقابل فئة الاناث.



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل

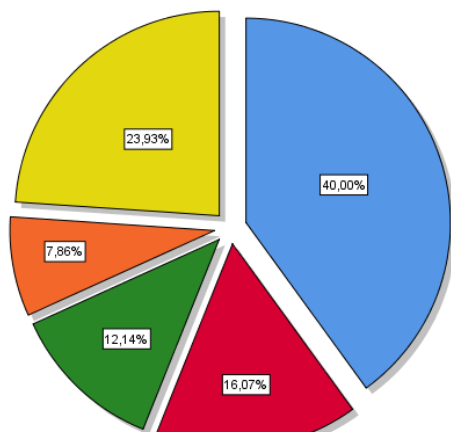
مواجهتها

رمز I05L02UN260120190001

جرائم المساس بتكنولوجيا الاعلام والاتصال التي كان الطالب ضحية لها

Quest_vectime2

- لم اكن ضحية جريمة الكترونية
- ضحية جريمة المساس بالحياة الخاصة
- ضحية جريمة المساس بالانظمة المعلوماتية
- ضحية جريمة المساس بالحياة الخاصة و
- المساس بالانظمة المعلوماتية
- لا اذكر



الشكل رقم (14) : صنف الجريمة الالكترونية التي تعرض لها

جدول رقم (05): صنف الجريمة الالكترونية التي تعرض لها المبحوثون

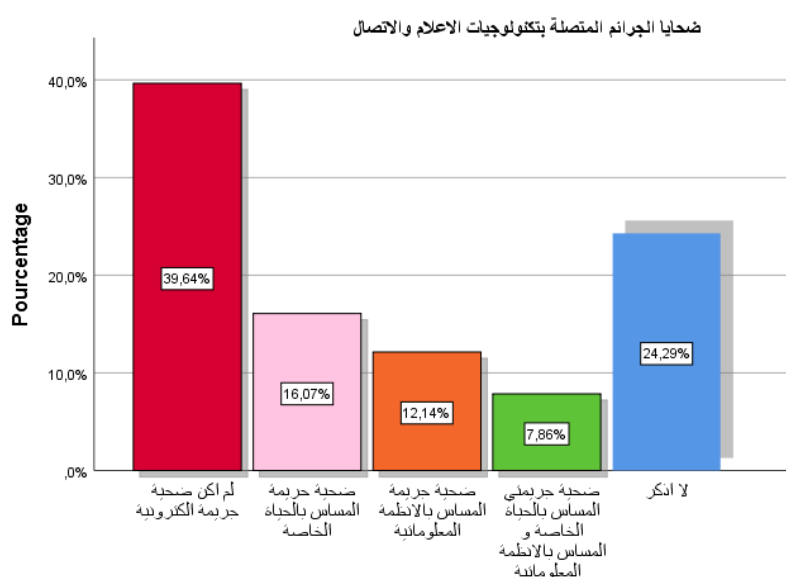
الجنس		نوع الجرائم		الالكترونية		ضحية	
المجموع	انثى	ذكر	انثى	ذكر	المجموع	انثى	ذكر
%	ك	%	ك	%	ك	%	ك
39.6	111	41.6	74	36.3	37	لم اكن ضحية جريمة الكترونية	
16.1	45	14	25	19.6	20	ضحية جرائم المساس بالحياة الخاصة	
12.1	34	11.8	21	12.7	13	ضحية جرائم المساس بالأنظمة المعلوماتية	
07.9	22	07.9	14	07.8	08	ضحية جرائم المساس بالحياة الخاصة وجريمة المساس بالأنظمة المعلوماتية	
24.3	68	24.7	44	23.5	24	لا اذكر	



100	280	100	178	100	102	المجموع
القرار الاحصائي: غير دال احصائيا		الدلالة الاحصائية $\alpha = 0.774$ (0.01)		درجة الحرية 04		$\chi^2 = 1.794$

من خلال قراءة معطيات الجدول أن المبحوثين كانوا ضحايا جرائم المساس بالحياة الخاصة بنسبة 16.1 % مقابل 12.1 % لجرائم المساس بالأنظمة المعلوماتية و 7.9 % للجريمتين معا.

نخلص من الجدول إلى عدم وجود فروق دالة احصائية لمتغير الجنس مع صنف الجرائم المتعرض لها.



الشكل رقم (15): صنف الجريمة الالكترونية التي تعرض لها

جدول رقم (06): عدد المرات التي كان الطالب ضحية للجريمة الالكترونية

37.1 % كانوا ضحايا للجرائم المتصلة بتكنولوجيات الاعلام

والاتصال، بين مرة واحدة وأكثر ثلاث مرات بالنسب

الاتية: 21.1 %، 7.1 %، 3.6 %، 5.6 %

عدد المرات التي كنت فيها ضحية	ك	%
ولا مرة	176	62.9
مرة واحدة	59	21.1
مرتين	20	07.1
ثلاث مرات	10	03.6
أكثر من ثلاث مرات	15	05.6
المجموع	280	100

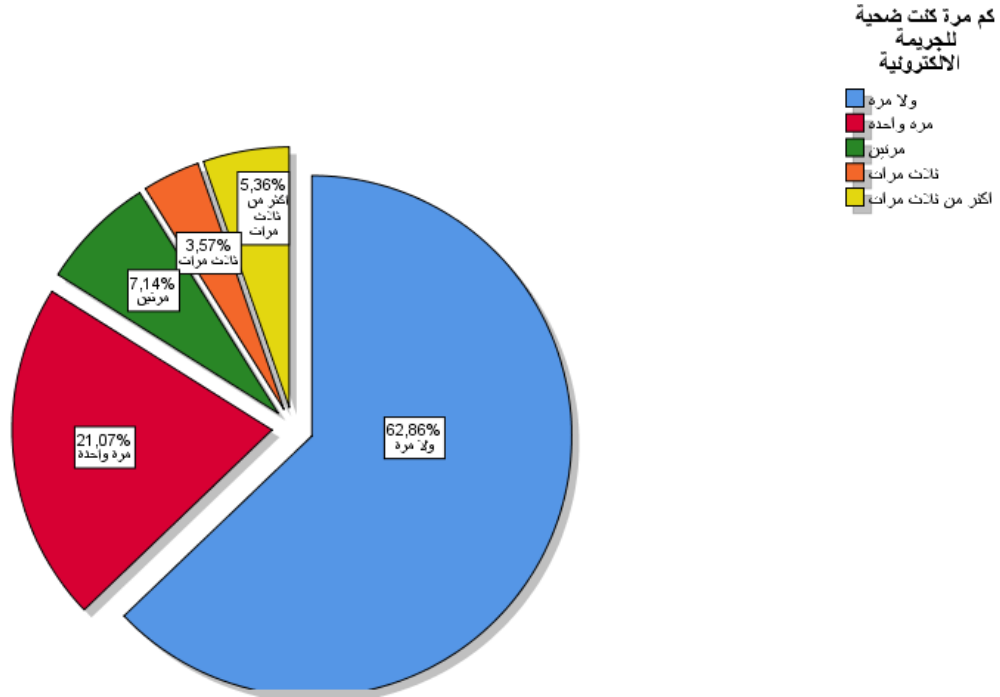


فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل

مواجهتها

رمز I05L02UN260120190001

عدد المرات التي كان فيها الطالب ضحية جريمة الكترونية



الشكل رقم (16): عدد مرات وقوع المبحوثين ضحية للجريمة

جدول رقم (07): كيفية اكتشاف الجريمة الالكترونية

كيفية اكتشاف القضية	ك	%
من طرفك	176	62.9
عن طريق الأجهزة الأمنية	59	21.1
عن طريق صديق	20	07.1
لم تكتشف	10	03.6
المجموع	280	100

تم اكتشاف القضية من طرف الضحية بنسبة 62.9 %، مقابل

21.1 % عن طريق الأجهزة الأمنية ، وبنسبة 7.1

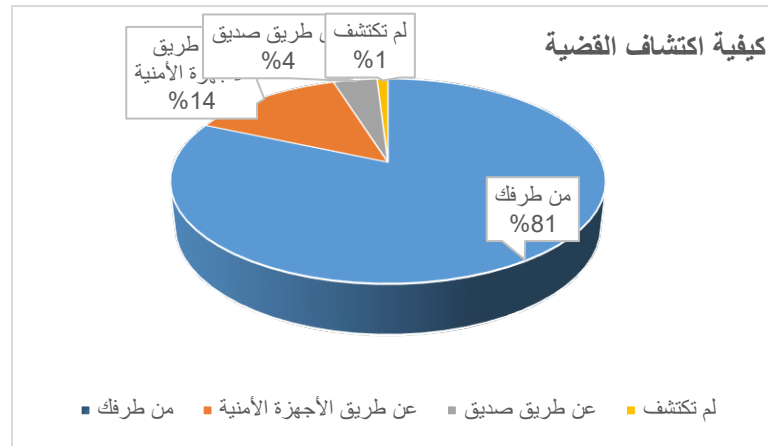
% من طرف صديق ، ونسبة 3.6 %، تعبر عن عدم

اكتشافها .



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها

رمز I05L02UN260120190001



جدول رقم (08): تقديم شكوى من طرف الضحية

تقديم شكوى من طرف الضحية	ك	%
نعم	07	6.8
لا	96	93.2
المجموع	103	100

93.2% لا يقدمون شكوى جراء وقوعهم ضحية الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال ، وهذا يؤكد غياب ثقافة التبليغ حتى في الوسط الجامعي.

ويمكن استخلاص ما يلي:

نسبة 32.1% من الطلبة الجامعيين كانوا ضحية لجرائم مرتبطة بتكنولوجيات الاعلام والاتصال مقابل نسبة 7.9% لا يذكرون ذلك مع احتمال كونهم ضحايا أيضا لجرائم المساس بالحياة الخاصة " 16.1% " سب وشتم ، نصب واحتيال، تشهير وابتزاز، طلب فدية " وجرائم المساس بالأنظمة المعلوماتية بنسبة 12.1% " قرصنة حساب شخصي، وسرقة معطيات شخصية ، وكلا الجريمتين بنسبة 07.9% ، وذلك لمرة واحدة 21.1 ومرتين بنسبة 7.1% وأكثر من ثلاث مرات 3.6% ، وقد تم اكتشاف القضية من طرف الضحايا بنسبة 62.9% مقابل 21.1% عن طريق الأجهزة الأمنية، بالإضافة الى أن نسبة 93.2% من الضحايا لم يتقدموا بشكوى للجهات الأمنية.

البنية العائلية لتغير الطالب الجامعي كضحية للجريمة الالكترونية من وجهة نظر الطالب

نظرا لوجود عدد كبير من المتغيرات أو البنود الممثلة للمتغير والتي تضمنت 19 i بندا، ونظرا لاهميتها ولوجود علاقات ارتباط قوية وذات دلالة احصائية عالية بين غالبية هذه البنود تطلب الأمر تطبيق التحليل العائلي (Analyse factorielle) لهذه البنود أو الفقرات، والذي من شأنه العمل على تقليل عدد هذه البنود وتصنيفها وترتيبها ضمن مجموعات مستقلة "أبعاد أو مجالات".



وقد تم اجراء التحليل العاملي ل 19 بندا باستخدام طريقة تحليل المركبات الاساسية (Composantes Principales)، وقد أظهرت عملية التحليل وجود أربعة أبعاد .

وبعد اجراء عملية التدوير (Rotation) وفق طريقة (Rotation Vari max) أي التدوير المتعامد ، لاستخراج مصفوفة الأبعاد المدورة لبيان تشبع كل عامل من العوامل بالبنود، والذي يمثل معاملات الارتباط بين البنود والأبعاد ، حيث أظهرت عملية التدوير وجود أربعة أبعاد رئيسية فسرت 59,230% من التباين الكلي لآراء المبحوثين حول متغير سبب وقوع الطالب الجامعي ضحية الجرائم الالكترونية .

وقد بينت نتائج التحليل العاملي وجود درجة تشبعات عالية للأبعاد بمتغيراتها أو بنودها، وقد بلغ الحد الأدنى لتشبعات الأبعاد 1.261 وهو اعلى من 0.6 وهو يعتبر مستوى عالي في الحالات التي يستخدم فيها مقياس ليكارت الخماسي ، كما أن عدد بنود كل بعد قد تجاوز ثلاثة أبعاد

لدينا :- حسب جدول مصفوفة معاملات الارتباطات البيئية : معظمها أكبر من 0.30 ودالة احصائية، وهذا ما يدل على أن المتغيرات الداخلة في المقياس جيدة . كما أن قيمة معامل التحديد للمصفوفة معامل التحديد $0.00001 \text{Determinant} = 0.001 >$

أي عدم وجود ارتباطات مرتفعة جدا أو عدم وجود اعتماد خطي بين المتغيرات (تكرار واستنساخ للمعلومات التي يشارك بها كل متغير)

اختبار جودة المعاينة KMO Indice de Kaiser-Meyer-Olkin pour la mesure de la qualité d'échantillonnage.

الدلالة الاحصائية	د رجة الحرية	اختبار كا2	اختبار دقة المعاينة
Sig,000=	Ddl=171	Khi-deux approximé=2128,897	KMO=,876

اختبار دقة المعاينة $KMO = 0.876$ والذي يعني ان النتائج المستخلصة فيما يخص الارتباط خطأها لا يعود إلى المعاينة " حجم العينة كافية لإجراء التحليل العاملي .

إلى جانب اختبار الكروية Bartlett's test of sphericity والذي يعتمد على اختبار كا2 والذي في حالة دلالاته الاحصائية على انه يوجد على الأقل ارتباط دال بين الفقرات مما يؤهلنا للتحليل العاملي .

مقياس Measures of Sampling Adequacy(MSA) لكل متغير (أو فقرة إذا كانت المتغيرات فقرات) أعلى من 0,5 مما يدل على أن مستوى الارتباط بين كل متغير بالمتغيرات الأخرى في مصفوفة الارتباطات كاف لإجراء التحليل العاملي .

- التباين الكلي المفسر

يظهر الجدول الجذر الكامن للمكونات (العوامل) في العمود المعنون Total . وتوجد 4 جذور كامنة أعلى من الواحد الصحيح. ويدل على حجم التباين المستخرج أو المفسر من قبل كل مكون أو عامل. كما يظهر الجدول هذا القدر من التباين المفسر



بشكل نسب مئوية من التباين المفسر والنسب المئوية من التباين المفسر التراكمي. مثلا نجد أن الجذر الكامن للعامل الأول يفسر (6,400) ، ويفسر نسبة مئوية من التباين الكلي قدرها (33,683). ويلاحظ أن التدوير يوزع نسب التباين الموزع بين العوامل بشكل متوازن نسبيا ولا يجعله يتركز في العامل أو العاملين الأولين. ويظهر ذلك جليا عند مقارنة العمود السادس والعمود التاسع.*

جدول رقم(09): مصفوفة العوامل بعد التدوير " مصفوفة النمط"

Rotation de la matrice des composantesa					
الفقرات او البنود	Composante				قيم الشيوع أو الاشتراكيات Communalities
	سبب وقوع الطلبة ضحايا سرقة معطيات شخصية قرصنة ضحايا حساب شخصي	سبب وقوع الطلبة ضحايا سرقة معطيات شخصية قرصنة ضحايا حساب شخصي	سبب وقوع الطلبة ضحايا سرقة معطيات شخصية قرصنة ضحايا حساب شخصي	سبب وقوع الطلبة ضحايا سرقة معطيات شخصية قرصنة ضحايا حساب شخصي	
البند20	,852				,684
البند18	,801				,722
البند19	,786				,558
البند21	,748				,476
البند17	,705				,581
البند12	,512	,407			,673
البند10	,502				,614
البند14		,775			,438
البند13		,678			,491
البند16		,673			,456
عدالبند11		,632			,596
البند15		,541			,651
البند8			,770		,509
البند9			,731		,479
البند7			,718		,602
البند6			,644		,681
البند4				,823	,665
البند3				,774	,740
البند5				,704	,638

* جدول التباين الكلي المفسر Variance totale expliquée مخرجات التحليل العاملي ، والذي أدرجت نتائجه في الجدول الموالي



نسبة التباين الكلي المفسر 59.230	1.261	1.464	2.129	6.400	الجذر الكامن
30	6.637	7.706	11.208	33.683	نسبة التباين المفسر

تسمية العوامل بناء على مصفوفة النمط:

العامل الأول: ساهم هذا البعد في تفسير 33.683 % من مجموع التباين الكلي المفسر 59.230 % والذي يعبر عن سبب وقوع الطلبة ضحايا جرائم النصب والاحتيال وقد تضمن سبعة بنود "10.12.17.21.19.18.20" وتتجلى في : الاغراء بعروض مالية، دفع مبالغ شراء سلع من الانترنت دون استلامها، المشاركة في حملات التبرع الوهمية، تقديم معلومات شخصية مقابل وعد بالاستفادة من سلع وخدمات، القرصنة وسرقة البيانات لاستغلالها في عمليات النصب والاحتيال"

العامل الثاني: ساهم هذا البعد في تفسير 11.208 % من مجموع التباين الكلي المفسر 59.230 % والذي يعبر عن سبب وقوع الطلبة ضحايا جرائم التشهير والابتزاز وقد تضمن أربعة بنود: "11.16.13.14" من خلال مشاركة الصور والفيديوهات مع الاصدقاء عبر مواقع التواصل، عرض معطيات وصور وفيديوهات الحياة الشخصية، عدم قبول الاناث الصداقات مع الاشخاص المجهولين، وعن طريق القرصنة وسرقة المعلومات الشخصية بسبب عدم تحديد كلمات المرور الخاصة بالحسابات، الصداقات مع الاشخاص المجهولين.

العامل الثالث: ساهم هذا البعد في تفسير 7.706 % من مجموع التباين الكلي المفسر 59.230 % والذي يعبر عن سبب وقوع الطلبة ضحايا سرقة معطيات شخصية قرصنة حساب شخصي وتضمن أربعة بنود : "7.6.9.8" التواصل مع الاشخاص المجهولي الهوية، التصفح عبر المواقع المشبوهة الى سهولة الوصول الى بيانات ومعطيات حساب الطالب، كثرة النشر، المشاركة والردشة عبر مواقع الانترنت، استخدام هوية حقيقية إلى سهولة التعرف على الطالب من طرف المجرمين.

العامل الرابع : ساهم هذا البعد في تفسير 6.637 % من مجموع التباين الكلي المفسر 59.230 % والذي يعبر عن سبب وقوع الطلبة ضحايا السب والشتيم وتضمن ثلاثة بنود : "5.3.4"، قبول الصداقات دون التأكد من هوية طالبها، التواصل مع الاشخاص المجهولين، استخدام هوية مزيفة.

- هل يتوفر مقياس " ضحية " المطبق على عينة الطلبة الجامعيين على دلالات ثبات مقبولة؟



❖ معامل ثبات ألفا كرونباخ

تم حسابه بالنسبة للمقاييس الفرعية والمقياس ككل فكانت النتائج كالتالي:

جدول رقم (10): معاملات ثبات ألفا كرونباخ لمقياس " الضحية".

أبعاد المقياس	عدد الفقرات	معامل ألفا كرونباخ %
سبب وقوع الطلبة ضحايا النصب والاحتيال	07	78.6
سبب وقوع الطلبة ضحايا التشهير والابتزاز	05	78.6
سبب وقوع الطلبة ضحايا سرقة معطيات شخصية قرصنة حساب شخصي	03	80
سبب وقوع الطلبة ضحايا السب والشتم	03	82.2
المقياس ككل	19	78.8

يتضح من الجدول السابق أن معاملات الثبات بطريقة ألفا كرونباخ بين أبعاد مقياس التمكين الوظيفي تراوحت بين (0.786-0.822) وهي معاملات ثبات مقبولة، كما بلغ معامل الثبات الكلي للمقياس (0.788) وهي قيمة مرتفعة مما يعني أن المقياس يتمتع بدرجة عالية من الثبات.

- هل يتوفر مقياس سبب وقوع الطالب شحبة للجرائم الالكترونية المطبق على عينة الكلية الجامعين على دلالات صدق مقبولة؟

تم التحقق من صدق المقياس من خلال الطرق التالية:

❖ صدق الاتساق الداخلي

• الارتباط بين الدرجة الكلية لكل بعد والدرجة الكلية للمقياس

• الجدول رقم (11): معامل ارتباط كل بعد مع الدرجة الكلية لمقياس الضحية

الرقم	البعد	معامل الارتباط	الدلالة الإحصائية Sig , $\alpha = 0.01$
01	سبب وقوع الطلبة ضحايا النصب والاحتيال	.846**	0.000
02	سبب وقوع الطلبة ضحايا التشهير والابتزاز	.816**	0.000
03	سبب وقوع الطلبة ضحايا سرقة معطيات شخصية قرصنة حساب شخصي	.709**	0.000
04	سبب وقوع الطلبة ضحايا السب والشتم	.816**	0.000

يتضح من الجدول رقم (11) أن قيم معاملات الارتباط بين أبعاد مقياس سبب وقوع الطالب الجامعي ضحية

الجرائم الالكترونية الابعاد الأربعة والدرجة الكلية كانت ذات دلالة إحصائية عند مستوى 0.01، حيث كانت معاملات



الارتباط مرتفعة إذ تراوحت بين 0.709 كأدنى قيمة لبعده سبب وقوع الطلبة ضحايا سرقة معطيات شخصية قرصنة حساب شخصي و 0.846 كأقصى قيمة لبعده سبب وقوع الطلبة ضحايا النصب والاحتيال ، وهذا ما يعطي مؤشرا للتجانس الداخلي للمقياس، أي انه يتمتع بدرجة مرتفعة من الصدق.

- اتساق كل فقرة مع البعد

الجدول رقم (12): معاملات الارتباط بين كل فقرة والدرجة الكلية للبعد الذي تنتمي إليه لمقياس الضحية

ضحايا السب والشتم		ضحايا سرقة معطيات شخصية قرصنة حساب شخصي		ضحايا التشهير والابتزاز		النصب والاحتيال	
الارتباط	الفقرة	الارتباط	الفقرة	الارتباط	الفقرة	الارتباط	الفقرة
.807**	04	.770**	08	.787**	14	.808**	20
.825**	03	.727**	09	.734**	13	.810**	18
.740**	05	.777**	07	.702**	16	.796**	19
		.758**	06	.723**	11	.781**	21
				.962**	15	.783**	17
						0.647	10
						0.673	12

يتضح من الجدول السابق أن جميع معاملات ارتباط العبارات بالمقاييس الفرعية التي تنتمي إليها دالة إحصائية عند مستوى دلالة 0.01 ، ما يعتبر مؤشرا على صدق الاتساق الداخلي لمقياس ، وقد تراوحت القيم الارتباطية بين درجات العبارات والدرجات الكلية للأبعاد التي تنتمي إليها ما بين 0.647** وهي دالة عند 0.01 كأدنى قيمة و 0.962** كأعلى قيمة، مما يعني أن عبارات الأبعاد الفرعية متناسقة فيما بينها وتقيس البعد نفسه الذي يفترض أنها تنتمي إليه وتقيس جانبا سلوكيا يعبر عنه بالتماسك الداخلي للمقاييس الفرعية وتقديره لمظاهر سلوكية واحدة.



الجدول رقم (12): درجات سبب وقوع الطالب ضحية الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال

درجات سبب وقوع الطالب ضحية الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال	ك	%
مرتفع	262	93.6
متوسط	08	02.9
منخفض	10	03.6
المجموع	285	100
$X^2 = 18.117$; ddl=8 ; sig=0.020		الوعي *
$X^2 = 14.701$; ddl=6 ; sig=0.023		التحكم

تعدت نسبة استجابة المبحوثين لأسباب وقوع الطالب ضحية الجرائم المتصلة بتكنولوجيات الاعلام والاتصال بدرجة مرتفعة 93 %. مع الإشارة الى وجود فروق دالة احصائية حسب متغيري درجة الوعي بالأمن السيبراني ومدى تحكم الطالب في التكنولوجيا الحديثة

3. أسباب وقوع الطالب الجامعي ضحية جرائم تكنولوجيا الاعلام والاتصال:

يقع الطالب الجامعي ضحية للجرائم المتعلقة بتكنولوجيات الاعلام والاتصال عبر الفضاء السيبراني بسبب اخلاله بإحدى قواعد الاستخدام السليم لهذا الفضاء، من وجهة نظر الطلبة الجامعيين.

وبناء على تحليل البنية العاملي للمتغير يمكن استخلاص الأسباب فيما يلي :

أ. يقع الطالب الجامعي ضحية جرائم النصب والاحتيال من وجهة نظر الطلبة الجامعيين : نتيجة جهله للمستعملين دون وعي من خلال : الاغراء بعروض مالية، دفع مبالغ شراء سلع من الانترنت دون استلامها، المشاركة في حملات التبرع الوهمية، تقديم معلومات شخصية مقابل وعد بالاستفادة من سلع وخدمات، القرصنة وسرقة البيانات لاستغلالها في عمليات النصب والاحتيال"

ب. يقع الطالب الجامعي ضحية جرائم التشهير والابتزاز من وجهة نظر الطلبة الجامعيين: بسبب نشر خصوصياته عبر شبكة الانترنت من خلال مشاركة الصور والفيديوهات مع الاصدقاء عبر مواقع التواصل، عرض معطيات وصور وفيديوهات الحياة الشخصية، عدم قبول الاناث الصداقات مع الاشخاص المجهولين، وعن طريق القرصنة وسرقة المعلومات الشخصية بسبب عدم تحديد كلمات المرور الخاصة بالحسابات، الصداقات مع الاشخاص المجهولين.



ت. يقع الطالب الجامعي ضحية جرائم سرقة معطيات شخصية وقرصنة حساب شخصي " جرائم

المساس بالأنظمة المعلوماتية من وجهة نظر الطلبة الجامعيين: بسبب ضعف ادراكه لأساليب حماية معطياته الشخصية عبر شبكة الانترنت ويتجلى ذلك من خلال التواصل مع الاشخاص المجهولي الهوية، التصفح عبر المواقع المشبوهة الى سهولة الوصول الى بيانات ومعطيات حساب الطالب، كثرة النشر، المشاركة والردشة عبر مواقع الانترنت، استخدام هوية حقيقية إلى سهولة التعرف على الطالب من طرف المجرمين.

ث. يقع الطالب الجامعي ضحية جرائم السب والشتيم من وجهة نظر الطلبة الجامعيين: بسبب سوء استخدامه لمواقع التواصل وشبكة الانترنت. ويتجلى ذلك من خلال قبول الصداقات دون التأكد من هوية طالبها، التواصل مع الاشخاص المجهولين، استخدام هوية مزيفة.

مع وجود فروق دالة احصائية في الدرجة الكلية لمتغير سبب وقوع الطالب ضحية الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال حسب متغيري درجة التحكم في التكنولوجيات الحديثة ودرجة الوعي بالأمن السيبراني.

خاتمة:

ان التطور العالمي ودخول التقنية الالكترونية والشبكة العالمية قرب المسافات البعيدة وممكن من التواصل في ظل وسائل الاتصال الحديثة هذا ما أدى إلى تمادي المتطفلين والمجرمين وارتكاب جرائم عبر شبكة الانترنت كجرائم النصب والاحتيال ، التشهير والابتزاز، الاعتداء على حرية الحياة الخاصة ، الازعاج التطفل ، القذف السب والشتيم وغيرها ، هذه الاخيرة التي تتعدى آثارها القانونية والشرعية حياة وحقوق افراد المجتمع بجميع مكوناته ولم تسلم منه حتى فئة الطلبة الجامعيين، لذا وجب اعتماد العديد من الإجراءات والتدابير التي ان لم تحد من هذا النوع المستحدث من الجرائم فإنها تساهم في خفض نسبة وقوعها .

توصيات :

1. دورات تكوينية في الامن السيبراني للطلبة الجامعيين لخلق وعي بالأمن السيبراني.
2. حرص الطالب على وضع حماية ضد الفيروسات والتجسس.
3. تحديث أنظمة الحماية المستخدمة وبرامج مكافحة الفيروسات
4. التأكد من العناوين الالكترونية التي تتطلب معلومات سرية "كبطاقات الائتمان" كي لا يقع ضحية النصب والاحتيال
5. عدم الإفصاح عن كلمة السر، مع عدم حفظها في الحاسوب.
6. تجنب حفظ الصور والمعلومات الشخصية في الحاسوب والهاتف الذكي ، مع عدم تنزيل ملفات أو برامج من مصادر غير معروفة.
7. التحلي بثقافة التبليغ ونشرها في الوسط الطلابي ، في حالة وقوع الطالب ضحية الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال
8. تنظيم عمليات توعية وتحسيس مشتركة مع المؤسسات الامنية قصد تعريف الطالب الجامعي بالجرائم الالكترونية وسبل تفاديها .



قائمة المراجع :

1. <https://criminologie-victimo.forumactif.org/t26-17-2009> . (بلا تاريخ).
2. https://emirate2.wiki/wiki/Routine_activity_theory . (بلا تاريخ). نظرية النشاط الروتيني.
4. الأمر رقم 156-66 المتضمن قانون العقوبات. (08 يونيو 1966). قانون العقوبات. الجزائر: الجريدة الرسمية.
5. السعد صالح. (1999). علم المجني عليه، ضحايا الجريمة . عمان: دار الصفا للنشر والتوزيع.
6. صالح السعد. (1999). علم المجني عليه ضحايا الجريمة. عمان: دار الصفاء للنشر والتوزيع.
7. علي جعفر. (2013). جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة - دراسة مقارنة-. بيروت -لبنان : منشورات زين الحقوقية .
8. فاطمة عوض صابر، ميرفت علي خناجة. (2002). اسس ومبادئ البحث العلمي.
9. مجلة الشرطة العلمية والتقنية. (2019). التحقيقات الجنائية في مجال مكافحة الجريمة المعلوماتية. وحدة الطبع روية الجزائر.
10. محمد الامين البشير. (2005). علم الضحايا وتطبيقاته في الدول العربية. الرياض: جامعة نايف للعلوم الامنية الرياض.
10. مورييس انجرس. (2006). منهجية البحث في العلوم الانسانية. (بوزيد صحراوي وآخرون، المترجمون) الجزائر، الجزائر: دار القصة للنشر.

تم استبعاد بندين لعدم تشبعهما على احد العوامل وهما البند 1 و2^أ

البعد القانوني

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني



دور القطب الجزائري في مكافحة الجريمة السيبرانية

د/رمال أمين

جامعة أبي بكر بلقايد تلمسان

مقدمة :

أمام التطور التكنولوجي الحاصل اليوم و الذي ترتب عنه بروز مجتمع رقمي، جعل المجتمعات قرية صغيرة تعبر عن سلوكياتها بأحداث التقنيات في مجال المعلوماتية، سواء على مستوى الدولة أو الأفراد، حيث أصبحت الخدمات العامة اليوم تقدم بسهولة وفي فترة قصيرة نتيجة رقمنة المرافق العامة للدولة، وذلك أمام التحديات التي تواجه الدولة بغرض تعزيز مكانة المواطن من خلال حقه في الحصول على خدمة عمومية راقية، في مقابل ذلك أصبحت الدولة والمجتمع تحت تهديد ما يعرف بالجرائم السيبرانية أو جرائم الفضاء الافتراضي ذات الخطورة العالية، نتيجة الاستعمال السلبي للحاسوب من طرف محترفي الإجرام الإلكتروني بهدف المساس بالأمن المعلوماتي للدولة من خلال تدمير البيانات المعلوماتية وكذا المعطيات واختراق المواقع وتخريبها بالإضافة الى المساس بخصوصيات الأفراد التشهير والقتل عبر مواقع التواصل الاجتماعي، أمام التهديدات السيبرانية المتتالية الذي ترتب عنه انتشار مخيف لهذا النوع من الجرائم إلا أن الدولة تصدت للجرائم السيبرانية من خلال هيئاتها القضائية وهيئات أخرى كالهئية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و لتدعيم هذه الهيئات استحدثت المشرع الجزائري القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك بموجب الأمر 11-21 الأمر رقم 11-21 مؤرخ في 25 أوت 2021، يتم الأمر رقم 66-155، المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، ج ر عدد 65 مؤرخة في 26 أوت 2021، الذي جاء بهدف تعزيز دور الجهات القضائية في مكافحة الجريمة السيبرانية .

و لدراسة الموضوع وتحليله ننتقل من الإشكالية التالية:

ما مدى فعالية القطب الجزائري الوطني في الحد من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال؟

1. مفهوم الجريمة السيبرانية :

تعد الجريمة السيبرانية من أخطر وأعقد الجرائم المستحدثة، نظرا لما ترتبه من آثار سلبية على المحني عليه سواء كانت مؤسسة أو أشخاص، فالجريمة السيبرانية أو الالكترونية تختلف عن الجريمة الكلاسيكية كون أن مرتكبها يتميز بذكاء عال، بالشكل الذي يجعل منه يتحكم في هذه الوسيلة الإجرامية بسهولة ودون اكتشاف أمره، فهو لا يترك أي أثر في الفعل الإجرامي، بخلاف الجريمة الكلاسيكية أين يمكن اكتشاف الجاني وفي غالب الأحيان بسهولة، ويرجع حجم انتشار الجريمة السيبرانية إلى التطور التكنولوجي الهائل اليوم في مجال المعلوماتية حيث أصبحت مؤسسات الدولة و الأفراد في تنافس على استعمال التقنيات الحديثة في ما يعرف بمجتمع المعلومات، هذا المجتمع الذي بات يهدد الأمن المؤسساتي وأمن الأفراد من خلال الجرائم السيبرانية المرتكبة في حقهم، لذا نجد أغلب التشريعات واكبت وسايرت وتصدت لهذا النوع من الجرائم حسب إمكانيات كل دولة بل وصل الأمر إلى إبرام اتفاقيات تعاون بين الدول لمكافحة الجريمة السيبرانية، والمشرع الجزائري كغيره من التشريعات حرص على تجريم الاستعمال المحظور للحاسوب ورتب على ذلك عقوبات لمقتري جرائم الانترنت أو الجرائم الالكترونية، حماية لحق المجتمع في الأمن المعلوماتي وخصوصية الأفراد.



1.1 . تعريف الجريمة الالكترونية:

اختلفت التعريفات الفقهية بشأن الجريمة السيبرانية أو الالكترونية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حسب الزاوية التي ينظر إليه كل فقيه ، و الأمر نفسه بالنسبة للتشريعات التي عادة ما تترك مسألة التعاريف للفقه والقضاء ويقتصر دورها على الإشارة إلى الجرائم الالكترونية دون تعريفها ، كون التعريف ليس من اختصاص المشرع ، هذا من جهة ، من جهة ثانية تتميز الجريمة الالكترونية بخصائص ومميزات تجعلها تختلف عن باقي الجرائم الأخرى ، غير أن الجريمة الالكترونية تتفق مع الجرائم الأخرى من حيث الأركان التي تقوم عليها الجريمة والمتمثل في الركن المادي والمعنوي والشرعي ، وهي أركان تقوم عليها كل الجرائم سواء كانت تقليدية أو حديثة.

2.1. تعريف الجريمة السيبرانية :

لا يوجد هناك اتفاق على مصطلح واحد للدلالة والتعبير عن الجريمة الالكترونية أو السيبرانية ، فهناك من يطلق عليها الجرائم السيبرانية، الجرائم الالكترونية ، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم الكمبيوتر، جرائم المعلوماتية . إن عدم الاستقرار على مصطلح واحد دلالة على اتساع موضوع الجريمة الالكترونية كمجال للدراسة القانونية والاجتماعية، لهذا لم يستقر الفقه على تعريف موحد بل اختلفت التعريفات حسب كل زاوية.

1.2.1. التعريف الفقهي:

يعرفها الفقه بأنها كل نشاط إجرامي يستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي المقصود (حجازي عبد الفتاح ، 2007 : ص 20) .
يرتكز هذا التعريف على الوسيلة المستخدمة في ارتكاب الجريمة و المتمثلة في الحاسب الآلي أو قد يكون الحاسب الآلي هو المستهدف بأن تقع عليه الجريمة.

عرفها الباحث محمد الشوا " بأنها تلك الافعال الاجرامية الناتجة من خلال أو بواسطة استخدام المعلوماتية والتقنية الحديثة المتمثلة في الكمبيوتر أو أي من الوسائل الالكترونية (الشوا محمد سامي ، 1994 : ص 5) .
و هو التعريف الذي يركز على الوسيلة كأداة لارتكاب الجريمة وقد تكون هي الهدف أي المستهدفة.

يعرف عبد الفتاح مراد جرائم الانترنت على أنها " مجموعة الأفعال و الأعمال غير القانونية التي تتم عبر معدات أو أجهزة الكترونية أو شبكة الأنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها (عبد الفتاح مراد ، بدون سنة : ص 40) .

أما بالنسبة للفقه الجزائري أخذ بالتعريف الذي جاء به المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته، حيث عرفها بأنها "كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة اليكترونية " (بولحية شهرزاد ، خلوفي رشيد ، 2019 : ص 1974) .



أكد مؤتمر القانون والانترنت المنعقد في لشبونة عاصمة البرتغال يوم 2001/01/26 على وجوب عدم الاهتمام بالمصطلحات غير الدقيقة للدلالة عن الجرائم الانترنت، واستعمال فقط مصطلح سبير كرائم Cyber crime «» دون غيره من المصطلحات (أبو بكر بن يونس محمد ، 2004 : ص 158) .

2.2.1. التعريف القانوني:

جرت العادة عند القانونيين أن التعاريف من اختصاص الفقه والقضاء ، وبالتالي عادة ما يتجنب المشرع الخوض في التعاريف، غير أن المشرع في الجريمة الالكترونية استعمل مصطلح الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات لتعبير عن الجريمة السيبرانية ، وهذا ما يظهر من خلال القانون 04-09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث جاء في المادة 2 منه " يقصد في مفهوم هذا القانون الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم الماسة بأنظمة المعالجة الآلية للمعطيات..."

استعمل بموجب الأمر 11-21 المؤرخ في 25 أوت 2021، المتضمن قانون الإجراءات الجزائية ، مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية في المادة 211 مكرر 24 . أما المادة 211 مكرر 22 استعمل الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، كل جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال.

3.1. خصوصيات الجريمة السيبرانية :

تتميز الجريمة السيبرانية عن غيرها من الجرائم التقليدية بالعديد من المميزات والخصائص تجعلها تختلف من حيث مرتكبيها و الآثار المترتبة على ارتكابها والوسيلة المستعملة لهذا الغرض، ذلك أن الجرائم السيبرانية جرائم وطنية وعابرة للحدود نظرا لتعدد مرتكبيها .

1.3.1. الجريمة السيبرانية جريمة منظمة عابرة للحدود الوطنية :

نظرا لتغطية الشاملة للشبكة العنكبوتية و الانترنت في كافة دول العالم ،والذي أصبح مجرد مدينة او قرية صغيرة بسبب التطور التكنولوجي في تقنيات المعلوماتية ، إذ أصبح التواصل بين مختلف الدول و الأفراد في العالم بشكل سريع، ما جعل الاتصالات والمعلوماتية تتخطى حدود الدولة ، وبالتالي فإنه من السهل أن ترتكب جريمة في دولة ما ويكون أثرها ومرتكبها في دولة أخرى ، اذ لم تعد الحدود عائقا أمام الجرائم السيبرانية ، ما جعل الدول تعيش حالة من التهديد الذي يجب تأمينه من خلال وضع تشريعات وطنية ودولية لمكافحة الجرائم السيبرانية، وهو ما حصل فعلا من خلال التعاون الدولي بين الدول كاتفاقية بودابست لسنة 2001 المتعلقة بالجريمة الالكترونية، وإن كانت الجرائم السيبرانية العابرة للحدود تثير إشكالية القانون الواجب التطبيق، والجهة القضائية المختصة.

2.3.1. الجريمة السيبرانية صعبة الإثبات :

الجريمة السيبرانية كونها من الجرائم السريعة التنفيذ نظرا لخصوصية مرتكبيها من بين ذوي الذكاء العالي، فانه في حالة ارتكاب الجريمة الالكترونية يقوم الجاني بسرعة إخفاء ومحو آثارها ، بخلاف الجرائم التقليدية أين يترك الجاني آثار مادية من خلالها يتم اكتشاف المجرم، ذلك أن اغلب الجرائم الالكترونية لا يتم الكشف عنها، و ما يتم تداوله لا يمثل إلا القليل من الجرائم الالكترونية

المكتشفة من طرف المختصين، عادة ما تكون متبوعة بالخداع وتدمير البرامج ووضع كلمات سرية ورموز تحول دون الوصول إلى الدليل، كما قد يتم تشفيرها (طالة لامية، سلام كهينة، 2020: ص 75).



3.3.1. أن يكون الجاني مجرم معلوماتي:

تتميز الجريمة السيبرانية كونها جريمة غير عادية، ذلك أن مرتكبها شخص ذو ذكاء حاد ويتميز بقدرته في التحكم في تقنيات الحاسوب بالشكل الذي يسمح له ارتكاب الجريمة بسهولة، وبهذا يكون قادر على حجب واختراق وتدمير أي موقع أو برنامج أو نظام معلوماتي، وينقسم الجرم المعلوماتي الى :

1.3.3.1. الهاكر - المخترقون - :

وهم فئة المجرمين الأقل خطورة، حيث تتوفر لديهم خبرة معتبرة في مجال الحاسوب الآلي ووظائفه ومكوناته ونظم المعلوماتية، ومعرفة البرامج التي يجري العلم بها كالبرامج المحاسبية (يعيش تمام شوقي، 2019، ص 22). ويسمون أيضا بالمخترقون وهم عبارة عن أشخاص متطفلون، غالبا ما يكون ارتكابهم للجرائم بدافع التحدي ودخول الى المواقع لإثبات الذات وهم في الغالب في سن المراهقة.

2.3.3.1. الكراكرز - المخترقون - :

يتميزون بخطورة إجرامية كبيرة مقارنة بالنوع الأول، قد يكون هدفهم الاعتداء لكسب المال وذلك من خلال الدخول إلى البنوك والمؤسسات المالية، وقد يرتكبها الجاني بهدف تحقيق أبعاد سياسية أو طرح فكرة معينة أو توجه معين، أو قد يمس منشآت ومؤسسات أخرى، فهذا النوع من الجرائم يرتكب من طرف محترفي الاجرام الالكتروني، وعادة ما يكون متطرف أو جاسوس أو محترف الانظمة (طالة لامية، سلام كهينة، 2020: ص 73).

4.3.1. جريمة السيبرانية أقل عنفا وجهدا :

تختلف الجريمة السيبرانية عن الجريمة التقليدية، كون الاولى تنفيذها لا يتطلب مجهودات كبيرة بل تحتاج فقط الى مجرم بارع ذكي ومتخصص في المعلوماتية بإمكانه ارتكاب أية جريمة الكترونية في فترة قصيرة جدا وبدون أية جهد أو عناء أو تنقل أو امكانيات كبيرة، فقط يركز على قوة ذكائه وخبرته في مجال المعلوماتية ليستغلها في ارتكاب الجريمة الالكترونية لهذا تسمى بالجريمة الخفيفة المؤمنة.

4.1. أركان الجريمة الالكترونية :

الجريمة السيبرانية كغيرها من الجرائم، لا تقوم إلا بتوافر أركان الجريمة المتفق عليها في الفقه الجنائي والمتمثلة في الركن الشرعي والركن المادي والركن المعنوي.

1.4.1. الركن الشرعي:

يقصد بالركن الشرعي قيام المشرع بتجريم سلوك معين وتحديد العقوبة التي تناسبه من خلال النص على الجريمة في قانون العقوبات، وذلك كله في اطار مبدأ الشرعية الجنائية، ذلك أن الاصل في الأفعال الإباحة، غير أنه إذا أصبح فعلا ما يشكل خطرا على الأمن الاجتماعي، ففي هذه الحالة يتدخل المشرع ويجرمه ويقرر له عقوبة بمقتضى قانون العقوبات، حيث ينص قانون العقوبات في مادته الأولى " لا جريمة و لا تدبير أمن الا بنص قانوني".

وعليه فالركن الشرعي في الجريمة الالكترونية كل فعل إجرامي يعاقب عليه القانون والذي يمس بأنظمة المعالجة الآلية للمعطيات.

2.4.1. الركن المادي:

يقصد بالركن المادي السلوك الذي يأتيه الجاني أو الامتناع عن اتبانه والذي من شأنه أن يحدث ضررا للضحية، فالسلوك الاجرامي في الجريمة الالكترونية يقوم على الفعل المادي والنتيجة والعلاقة السببية.



حيث يتطلب السلوك المادي في الجريمة الالكترونية توفر بيئة رقمية، أو معلوماتية ووسائل الكمبيوتر حيث يكون الجاني على علم بالسلوك الاجرامي من بدايته الى غاية تحقيق النتيجة ، بالنسبة للأعمال التحضيرية في الجريمة السيبرانية التي تسبق السلوك الاجرامي ، كسواء معدات وادوات وأنظمة قصد استعمالها في ارتكاب الجريمة، فالقانون لا يعاقب على الشراء غير ان استعمالها في تنفيذ الجريمة يكون قانون العقوبات له بالمرصاد في حالة استعمالها في اختراق أو تدمير أنظمة معلوماتية، وان كان السلوك المادي في الجريمة الالكترونية يثير تساؤلات كونه يصعب معرفة بداية السلوك ونتيجته، نظرا لسرعة ارتكاب الجريمة الالكترونية ولصعوبة اثباتها بالدليل المادي.

1.3.4.3. الركن المعنوي:

يقصد بالركن المعنوي أو القصد الجنائي، اتجاه ارادة الجاني لارتكاب الجريمة مع وجوب العلم بكافة أركانها القانونية ، ذلك أنه متى تحقق العلم و الإرادة لدى الجاني توفر القصد الجنائي (عبد الله سليمان ، 2005 : ص 249) وعليه تحقق الركن المعنوي في الجريمة السيبرانية ضروري لتحديد السلوك الاجرامي و القانون الواجب التطبيق، ذلك أن عدم توافر الركن المعنوي يؤدي الى قيام جريمة الدخول والخروج غير المشروع فقط، وبالتالي فالركن المعنوي في الجريمة الالكترونية يستلزم أن تتجه ارادة الجاني نحو الدخول الى البيانات أو المعطيات المخزنة في أي حاسوب.

2. صور الجرائم السيبرانية المحددة في قانون العقوبات والقوانين ذات الصلة :

أمام الفراغ القانوني الذي عرفه التشريع الجزائري في مجابهة الجرائم السيبرانية، عمل المشرع الجزائري على وضع نصوص قانونية أكثر صرامة تتعلق بتحديد الجرائم الالكترونية والعقوبات المقررة لها سواء في قانون العقوبات أو القوانين الاخرى ، وذلك بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل لقانون العقوبات المتضمن أحكام المساس بأنظمة المعالجة الآلية للمعطيات بمقتضى القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الامر رقم 66-165، مؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، ج ر عدد 71 مؤرخة في 10 نوفمبر 2004. والقانون 04-09 المؤرخ في 04-09 المؤرخ في 5 أوت 2009 ج ر عدد 47 مؤرخة في 16 أوت 2009 و المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.

1.2. القانون رقم 04-15 المتضمن قانون العقوبات المعدل و المتهتم:

ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات ، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وذلك في المواد من 394 مكرر الى 394 مكرر 7 .

1.1.2. جريمة الدخول و الإبقاء:

تحديد السلوك الاجرامي لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، حيث أقرت المادة عقوبة الحبس من ثلاثة أشهر الى سنة ، وبغرامة مالية من 50000 دج الى 200000 دج وتضاعف العقوبة اذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

أما اذا ترتب على الافعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة(6) أشهر الى سنتين(2) والغرامة من 50000 دج الى 150000 دج .

فالمشرع في نص المادة تحدث عن الدخول أو البقاء في نظام المعلوماتي دون تحقيق النتيجة أى محاولة ارتكاب الجريمة والتي أقر لها عقوبة الجريمة التامة.



2.1.2. الجريمة الماسة بالمنظومة المعلوماتية :

كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها والتي يقصد بها تدمير وتخريب المعطيات، ذلك أن الدخول المعتمد الى أنظمة المعلومات يعد جريمة عمدية يعاقب عليها القانون، في حين لم يعاقب القانون على الدخول عن طريق الخطأ ، (بخوش هشام ، 2017 : ص 98) . ذلك أن فعل الادخال و الازالة والتعديل يترتب عنه التلاعب بالمعطيات التي يتضمنها نظام المعالجة الآلية للمعطيات من خلال زيادة معطيات خاطئة أو تعديل معطيات ومعلومات موجودة من قبل، حيث يعاقب بالحبس من ستة(6) أشهر الى ثلاث سنوات (3) وبغرامة من 500.000 دج الى 2.000.000 دج حسب المادة 394 مكرر 1.

3.1.2. جرائم التصميم أو البحث أو تجميع أو الحيازة أو أنشر المعطيات:

كل من يقوم عمدا أو عن طريق الغش، بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلية عن طريق منظومة معلوماتية، يمكن أن ترتكب بها الجرائم الواردة في هذا القسم.

حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المذكورة في هذا القسم. ويقصد بذلك الفيروسات المعلوماتية، برامج القرصنة التي تستعمل ضد الأنظمة المعلوماتية أو المعطيات المعلوماتية ، حسب المادة 394 مكرر 2 يعاقب بالحبس من شهرين (2) الى ثلاث (3) سنوات وبغرامة من 1.000.000 دج الى 5.000.000 دج .

2.2. الجرائم السيبرانية في ظل القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها :

قصد حماية أكثر لنظام المعلوماتية ، صدر القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها حيث تضمن القانون تسعة عشر (19) مادة، حددت المادة 2 منه الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وهي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

كما تحدثت المادة 2 منه عن المنظومة المعلوماتية والتي يقصد بها أي نظام منفصل أو مجموعة من الانظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آليات للمعطيات تنفيذا لبرنامج معين.

كما حددت المعطيات المعلوماتية الفقرة ج من المادة 2 بأنها "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

كما حدد الفصل الثاني منه الحالات التي تسمح باللجوء الى المراقبة الالكترونية وذلك في المادة 4 منه يمكن القيام بعمليات المراقبة"....في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

3.2. القانون رقم 18-04 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية :

وفق القانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر عدد 27، مؤرخة في 13 ماي 2018 حيث جاء في الفصل الثاني من القسم الثاني تحت عنوان الاتصالات الالكترونية، وذلك في المادة 10 فقرة 3 الامن السيبراني: مجموع الأدوات والسياسات ومفاهيم الامن والآليات الامنية والمبادئ التوجيهية وطرق تسير المخاطر والأعمال التكويني والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية ضد أي حدث من شأنه المساس بتوفير وسلامة وسرية البيانات المخزنة أو المعالجة او المرسلية.



3. اختصاص القطب الجزائري الوطني بالنظر في الجرائم السيبرانية :

استحدثت الامر 11-21 المتعلق بقانون الإجراءات الجزائية القطب الجزائري صاحب الاختصاص الوطني في مكافحة الجرائم السيبرانية، حيث يندرج ذلك ضمن سياسة الدولة في مواجهة الجرائم المنظمة لاسيما الجرائم السيبرانية التي أصبحت تشكل خطرا كبيرا كونها تمس بالأمن العام للدولة بكل أبعاده.

إذ يعد هذا البناء المؤسسي إضافة جديدة الى الهيئات الأخرى المكلفة بمكافحة الجرائم الالكترونية، حيث كاهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المستحدثة بموجب القانون 04-09.

هذا يدل على أن المشرع الجزائري دائما حريص على الوقاية ومكافحة الجرائم السيبرانية ، ويظهر ذلك من خلال التطور المؤسسي للهيئات المختصة بمكافحة الجرائم السيبرانية ، اذ لأول مرة يتم استحداث قطب جزائي يختص بالجرائم السيبرانية ، وبذلك يعد قفزة نوعية في القضاء الجنائي.

1.3.1. الأساس القانوني لاستحداث القطب الجزائري :

أمام تعدد وتنوع الجريمة المنظمة التي تهدد الامن الاجتماعي للدولة ومؤسساتها، نظرا لخطورتها، والتي تعد الجريمة السيبرانية أحد صورها و الأكثر انتشار اليوم بات من الضروري على الدولة الجزائرية لمجابهة الجرائم الالكترونية وبغرض سد النقص الحاصل في الهيئات القضائية التي أصبحت غير قادرة لوحدها معالجة مثل هذا النوع من الجرائم المستحدثة، التي أصبحت تتخطى الحدود الوطنية سواء من حيث مرتكبيها أو من حيث الآثار المترتبة على ارتكابها والخسائر التي تكلف الدولة في هذا الشأن، ونظرا لخصوصياتها وتميزها عن الجريمة التقليدية ، دفع بالمشرع الجزائري الى استحداث قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وذلك لأول مرة في الجزائر. بموجب الامر رقم 11-21 المؤرخ في 25 أوت 2021 المتضمن قانون الاجراءات الجزائية.

1.1.3. الأساس التشريعي لاستحداث القطب الجزائري :

بالعودة الى أحكام الامر رقم 11-21 المتضمن قانون الاجراءات الجزائية والذي نص في المادة 211 مكرر 22 منه على استحداث قطب جزائي بقولها " ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.

كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب اذا كانت تشكل جنحا".

وبهذا يكون المشرع قد أنشأ لأول مرة قطب جزائي يهتم بمعالجة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال نظرا لكونها من الجرائم الأكثر انتشارا وخطورة وتعقيدا ما استلزم تخصيص قطب جزائي لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

كما أكدت على ذلك المادة 32 من قانون الاجراءات الجزائية بقولها " المحكمة هي الجهة القضائية ذات الاختصاص العام وتشكل من أقسام يمكن أيضا أن تتشكل من أقطاب متخصصة"

أما المادة 329 فقرة 5 أكدت على الاختصاص المحلي الذي يتمدد حسب الحالات بقولها " يجوز تمديد الاختصاص المحلي للمحكمة الى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الاموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف " وهذا ما تعزز أكثر من خلال المادة 211 مكرر 23.

2.1.3. دوافع استحداث القطب الجزائري :

يعد القطب الجزائري جهة قضائية تختص بالنظر في الجرائم المذكورة في المادة 211 مكرر 24 ، وبالتالي تم استحداث هذا القطب خصيصا لمواجهة الجريمة المنظمة لاسيما الجرائم السيبرانية، ذلك أنه بات من الضروري استحداث هذا النوع من الهيئات القضائية ،



لمواجهة التهديدات التي تواجه الدولة والمجتمع فيما يخص الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، التي أصبحت تحتل المرتبة الاولى من حيث الجرائم المرتكبة وذلك لسهولة ارتكابها وصعوبة إثباتها لهذا يظهر جليا دوافع وخلفيات استحداث القطب الجزائري الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وذلك من حيث:

- تزايد حجم الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والتي أضحت من الجرائم العابرة للحدود الوطنية بحكم التطور التكنولوجي الهائل في تقنيات المعلوماتية.
- تعقد وصعوبة مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال استدعى استحداث قطب جزائي لمكافحة هذه الجرائم.
- عدم قدرة القضاء الجنائي الغير متخصص في مواجهة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، وبالتالي محاربة الجريمة السيبرانية التي تحتاج لقضاء متخصص ذو خبرة وكفاءة، حتى يتسنى لهم الكشف عن مرتكبي الجريمة من خلال استجواب الجناة ، وبالتالي بات من الضروري الاستناد على قضاء جنائي متخصص في مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.
- ضرورة تجاوز الاختصاص الاقليمي للمحاكم التي تستند عليه في الجرائم التقليدية، والعمل على اعتماد جهات قضائية ذات اختصاص وطني .
- خصوصية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وصعوبتها وتعقدها، جعل من المشرع ينظر اليها من خلال تخصيص جهة قضائية أكثر تطورا ماديا وبشريا للحد من هذه الجرائم، ذلك أن واقع هذه الجرائم حتم على الدولة أن تتدخل بشكل متميز وتفرض سلطتها العقابية من خلال استحداث القطب الجزائري.
- ضرورة التعاون الدولي بين الدول لمكافحة الجرائم السيبرانية دفع المشرع الى استحداث القطب الجزائري الوطني .

3.1.3. مميزات القطب الجزائري الوطني :

يتميز القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال بعدة مميزات تجعله

يختلف عن باقي الاجهزة القضائية من حيث:

- من حيث التسمية: اعتماد مصطلح قطب جزائي بدلا من محكمة جزائية، وبهذا يكون المشرع قد وفق في استعمال مصطلح القطب الجزائري، كون القطب يعتمد على التخصص في إنشائه.
- من حيث التشكيلة: يتشكل القطب الجزائري من تشكيلة جماعية ، وكيل جمهورية وقاضي التحقيق ورئيس ذات القطب.
- من حيث الهيكلة: القطب الجزائري عبارة عن محكمة تنشأ على مستوى مقر مجلس قضاء الجزائر للنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.
- من حيث التخصص: القطب الجزائري الوطني يختص وحده بمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

2.3. الاختصاص الاقليمي والنوعي للقطب الجزائري الوطني في الجرائم السيبرانية :

يمارس القطب الجزائري الوطني اختصاصاته الاقليمي والنوعي وفقا للأمر 21-11 المتضمن قانون الاجراءات الجزائية، حيث منح القانون للقطب الجزائري اختصاص اقليمي موسع يشمل التراب الوطني، وهذا يعود لخصوصية الجريمة السيبرانية وعدم قدرة المحاكم على متابعة هذه الجرائم لتنوعها وكثرتها ، كما حدد القانون للقطب الجزائري اختصاصات حصرية في الجرائم الواردة في المادة 211



مكرر 24. حيث يؤول الاختصاص النظر في الجرائم المذكورة في المادة 211 مكرر 24 الى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

1.2.3. الاختصاص الإقليمي للقطب الجزائري الوطني :

حدد القانون 04-14 الاختصاص المحلي للأقطاب الجزائية كأصل عام وذلك في المواد 40، 37، 329 منه، من خلال هذه المواد تم توسيع الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق والمحكمة الى دائرة اختصاص محاكم أخرى ، وهذا ما تجسد فيما بعد من خلال المرسوم التنفيذي رقم 06-384 المرسوم التنفيذي رقم 06-348 مؤرخ في 05/10/2006 يتضمن تمديد اختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر عدد 63، المعدل بموجب المرسوم التنفيذي رقم 16-267 مؤرخ في 17/10/2016، ج ر رقم 62 والذي حدد هذه المحاكم.

وفي هذا الاطار تنص المادة 329 فقرة 1 من قانون الاجراءات الجزائية " تختص محليا بالنظر في الجنية محكمة محل الجريمة أو محكمة اقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ، ولو كان هذا القبض لسبب آخر" غير أن الفقرة 5 من المادة 329 جاءت باستثناء بقولها " يجوز تمديد الاختصاص المحلي للمحكمة الى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية ، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الاموال و الارهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

حيث تجسد ذلك من خلال المرسوم التنفيذي رقم 06-348 مؤرخ في 05-10-2006 بموجبه تم تحديد أربعة محاكم على المستوى الوطني وتوسيع اختصاصها الاقليمي.

تجدر الاشارة أن الاختصاص الاقليمي للقطب الجزائري يشمل كافة مراحل الدعوى العمومية الى غاية صدور الحكم ليشمل دوائر اختصاص محاكم أخرى موزعة على أربع جهات من الوطن:

- محكمة سيدي محمد
- محكمة قسنطينة
- محكمة وهران
- محكمة ورقلة

وفقا للمواد 3-4-5 من المرسوم التنفيذي رقم 06-348 المذكور اعلاه ، يمتد اختصاص هذه المحاكم الى المجالس القضائية حسب التقسيم الجهوي هذا كله لمواجهة الاجرام المنظم من خلال اختراق الاجرام عن طريق التسرب، والتصنت واعتراض الاتصالات، والتقاط الصور، غير أن معيار الاختصاص الاقليمي التقليدي لا يسري على الجرائم السيبرانية، وذلك ما أكدته المادة 211 مكرر 23 من الامر 11-21 بقولها " يمارس وكيل الجمهورية لدى القطب الجزائري الوطني المختص لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الاقليم الوطني،

وبهذا يكون القطب الجزائري الوطني المختص بمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، يتمتع باختصاص وطني في ممارسة صلاحياته وهذا كاستثناء من القاعدة العامة أن الاختصاص يكون محليا هذا من جهة بالإضافة الى تفرغ القطب الجزائري وحده بالجرائم المستحدثة التي تتميز بالتعقيد والخطورة.



1.1.2.3. حالة انفراد القطب الجزائري باختصاص حصري :

بالعودة الى المادة 211 مكرر 26 من الأمر 11-21 التي منحت الاختصاص الحصري للقطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، المنصوص عليها في المادتين 211 مكرر 24 و 211 مكرر 25 منه.

2.1.2.3. حالة الاختصاص المشترك للقطب الجزائري لمكافحة الجرائم الالكترونية

تنص المادة 211 مكرر 27 من القانون 11-21 دون الاخلال بأحكام المادتين 211 مكرر 24 و 211 مكرر 25 أعلاه، بمارس وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب، اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد 37 و 40 و 329 من هذا القانون. ذلك أن خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات استدعت ضرورة العمل المشترك بين سلطة النيابة والتحقيق ورئيس ذات القطب الجزائري.

3.1.2.3. حالة الاختصاص الوجوبي :

في حالة تزامن اختصاص القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال مع اختصاص القطب الاقتصادي والمالي، في هذه الحالة يؤول الاختصاص وجوبا لهذا الاخير. كذلك الأمر بالنسبة لاقتزان اختصاص القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال مع اختصاص محكمة مقر مجلس قضاء الجزائر.

طبقا للمواد 211 مكرر 16 الى 211 مكرر 21 من الامر رقم 11-21، في هذه الحالة يؤول الاختصاص وجوبا الى محكمة مقر المجلس قضاء الجزائر.

3.3. الاختصاص النوعي للقطب الجزائري :

يتحدد الاختصاص النوعي كقاعدة عامة على اساس نوع الجريمة ومقدار العقوبة المقررة لها حسب المواد 5-27 من قانون العقوبات ، ان كانت جنائية أو جنحة أو مخالفة ، غير أن الاختصاص النوعي للقطب الجزائري يتحدد من خلال الجرائم التي ورد ذكرها على سبيل الحصر في المادة 211 مكرر 22، ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتبطة بها، كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب اذا كانت تشكل جنحا.

أما المادة 211 مكرر 24 من الامر 11-21 نصت " مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وقاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها:

- الجرائم التي تمس بأمن الدولة أو الدفاع الوطني،
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع،
- جرائم نشر وترويج انباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية،
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية،
- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين،
- جرائم التمييز وخطاب الكراهية،



اضافة الى الجرائم المحددة في المادة 211 مكرر 24 المذكورة اعلاه، يختص وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، وكذا قاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال الاكثر تعقيدا والجرائم المتصلة بها، والتي يقصد بها الجريمة التي بالنظر الى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامتها اثارها أو الاضرار المترتبة عليها أو لطابعها المنظم العابر للحدود الوطنية أو لمساسها بالنظام العام والامن العموميين ، حيث تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء الى تعاون قضائي دولي.

4.3. القواعد الخاصة المتعلقة بالمتابعة والتحقيق :

اسند قانون الاجراءات الجزائية مهمة المتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال الى القطب الجزائري، فهو وحده من خلال النيابة العامة وقاضي التحقيق ورئيس ذات القطب متابعة الملف ابتداء من الدعوى العمومية الى غاية صدور الحكم.

1.4.3. اختصاص وكيل الجمهورية :

أوكلت المادة 211 مكرر 25 من قانون الاجراءات الجزائية الى وكيل الجمهورية لدى القطب الجزائري اختصاص النظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، حيث يتولى وكيل الجمهورية لدى الجهات القضائية المختصة اقليميا في حدود اختصاصه ارسال تقارير الخبرة والتحقيق في الجرائم المنصوص عليها في المادة 211 مكرر 24 من الامر 21-11. طبقا لنص المادة 211 مكرر 6 من قانون الاجراءات الجزائية، يتلقى وكيل الجمهورية لدى القطب الجزائري تقارير الخبرة والتحقيق التي قامت بها جهاز الضبطية القضائية في الجرائم المنصوص عليها في المواد من 211 مكرر 24 و 211 مكرر 25 من قانون الاجراءات الجزائية اذا كانت الجريمة تدخل ضمن اختصاص وكيل الجمهورية لدى القطب الجزائري، فانه بإمكانه أن يطلب ملف الاجراءات وذلك بعد أخذ رأى النائب العام لدى مجلس قضاء الجزائر، وفقا للمادة 211 مكرر 7 من قانون الاجراءات الجزائية المعدل بموجب القانون رقم 04-14.

حيث يمكن لوكيل الجمهورية أن يطلب ملف الاجراءات عبر كافة مراحل الدعوى العمومية حسب المادة 211 مكرر 8 منه. في حالة التماس وكيل الجمهورية لدى القطب الجزائري بالمطالبة بملف الاجراءات ، فانه لوكيل الجمهورية المختص اقليميا أن يصدر مقرر بالتخلي لصالح الاول، وذلك خلال مرحلتي التحريات الاولى والمتابعة حسب المادة 211 مكرر 9 من قانون الاجراءات الجزائية. غير أنه اذا تبين لوكيل الجمهورية أن الوقائع المبلغ عنها لا تدخل ضمن اختصاصه فانه، يصدر مقرر بالتخلي لصالح وكيل الجمهورية المختص اقليميا حسب المادة 211 مكرر 20 منه. تم اخطار القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ب72 ملف خلال سنة 2020-2021.

2.4.3. اختصاص قاضي تحقيق :

حسب المادة 211 مكرر 10 من قانون الاجراءات الجزائية ، في حالة فتح تحقيق قضائي تحال التماسات وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المتضمنة المطالبة بملف الاجراءات من قبل وكيل الجمهورية، وفي هذه الحالة يصدر قاضي التحقيق أمرا بالتخلي لصالح قاضي التحقيق لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال.



حسب المادة 211 مكرر 13 من قانون الاجراءات الجزائية ، ولتحقيق الضمانات اللازمة ، فان اوامر القبض واوامر الوضع رهن الحبس المؤقت الصادرة تبقى منتجة لآثارها الى غاية صدور أمر مخالف عن قاضي التحقيق بالقطب الجزائري الذي يتولى ضمان صحة الاجراءات .

خاتمة:

ختاما لموضوع الدراسة ، تظهر الجريمة السيبرانية من أخطر وأعقد و أكثر الجرائم انتشارا، نظرا لخصوصيتها و خبرة مرتكبي هذه الجرائم بتكنولوجيات الاعلام و الاتصال ، بالإضافة الى تعديها الحدود الوطنية بات من الضروري على الدولة وضع الأطر التشريعية والمؤسسية للحد أو التقليل من هذه الجرائم ، وهو ما يتطلب تكاثف الجهود الوطنية من خلال التنسيق بين مختلف أجهزة الدولة القضائية و الأمنية ، بالإضافة الى الجهود الدولية بغرض التعاون بين الدول سواء في مجال التكوين أو مكافحة الجريمة، ولقد تجسد فعلا من خلال استحداث المشرع لقطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال كجهاز يدعم المحاكم العادية والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في مكافحة الجريمة السيبرانية. يظهر جليا، أن الجريمة السيبرانية جريمة معقدة وخطيرة وسريعة التنفيذ وصعبة اثبات ، بالإضافة الى أنها من الجرائم العابرة للحدود الوطنية ، فهي تتميز بخصوصيات تختلف عن الجرائم التقليدية حيث وصل الامر الى عدم وضع تعريف موحد لها، وقصد مكافحتها سخرت الدولة امكانيات مادية وبشرية لذلك كونها تمس بالنظام العام للدولة وبالحياة الخاصة للأفراد، لهذا عمد المشرع الى تشديد العقوبة لمرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، هذا ما يظهر من خلال تعديلات قانون العقوبات ، هذا من جهة، من جانب آخر عمل المشرع على انشاء القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، كقطب متخصص في الجريمة السيبرانية، حيث منحه المشرع اختصاص وطني لمجابهة هذه الجرائم، كما أن تشكيلته جماعية من وكيل جمهورية وقاضي التحقيق ورئيس ذات القطب ، . ومن أهم التوصيات التي نقدمها في هذا الموضوع:

- ضرورة استحداث أقطاب جزائية جهوية لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، نظرا لسرعة انتشار هذه الجرائم.
- توسيع تشكيلة أعضاء القطب الجزائري الوطني ، اذ يعد هذا الاخير وحده غير قادر على مجابهة الجريمة الالكترونية من خلال هذه التشكيلة، وذلك عن طريق ادراج خبراء في المعلوماتية في تشكيلة المحكمة بصفتهم مساعدين للقضاء.
- ضرورة انشاء هياكل مستقلة للقطب الجزائري الوطني المتخصص، بدلا من الاكتفاء بمحكمة مقر المجلس.
- التكوين الجيد للقضاة في مجال المعلوماتية لتأهيلهم لمعالجة القضايا بسهولة .
- ضرورة نشر الوعي السيبراني من خلال القيام بملتقيات وأيام دراسية لفائدة الطلبة من تأطير وتنظيم القطب الجزائري.
- تحديد مجال أولوية تدخل القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال مع القطب الجزائري المالي والاقتصادي في الجرائم المالية والاقتصادية المرتكبة عبر الكمبيوتر.

قائمة المصادر و المراجع:

- 1- حجازي بيومي عبد الفتاح، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي : دراسة قانونية معمقة في القانون المعلوماتي، دار الكتب القانونية، دار شتات للنشر والبرمجيات ،مصر، سنة 2007.
- 2- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994.
- 3- عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، بدون دار النشر، بدون سنة النشر.



- 4- بولحية شهرزاد، خلوفي رشيد، تحديات الجريمة الالكترونية في الجزائر، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 02، السنة 2019.
- 5- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، الاحكام الموضوعية والجوانب الاجرائية، الطبعة الاولى، دار النهضة العربية، القاهرة ، 2004.
- 6- لامية طالة، كهينة سلام، الجريمة الالكترونية، بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والانسانية، المجلد 6، العدد 02، سنة 2020.
- 7- يعيش تمام شوقي، الجريمة المعلوماتية، دراسة تأصيلية مقارنة، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة ، الطبعة الأولى ، 2019.
- 8- عبد الله سليمان، شرح قانون العقوبات الجزائري، الجريمة، القسم العام، ديوان المطبوعات الجامعية، الجزائر، سنة 2005.
- 9- بخوش هشام ، الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في ظل التشريع الجزائري، مجلة الحقوق والعلوم السياسية ، جامعة خنشلة، العدد 07 ، جانفي 2017.

النصوص القانونية:

- الأمر رقم 21-11 مؤرخ في 25 أوت 2021، يتم الأمر رقم 66-155، المؤرخ في 8 يونيو 1966 والمتضمن قانون الاجراءات الجزائية، ج ر عدد 65 مؤرخة في 26 أوت 2021.
- القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتم الامر رقم 66-165، مؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، ج ر عدد 71 مؤرخة في 10 نوفمبر 2004.
- القانون رقم 09-04 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ج ر عدد 47 مؤرخة في 16 أوت 2009.
- القانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر عدد 27، مؤرخة في 13 ماي 2018.
- المرسوم التنفيذي رقم 06-348 مؤرخ في 05/10/2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر عدد 63، المعدل بموجب المرسوم التنفيذي رقم 16-267 مؤرخ في 17/10/2016، ج ر عدد 62.

المواقع الإلكترونية

<https://elmaghrebelwassat.dz>

تاريخ زيارة الموقع: 02 فيفري 2021 توقيت الساعة العاشرة ونصف



الجهود الدولية لمكافحة الجريمة الالكترونية

د. بن عائشة نبيلة

كلية الحقوق جامعة المدينة

د. القيني بن يوسف

كلية الحقوق جامعة المدينة

مقدمة

استعمل المشرع في الجريمة الالكترونية مصطلح الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات لتعبير عن الجريمة السيبرانية، وهذا ما يظهر من خلال القانون 04-09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها حيث جاء في المادة 2 منه " يقصد في مفهوم هذا القانون الجرائم المتصلة بتكنولوجيات الاعلام والاتصال : جرائم الماسة بأنظمة المعالجة الآلية للمعطيات..."

واستعمل بموجب الأمر 11-21 المؤرخ في 25 أوت 2021، المتضمن قانون الاجراءات الجزائية، مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية في المادة 211 مكرر 24 .

أما المادة 211 مكرر 22 استعمل الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، كل جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الاعلام والاتصال.

وعليه تطرح الاشكالية التالية : ما مفهوم الجريمة الالكترونية ومدى معالجتها ومكافحتها دوليا ووطنيا ؟.

1. مفهوم الجريمة الإلكترونية:

لقد أدى ظهور شبكات الإعلام الآلي والانترنت وانتشارها إلى العمل على تعزيز التواصل الاجتماعي والثقافي والحضاري، وإلى كسر الحواجز والحدود الجغرافية بين الأمم، إلا أنها من جانب الآخر ساعدت على انتشار الجريمة بمختلف أشكالها، حتى أصبحت تسمى بعوالة الجريمة الإلكترونية. (غريب، ص73)

1.1. تعريف الجريمة الإلكترونية:

أمام تعدد الآراء بشأن مفهوم الجريمة الإلكترونية، تبنى كل رأي مفهومًا مرتبطًا بالزاوية التي ينظر من خلالها إلى الموضوع، فهناك جانب من المختصين عرفها من زاوية تقنية، وأخرى قانونية، وهناك من عرفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استنادا لمعايير أخرى حسب القائلين بها. وهذا ما أعاق منظمة الأمم المتحدة إلى عدم التوصل لتعريف متفق عليه دولية، ولكن ورغم صعوبة إيجاد تعريف لهذه الظاهرة وحصرها في نطاق محدود وضيق، إلا أن مكتب تقييم التقنية في الولايات المتحدة عرفها من خلال تعريف جهاز الكمبيوتر بأنها: تمثل "الجرائم التي تقوم فيها بيانات الكمبيوتر والبرامج المعلوماتية بدور رئيسي"، كما أنه عرفها ب: "نشاط جنائي يمثل اعتداء على برامج وبيانات الحاسب الإلكتروني"، وأيضا بأنها: "كل استخدام في صورة فعل أو إمتناع غير مشروع للتقنية المعلوماتية ويهدف إلى الإعتداء على أية مصلحة مشرعة، سواء أكانت مادية أو معنوية. ورغم الفارق بين مجالات جرائم أجهزة الكمبيوتر وشبكات الإنترنت، فبينما تتم الأولى بالإعتداء على مجموعة الأدوات المكونة للكمبيوتر وبرامجه والمعلومات المخزنة به، فإن الثانية تتعلق بجرائم شبكات الإنترنت التي تتم عبر نقل المعلومات والبيانات بين أجهزة الكمبيوتر وخطوط الهاتف. إلا أن الواقع التكنولوجي أدى إلى تزاوج بين المجالين (الكمبيوتر والإنترنت) وظهور مصطلح الجريمة الإلكترونية .



وفي الواقع، فإن هذه الجريمة التي يكون الهدف منها الوصول إلى المعلومات هي في الأغلب تصنف ضمن حالات الجرائم الاقتصادية، وتكون بغرض الحصول على مزايا أو مكاسب اقتصادية، لأن الحرب الاقتصادية لا تقل ضرورتها وخطرها الحالية عن الحروب العسكرية، إلا أنها تتحقق عبر شبكات الإنترنت.

والظاهر أن كل الدراسات والنظريات الخاصة بالجريمة الإلكترونية تلتقي عند نقطة مركزية، تنحصر عموما في الغاية المادية البحتة التي يسعى إلى إنجازها هؤلاء المجرمين، بواسطة الإعتداء على البيانات والمعلومات السرية، وتدمير البرامج المعلوماتية لأية دولة لتهديدها وضرب أمنها الوطني، وخلق حالة من الفوضى الإلكترونية والمعلوماتية في مؤسساتها الحساسة، ولعل خير مثال على ذلك اقتحام موقع البنتاغون الأمريكي، لتعود في صورة جديدة على شاكلة ما يعرف بالإرهاب الإلكتروني الذي بات خطرا حقيقيا يهدد سلامة وأمن المجتمع الدولي، عن طريق التهديد بنسف المعلومات وتدمير استراتيجية الدفاعات الاقتصادية والأمنية للبدان وعوائلها المالية، باستعمال أنواع الفيروسات المدمرة والخطط التخريبية لتدمير العديد من البرامج المعلوماتية الحساسة للدول. (حكيم غريب : المرجع السابق ، ص 74).

وعليه من خلال ما تقدم تعتبر هذه الجريمة التي ترتكب من تنظيم إجرامي هيكلي يتكون من ثلاثة اشخاص فاكتر ، تحكمه قواعد معينة اهمها قاعدة السرية ، ويعمل بشكل منتظم ، وبشكل مستمر لفترة غير محددة، ويعبر نشاطه حدود الدول، ويستخدم العنف و الفساد و الابتزاز و الرشوة في تحقيق اهدافه للحصول على الربح المادي. (سلمى سبع، ص 759).

جرت العادة عند القانونيين أن التعاريف من اختصاص الفقه والقضاء ، وبالتالي عادة ما يتجنب المشرع الخوض في التعاريف، غير أن المشرع في الجريمة الالكترونية استعمل مصطلح الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات لتعبير عن الجريمة السيبرانية، وهذا ما يظهر من خلال القانون 04-09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها (القانون 04-09 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال ومكافحتها، الجريدة الرسمية الصادرة بتاريخ 16 اوت 2009 ، العدد 47). حيث جاء في المادة 2 منه " يقصد في مفهوم هذا القانون الجرائم المتصلة بتكنولوجيات الاعلام والاتصال : جرائم الماسة بأنظمة المعالجة الآلية للمعطيات..."

استعمل بموجب الأمر 21-11 المؤرخ في 25 أوت 2021، المتضمن قانون الاجراءات الجزائية، مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية في المادة 211 مكرر 24. (الامر 21-11 المؤرخ في 25 اوت 2021، المتمم بالامر 66-155 المؤرخ في 08 جويلية 1966 المتضمن قانون الاجراءات الجزائية).

أما المادة 211 مكرر 22 استعمل الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، كل جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الاعلام والاتصال.

2.1. خصائص الجرائم الإلكترونية:

إن أهم ما تتصف به هذه الجرائم الإلكترونية سهولة إرتكابها بعيدا عن الرقابة الأمنية، وصعوبة التحكم في تحديد حجم الضرر الناتج عنها قياسا بالجرائم التقليدية، وأن مرتكبيها هم من بين فئات مختلفة تجعل من التنبؤ بالمشتبه بهم أمر في غاية الصعوبة وتنطوي على سلوكيات غير مؤلفة عن الأفراد، وسهولة إئتلاف من قبل الجناة، بالإضافة إلى كونها جريمة عابرة للحدود لا تعترف لا بمكان ولا بالزمان، فهي تتصف بالتباعد الجغرافي بين الجاني والمجني عليه، أما مرتكبيها فهم المحترفون Crachers والقراصنة Hackers، وكذا المخادعون Freudians، وأهم ميزات مرتكبي هذه النوعية من الجرائم هم أشخاص ذوو مهارات فنية عالية متخصصون في الإجرام الإلكتروني وأشخاص قادرين على إستعمال خبراتهم في الإختراقات وتغيير المعلومات.



وفي هذا الإطار، يدرك القراصنة إن الدافع لإرتكاب الجرائم الإلكترونية يغلب عليه الرغبة في قهر النظام، أكثر من شهوة الحصول على الربح، حيث يميل أغلبهم إلى إظهار تفوقهم ومستوى إرتقاء براعتهم وذكائهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة يحاولون بوساطة إيجاد الوسيلة التي تمكنهم من تحطيمها، بل والتفوق عليها).

ولقد تعددت الدراسات التي تتحدث عن سمات مرتكبي الجرائم الإلكترونية وشخصيتهم، ومدى جسامة جرمهم كأساس لتبرير وتقدير العقوبة التي يستحقونها، فنجد أن هناك سمات مشتركة بين هؤلاء المجرمين، أهمها ذلك المجرم المتخصص الذي له قدرة فائقة في المهارة التقنية، ويستغل مداركه ومهاراته في إختراق الشبكات، وإختراق كلمات المرور أو الشفقات، ويسبح في عالم الشبكات ليحصل على كل غايي وثمين من البيانات والمعلومات المتوفرة على أجهزة الكمبيوتر، وهناك أنموذج آخر من المجرمين وهو المجرم العائد للإجرام، حيث يتصف بأنه عائد للجريمة، فهو يوظف مهاراته في كيفية عمل أجهزة الكمبيوتر، وكيفية تخزين المعلومات والبيانات، والتحكم في أنظمة الشبكات والدخول المتكرر وغير المصرح به، فهو قد لا يحقق جريمة الإختراق بمهدف الإيذاء وإنما نتيجة شعور بقدرته ومهاراته في الإختراق، إضافة إلى صنف آخر وهو المجرم المحترف، والذي له من القدرات والمهارات التقنية ما يؤهله لأن يوظفها في الإختراق والسرقة والنصب، والإعتداء على حقوق الملكية الفكرية، وغيرها من الجرائم مقابل المال، أما المجرم الذكي، حيث يمتلك من المهارات ما يؤهله أن يقوم بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع جرائمه من خلال أجهزة الكمبيوتر.

ومن جانب آخر أكدت بعض الدراسات والأبحاث الأكاديمية على أن فئات المجرمين في عالم الجريمة الإلكترونية تنحدر من:

- 1 - مستخدموا كمبيوتر البيت.
 - 2- الموظفون الحكوميون الساخطون على مدرائهم ومسؤوليهم.
 - 3- المتسللون، ومنهم الهواة أو العابثون بقصد التسلية.
 - 4- المحترفون الذين يتسللون إلى مواقع مختارة بعناية، ويعبثون أو يتلفون النظام، أو يسرقون محتوياته، وتقع أغلب جرائم الإنترنت حالية تحت طائلة الأعمال الإرهابية.
 - 5- العاملون في الجريمة المنظمة.
- ولقد بات الإرهاب الإلكتروني Cyber Terrorism الذي يهدد البنية التحتية للمجتمعات الحديثة من خلال إستخدام التقنيات العالية والمعقدة في الهجمات ضد المؤسسات الحكومية والشركات الاقتصادية أداة في إمكان التنظيمات الإرهابية إستخدامه عبر شبكة الإنترنت وذلك من خلال توسيع أنشطتها الإرهابية في التجنيد والتوجيه، أو التمويل والتغلب على الإجراءات الأمنية والقضائية، والسماح لبعض الأشخاص والهيئات المطلوبة أمنية وقضائية في العديد من البلدان والمدرجون على قوائم الإرهابيين من إدارة المواقع على شبكات الإنترنت.

وبعد الإرهاب الإلكتروني نمطا جديدة من الإرهاب الذي لا يعتمد على إستخدام الأسلحة وإنما عبر توظيف الإرهابيين للأنظمة المعلوماتية للإعلام الآلي ضد الأنظمة المدنية والعسكرية، وهو ما يؤدي إلى تهديد الأمن الوطني والدولي على حد سواء، وخير دليل على ذلك إختراق ما يسمى بتنظيم داعش في الآونة الأخيرة مواقع شبكة "تي في 5 موند" وتعطيل شبكات القناة لمدة يوم كامل، والسؤال الذي يطرحه الكثيرون هو كيف يمكن ربط شبكة البث التلفزيوني بشبكة المعلوماتية العادية للشبكة، والتي يسهل النفاذ إليها؟ إلى حد أن الهجوم قد نجح بصورة كبيرة على المستوى الإعلامي في تلميع صورة التنظيم، كما نجح الهجوم الإلكتروني على المستوى التقني في شل قناة تلفزيونية، وهي سابقة خطيرة، ولإن الهدف الرئيسي للإرهابيين في السيطرة على القناة، يكمن في مقدرتهم على بث أفلام تنظيم "داعش" الدعائية. (حكيم غريب ، ص 74).



3.1. مظاهر تحديات الجريمة الإلكترونية:

ترتب على ظاهرة الجريمة الإلكترونية رهانات وتحديات عديدة، ومن أفدحها تنامي الأنشطة الإجرامية الإلكترونية، وتوصل مرتكبوها بتقنيات عالية التكنولوجيا غير مسبقة، في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم القيام بهذه الأعمال الإجرامية والإرهابية، داخل حدود الدولة وخارجها، وهو الأمر الذي أدى إلى دق ناقوس الخطر لدى المنظمات والمؤسسات الدولية والبحث عن الآليات والتدابير لمكافحة هذه الظاهرة، ودعوة المجتمع الدولي إلى التصدي لها ومجابهتها.

وعلى خلفية ما ذهب إليه البعض من أن القوانين القائمة تكفي في حد ذاتها لمواجهة الجرائم الإلكترونية، فالواقع إن كان لهذا الرأي شيئا من الواقعية، أن معظم النصوص الموجودة تواجه بعض الأنشطة المجرمة التي ترتكب عن طريق الإنترنت، فإنه ينبغي ألا ننكر أن هناك نصوص قانونية لم تعد تتماشى مع تطور الجريمة الإلكترونية، وظهور الإرهاب الإلكتروني كمبدأ الشرعية الجرائم المستحدثة والعقوبات والتفسير الضيق والمحدود لأبعادها.

فلقد إستغلت العديد من التنظيمات الإرهابية الطبيعة الإتصالية لشبكة الإنترنت من أجل نشر أفكارها ومعتقداتها، بل تعداه الأمر إلى ممارسات تهدد أمن الدول الذي أخذ منحى خطيرا في إستخدام الإنترنت في إرتكاب جرائم غاية في الفتك في حق المجتمعات، وبث ثقافة الإرهاب عبر الإنترنت عن طريق تصميم مواقع إفتراضية تمثل الجماعات الإرهابية، وهي مواقع أخذت في تنامي وارتفاع مع زيادة عدد الجماعات الإرهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى العمليات الإرهابية التي تم إرتكابها بها، ويبقى خير مثال في إستخدام الإنترنت بصورة مؤثرة وعالية الدقة في تصوير الجرائم المتوحشة والخطيرة، هو تنظيم داعش، فقد إستطاع هذه التنظيم من خلال الإنترنت تجنيد المقاتلين الأجانب، وهم في أغليبتهم من فئة الشباب ضعاف العقيدة والفكر، فتعلن الجماعات الإرهابية عبر مواقعها على الإنترنت عن حاجتها إلى عناصر إنتحارية، كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب الديني، ف دائما ما تصف الأهداف التي تستهدف عملياتهم بالكافرة، وتقوم بدعوة الشباب إلى الجهاد وحثهم على الإستشهاد في سبيل الله، والفوز بالجنة.

للإشارة، أنه إذا كانت الجماعات الإرهابية تعمل إلى الدعاية والترويج لنفسها عن طريق آليات مختلفة، منها جذب إنتباه وسائل الإعلام المعروفة لتغطية أخبارها وجرائمها، كل ذلك يمثل قيودا على إفادة التنظيمات الإرهابية من نشر وسائل الإعلام عنها، بينما في المقابل تتيح المواقع الإلكترونية للتنظيمات الإرهابية قدرة كبيرة من التحكم في نظام المعلومات، ونشر رسائلها الإعلامية التي تود ترويجها، بل أيضا تتيح لها المرونة في توجيه الرسائل لفئات مختلفة من الجمهور المستهدف، ورسم صورة ذهنية عن الجماعة وعن أعدائها أيضا.

وتستعمل الجماعات الإرهابية - الإنترنت إلى جانب أغراض الدعاية والترويج. في نشر معلومات مضللة أو مغلوطة، ونشر تهديدات وصور ولقطات فيديو مرعبة. وبناء على مميزات الشبكة العالمية للإنترنت التي منحت للجماعات الإرهابية الكثير من المساحات الحرة والخيارات من خلال عدم خضوعها لأي رقابة، وعبرها للحدود الجغرافية بين الدول، ونموها السريع المتواصل، مع ما تمنحه من القدرة للجماعات الإرهابية في التخفي وعدم المواجهة نتيجة للإفتراضية التي تعد من أهم خصائص هذه الشبكة التي باتت من أهم مقومات المجتمع المعلوماتي التي تؤدي إلى الانحراف الفكري، من خلال تعرض فئات الشباب الى الكثير من المؤثرات الفكرية و الإيديولوجية.

2. الجهود الدولية و الوطنية في مكافحة هذه الجريمة:

عملت المجتمعات والدول عبر فترات متلاحقة في سن تشريعات ونصوص من أجل مكافحة الجريمة الإلكترونية، إلا أن هناك صعوبات كثيرة تواجه التعاون الدولي، لاسيما فيما يخص عدم وجود نموذج موحد للنشاط الإجرامي، الأمر الذي يقتضي توحيد



هذه النظم القانونية، ولإستحالة ذلك فإنه لا مناص من البحث عن وسائل متعددة تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع الجديد من الجرائم، ويخفف من كثرة الفوارق بين الأنظمة القانونية والأمنية بين الدول، وتمثل هذه الوسيلة في تحديث التشريعات الوطنية المعنية بالجرائم الإلكترونية، وعقد إتفاقيات متعددة الأطراف وثنائية، يراعى فيها هذه النوع من الجرائم، إضافة إلى أن وجود الصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من الفوارق وأوجه الاختلاف بين الأنظمة القانونية والإجرائية، ويفتح المجال أمام تعاون دولي فعال، فمثلا المادة (20) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، تشير في هذا النطاق إلى التسليم المراقب والمراقبة الإلكترونية وغيرها، من أشكال المراقبة والعمليات المخفية، والتي تعد من أهم التقنيات المستخدمة في التصدي للتنظيمات الإجرامية المنظمة، وذلك بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات، لاستخدامها فيما بعد في المتابعات القضائية الوطنية منها أو الدولية، في دول أطراف في سياق نظم المساعدة القانونية المتبادلة وهذا ما أكدت عليه الإتفاقية الأوروبية للإجرام الإلكتروني، حيث نصت المادة (29) على سرية حفظ البيانات المعلوماتية المخزنة، وأجازت لكل طرف أن يطلب الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك، كما نجد في النص الثاني من المادة (27) من الإتفاقية الأوروبية بشأن الإجرام الإلكتروني، التي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة الإتصال التي تعمل لمدة 24 ساعة يوميا، طوال أيام الأسبوع، لكي تؤمن المساعدة المباشرة التحقيقات المتعلقة بجرائم البيانات والشبكات، هذا بالإضافة إلى القيام ببعض العمليات المشتركة بين الدول، في مجال تدريب مختصين في هذا المجال الواسع.

ولأجل ذلك كان لا بد أن تكون هذه الأجهزة على درجة كبيرة من الكفاءة والمعرفة، والقدرة على كشف غموض هذه العمليات الإجرامية التي قد تمس بكيان الدولة، والقبض على مرتكبيها بسرعة ودقة متناهيين، وهذا لا يتحقق إلا بالتدريب، لأن المواجهة والتصدي لها لا بد أن تركز على كيفية تطوير أساليب العمل والتكوين والتأهيل وكسب الخبرات في إطار التعاون الدولي المكثف والفعال، وليس هذا فحسب، بل يجب على السلطات الأمنية أن تعمل إلى استقطاب المتخصصين والكفاءات في المجال الإلكتروني والمعلوماتي وضمهم إلى مصالحهما. (حكيم غريب ، ص 78).

1.2. التعاون الأمني على المستوى الدولي:

تستدعي عملية الإستمرار في محاربة هذه الظاهرة المتعددة الأوجه والمخاطر تظافر جميع الدول المساهمة فيها إلى توفير قدر من الأمن والنظام، ولاسيما وأن الواقع العملي قد ظهر أن الدولة لا تستطيع بمجهودها المنفردة القضاء على الجريمة بكل أشكالها، في ظل التطور المذهل في كافة مجالات الحياة، خاصة في ميدان الإتصالات وتكنولوجيا المعلومات وظهور الإنترنت، ولإن الإنتشار الكبير والسريع لها قد أدى إلى ظهور أشكال وصور جديدة من الجرائم الإلكترونية، التي أصبحت خطرا على سرية النظم الحاسوبية، بل تعدت إلى أمن البنى الأساسية والإستراتيجية للدول، نظرا لتمييزها بطابع العالمية، وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الأمني، حيث يسمح بالإتصال المباشر بين مختلف مصالح الأمن في الدول، وذلك بتأسيس مكاتب متخصصة لجمع المعلومات عن مرتكبي هذه الجرائم وتعميمها، ثم التبادل المعلوماتي بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من العقاب.

وعلى الرغم من أن التعاون الدولي بكافة صوره في عالم مزدحم بشبكات إتصالية حساسة ومتطورة تنقل المعلومات والبيانات من مناطق متباعدة بإستخدام التقنيات، إلا أن لا تكفل لها أمنا فعالا، ويتاح في ظلها التلاعب - عبر الحدود - بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أضرارا خطيرة، خاصة في ظل عدم وجود نموذج موحد للنشاط الإجرامي.



2. الجرائم الإلكترونية والمشرع الجزائري:

لقد عمل المشرع الجزائري على مواكبة مختلف التطورات التشريعية التي تم سنّها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الإلكترونية، بما فيها شبكة الإنترنت، تلك خاصة التي تسعى إلى الحد من الإستخدام غير المشروع لها، وذلك مراعاة منه لما يشهده العالم من تطورات حديثة في مجال تكنولوجيا الاتصالات والمعلومات، وكذلك إيماناً منه أن السلطات الجزائرية ليست بمعزل عن التهديدات الأمنية الجديدة في الفضاء الافتراضي، وقد تطرق المشرع الجزائري إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين أهمها (الأمر 03-06 المؤرخ في 19 جويلية 2003)، والمتعلق بالعلامات التجارية، لذلك نجد أن أصحاب البرنامج عمدوا إلى تسجيل هذا الإسم كعلامة تجارية للبرنامج، وذلك لما يتضمنه هذا النوع من أهمية في الحماية. (الأمر 03-06 الجريدة الرسمية العدد 44).

ولقد تدارك المشرع الجزائري خلال الأعوام الأخيرة، ولو نسبية، الفراغ القانوني في مجال الإجرام الإلكتروني، خصوصا بموجب القانون 04-15 المتضمن تعديل قانون العقوبات، (القانون 04-15 قانون العقوبات). الذي بموجبه جرم جريمة التوصل أو الدخول غير المصرح به، وجريمة التزوير المعلوماتي وجريمة الإستلاء على المعطيات المخزنة أو المعالجة عن طريق منظمة معلوماتية، إضافة إلى جريمة إتلاف وتدمير المعطيات.

وبالمحصلة، فإن المشرع الجزائري رغم تداركه لهذا الفراغ القانوني في مجال الإجرام المعلوماتي، والجهود المبذولة للحد من هذه الظاهرة، سواء كانت من طرف السلطات الأمنية أو الضبطية القضائية، إلا أن هذه الجهود تصطدم بعدة صعوبات منها التي تظهر من خلال لا مادية الجريمة الإلكترونية، وصعوبة إكتشاف وإثبات الجريمة الإلكترونية يقودنا إلى صعوبة إثباتها، لأن المجرمين يسعون بشتى الوسائل لكي لا يتركوا ورائهم آثارا تدل على ارتكابهم للجريمة، وتكمن الصعوبة في نطاق الجرائم المرتكبة عبر الإنترنت في ظل لا ماديتها، وهو الأمر الذي يجعل إسناد الفعل غير المشروع إلى المجرم شبه مستحيل وتبقى الجريمة الإلكترونية من أهم الجرائم المستحدثة لا تصل إلى علم الجهات الأمنية والقضائية بطريقة إعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية لا تخلف آثار مادية، كتلك التي تخلفها الجريمة العادية.

إن العديد من الجرائم المرتكبة عبر الشبكة العنكبوتية تتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية، كجرائم التجسس العسكري والإقتصادي وجرائم الإختلاس، التي تتم عبر تعديل البرامج.

والتلاعب بالأنظمة المعلوماتية، فالجناة يعمدون عادة إلى إخفاء جرائمهم، وبوساطة إزالة آثارها عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الحاسوب الآلي والبرامج، ودون ترك أثر، سيما في ظل تطور الوسائل الإلكترونية الحديثة، المعززة بأنظمة متطورة يستغلونها الجناة الأذكياء في ضرب حزام أمني على جرائمهم قبل إرتكابها، لكي لا يقعوا تحت طائلة العقاب، وفي هذا المجال حذرت المصالح الأمنية من إرتفاع الجرائم الإلكترونية في الجزائر، حيث إرتفعت من 153 جريمة إلكترونية سنة 2011م، إلى 175 جريمة سنة 2012م، أغلبها تتعلق بالمساس بالحياة الخاصة للأشخاص، على غرار التهديد والتشهير ونشر صور غير لائقة مخلة والنصب والإحتيال، فضلا عن إستغلال العديد من المواقع من طرف الجماعات الإرهابية. (حكيم غريب : المرجع السابق، ص 79).

خاتمة:

يتجلى لنا من خلال هذه الدراسة للجريمة الإلكترونية و التي لم يتفق فيها الفقه الجنائي على تسمية موحدة فأحيانا يطلق عليها تسمية: "الجريمة السيبرانية" و "الجريمة المعلوماتية" و "الجريمة اإساءة استخدام تكنولوجيايات الاعلام و الاتصال" و "جريمة الكمبيوتر و الانترنت"....، ولأنها من أعقد وأخطر الجرائم التي عرفها العالم المعاصر، وذلك لما تتصف به من تحديات وصعوبات في محاربتها



ومحاصرتها، في ظل ثورة الإتصالات المتسارعة والتقدم المتواصل في تكنولوجيا الحاسوب الآلي، والإنترنت يفرض على الجهات المعنية أن تسير في خطوات متناسقة مع التطورات السريعة، التي تشهدها هذه التكنولوجيات والإلمام بها، حتى يمكن التصدي لهذه الجرائم التي صاحبته ومواجهتها، هذا من ناحية، كما يستلزم إتخاذ إجراءات قد تتعدى المفاهيم والمبادئ الثابتة في القوانين الوطنية ومن ناحية ثانية لما تتصف به هذه الجرائم من عصرنة وتطور وتحول وسرعة فائقة في أساليبها.

إن غرس الثقافة الحاسوبية وسط المجتمع، وخاصة لدى رجال الأمن والقانون، يمكن أن يحقق للدولة النجاح في مواجهة الجرائم المعلوماتية، التي تبقى من أهم التحديات التي توجه كل الدول، دون إستثناء وفي هذا الصدد يمكن الإشارة إلى موقف الجزائر، المعبر عنه بمناسبة إفتتاح الدورة (32) المجلس وزراء الداخلية العرب 2015 بالجزائر العاصمة: في كلمة مفادها: "وفي هذا المقام، أود أن أخص بالذكر الجريمة الإلكترونية نظرا لارتباطها بظاهرة الإرهاب، إستحداث الصيغ والأليات الضرورية لتفعيل الرقابة الإلكترونية برفع مستويات التعاون في هذا المجال لسد الثغرات التي قد تستغلها هذه الجماعات لضرب إستقرار دولنا ونشر الفكر المتطرف الدخيل وسط مجتمعاتنا وتجنيب الشباب في صفوفها". وعليه، فلا مفر من مواصلة السلطات المعنية في أنحاء العالم الإلتزام بتطوير القدرة على التعاون الدولي الفعال، في مجال مكافحة الجريمة الإلكترونية، من خلال إيجاد أرضية صلبة من التعاون والتفاهم من أجل عالم يسوده الأمن والاستقرار.

لذا لا بد من تعديل القوانين الالكترونية خاصة تعديل القانون 04-15 بما يتماشى مع التطورات الالكترونية.

وكذا إيجاد وحدة البحث و التحري الالكتروني الموحدة دوليا.

دون ان ننسى ضرورة التفاعل الشرطي لكل الدول المنطوية تحت منظمة انتربول ، وذلك بتوحيد الجهود الوطنية مع جهود المنظمة الدولية وخلق جسر تعاون دائم. (حاجي نعيمة ،ص 73).

اهم المراجع المعتمدة :

- الامر 06-03 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات، الجريدة الرسمية الصادرة بتاريخ 23 جويلية 2003، العدد 44.

- القانون 15-04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 66-154 المتضمن قانون العقوبات.

- القانون 04-09 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال ومكافحتها، الجريدة الرسمية الصادرة بتاريخ 16 اوت 2009 ، العدد 47.

- الامر 11-21 المؤرخ في 25 اوت 2021، المتمم بالأمر 66-155 المؤرخ في 08 جويلية 1966 المتضمن قانون الاجراءات الجزائية.

- عبد الصبور عبد القوي: الجريمة الالكترونية، دار العلوم للنشر، طبعة 2007.

- محمد السيد سلطان : قضايا قانونية في امن المعلومات ، دار سر ناشري للنشر الالكتروني، سنة 2012.

- حاجي نعيمة : الجريمة السيبرية و الجهود الدولية لمكافحتها، مجلة النبراس للدراسات القانونية، المجلد 06، العدد 01.

- سبيع زيان، المفتي سلمى : الجريمة المنظمة و الجهود الدولية لمكافحتها، مجلة ابحاث ، المجلد 06، العدد 01.

- سعيداني نعيم. (2013). اليات بحث و التحري عن الجريمة المعلوماتية في القانون الجزائري. رسالة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة مولود معمري تيزي وزو.

- غريب حكيم: الجريمة الالكترونية والجهود الدولية لمكافحتها، المجلة الالكترونية للدراسات القانونية، العدد 01 المجلد 02.

قائمة الهوامش:



- حكيم غريب: الجريمة الالكترونية و الجهود الدولية لمكافحةها، المجلة الجزائرية للدراسات السياسية، المجلد 02، العدد 01 الصفحة 73.
- حكيم غريب: المرجع السابق، ص 74.
- سبع زيان، المفتي سلمى : الجريمة المنظمة و الجهود الدولية لمكافحةها، مجلة ابحاث ، المجلد 06، العدد 01، ص 759.
- القانون 04-09 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال ومكافحتها، الجريدة الرسمية الصادرة بتاريخ 16 اوت 2009 ، العدد 47.
- الامر 11-21 المؤرخ في 25 اوت 2021، المتمم بالأمر 66-155 المؤرخ في 08 جويلية 1966 المتضمن قانون الاجراءات الجزائية.
- حكيم غريب: المرجع السابق، ص 74.
- سعيداني نعيم. (2013). البات بحث و التحري عن الجريمة المعلوماتية في القانون الجزائري. رسالة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة مولود معمري تيزي وزو.
- عبد الصبور عبد القوي: الجريمة الالكترونية، دار العلوم للنشر، طبعة 2007.
- محمد السيد سلطان : قضايا قانونية في امن المعلومات ، دار سر ناشري للنشر الالكتروني، سنة 2012.
- حكيم غريب: المرجع السابق، ص 78.
- الامر 06-03 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات، الجريدة الرسمية الصادرة بتاريخ 23 جويلية 2003، العدد 44.
- القانون 15-04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 66-154 المتضمن قانون العقوبات.
- حكيم غريب: المرجع السابق، ص 79.
- حاجي نعيمة : الجريمة السيبرية و الجهود الدولية لمكافحةها، مجلة النبراس للدراسات القانونية، المجلد 06، العدد 01.



إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية

رضا بوعافية

جامعة برج بوعريش

redha.bouafia@univ-bba.dz

مقدمة

إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، استدعى تدخلا تشريعا صريحا سواء على المستوى الدولي أو الداخلي، فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي، أما على المستوى الوطني، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات بموجب القانون 15/04 باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه " المساس بأنظمة المعالجة الآلية للمعطيات " ، ويشمل المواد من (394 مكرر) إلى (394 مكرر 7)، وكذلك تقرر عقوبات للاعتداء على أنظمة المعلومات في قانون حماية حقوق المؤلف رقم 05/03.

إضافة إلى ما سبق، تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها بسبب ارتكابها بطريقة تقنية كثيرة التعقيد وسهولة تدمير ومحو المعلومات الخاصة بارتكابها وأنها أيضا ذات طبيعة دولية متعددة الحدود حيث تتجاوز الفواصل الجغرافية لعدة دول.

تعتبر الضبطية القضائية صاحبة الاختصاص الأصل في الكشف أو في التحري عن الجرائم عموما، وفي سبيل كشفها عن هذه الجرائم، أعطاه القانون سلطة التحري عن الجرائم، كما منحهم قانون الوقاية من الفساد ومكافحته وكذا قانون الإجراءات الجزائية الجديد أساليب جديدة للتحري، أسماها " أساليب التحري الخاصة "، كما أضافت التأكيد على اعتبار جرائم المساس بأنظمة المعالجة الآلية للمعطيات من الجرائم التي قرر المشرع صراحة وبنص صريح إمكانية إتباع إجراءات التحري الخاصة في الكشف عنها ومكافحتها، نص المادة 04 من القانون 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي قررت الفقرة الثانية منها أنه: " في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ".

و عليه فإن إشكالية هذه الدراسة هي مدى فعالية السياسة الجنائية المتبعة من قبل المشرع الجزائري في مجال التحري والكشف ومكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات؟.

لمعالجة هذه الإشكالية ، تم تقسيم الدراسة الى ثلاث محاور:

- توسيع الإجراءات الخاصة بالاختصاص في الجرائم المعلوماتية
- الإجراءات المتعلقة بالتحري والكشف عن الجريمة المعلوماتية في قانون العقوبات.
- إجراءات التحري والحجز والكشف عن الجرائم المعلوماتية بموجب القانون 09/04



1. توسيع الإجراءات الخاصة بالاختصاص في الجرائم المعلوماتية :

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه تطويرها والقضاء عليها أو على الأقل الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث وضع قواعد وأحكام خاصة لسلسلة التحري والمتابعة الغرض منها هو مواجهتها، وقد وردت هذه الأساليب في قانون الإجراءات الجزائية المعدل والمتمم بموجب القانون 22/06 الصادر في 2006/12/20، وقانون الوقاية من الفساد ومكافحته رقم 01/06 المؤرخ في 20 فيفري 2006، وهي: أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وكذلك أسلوب التسرب أو كما سماه قانون الوقاية من الفساد ومكافحته أسلوب الاختراق.

لذلك لا بد من شرح هذه الأساليب، وكيف يمكن التوفيق بين هذه الأساليب التي تتم خلسة وما تحمله من معنى الاعتداء على الحريات والحقوق الخاصة للأفراد، خاصة إذا علمنا أن الحرية الخاصة للأفراد وسرية المراسلات مضمونة دستوريا حيث المادة (39) من الدستور الجزائري لعام 2016، معدل ومتمم، التي تنص على أنه: " لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة ".

1.1. جواز تمديد الاختصاص المحلي والنوعي الدولي للمحاكم الجزائرية:

حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05).

كما أنشئت الأقطاب القضائية الجزائية المتخصصة بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية من بين الجرائم التي تختص بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المواد 37 و 40 و 329 من قانون الإجراءات الجزائية).

كذلك، نظم المشرع الجزائري في القانون رقم 04/09 المؤرخ في 05 أوت 2009، أحكاما جديدة خاصة بالاختصاص في مجال بالجريمة المعلوماتية تماشى والتطور الذي لحق الجريمة، من هذه القواعد ما نصت عليه المادة الثالثة التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات من ترتيبات تقنية، بالإضافة إلى ذلك، قررت المادة 15 من القانون 04/09 أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

2.1. توسيع مجال اختصاص النيابة العامة :

بموجب المادة 37 من قانون الإجراءات الجزائية، تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها بها من قبل، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.



كذلك سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و144 مكرر 2 من قانون العقوبات المعدل والمتمم بالقانون رقم 09/01 المؤرخ في 26 يونيو 2001 (طرشي، 2012، صفحة 137).

2. الإجراءات المتعلقة بالتحري والكشف عن الجريمة المعلوماتية :

إضافة لما سبق ودائما في إطار المكافحة الإجرائية للجرائم المعلوماتية تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور حسب نص المادة 65 مكرر 5 في إطار تعديل من قانون الإجراءات الجزائية الجزائري بالقانون 22/06 المؤرخ في 20/12/2006 التي تنص: " إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية، أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون، وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

1.2. الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات و التقاط الصور :

مكن المشرع الجزائري ضابط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة (خلفي، 2010، الصفحات 72-73).

إلتقاط الصور يكون بالتقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص، ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة.

أما تسجيل الأصوات، فيتم عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع إلتقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية (المرصفاوي، 1990، صفحة 78).

إن ما يهم هو أن مثل هذا الإجراءات يمكن له المساس بالحرية الشخصية، خصوصا إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة



بتكنولوجيا الإعلام والاتصال ومكافحتها و يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال في إطار المادة 2 /أ من القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية و أنه: " مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية " و يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال في إطار المادة 2 /أ من القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

بالإضافة إلى أن كل متهم بريء حتى تثبت إدانته وتنص المادة (45) من دستور عام 1996 على أنه: " كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته مع كل الضمانات التي يتطلبها القانون ". ، لذلك هل يجوز إثبات أو نفي الاتهام عن المشتبه فيه، باللجوء إلى وسيلة التسجيل الصوتي أو اعتراض المراسلات أو التقاط الصور في الأماكن العامة والخاصة، وخصوصا أن مثل هذه الإجراءات أو الوسائل قد لا تمس بشخص المتهم فقط، وإنما كذلك بمن يحيطون به من أقاربه أو معارفه؟.

يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفية تحت المراقبة، فبينما يكون الأول دون رضا المعني، يكون الثاني برضا أو بطلب من صاحب الشأن، ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

يعد هذا الإجراء الحديث من أهم إجراءات التحقيق، مكن المشرع ضابط الشرطة القضائية ممارسته للكشف عن الجرائم التي حددها على سبيل الحصر في المادة 65 مكرر 5 بموجب قانون الإجراءات الجزائية، تباشره الجهة القضائية في بعض الجنايات والجناح التي وقعت أو التي قد تقع في القريب العاجل، بمعنى أنها إجراء للتحري والتحقق، وكل ما يتمخض عنها كدليل ضد كل شخص قامت تحريات جديده على أنه ضالع في ارتكاب هذه الجريمة أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية.

لكن مع ذلك، نجد المشرع حاول يوفق بين هذه المتعارضات، بأن أجاز هذه الأساليب، ولكن بضوابط وهي مباشرة التحري بإذن من وكيل الجمهورية المختص، وإلتزام أعوان وضباط الشرطة القضائية القائمين بالإجراء السر المهني، وفيما يلي نتولى شرح كلا الضابطتين، فالمشرع على الرغم من إقراره أساليب تحري خاصة قد تمس بحرية الحياة الخاصة إلا أنه يعاقب على اللجوء لاستعمالها بطرق غير مشروعة وفق المادة (303 مكرر) من الأمر رقم 156/66 معدلة ومتممة بموجب المادة (33) من القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 ، وهو ما سنشير إليه على النحو التالي:

1.1.2. مباشرة التحري بإذن من وكيل الجمهورية :

لم يسمح المشرع بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته، وهذا ما قرره المادة 04 من القانون 04/09 التي جاء فيها أنه: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة " .



ويجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء أكانت سكنية أو غير سكنية، كما يجب أن يتضمن نوع الجريمة التي تبرز اللجوء إلى هذه التدابير ومدة هذه التدابير وفق المادة (65) مكرر (7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06، لذلك فإن الإذن المسلم من قبل وكيل الجمهورية للتحقيق في جريمة ما لا يصلح للتحقيق في جريمة أخرى، إلا بإذن جديد، كذلك يجب أن يتضمن الإذن كل الأماكن التي توضع فيها الترتيبات التقنية من أجل التقاط وتسجيل وتثبيت الكلام المتفوه به بصفة خاصة من شخص أو عدة أشخاص وفق المادة (65) مكرر (7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

وعند مباشرة التحريات والتحقيقات، يحزر ضابط الشرطة القضائية المأذون له أو النائب من طرف القاضي المختص، محضر عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط للصور، وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانهاء منها وفق المادة (65) مكرر (9) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06، بحيث يشمل المحضر على كل البيانات المذكورة سابقا وتكون محددة تحديدا نافيا للجهالة، ويجب أن يشمل المحضر على توقيع محرره في نهايته (الرخاوي، 2000، صفحة 271)، بعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له أو النائب، المراسلات أو الصور أو المحادثات المسجلة أو المفيدة في إظهار الحقيقة في محضر يودع بملف المتهم، وتنسخ وترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض وذلك حسب المادة (65) مكرر (10) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06 .

2.1.2. إلزام السر المهني :

تكون إجراءات التحري والتحقيق سرية، ومن ثم، فإن بحثها ضمن الضمانات الممنوحة للمتعمم وفق المادة (11) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06، والسرية تعني القيام قدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وبالتالي صارت السرية ليس هدفها كما كان عليه من قبل هو تسهيل قمع المتعمم، بل صارت وسيلة لضمان الحريات الشخصية (بوزيرة، 2008، صفحة 127) .

فقد نص المشرع صراحة على أن هذه العمليات تتم بمراعاة السر المهني ودون المساس به حسب المادة (65) مكرر (7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06، فالضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ملزم قانونا بكتمان السر المهني ويجب أن يتخذ مقدا التدابير اللازمة لضمان احترام ذلك السر وفق المادة (45) (3) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06. وقد نص قانون الإجراءات الجزائية على أن تكون إجراءات التحري والتحقيق سرية وفق المادة (11) الأمر رقم 155/66 معدل ومتمم ، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع، وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه، لذلك فعملية التحري عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات تتم بسرية مطلقة، فيمنع منعاً باتاً أن يخبر المشتبه فيه بهذه التحريات أو أي شخص آخر، كذلك يمنع على ضابط الشرطة المأذون له أو النائب أن يفصح عن مضمون محضر التحريات لأي شخص كان، وإلا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضابط الشرطة القضائية ومرؤوسيه عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين لا يجوز أن تظل مهددة ببيانات غير مؤكدة.



2.2. أسلوب التسرب أو الاختراق :

يعتبر التسرب تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر 5)، كما يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة وفق المادة (65 مكرر 11) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06 ويشترط حصول الضابط المكلف بالتسرب على الإذن من وكيل الجمهورية المختص، ويجب أن تتم العملية تحت أشرفه ومراقبته، فإن قرر قاضي التحقيق مباشرة هذا الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح الإذن مكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه (حزيط، 2009، صفحة 115)، وهذا تحت طائلة البطالان المطلق، فيجب أن يكون الإذن مكتوبا يتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب.

والتسرب هو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم بمقتضى المادة (65 مكرر 12) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06 ، فالتسرب إذن هو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم جريمة، أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم، ويسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة بعض الجرائم، دون أن يكون مسؤولا جزائيا، وذلك بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية (خلفي ، 2010، الصفحات 74-75).

ولهذا يجوز لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا القيام بما يلي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم، الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الإيذاء أو الحفظ أو الاتصال بمقتضى المادة (65 مكرر 14) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

ويحظر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب إلا لرؤسائهم السلميين، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعرض العضو المكشوف عن هويته للخطر، وهو ما أكدته المشرع بموجب المادة (65 مكرر 16) بأن نصت صراحة أنه: "لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات".

كما عاقب المشرع كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من 50000 دج إلى 2000000 دج، وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح أحد هؤلاء الأشخاص أو أزواجهم أو آبائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس سنوات إلى 10 سنوات والغرامة من 200000 دج إلى 500000 دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من 10 إلى 20 سنة والغرامة من 500000 دج.



إلى 1000000 دج بمقتضى المادة (3/65 - 4 مكرر) من الأمر رقم 155/66 المعدل والمتمم ومعدل بموجب المادة (14) من القانون رقم 22/06.

ولضمان نجاح عملية التسرب للكشف عن جرائم الصفقات العمومية، يلتزم المتسرب القيام بهذه العملية بكل الإجراءات المحددة قانونا، وأهمها حصوله على الإذن المكتوب من قبل وكيل الجمهورية المختص بحيث يلتزم هذا الأخير بالإشراف والمراقبة على نجاح العملية، وكما يلتزم المتسرب حفاظا على أمنه وسلامة العملية بعدم الكشف عن هويته، وذلك لخطورة مهمته التي تتطلب جرأة وكفاءة ودقة في العمل.

ورغم أن المشرع أجاز مثل هذه الأفعال التي تعتبر في حقيقة الأمر جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم والنجاح في إيهامهم بأنهم شركاء أو فاعلون، مع ذلك منع المشرع هؤلاء الضباط أو الأعوان من أن يحرضوا المشتبه فيهم على ارتكاب الجريمة، بمعنى أنه يمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه لارتكاب الجريمة، فهذا الفعل ممنوع تحت طائلة بطلان الإجراء.

3. إجراءات التحري والحجز والكشف عن الجرائم المعلوماتية بموجب القانون 09/04 :

بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إجراءات مراقبة الاتصالات الإلكترونية، وتفتيش وحجز المنظومة المعلوماتية، وعليه سنوجزها كالتالي:

1.3. مراقبة الاتصالات الإلكترونية وتجميعها :

القاعدة أنه أضفى المشرع الجزائري الحماية القانونية للبيانات ذات الطابع الشخصي من خلال أسمى نص في النظام القانوني الجزائري ، ألا وهو الدستور، وهذا في إطار القواعد العامة التي تنص على الحماية القانونية للحياة الخاصة للأفراد ، وهو ما ينطوي عليه بالضرورة حماية بياناتهم الشخصية من المعالجة الآلية، بحيث اعترف المشرع الدستوري الجزائري بها في المادة 77 التي تنص على أنه: "يتمتع كل واحد بجميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما احترام الحق في الشرف، وستر الحياة الخاصة..."

كما أيدت ذلك المادة 46 من دستور سنة 1996 التي نصت على أنه: " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة" ، إلا أنه في تعديل الدستوري لسنة 2016 ، حاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات الشخصية، من خلال إضافة فقرتين للمادة أعلاه تنصان على أنه: " لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون انتهاك هذا الحكم" القانون رقم 16 - 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14.

إن أضافت الفقرتين الثالثة والرابعة في التعديل الأخير، إنما ينم عن اقتناع المشرع الجزائري بضرورة المبادرة إلى وضع الآليات القانونية الكفيلة بحماية البيانات الخاصة بالأشخاص الطبيعيين خلال عملية المعالجة الآلية لها، كما يدل الإقرار الدستوري على أن القانون الخاص بالحماية البيانات هو مسألة وقت فقط، خاصة في ظل النشاط التشريعي الذي الجزائر في العشرة الأخيرة، وأن وزارة البريد وتكنولوجيا الإعلام والاتصال تدرس ابتداء من نوفمبر 2014 مشروع قانون حول حماية البيانات الشخصية على الانترنت والذي يفترض أن يصدر قريبا.



علما أن الجزائري هو الوحيد بين الدساتير العربية الذي تطرق لحزمة البيانات الخاصة من المعالجة الإلكترونية، بحيث تكتفي جلها بتكريس الحماية الدستورية للمراسلات بكل أشكالها فقط بمقتضى القانون رقم 16 - 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14.

وبهذا يكون المشرع الجزائري رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها، قد خول استثناء السلطة القضائية وفي إطار قرار معلل بأن تتبع إجراءات تمس البيانات الشخصية، بالنظر لخطورة بعض الجرائم المعلوماتية المحددة حصرا: تسجيل الاتصالات الإلكترونية في حينها.

كما بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته الرابعة، الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية، وذلك على سبيل الحصر، وهذه الحالات هي:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية.

يظهر من خلال استقراء نص هذه المادة، أن المشرع الجزائري يحاول الاستفادة بدوره من التطور التكنولوجي والمميزات التي يخولها، من خلال وضع المشتبهين فيهم تحت المراقبة الإلكترونية، وهي على عكس المراقبة الشخصية أقل تكلفة من حيث الوقت والمال والمخاطر الأمنية إضافة إلى فعاليتها، إلا أنه من جهة أخرى، فإن وضع الشخص تحت المراقبة الإلكترونية سواء ما تعلق باتصالاته الهاتفية أو نشاطاته عبر الانترنت، من شأنه انتهاك حرمة البيانات ذات الطابع الشخصي له، باعتبار أنه لدواعي فرز المعلومة للتأكد من قيمتها كدليل إثبات أو نفي، يستدعي سماعها أو قراءتها بكل تأني، وهذا ما من شأنه الوصول إما لأنها معلومة ضرورية لاستكمال التحقيقات، أو أنها معلومات شخصية لا دخل لها بالقضية، كما يمكن أن يصار إلى تبرئة الشخص تماما، لكن بعد ماذا؟.

بغرض تأطير هذه العملية الحساسة وتخفيف تأثيراتها السلبية على حماية الحياة الخاصة للأفراد وضع المشرع عدة ضمانات هي:

1.1.3. حصر الحالات التي يمكن اللجوء فيها إلى المراقبة الإلكترونية :

هي الحالات التي أوضحتها المادة الرابعة من القانون 04/09 على سبيل الحصر:

- 1- للوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .
- 2- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- 3- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- 4- في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.



باستقراء الحالات هذه، نجد أن المشرع قد حرص على أن تكون الإجراءات التي يمكن فيها اللجوء إلى عملية المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، ذلك أنه عندما يتعلق الأمر مثلاً بالجرائم الإرهابية والتي تطال المدنيين فإنه لا يمكن الحديث عن حقوق الإنسان، وكذا في حالات تنفيذ المساعدة، إلا أن إضافة الحالة "ج" والتي تعني إمكانية اللجوء في كل قضية مستعصية إلى المراقبة الإلكترونية صغيرة القضايا كانت أو كبيرة، يؤدي إلى تعميم استخدام الآلية دون حد.

2.1.3. وضع آلية إقرار المراقبة الإلكترونية تحت سلطة القضاء :

تضيف المادة 2/4 من القانون 04/09، بأنه: "لا يجوز إجراء عمليات المراقبة، إلا بإذن مكتوب من السلطات القضائية المختصة."

كما أنه عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية، إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها حيث نصت المادة 65 مكرر 7 من قانون الإجراءات الجزائية، على أنه: "يتضمن الإذن كل العناصر التي تسمح على التعرف على الاتصالات ويسلم مكتوبا ويكون صالحا لمدة أربعة أشهر قابلة للتجديد بنفس الشروط الشكلية والزمنية، يسلم الإذن لوضع الترتيبات بغير رضا أو علم الأشخاص الذين لهم حق على تلك الأماكن".

كما تنص المادة 41 من المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حسب الجريدة الرسمية العدد 53، الصادرة في 08 أكتوبر 2015، على أن الهيئة تمارس اختصاصاتها الحصرية في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص.

كما يخضع الموظفون الذين يدعون إلى الاطلاع على معلومات سرية إلى أداء اليمين أمام المجلس القضائي قبل تنصيبهم، وهم يلزمون بذلك بالسرية المهنية (المادتين 27 و28 المرسوم الرئاسي 261/15).

يعتبر وضع هكذا آلية تمس بالحريات الفردية والحياة الخاصة للأفراد تحت يد القضاء المستقل، ضمانا حقيقية باعتبار أن القاضي يهدف إلى الموازنة بين ضرورات التحقيق والإلزامية حماية الأفراد المشتبه فيهم، فمجرد الاشتباه لا يجعل من الفرد مجرما، وهذا ما يسمى ضمانات المحاكمة العادلة.

3.1.3. تحديد تقنيات الرقابة الإلكترونية وحدود استعمال المعطيات المتحصل عليها :

تكون الترتيبات التقنية الموضوعة للأغراض المراقبة الإلكترونية موجهة حصريا لجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر أعلاه على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة.

أما عن التقنيات التكنولوجية التي يمكن أن تستعمل في إطار المراقبة الإلكترونية فهي تتمثل في: اعتراض المراسلات الإلكترونية، تعرف المادة 2/3 من القانون رقم 04/09 المؤرخ في 5 أوت 2009 الاتصالات الإلكترونية على أنها: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية". تسجيل الأصوات، النقاط الصور المادة 65 مكرر 5 من القانون رقم 15 - 19 المؤرخ في 30 ديسمبر 2015 يعدل ويتمم الأمر رقم 66 - 156



المؤرخ في 8 جوان 1966 ، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 ، الصادرة في 30 ديسمبر 2015 ، تفتيش المنظومات المعلوماتية وحجزها(المادة 5 و 7 من القانون 04/09)، إلا أن السؤال الأهم هو ما مصير المعلومات المتحصل عليها؟ أجابت المادة 09 من القانون 04/09 المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الإلكترونية يتحدد بحدود ضرورات التحقيقات، وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار.

4.1.3. سن عقوبات لجرمة إفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الإلكترونية :

يكون الموظفون القائمين على عمليات المراقبة الإلكترونية قادرين على الاطلاع على معلومات ذات طابع مجرم وأخرى ذات طابع شخصي، وفي كلتا الحالتين يكون هؤلاء مطالبين باحترام السر المهني.

لهذا جرم المشرع كل محاولة من قبل هؤلاء الموظفين نحو استغلال عمليات المراقبة لأغراض شخصية، أو كل تجاوز لحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الشخصية للأفراد أيا كان السبب، أو إفشاء مستندات ناتجة عن التفتيش أو إطلاع عليها شخص لا صفة له قانونا في الاطلاع عليه، وذلك بغير إذن مكتوب من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى غير ذلك المادة 46 من الأمر رقم 15 - 02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 - 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40 .

2.3. إجراءات تفتيش المنظومة المعلوماتية :

قررت المادة 5 من القانون رقم 04/09، أنه يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذلك المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة - أ- من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وإذا تبين مسبقا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

والمشرع الجزائري في المادة الخامسة من القانون رقم 04/09 نص على التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وأن اختلف مضمونه عن التفتيش العادي بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة 45 من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.



غير أن القانون رقم 09/ 04 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد، وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها (طرشي، 2012، الصفحات 131-132).

ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها المادة 05 من القانون رقم 09/04 المؤرخ في 5 أوت 2009.

كما نص المشرع الجزائري، ودائما في نفس القانون 09/04 على إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 5، وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسبات لإجراء عمليات التفتيش على المنظومة المعلوماتية، وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات (طرشي، 2012، الصفحات 132-133).

3.3. حجز المعطيات المعلوماتية :

أكدت المادة 6 من القانون رقم 09/04، أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات، وإذا استحال إجراء الحجز وفقا لما هو منصوص عليه في أحكام المادة 06 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية وإلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة المادة 07 من القانون رقم 09/04 المؤرخ في 5 أوت 2009.

ويمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك المادة 08 من القانون رقم 09/04 المؤرخ في 5 أوت 2009.

وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريرات أو التحقيقات القضائية المادة 09 من القانون رقم 09/04 المؤرخ في 5 أوت 2009 .

وفي إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريرات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من القانون رقم 09/04 تحت تصرف السلطات المذكورة، وذلك لتمكين سلطات التحقيق من التعرف على مستعملي الخدمة.



ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق المادة 10 من القانون رقم 04/09 المؤرخ في 5 أوت 2009 .

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب من خلال المادة 12 من القانون رقم 04/09، على مقدمي الخدمات إلتزامات خاصة، هي:

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.
- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجود (طرشي، 2012، صفحة 134).

خاتمة

في الأخير نخلص، إلى أن المشرع الجزائري لا يتوفر على آليات قادرة على الاضطلاع بالآثار الخطيرة التي ترتبها جرائم المساس بأنظمة المعالجة الآلية للمعطيات سواء على مستوى النصوص التشريعية أو على مستوى طبيعة الكوادر والأجهزة المتخصصة لمواجهة هذا النوع من الإجرام، ومن ثم كان لابد أن يبادر إلى تبني سياسة موسعة ومحكمة، تستهدف إيقاف كل التحديات التي يطرحها هذا الإجرام، وإيماننا بأهمية الوقوف أمام التحديات التي تفرضها هذه الجريمة، ارتأينا ختم هذه الدراسة ببعض الاقتراحات والتوصيات التي قد تساهم في التقليل من الآثار السلبية لكثير من التحديات المصاحبة لوسائل الاتصال الجديدة، وتندرج هذه التوصيات تحت النقاط الآتية:

- إعطاء جرائم التقنية حقها من الأهمية في مؤسسات التشريع الوطنية والدولية على السواء، مع التركيز على أهمية إدراج نصوص هذه الأخيرة ضمن التشريعات الوطنية المختلفة، باعتبار أن جرائم الإنترنت ذات بعد دولي تتطلب الانخراط في اتفاقيات دولية، والاهتمام بالتعاون الدولي في مجال مكافحة لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية والكمبيوتر وشبكة الانترنت ككل.

- نظرا لطبيعة الجريمة المعلوماتية الخاصة وكيان بيئتها غير المحسوس تظهر صعوبة مهام السلطات شبه القضائية والسلطات القضائية في أداء دورها للكشف عن الجريمة والبحث عن أدلتها فحتى؛ وإن نجحت الدول نسبيا في تطبيق الأساليب الإجرائية التقليدية كالمعانة والتفتيش والضبط وإضفاء بعض الخصوصيات والشروط عليها، لتتلاءم وطبيعة الجريمة المعلوماتية، تبقى بعض الصعوبات دائما للكشف عن هذه الجريمة والمتمثلة في قلة الآثار المادية التي تتركها وكثرة الأشخاص الذين يترددون على مسرحها بين فترة ارتكابها وفترة اكتشافها، مما يصعب عملية الكشف عنها.

- عقد دورات مكثفة للعاملين في حقل التحري والتحقيق، والمحكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسبات، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن جرائم الإنترنت.

- التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم، حيث أن جريمة الإنترنت لا تحدها حدود وطنية، أو قومية.



- كما تظهر ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات وتسليم المجرمين وقبول أي دولة للأدلة المجموعة في دول أخرى.
- ان أحسن حماية هي الحماية الوقائية ن بحيث من الأفضل نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية (عدم الاحتفاظ ببيانات شخصية أو مالية على الأجهزة، عدم نشر معلومات شخصية، عدم إعطاء كلمة السر. الخ.)

قائمة المراجع :

- حسن صادق المرصفاوي. (1990). المرصفاوي في التحقيق الجنائي (المجلد 2). الإسكندرية، مصر: منشأة المعارف.
- خلفي , ع. (2010). محاضرات في قانون الإجراءات الجزائي . عين مليلة :دار الهدى عين مليلة.
- سهيلة بوزيرة. (2008). مواجهة الصفقات العمومية المشبوهة. ملكرة ماجستير في القانون الخاص. كلية الحقوق جامعة جيجل.
- كمال كمال الرخاوي. (2000). إذن التفتيش فقها وقضاء (المجلد 1). المنصورة القاهرة: دار الفكر والقانون.
- محمد حزيط. (2009). قاضي التحقيق في النظام القضائي الجزائري (المجلد 2). الجزائر: دار هومة.
- نورة طرشي. (2012). مكافحة الجريمة المعلوماتية. ملكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق. جامعة الجزائر 1.



مكافحة الجرائم الالكترونية في التشريع الجزائري

بوخالفة سعاد

Sboukhalifa55@yahoo.com

مقدمة

السيبرانية فكرة واسعة ولها قوانينها الضابطة، ويمكن تعريف قانون السيبرانية بأنه "مجموع القواعد و الأحكام الواردة في شتى فروع القانون، والتي يمكن تطبيقها على مسألة معلوماتية بحسب نوع المشكلة المثارة و التي قد تخضع لأحكام قانونية متعددة"، و تثير فكرة المعلوماتية قلقا بالغاً إذا استخدمت أنظمة المعلومات في انتهاك حقوق الأفراد و حرياتهم العامة.

أدى التطور الكبير في نظم الفضاء السيبراني إلى ظهور مجالات أوسع لاستخدام هذه التقنية و ذلك لما تتميز به الحاسبات من سرعة في تنفيذ العمليات و الأوامر، و من إمكانية تخزين كميات هائلة من البيانات و استرجاعها بكفاءة، بالإضافة إلى إجراء الاتصالات و على إثر ذلك ظهرت علاقات قانونية تنظم كيفية التعامل و التعاطي مع هذا المستحدث المعلوماتي، و حمايته من الاعتداءات و الاستعمال غير المشروع، و وضع قواعد كفيلة بنقل تكنولوجيا المعلومات على وجه الصحيح، و على ذلك فقد ظهرت علاقات تربط منظومة الحماية القانونية من الجرائم السيبرانية بالمنظومة القانونية من خلال ما يسمى بقانون المعلوماتية، هذا الأخير يعمل على حماية النظم المعلوماتية من الاعتداء و يضع الاطار الصحيح لتداولها، كما يعمل على تحقيق هذه الحماية من خلال نصوص خاصة أو من خلال أعمال النصوص التقليدية.

وعليه فإن الحماية القانونية للنظم السيبرانية و للموضوعات الناشئة عنها لا تتحقق إلا من خلال قواعد قانونية تجرم كل فعل يهدف إلى الاعتداء ضد هذه النظم أو يهدف إلى استخدامها كوسيلة لارتكاب إحدى الجرائم التقليدية و هذا يتطلب تدخل القضاء لتوسيع نطاق النص الجنائي ليستوعب هذا النوع من الجرائم، و قد يتطلب تدخل التشريع لسن قواعد قانونية خاصة بها و هذا ما حدث في أغلب دول العالم و منها الجزائر، و لهذا فقد كان لزاما إيجاد منظومة قانونية تتصدى لجميع الموضوعات الناشئة عن هذه العلاقات و ذلك بتطويع النصوص التقليدية و استحداث تشريعات جديدة خاصة بنظم المعلوماتية على اعتبار أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الاجرامية المستحدثة و بالتالي تطبيقها على مرتكبيها و على ضوء هذا يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.

لمعالجة ما سبق نطرح الاشكالية الآتية:

ما هو الاطار القانوني الذي يحكم الجرائم الالكترونية في التشريع الجزائري؟ و ما مدى فعاليته؟

ومن أجل الإجابة على هذه الإشكالية قسمنا دراستنا إلى محورين خصصنا المحور الأول لدراسة آليات مكافحة الجريمة الإلكترونية بموجب القواعد القانونية العامة، أما المحور الثاني فخصصناه لدراسة آليات مكافحة الجرائم الالكترونية بموجب القوانين و الهياكل الخاصة.

1. آليات مكافحة الجريمة الإلكترونية بموجب القواعد القانونية العامة :

حاول المشرع الجزائري التصدي للجرائم الإلكترونية من خلال اللجوء إلى تطبيق القواعد العامة التي جاء بها الدستور و كذا القوانين التقليدية منها القانون المدني و قانون العقوبات و قانون الإجراءات الجزائية.



1.1 مكافحة الجرائم الإلكترونية في إطار القواعد العامة للدستور و القانون المدني :

حاول المشرع الجزائري في سعيه لمكافحة الجرائم الالكترونية الاستعانة بالقواعد القانونية العامة التي تضمنها الدستور و كذا القانون المدني و التي في أغلبها تنص على حماية الحقوق و الحريات المعترف بها للأفراد قانونا من أي مساس يلحق بها حتى و لو كان باعتماد الوسائل الحديثة أي التقنيات الحديثة مع حق المتضررين المطالبة بالتعويضات اللازمة.

1.1.1 مكافحة الجريمة الإلكترونية بموجب القواعد الدستورية :

بالرجوع الى دستور الجزائر لسنة 2020 فإنه يتضح لنا اهتمام المشرع بحماية الحقوق الأساسية و الحريات الفردية مع تأكيد على حرص الدولة على ضمان عدم انتهاك حرمة الإنسان (الجريدة الرسمية، العدد 2020/82) و قد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات و كذلك قانون الإجراءات الجزائية...و التي تحظر المساس بالحقوق الأساسية و الحريات الفردية و من أهم المبادئ الدستورية العامة نجد ما نصت عليه:

المادة 47 " لكل شخص الحق في حماية حياته الخاصة و شرفه.

لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى و الثانية إلا بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي "

المادة 55 " يتمتع كل مواطن بالحق في الوصول إلى المعلومات و الوثائق والإحصائيات و الحصول عليها و تداولها.

لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير و بحقوقهم, و بالمصالح المشروعة للمؤسسات بمقتضيات الأمن الوطني.

يحدد القانون كيفية ممارسة هذا الحق "

2.1.1 مكافحة الجريمة الإلكترونية بموجب القانون المدني الجزائري :

بالرجوع الى نص المادة 124 من القانون المدني الجزائري و التي جاء فيها أن "كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض " , الملاحظ أن نص المادة ورد شاملا و عاما ينطبق على أي اعتداء يمكن أن يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة, كما تضمن المادة النص على حق من وقع اعتداء على حياته الخاصة في المطالبة بالتعويض عما لحقه من ضرر باعتبار أن الفعل الضار هو أساس المسؤولية و هو ركن أساسي يمكننا الاستناد إليه و تأسيس الحق في رفع الدعوى القضائية عن الاعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الإنترنت (الجريدة الرسمية، العدد 2007/31)

الملاحظ أن المشرع الجزائري أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات, فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل الى درجة الخطأ الذي يشكل اعتداء قابل للإثبات و إن وقع على الشبكة.

2.1 مكافحة الجريمة الإلكترونية بموجب قانون العقوبات و قانون الإجراءات الجزائية :

سعى المشرع الجزائري لتدارك الفراغ القانوني الذي عرفه مجال الإجرام الإلكتروني بتعديل قانون العقوبات باستحداث جملة من النصوص جرم من خلالها الأفعال الماسة بنظم المعالجة الآلية للمعطيات , الى جانب سن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجرائم الإلكترونية و ذلك بتعديله أيضا لقانون الاجراءات الجزائية.



1.2.1 مكافحة الجريمة الإلكترونية بموجب قانون العقوبات :

بهدف تدارك الفراغ القانوني قام المشرع الجزائري بإدراج قسما كاملا في قانون العقوبات الجزائري رقم 04-15 متعلقا بجرائم المساس بأنظمة المعالجة الآلية للمعطيات و هذا ضمن القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الأموال , حيث قام المشرع بسن جملة من القواعد القانونية الموضوعية و التي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات و ما يقابلها من جزاء أو عقوبة , وتأخذ هذه الأفعال إما وصف الاعتداء على نظام المعالجة الآلية أو وصف الاعتداء على معطيات نظام المعالجة الآلية كما يمكن لها أن تأخذ وصف الاعتداء على سير نظام المعالجة الآلية (الجريدة الرسمية, العدد 2004/71).

1.1.2.1 الاعتداء على نظام المعالجة الآلية للمعطيات :

عرف المشرع الجزائري نظام المعالجة الآلية للمعطيات بأنه " كل نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة ببعضها البعض أو المرتبطة و التي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين , و قد جعل المشرع من وجود نظام المعالجة الآلية شرطا أساسيا للبحث عن مدى تحقق الاعتداء أولا, هذه الجريمة التي تتحقق بصورتين:

الصورة الاولى و هي البسيطة و تتمثل في جرمي الدخول و البقاء غير المرخص بهما في النظام و التي نصت عليها المادة 394 مكرر من قانون العقوبات الجزائري و التي جاء فيها " يعاقب بالحبس من ثلاثة أشهر الى سنة و بغرامة من 50000 دج الى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل او جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك " .

الصورة الثانية و هي الصورة المشددة و التي تتحقق عندما يترتب على فعل الدخول أو البقاء نتائج غير مشروعة ضد معطيات النظام, وقد نصت المادة 394 مكرر في فقرتها الثانية على أن "...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة العقوبة الحبس من 6 أشهر الى سنتين و الغرامة من 50000 دج الى 150000 دج " .

الملاحظ أن المشرع أورد طرفين لتشديد العقوبة في هذه الجريمة و هذا في حالة ما إذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام , و الشرط الثاني عندما يترتب على الدخول أو البقاء تخريب نظام اشتغال المنظومة و إعاقته عن أداء وظيفته , و الغاية من هذا التشديد في العقوبة المفروضة هو السعي للحد من تفاقم الإجرام المعلوماتي و ما يصاحبه من أضرار بالغة و تحقيق الائتمان في المعاملات الإلكترونية.

2.1.2.1 الاعتداء على معطيات نظام المعالجة الآلية :

يقصد بجريمة الاعتداء على معطيات نظام المعالجة الآلية هم الاعتداء الذي يكون هدفه الإضرار بمعلومات الكمبيوتر أو وظائفه عن طريق المساس بسريتها أو سلامة محتوياتها أو تعطيلها بشكل يمنعها من أداء وظيفتها بشكل سليم و هذا الاعتداء يتخذ صورتين: الصورة الاولى و هي الاعتداء على المعطيات الداخلية للنظام و التي يقصد بها المعطيات و المعلومات التي يحتويها النظام و تشكل جزء منه و التي تمت معالجتها أليا و أصبحت عبارة عن رموز و إشارات تمثل تلك المعلومات و ليس المعلومات ذاتها باعتبارها أحد عناصر المعرفة , و قد جرم المشرع الجزائري أي اعتداء يقع على المعطيات الموجودة داخل نظام المعالجة الآلية من خلال المادة 394 مكرر 1 من قانون العقوبات و التي نصت على أنه " يعاقب بالحبس من 6 أشهر الى 3 سنوات و بالغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها " .



الصورة الثانية و هي الاعتداء على المعطيات الخارجية للنظام و التي يقصد بها المعطيات التي لها دور في تحقيق نتيجة معينة تتمثل في المعالجة الآلية للمعطيات وبالرجوع الى المادة 394 مكرر 2 و التي جاء فيها " يعاقب بالحبس من شهرين الى 3 سنوات و بغرامة من 1000000 دج الى 5000000 دج كل من يقوم عمدا أو عن طريق الغش ب:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم.

وعليه فإن أي تلاعب بالمعطيات المذكورة في المادة - سواء كانت معطيات مخزنة أي تلك المفرغة في دعامة مادية خارج النظام كالأقراص أو تلك المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب , أو كانت معطيات المعالجة أي تلك التي تحولت الى اشارات أو رموز أو المرسلة عن طريق منظومة معلوماتية - يعد جريمة اعتداء على المعطيات الخارجية لنظام المعالجة و بالتالي يعاقب الجاني.

3.1.2.1 الاعتداء على سير نظام المعالجة الآلية :

بالرجوع الى قانون العقوبات الجزائري فإننا لا نجد أي نص صريح ينص على تجريم الاعتداء على سير نظام المعالجة الآلية للمعطيات , إلا أنه يمكن للقاضي الجزائري استخلاص الحماية الجزائية لسير نظام المعالجة الآلية للمعطيات من النصوص القانونية التي تجرم أفعال الاعتداء على أنظمة المعالجة و معطياتها الداخلية و الخارجية, و مثال ذلك ما نصت عليه المادة 393 مكرر و المتعلقة بالاعتداء على النظام بتخريبه و الاعتداء على المعطيات الداخلية للنظام باستعمال برامج الفيروسات و الذي من شأنه أن يعيب السير الحسن للنظام المعلوماتي , ولذلك كان من الأحسن وضع نص خاص بتجريم الاعتداء على سير النظام لرفع اللبس و الحرج على القاضي الذي هو مقيد بقاعدة التفسير الضيق للنص الجزائري.

2.2.1 مكافحة الجريمة الإلكترونية بموجب قانون الإجراءات الجزائية :

إدراكا من المشرع الجزائري بأن المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية و إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية و وقائية و تحفظية , هذا الذي من شأنه تفادي وقوع الجريمة الالكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها , لهذا قام بتضمين القانون رقم 06-22 المعدل لقانون الاجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية تتمثل في مراقبة الاتصالات الالكترونية وتسجيلها و التسرب (الجريدة الرسمية, العدد 84/2006).

1.2.2.1 مراقبة الاتصالات الالكترونية :

و يقصد بها تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج و التوزيع, التخزين, الاستقبال و العرض و التي تتم عن طريق قنوات أو وسائل الاتصال السلكية و اللاسلكية في اطار البحث و التحري عن الجريمة و جمع الأدلة عنها. أشار المشرع الجزائري الى ظروف و كيفية اللجوء الى تطبيق هذا الاجراء في المادة 65 مكرر 5 من قانون الاجراءات الجزائية و التي نصت على أنه يسمح لسجلات التحقيق و الاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها أو التحقيق في الجريمة الإلكترونية اللجوء الى إجراء اعتراض المراسلات السلكية و اللاسلكية و تسجيل المحادثات و الأصوات و التقاط الصور و الاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول الى الكشف عن ملابسات الجريمة و اثباتها دون أن يتقيدوا بقواعد التفتيش و الضبط المألوفة , مع إحاطة هذا الإجراء بمجموعة من الضمانات القانونية أهمها حصول ضابط الشرطة القضائية على إذن مكتوب و مسبب من طرف وكيل الجمهورية أو قاضي التحقيق مع مراعاة الجرائم



التي يجوز فيها المراقبة و كذا تحديد مدة هذا الاجراء وهذا بهدف الحد من تعسف السلطات المطبقة لها و كذا حماية الحقوق و الحريات العامة و الحياة الخاصة للأفراد (براهيم ص ص 139-140).

2.2.2.1 التسرب :

و المقصود بعملية التسرب في نطاق جرائم الاعتداء على أنظمة المعالجة الآلية هو ولوج ضابط أو عون الشرطة القضائية الى العالم الافتراضي و اشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش و الاتصال المباشر في كيفية قيام أحدهم باختراق شبكات أو بث الفيروسات ,منتحلا في ذلك هوية مستعارة أو باستخدام أسماء و صفات هيئات وهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعل مثلهم سعيًا منه الى الكشف عن الجريمة و الاطاحة بالمجرمين, و قد تطرقت المادة 65 مكرر 12 الى تعريف هذا الاجراء (براهيم ص ص 142- 143- 144).

و نظرا لكون إجراء التسرب غير مألوف عند سلطات الضبط القضائي و هو يعتبر من أخطر إجراءات التحقيق انتهاكا لحرمة الحياة الخاصة للمتهم فإنه كان من الضروري على المشرع إحاطته بمجموعة من الضمانات و الضوابط التي يجب مراعاتها عندما تقتضي ضرورات التحري أو التحقيق اللجوء اليه و من أهم هذه الضمانات ضرورة صدور إذن قضائي بالتسرب من طرف وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية مع احترام المدة المقررة للتسرب إضافة الى تسبب عملية التسرب أي الدفع الحقيقي الذي يبرر اللجوء الى هذا الاجراء مع تحديد محل التسرب أي الجرائم التي ينصب عليها الاجراء .

2. آليات مكافحة الجرائم الالكترونية بموجب القوانين و الهياكل الخاصة :

إن مكافحة الجرائم الالكترونية بطريقة فعالة تقتضي من المشرع الجزائري اللجوء الى القوانين الخاصة الى جانب القوانين العامة إضافة للهياكل الخاصة بمكافحة هذا النوع من الجرائم بالنظر الى طبيعتها التقنية و المتطورة أيضا.

1.2 مكافحة الجرائم الالكترونية تطبيقا للقوانين الخاصة :

نظرا للطبيعة الخاصة لبعض الجرائم الإلكترونية و قصور القواعد القانونية التقليدية عن معالجتها كما يجب دفع الأمر بالمشرع الجزائري الى النص على هذه الجرائم في إطار القوانين الخاصة لا سيما و التي تتلاءم مع هذا النوع من الجرائم.

1.1.2 القانون الخاص بحماية حق المؤلف والحقوق المجاورة :

عالج الأمر 97-10 المتعلق بحماية حق المؤلف و الحقوق المجاورة الملغى بالأمر 03-05 مسألة التعدي على المصنفات المعلوماتية إذ أدرج هذه الأخيرة ضمن المصنفات المحمية قانونا بموجب المادة 4/أ, و قد ترتب على جعل المشرع الجزائري برامج و بيانات الحاسب مصنفا فكريا و إدماجها ضمن المصنفات الأصلية اعتبار أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج و البيانات يشكل فعلا من أفعال التقليد المنصوص عليها في المادة 151 من الأمر 03-05 المذكور سالفًا يترتب عليها العقوبات الجزائية المقررة (الجريدة الرسمية , العدد 2003/44).

و تنقسم جنح التقليد التي تمس مصنف برامج و بيانات الحاسب الآلي إلى ثلاثة أنواع هي:

1.1.1.2 الجنح المرتبطة بالحق المعنوي للمؤلف: حددتها المادة 1/151 من الأمر 03-5 و تتمثل أساسا في الكشف غير المشروع عن المصنف الأدبي والفني, و المساس بسلامة المصنف الأدبي أو الفني.



2.1.1.2. الجنح المرتبطة بالحق الأدبي للمؤلف : و تم التطرق اليها من طرف المشرع في كل من المادة 1/151 و التي تناولت جنحة الاستنساخ غير الشرعي للمصنف , إضافة الى المادة 152 و التي تناولت جنحة الابلاغ غير الشرعي للمصنف.

3.1.1.2. الجنح المرتبطة بالمصنف المقلد: و تتعلق هذه الجنح في التصرفات و التعاملات التي ترد على المصنف المقلد الذي يمكن أن يكون برنامج أو بيانات الحاسب الآلي و قد تم التطرق الى هذه الجنح في المادة 5.4.3/151, و المادة 155 و تتمثل أساسا في استيراد أو تصدير نسخ مقلدة من المصنف, بيع نسخ مزورة من المصنف, تأجير مصنف مقلد أو عرضه للتداول و الرفض عمدا دفع المكافأة المستحقة بمقتضى الحقوق المقررة للمؤلف

و قد حدد المشرع العقوبات التي توقع على جنح تقليد المصنفات المعلوماتية و التي تتمثل في **العقوبات الأصلية** و يقصد بها عقوبة الحبس و الغرامة المالية, إضافة الى **العقوبات التكميلية** و المتمثلة في مصادرة المبالغ المساوية لأقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف, مصادرة و إتلاف كل عتاد خصص لمباشرة النشاط غير المشروع و كل النسخ المقلدة , الأمر بتسليم العتاد و النسخ المقلدة أو قيمة ذلك للمؤلف أو أي مالك حقوق أخرى لتكون بمثابة تعويض , الأمر بطلب من المتضرر بتعليق و نشر أحكام الإدانة على نفقة المحكوم عليه , الأمر بحجز الوثائق و النسخ الناتجة عن الاستنساخ غير المشروع أو التقليد أو حجز الدعائم المقلدة و الإيرادات الناتجة عن الاستغلال غير المشروع للمصنفات.

الملاحظ أن المشرع خول للقاضي الجزائي أن يضاعف و يشدد العقوبات الأصلية في حالة توفر ظرف العود و أن يأمر بغلق المؤسسة التي يستغلها المقلد أو شريكه لمدة لا تتجاوز 6 أشهر, و عند الاقتضاء الأمر بالغلق النهائي و هذا حسب نص المادة 156 من الأمر 05/03.

2.1.2. القانون الخاص بالحماية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها رقم 04/09 :

يعتبر القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها الاطار القانوني الأكثر ملائمة مع خصوصيات الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت (الجريدة الرسمية , العدد 2009/47) وقد تضمن مجموعة من **التدابير الوقائية** التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها و عن مرتكبيها في وقت مبكر و المتمثلة أساسا في:

- 1.2.1.2. مراقبة الاتصالات الالكترونية :** و هذا في أربعة حالات نصت عليهم المادة 04 من القانون رقم 04/09 نظرا الى خطورة التهديدات المحتملة و أهمية المصلحة المحمية و تتمثل في :
- الوقاية من جرائم الإرهاب و التخريب و جرائم ضد أمن الدولة.
 - حالة توفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع أ, الدفاع الوطني أو النظام العام.
 - للمساعدة في التحقيقات و المعلومات القضائية في حالة ما كان من الصعب الوصول الى نتيجة للأبحاث دون اللجوء للمراقبة الالكترونية.

- في اطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

2.2.1.2. إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية : وهذا من خلال فرض مجموعة من الالتزامات و المتمثلة أساسا في :

- التعاون مع المكلفين بالتحقيق القضائي عن طريق جمع و تسجيل المعطيات المتعلقة بالاتصالات و المراسلات و وضعها تحت تصرف مصالح الأمن مع مراعاة سرية الإجراءات و التحقيق.



- الالتزام بحفظ المعطيات و المعلومات المساهمة في الكشف عن الجرائم و مرتكبيها.
- السحب الفوري لكافة المحتويات التي يسمح الاطلاع عليها بمخالفتها للقانون و العمل على تخزينها أو جعل الوصول إليها غير ممكن.
- القيام بما يلزم من أجل الحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية للنظام العام و الآداب العامة.
- إضافة إلى هذه التدابير الوقائية فقد تبني المشرع الجزائري في القانون 04/09 مجموعة من التدابير الإجرائية إضافة إلى تلك المنصوص عليها في قانون الإجراءات الجزائية و تتمثل أساسا في:
- السماح للجهات المختصة بالدخول إلى المنظومة المعلوماتية أو جزء منها و كذا للمعطيات المخزنة فيها و استنساخها بهدف القيام بمهمة التفتيش.
- في حالة تواجد المعطيات المخزنة في منظومة معلوماتية خارج الإقليم الوطني و تطبيقا للاتفاقيات الدولية و مبدأ المعاملة بالمثل يمكن الاستعانة بالسلطات الأجنبية المختصة.
- في حالة ما إذا كانت الدولة الجزائرية و مصالحها الإستراتيجية هدف للجرائم الالكترونية أجنبية المصدر فإنه يمكن توزيع الاختصاص القضائي خارج الإقليم الوطني.
- ما يمكننا قوله هو شمولية و عمومية القانون رقم 04/09 لكونه يغطي كافة الجرائم الالكترونية القديمة و الجديدة و هذا الذي جعله فعالا و مساهما للتطور التكنولوجي السريع.

3.1.2 معالجة قانون البريد والاتصالات اللاسلكية و قانون التأمينات لبعض الجرائم الالكترونية.

1.3.1.2 قانون البريد والاتصالات اللاسلكية :

بالنظر إلى قانون البريد والاتصالات اللاسلكية و ما جاء به من قواعد عامة فإنه يتضح لنا مواكبته للتطور التكنولوجي حيث أصبح بالإمكان إجراء التحويلات المالية باعتماد الطريقة الالكترونية و هذا ما نصت عليه المادة 2/84 منه عن طريق استعمال حوالات دفع عادية أو الكترونية أو برقية , كما تطرقت المادة 105 منه إلى وجوب احترام المراسلات , وعالجت المادة 127 منه حالة استغلال الوظيفة من أجل فتح أو تحويل أو تخريب للبريد أو انتهاكا له بمعاقة الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من 5 إلى 10 سنوات (عاقلي, ص 131).

2.3.1.2 قانون التأمينات :

تمت معالجة تنظيم الجريمة الالكترونية من خلال هيئة الضمان الاجتماعي و هذا في نصوص قانونية متعددة تتعلق بالبطاقة الالكترونية و الجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلياً أو جزئياً للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعياً أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية و هذا حسب نص المادة 93 مكرر 2 (عاقلي, ص 132).

2.2 مكافحة الجرائم الالكترونية في إطار الهياكل الخاصة :

إن طبيعة هذا النوع من الجرائم الالكترونية استدعى وجود هيئات متخصصة تتكفل بها , خاصة مع ما تتطلبه خلال مختلف مراحل معالجتها لهذه الجرائم من شروط و امكانيات مادية و بشرية .



1.2.2 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال :

تم إنشاء هذه الهيئة بموجب المادة 13 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها و التي جاء فيها أنه " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ,تحدد تشكيلة الهيئة و تنظيمها وكيفية سيرها عن طريق التنظيم" و قد أعطى لها في المرسوم الرئاسي رقم 15-261 (الجريدة الرسمية , العدد 2015/52)صفة السلطة الإدارية المستقلة التي تراجع عنها لاحقا بموجب المرسوم الرئاسي 19-172 و اعتبرها مؤسسة عمومية ذات طابع إداري توضع تحت سلطة وزارة الدفاع (الجريدة الرسمية , العدد 2019/37).

بالعودة إلى دور هذه الهيئة فقد كانت المادة 4 من المرسوم الرئاسي رقم 15-261 تحدد هذه المهام , فهي تتنوع بين كونها هيئة استشارية و هيئة تحري و مرصد لجمع و تسجيل وحفظ المعطيات الرقمية وهي مساعدة للقضاء ,بالإضافة إلى أنها هيئة تكوين للمحققين , لكن بعد إلغاء المرسوم 15-261 و تعويضه بالمرسوم 19-172 لم يحصر هذا الأخير مهام الهيئة ككل بل وزع المهام على تشكيلتها و المتمثلة في مجلس توجيه و مديرية عامة , و المتمثلة أساسا في دور الهيئة الحصري للوقاية و الكشف عن الجرائم الإرهابية و التخريبية بأمن الدولة حيث تكلف الهيئة حصريا ب

- ضمان المراقبة الوقائية للاتصالات الالكترونية بخصوص الجرائم الارهابية و التخريبية و الماسة بأمن الدولة وهذا عن طريق مراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و هو ما أشارت إليه ضمنا المادة 04 من قانون رقم 04/09 , عن طريق وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وذلك لمقتضيات النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية و هذا في حالات الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة و تختص بهذه الحالة الشرطة القضائية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها.

- دور الهيئة في القيام بإجراء التفتيش الوقائي و الحجز في الأنظمة المعلوماتية بصدد الجرائم الإرهابية و التخريبية و الماسة بأمن الدولة ورغم أن المرسوم الرئاسي رقم 19/172 لم يتطرق إلى إجراء التفتيش و لكن أخذنا بالمادة 05 من القانون رقم 04/09 التي نصت على إجراء التفتيش فإنها تحيلنا في تحديد حالات اللجوء إليه الى المادة 04 من نفس القانون و المتعلقة بحالات اللجوء للمراقبة الالكترونية,هذه الأخيرة كما رأينا تميز بين الطابع الوقائي للوقاية من الأفعال الموصوفة بالجرائم الإرهابية و التخريبية و الماسة بأمن الدولة, خاصة و أن المادة 21 من المرسوم رقم 15/261 الملغاة نصت صراحة على هذا الإجراء الذي يسفر عنه أدلة لا بد من الحجز عليها .

2.2.2. دور الهيئة المساعدة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال :

من مهام الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال:

- مساعدة السلطات القضائية الداخلية و تتمثل في مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية , و عليه تتدخل الهيئة بطلب من الجهات القضائية المختصة لتقوم في إطار الخبرات القضائية بالإجراءات المنصوص عليها في قانون رقم 04/09 خاصة المراقبة الالكترونية للاتصالات و تفتيش النظم المعلوماتية , و الملاحظ أن المشرع في المرسوم الرئاسي رقم 19/172 سحب اختصاص المراقبة الالكترونية من جميع الهيئات الأخرى و خوله لهذه الهيئة بصفة مباشرة في حالة الوقاية من الجرائم الارهابية و الماسة بأمن الدولة , و بصفتها مساعد أي بطلب من جهات قضائية في حالات أخرى حسب نص المادة 12 من المرسوم الرئاسي رقم 19/172.



- مساعدة السلطات القضائية الأجنبية بالرجوع الى القانون رقم 04/09 فإنه يمكن اللجوء في إطار التعاون الدولي الى طلب المساعدة القضائية الدولية بواسطة إجرين هما تبادل المعلومات و طلب إجراءات تحفظية كما يعود للهيئة السهر على تنفيذ طلبات المساعدة الدولية و تبادل المعلومات مع نظيرتها في الخارج .

2.2.2 المعهد الوطني للأدلة الجنائية و علم الإجرام :

بموجب المرسوم الرئاسي رقم 04/183 تم إحداث المعهد الوطني للأدلة الجنائية و علم الإجرام تحت وصاية القيادة العامة للدرك الوطني، يتكون من إحدى عشر دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة ، التكوين و التعليم و تقديم المساعدات التقنية (عائلي ، ص 133).

يحتوي هذا المعهد على قسم الإعلام الآلي الذي يختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية ، و الى جانب ذلك يوجد مركز الوقاية من جرائم الاعلام الآلي و الجرائم المعلوماتية تابع أيضا لقيادة الدرك الوطني أما على مستوى المديرية العامة للأمن الوطني فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية و من الفروع التقنية التي تتضمنها هذه المخابر خلية الاعلام الآلي و التي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية. و تحليل وتقديم كل دليل رقمي يساعد العدالة كما تقدم مساعدة تقنية للمحققين في المعاينات.

3.2.2 الهيئات القضائية الجزائية المتخصصة :

قامت وزارة العدل ومنذ سنة 2003 بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة، ليواكب التطور القانوني الجاري الخاص بجرائم المعلوماتية.

ويتجه النظام القضائي الجزائري إلى إرساء فكرة القضاء المتخصص ، و ما يؤكد ذلك ما نص عليه القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون الاجراءات الجزائية على أنه يجوز تمديد دائرة الاختصاص للمحكمة و كذا لوكيل الجمهورية و قاضي التحقيق عن طريق التنظيم في جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية ، و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف ، كما نصت المادة 40 مكرر من قانون الاجراءات الجزائية على أنه " تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية و التحقيق و المحاكمة أمام الجهات القضائية التي يتم توسيع اختصاصها المحلي طبقا للمواد 37-40-329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر إلى 40 مكرر 5 أدناه ."

تعد الجرائم المعلوماتية بشكل من الأشكال جريمة منظمة ترتكب عن طريق الشبكات الرقمية ، والتي يمكن معالجتها عن طريق الأقطاب الجزائية المتخصصة و هذا طبقا لنصوص المرسوم التنفيذي رقم 348/06 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق وهذا في "جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم الصرف..." (بوضياف ، ص ص 370-371).

خاتمة:

من خلال ما سبق يمكننا القول أن المشرع الجزائري قد اجتهد للتصدي للجرائم الالكترونية من خلال تعديل الجوانب الموضوعية و الاجرائية للقوانين العامة و السعي لجعلها تواكب التطورات التكنولوجية الحديثة كما قام باستحداث قوانين أخرى و هيئات خاصة أكثر تحاوبا مع طبيعة الجرائم الالكترونية ، وهذه الازدواجية في المعالجة ساهمت بشكل فعال في الحد من تفاقم ظاهرة الاجرام الالكتروني في الدولة الجزائرية ورغم هذا فإن الواقع أثبت عدم كفايتها بالنظر الى التطور السريع و المستمر لهذا النوع من الجرائم التي تتميز بطبيعة قانونية مغايرة تماما للجرائم التقليدية .



التوصيات :

- لهذا و من أجل الحد من تفاقم ظاهرة الاجرام الالكترونية في الدولة الجزائرية فإنه من الضروري:
- مراجعة التشريعات الوطنية من خلال تشديد الوصف الجنائي و العقوبات المقررة للأنماط الاجرامية للجريمة المعلوماتية بهدف تحقيق الردع و القضاء على الاجرام المعلوماتية.
- التوجه الى التعاون التشريعي و القضائي و الأمني الخارجي مع الدول الأكثر دراية بالجرائم الالكترونية و الاستفادة من خبراتها في مجال مكافحة هذه الجرائم.
- ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الاجرائية من أجل التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات و تسليم المجرمين و قبول أي دولة للأدلة المجموعة في دول أخرى بهدف ضمان حماية فعالة لبرامج المعطيات الآلية للكمبيوتر و شبكة الانترنت.
- ضرورة تفعيل أسلوب التوعية لدى مستخدمي شبكة الاتصالات العالمية و تعريفهم بحجم الخطورة التي يمكن التعرض لها عند عدم اتخاذ الاحتياطات الوقائية اللازمة.
- العمل على تنظيم الندوات و المؤتمرات التي تدرس تطور الاجرام المعلوماتية و البحث في تطوير طرق و وسائل مكافحة الجريمة المعلوماتية و الحد من أثارها.

قائمة المصادر و المراجع

- 1- دستور الجمهورية الجزائرية الديمقراطية الشعبية, الصادر بالجريدة الرسمية العدد 82 المؤرخة في 30 ديسمبر 2020.
- 2- قانون رقم 05/07 المؤرخ في 13 ماي 2007, يعدل و يتمم الأمر رقم 58/75 المؤرخ في 26 سبتمبر 1975 و المتضمن القانون المدني, الصادر بالجريدة الرسمية العدد 31 لسنة 2007.
- 3- قانون العقوبات رقم 04/15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المتضمن قانون العقوبات, الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية, العدد 71 الصادرة بتاريخ 10 نوفمبر 2004 معدل و متمم.
- 4- القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم للأمر رقم 155/66 المتضمن قانون الاجراءات الجزائية الصادر بالجريدة الرسمية العدد 84 الصادرة بتاريخ 24 ديسمبر 2006.
- 5- براهيمى جمال , مكافحة الجرائم الالكترونية في التشريع الجزائري , المجلة النقدية .
- 6- الأمر رقم 05/03 المؤرخ في 19 جويلية 2003 , المتضمن حقوق المؤلف و الحقوق المجاورة, الجريدة الرسمية , العدد 44 , الصادر بتاريخ 23 جويلية 2003.
- 7- القانون رقم 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الاعلام و الاتصال و مكافحتها , الجريدة الرسمية , العدد 47 الصادرة بتاريخ 16 أوت 2009.
- 8- عاقل فاضلة, الجريمة الالكترونية و اجراءات مواجهتها من خلال التشريع الجزائري, المؤتمر الدولي الرابع عشر "الجرائم الالكترونية" طرابلس , بتاريخ 24-25 مارس 2017.
- 9- المرسوم الرئاسي رقم 15/261 المؤرخ في 08 أكتوبر 2015 يحدد تشكيلة و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها, الجريدة الرسمية للجمهورية الجزائرية, العدد 53 الصادرة في 08 أكتوبر 2015.
- 10- المرسوم الرئاسي رقم 19/172 المؤرخ في 06 جويلية 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها و تنظيمها و كفاءات سيرها , الجريدة الرسمية للجمهورية الجزائرية, العدد 37 الصادرة بتاريخ 09 جويلية 2019.
- 11- بوضياف إسمهان , الجريمة الالكترونية و الاجراءات التشريعية لمواجهتها في الجزائر, مجلة الأستاذ الباحث للدراسات القانونية و السياسية, العدد 11, سبتمبر 2018 .



اللغة الجنائية في الجرائم الالكترونية نمط للتحقيق ووسيلة للإثبات

حاج الله مصطفى

hadjallahmustapha@gmail.com

جمعة محمد

Djemaa.mohamed@univ-medea.dz

مقدمة

شهدت العالم منذ القدم الجريمة على اختلاف أنواعها وأشكالها، فقد واكبت هاته الأخيرة المجتمعات البشرية منذ فجر الخليقة الى يومنا هذا، أين أخذت نمط المجتمع الذي تولد فيه وتتطور تبعا لتطوره، لذلك كانت أنماط الجرائم في تطور مستمر مع تطور الحضارات وظهور تكنولوجيا المعلومات ومختلف الخدمات الالكترونية وهو ما ساهم في تطور الجريمة الالكترونية وسرعة انتشارها في مختلف الأماكن والمؤسسات وأمام هذا التطور المذهل لأنماط ارتكابها وصعوبة كشفها كان لابد من تطور أساليب البحث والتحري والتحقيق والاثبات فيها لتكون مواكبة لها ومساهمة في اكتشاف الجريمة والمجرم، ومنه فقد ظهرت العديد من الأساليب المساهمة في البحث والتحري من بينها علم اللسانيات الجنائية الذي يعتبر نمط جديد لكشف الجريمة وتحقيق العدالة فما هو هذا العلم؟ كيف نشأ وتطور؟ وما أهميته في مجال التحقيق والاثبات الجنائي؟

1. مفهوم التحقيق الجنائي:

قبل التطرق لمفهوم اللسانيات الجنائية كعلم يستعمل في مجال التحقيق الجنائي والاثبات لا بد لنا من معرفة ماهية التحقيق والاثبات الجنائي.

التحقيق لغة هو البحث والتحري عن الحقيقة الخافية ومعرفتها.

أما **اصطلاحا** هو مجموعة من الإجراءات والوسائل المشروعة التي رسمها القانون والتي يتبعها المحقق للوصول الى الحقيقة، والتحقيق علم متمم لقانون العقوبات وقانون أصول المحاكمات الجزائية ويبدأ عادة بإخبار الى الجهات المختصة (بلاغ) لإعلامها بوقوع جريمة وينتهي بتقرير مفصل عن حقيقتها، وبين الاخبار والتقرير تدخل إجراءات التحقيق المختلفة كالكشف والتفتيش والتوقيف والاستجواب... الخ (غازي، 2018، صفحة 4)

- طريقة جمع الأدلة في التحقيق بطريقة كشف الاثار التي يتركها المجرم ومعرفة شكلها ووصفها والتحفظ عليها ثم رفعها وفحصها لمعرفة مادتها وطبيعتها ومدلول كل ذلك بالوسائل العلمية الحديثة التي تشمل العلوم الطبيعية والكيمائية والطب الشرعي وعلم طبائع الاجرام وأسلوب المجرم وتحقيق الشخصية.... الخ

- يعرفه البعض أيضا بأنه علم متمم لقانون الإجراءات والمحاكمات الجزائية يرشد المحقق الى كيفية السير في التحقيق من البداية الى النهاية، ويعلمه كيف يكشف الجرائم الغامضة ويجمع الأدلة المثبتة لوقوعها وكيفية ارتكابها ويرشده بالتالي نحو اقتفاء أثر الجاني والقبض عليه ومحاكمته.

- التحقيق هو مجموعة من الإجراءات والوسائل العلمية والفنية المشروعة قانونا والتي تباشرها السلطة المختصة للكشف عن جريمة وقعت وإزالة الغموض واللبس للوصول للجاني وتقديمه الى المحكمة المختصة. (محمد حمدان، صفحة 5)



2. تعريف الاثبات الجنائي:

من الناحية اللغوية يعرف على أنه اثبات الشيء أي معرفته حق المعرفة فالإثبات لدى علماء اللغة يعني تأكيد وجود الحق بالدليل، فالإثبات هو إقامة الدليل على ادعاء أمام القاضي.

فالإثبات بالشهادة هو: إثبات بأقوال أشخاص يقررون صدور وقائع من غيرهم تثبت حقوقا لأشخاص آخرين.

والإثبات بالشهرة: هو الإثبات بالأمر المشتهر.

الإثبات بالكتابة هو الدليل الخطي أي الاثبات بتقديم دليل مكتوب سواء أكان محررا رسميا أو عرفيا وقد يكون ورقيا أو الكترونيا.

الإثبات شرعا: هو الإتيان بالدليل الذي يثبت الحق أو الواقعة المطروحة أمام القضاء وفقا للطرق المحددة شرعا.

الإثبات قانونا: هو إقامة الدليل لدى القضاء على حقيقة واقعة ذات أهمية قانونية، ونسبتها الى المتهم بالطرق التي حددها القانون، في حين يعرف الإثبات في المواد الجنائية بأنه كل ما يؤدي لإظهار الحقيقة التي تتجلى في وقوع الجريمة بوجه عام ونسبتها للمتهم بوجه خاص. (ثنيان ناصر، 2012، الصفحات 5-6)

3. مفهوم اللسانيات الجنائية: اللسانيات الجنائية أو علم اللغة الجنائي (Forensic Linguistics)

هو العلم الذي يقوم على تحليل دقيق ومنهجي للخصائص الصوتية والبصرية والاجتماعية التي تتميز بها لغة شخص ما يكون مرتبطاً بإحدى الدعاوى القضائية، وتعمل على استخراج نتائج هذا التحليل مجموعة من المتخصصين في حقول لسانية شتى منها: اللسانيات الوظيفية واللسانيات الاجتماعية

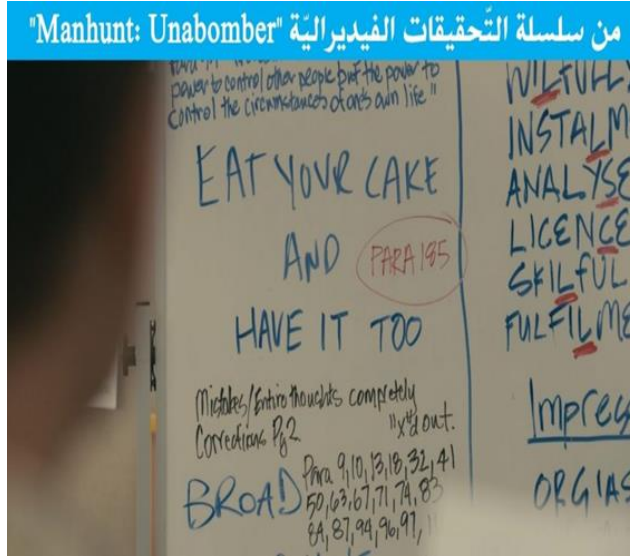
تُسهّم هذه التحليلات في توضيح دائرة المشتبه بهم وهي بذلك تزيد من فعالية العمل الجنائي، ويُعدّ تقييم الاستجابات والتصرّيات القضائية لدى الشرطة وفي المحاكم أبرز مجالات تطبيق هذا العلم، حيث تُقارن هذه التصرّيات لتبيان براءة المشتبه به أو لإعادة تحقيق العدالة في إحدى القضايا. (أنطونوس، 2019)

يقول الدكتور راشد بن حمد البلوشي عميد كلية الحقوق والمتخصص في القانون الجنائي: في بعض الأحيان لا يكون أمام المحقق إلا ورقة مكتوبة تركها الجاني خلفه، وهذا غالباً ما يقع في جرائم التهديد أو قضايا الانتحار هنا يحاول المحقق أن يقرأ بعض العبارات التي يتميز بها الخطاب، في محاولة لاستنباط معلومات منه فقد يشتمل الخطاب على مفردات تستخدم في منطقة معينة دون أخرى.

ويقول المحامي نايف القرني المدير التنفيذي لأحد مكاتب الاستشارات القانونية والمحاماة: ربما تكون هناك مؤشرات على عدم صدق المتهم أثناء التحقيق منها استخدام المتهم لمصطلحات لا يمكن أن تكون مصطلحاته وإنما تم تلقينه إياها ليلقيها أثناء التحقيق، كأن يستخدم مثلاً مصطلحات قانونية بحجة لا يستخدمها عادة إلا أهل المجال والمتهم هنا من خلال مستوى ثقافته وتخصّصه لا يُتصور معرفته بهذا المصطلح قبل التحقيق.

ويضيف إليه البلوشي: إن النص اللغوي قد يمنح المحقق كذلك دلالات عن عُمر الشخص ومستوى ثقافته، ومستواه التعليمي، وقد يكشف في بعض الأحيان عن جنسه أكان ذكراً أم أنثى. وفي الجرائم الكبرى لا يقوم المحقق الجنائي بتحليل النص بنفسه بل يستعين بخبراء من تخصصات مختلفة كعلم الاجتماع أو علم النفس الجنائي.

يُجبرنا المختصون في علوم اللغة عن اللسانيات الجنائية (Forensic Linguistics) أو اللسانيات القضائية كما يميل الأستاذ الدكتور الحواس مسعودي أستاذ بقسم اللغة العربية وآدابها إلى تسميته بوصفه علماً حديثاً يقول الدكتور: يدرس هذا العلم اللغة في إطار تحقيق أو محاكمة لفائدة مصلحة أمنية أو قضائية، ويتمثل الأمر في دراسة النصوص والتسجيلات من طرف مُحقق، ولم تتضح معالم هذا العلم إلا في تسعينيات القرن الماضي في أمريكا، أما في الدول العربية فمازال هذا العلم في مرحلة الطرح تسميةً ودراسةً (خلود، 2019، صفحة 2).

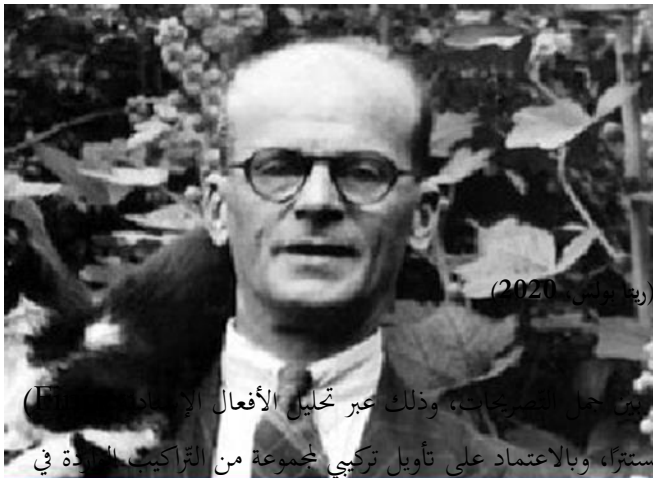


اللِّسانيات أو اللُّغويات Linguistic هي ذلك العلم الذي يهتم بدراسة اللُّغات الإنسانية خصائصها، وتراكيبها ودرجة التشابه فيما بينها أو التباين، فهو يدرس اللُّغة المكتوبة والمنطوقة من جوانبها كافّة، الصَّوتية، والصَّرفية، والتَّركيبية، والدلالية دراسةً شاملة.

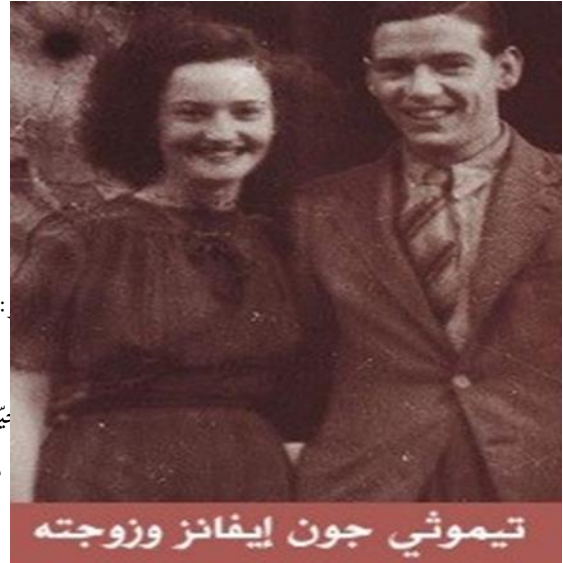
4. تاريخ ظهور المصطلح:

لعلّ مبدأ تحقيق العدالة كان الباعث الأساسي لولادة اللِّسانيات الجنائيّة إذ أبصر هذا المصطلح التّور للمرّة الأولى

عام 1968 عندما استخدمه أستاذ اللِّسانيات جان سفارتفيك في إعادة تحليل تصريحات تيموثي جون إيفانز. كان إيفانز مشتبهًا به بجرمة قتل زوجته وابنته وقد ثُبِّت إدانته فحكمت عليه المحكمة بالموت شنقًا. وبعد تنفيذ حكم الإعدام بثلاث سنوات شرع سفارتفيك يدرس التّصريحات الأربعة التي أدلى بها إيفانز خلال فترة استجوابه لدى الشّركة وقد لاحظ وجود علامات أسلوبية (Stylistics Signs) مختلفة بين التّصريح الأساسي الذي أعلن فيه إقدامه على قتل زوجته وتصريحاته الأخرى الأمر الذي جعلها متناقضة.



"جون كريستي John Christie"

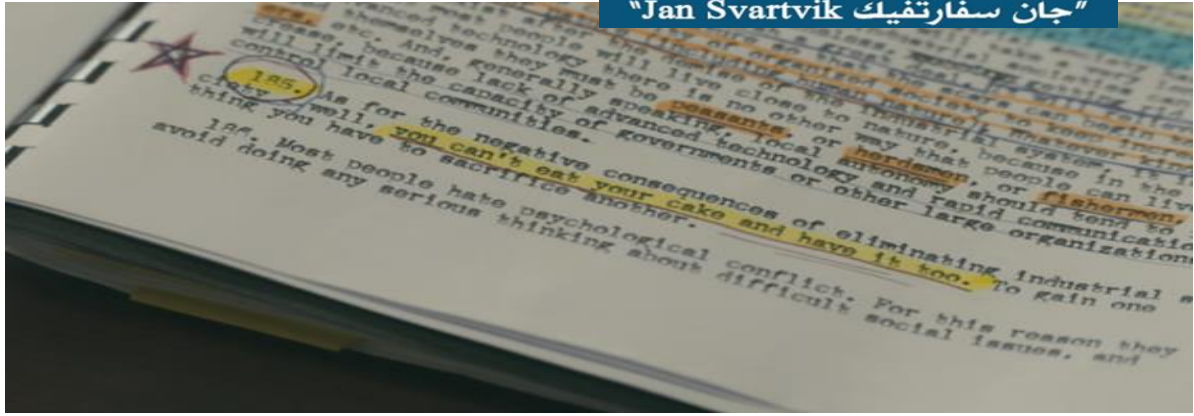


تيموثي جون إيفانز وزوجته

: (ريتا بولس، 2020)
نيّة من أجل التّصريحات، وذلك عبر تحليل الأفعال الإيجابية (F) مستترا، وبالاتماد على تأويل تركيبي لمجموعة من التّراكيب اللُّغوية في



"جان سفارتفيك Jan Svartvik"



نصوص التصريحات ومنها: "جمل صلة الموصول (Relative Clause)، الجمل التي تكثر فيها أدوات الربط وحروف العطف، فضلاً عن الجمل الفعلية حيث يكون المسند إليه مستتراً ومربطاً بتركيب فعلي آخر ورد في تصريح معين من التصريحات الأربعة، تبين أنّ جمل التصريح الأساسي، يكثر فيها استخدام أدوات الربط وحروف العطف مع إبقاء المسند إليه مستتراً. وكأنّ إيفانز كان يحاول إخفاء الفاعل الحقيقي المسؤول عن تلك الجرائم.

وبعد استجواب جون كريستي وهو جار إيفانز تمكّن هذا الأخير من خداع المحكمة مقدّمًا دلائل حاسمة تؤكّد أن إيفانز هو القاتل، وفي الواقع كان كريستي صاحب سجلّ إجرامي طويل وخطير، إذ أقدم على قتل ست نساء بما في ذلك زوجته، وبعد اكتشاف المحكمة الحقيقة وإصدار حكم الإعدام بحقه اعترف بقتل السيدة إيفانز وقد جاء تصريحه بعد تحليله لسانيًا مختلفًا تمامًا عن تصريح إيفانز الذي فشل يومها بإقناع المحكمة بأنّ جاره هو القاتل الحقيقي.

وفيما يلي صورتين لكل من جون إيفانز وزوجته وجون كريستي وسفارتفيك، وبعض الوثائق لكيفية تحليل اللغة. وانطلاقًا من هذه البيانات منحت المحكمة إيفانز عفوًا بعد الوفاة، وإلى الآن تعتبر أعمال سفارتفيك أولى الحالات الرئيسية التي تمّ فيها استخدام اللسانيات الجنائية بهدف إعادة تحقيق العدالة. دفعت أعمال هذا المحقّق إلى إعادة تدقيق كثير من التصريحات حول العالم، وفرضت إجراءات الشرطة المعروفة في ذلك الوقت أن تكون إفادات المشتبه بهم مدوّنة بحسب ورودها حرفيًا على ألسنتهم وليس بأسلوب الإبلاغ، ففي البداية كانت تصريحات الشهود قليلة جدًا وتفتقر إلى التنظيم المنطقي والكرونولوجي فترسل إلى المحكمة بطريقة غير متناسقة، وغالبًا ما كانت هذه الشهادات سريعة للغاية ممّا يؤدي إلى إهمال كثير من تفاصيلها المهمة.



5. كيف تكشف اللسانيات أو اللغة عن الجريمة:

يعتمد علم اللسانيات القضائية في كشف الجرائم على مجموعة من المعارف اللسانية وغير اللسانية أمثال: (الدراسات الصوتية والمعجمية، والصرفية، والتركيبية، والدلالية، واللهجية، وعلم الدلالة، واللسانيات الوظيفية، والاجتماعية، والنفسية، والعصبية، والحاسوبية، والسريية، وعلم الاجتماع، وعلم الجريمة، والقانون... إلخ. حيث يقوم الخبراء الجنائيون بكتابة التقارير عن الوثائق اللغوية (المسموعة والمكتوبة) ذات الصلة القضائية، التي تُسهم بدورها في تكوين الرأي والحكم القضائي في هذه القضايا. ويجب أن نلفت هنا إلى أن تقاريرهم هذه استرشادية لهيئة المحكمة وليست إلزامية. كما يمكنهم -عن طريق استخدام بعض الآليات والإجراءات والتقنيات العلمية- تحليل الوثائق اللغوية ذات الصلة الجنائية، كأن يستخدموا -على سبيل المثال- الأسلوبية الإحصائية في تحديد البصمة الأسلوبية للمؤلفين، وذلك عن طريق النظر في طريقة التخطيط العام للصفحة، واستخدام علامات الترقيم، وطريقة استخدام اللغة، وأفعال الكلام، والكلمات الأكثر دوراً في كلامهم (كثافة المعجم)، وطريقة استخدام المجاز، وكلمات الشكر... إلخ؛ بقصد التعرف على السرقات النصية، ونسبة النصوص إلى أصحابها الأصليين. (ريتا بولس، 2020، الصفحات 7-8).

6. أبرز مجالات تطبيق هذا العلم:

1.6. لغة النصوص القانونية: تشتمل اللسانيات الجنائية في جزء كبير من مجالات تطبيقها، على دراسة النصوص القانونية أو القضائية من زوايا مختلفة منها "نوع النصوص والتدرج المنطقي اللساني في الأحكام القضائية، إضافة إلى تحليل الكلمات المستعملة ودلالاتها المعجمية والنحوية والسياقية". ويتضمن هذا التحليل اللغوي-القانوني، مراجعة الوثائق المتنوعة الصادرة عن هيئات قانونية "كدساتير الدول والأحكام الشرعية والوصايا الخاصة وأحكام المحكمة واستدعاءاتها والقوانين الصادرة عن الدوائر الحكومية". ومن أبرز هذه الوثائق "قانون حمورابي"، الذي يعد أهم وثيقة قانونية تم العثور عليها وذلك لاكتمال نصوصها. وتجدر الإشارة إلى اعتبار أي نص أو عنصر من اللغة نصاً قضائياً، عندما يُستخدم في سياق قانوني أو جنائي.

2.6. المكالمات الطارئة: يشكل هذا المجال ميدان اختبار لقدرة المتخصص في علم اللغة الجنائي على اكتشاف الأحداث التي يمر بها المتكلم، وذلك عبر استخراج المعلومات اللغوية التي تدل على حالات معينة من قبيل التهديد مثلاً. ومن الأمور المهمة في تحليل المكالمات الطارئة وفق آليات اللسانيات الجنائية: ارتفاع الصوت وانخفاضه، نبرة الصوت ونغمته، والمدى الصوتي الذي يدل على أن هناك تدخل طرف ثالث في الاتصال على سبيل المثال، إن إلحاح المتكلم عبر تكرار الكلمات نفسها، يلعب دوراً مهماً في الكشف عن حالته وكذلك أيضاً التردد وعلامات التهرب والإجابات غير الكاملة أو القصيرة جداً...

هذه الأمور قد تدل على أن المتصل مخادع أو تحت تهديد معين، كما أن استخدام نبرة صوت عالية في نهاية كل جملة يدل على عدم الصدق، لأن ارتفاع الصوت في نهاية الكلام هو حيلة دفاعية لإخفاء معلومات معينة. بينما يتميز الاتصال العادي بتشابه الكلمات وبصفاء نبرة الصوت بشكل يثير لدى المتلقي، نوعاً من الثقة أو اليقين بأن المتصل به سيزوده بمعلومات دقيقة وواضحة.

3.6. طلبات الفدية أو الرسائل والاتصالات التهديدية: التهديد هو الأسلوب الذي يرافق طلب الفدية. وفي القضايا التي لا يوجد فيها مشتبه بهم، قد يكشف فحص الأدلة اللغوية، عن معلومات إثنية دينية أو اجتماعية محتملة عن المهدّد. أما في المواقف التي توجد فيها مجموعة محدودة من المشتبه بهم، فقد تساعد المقارنة والمباشرة (Analogy) بين لغة التهديد من جهة والوثائق المكتوبة لكل مشتبه به من جهة أخرى في تضيق نطاق مجموعة المشتبه بهم (أنطونيوس، 2019).

4.6. الرسائل الانتحارية: غالباً ما تكون الرسالة الانتحارية قصيرة ومختصرة جداً أقل من 300 كلمة وتتميز هذه الرسائل عادةً بالوضوح والدقة. تكون الرسالة موجهة إلى المرسل إليه (أو المرسل إليهم)، بحيث تُذكر أسماءهم بشكل صريح، وهم على علاقة معينة



مع المرسل. تحتوي الرسائل الانتحارية على جمل، تشير إلى طريقة الانتحار أو الوسيلة المعتمدة. وقد تشتمل على كلمات وعبارات لا تستعمل سوى بين المرسل والمرسل إليه. وهي تحمل عادةً مدلولات حميمية، النية من إيرادها جعل المرسل إليه يشعر بالذنب.

7. أهمية اللغة واللسانيات الجنائية:

من المعلوم أن اللغة تتداخل في مختلف أنشطتنا اليومية وبشكل مكثف، ومن ثم فلا غرابة أن تكون محور الاهتمام في المجالات العامة، يضاف إلى ذلك أنه لا بد من دراسة اللغة وتحليلها في المجالات الحديثة التي استثمرت في العالم المتقدم وبقية للأسف غير مستغلة في العالم العربي بالشكل الذي يتناسب مع أهميتها، فهناك جرائم تحدث وقد يكون المتاح لدينا اللغة فقط، مثل جرائم العنصرية اللفظية كإطلاق الأوصاف الغير لائقة والسب على فئة أو ديانة أو عرق أو جنس، وهناك جرائم يمكن لنا لو تأملنا لغة التواصل بين أطرافها لوجدنا ما يمكن أن يفيدنا في تحليل الحدث والتوصل إلى نتائج مفيدة، هذه الجرائم التي لا يمكن لنا تجاهل الدور الحيوي للتحليل اللغوي واللساني فيها، ويمكننا الإشارة إلى مقولة لكاتب الإنجليزي إدوارد بولير ليتون 1839 التي يشير فيها إلى قوة القلم أو ما يعرف الآن بالقوة الناعمة للإعلام واللغة المكتوبة في مقابل القوة الجسدية وقوة السلاح قائلا:

" the pen is mightier than the sword " أي: القلم أمضى من السيف.

فيما يلي قصة واقعة إجرامية يبرز لنا أهمية اللغة في التحقيق الجنائي حيث وفي أحد الأيام سطا شخصان على محل تجاري فحاصرها رجال الشرطة وكان بجوزتهما سلاح (مسدسان)، فطلب رجال الشرطة إلقاء السلاح فقال أحدهما لزميله: أطلق المسدس، فأطلق النار على رجال الشرطة وقتل أحد الرجال ثم اشتبك الجميع وألقي القبض على اللصين (القاتل وزميله)، ولما بدأت المحاكمة احتج محامي القاتل الذي أطلق النار بأن زميله أمره بإطلاق النار فهو إذا شريكه في جريمة القتل، في المقابل احتج محامي اللص الآخر (الذي قال لصاحبه أطلق المسدس) ببراءته في جريمة القتل لأنه كان يقصد إطلاق المسدس وألقه واره لهم وليس القصد إطلاق الرصاص أو إطلاق النار من المسدس، فالملاحظ هنا أن الجدل جدل لغوي يدور حول اللغة ويغوص في استخدامها وفي النية حول استخدامها وهو ما يبر أهمية وجود العلم (علم اللسانيات الجنائية) في حد ذاته. (العصيمي، 2020، الصفحات 36-37)

خاتمة:

إن التطور الكبير والسريع والمتواصل الذي تشهده المجتمعات في مختلف المجالات من بينها مجال الجريمة عامة والجريمة الالكترونية خاصة، ألزم أهل العلم والاختصاص مواكبة هاته التطورات من خلال تقديم دراسات جادة وأساليب مستحدثة وعلوم متنوعة حول سبل مكافحتها والحد من خطورة انتشارها، في سبيل ذلك لا بد أيضا من تطوير وسائل التحقيق والاثبات وعدم اقتصرها على وسائل تقليدية وامكانيات بسيطة تزيد من صعوبة الوصول للجاني وتقديمه للعدالة من بينها علم اللسانيات الجنائية الذي أحدث قفزة نوعية في مجال التحقيق والاثبات الجنائي، حيث أصبح الكلمة المسموعة أو المكتوبة لها أهمية كبيرة في كشف مجرم أو جريمة.

قائمة المراجع

أنطونيوس، ن. (2019). جوان 13. (اللسانيات الجنائية تحقيق العدالة عن طريق اللغة Consulté le 8 أفريل 2021, sur الموقع العربي

الالكتروني " معنى: <https://mana.net/linguistics> "

ثنيان ناصر، آ. (2012). إثبات الجريمة الالكترونية. الرياض، كلية الدراسات العليا، السعودية: جامعة نايف العربية للعلوم الأمنية.

حنين، غ. (2018). محاضرات في التحقيق الجنائي .

خلود، أ. ف. (2019). نوفمبر 19. (المحقق الجنائي والنص اللغوي. اللغة دليلا جنائيا 2. Récupéré sur 6(1), المحقق الجنائي والنص اللغوي.

ريتا بولس، ش. (2020). جانفي 20. (كيف تكشف اللسانيات القضائية المجرم 7-8. جريدة الخبر- Récupéré sur <https://www.al-khabar.co/arabic/ar/2020/01/20/>

[khabar.co/arabic/ar/2020/01/20/](https://www.al-khabar.co/arabic/ar/2020/01/20/)



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها

رمز I05L02UN260120190001

غازي, ح. (2018). محاضرات في التحقيق الجنائي.

فهد بن صالح العصيمي. (2020). اللسانيات الجنائية: تطبيقاتها ومجالاتها (الإصدار ط1). الرياض: مركز الملك عبد الله بن عبد العزيز لخدمة اللغة.

محمد حمدان, ع. (s.d.). أساليب البحث والتحقيق الجنائي /العدد 5. قسم المناهج, فلسطين.



إجراءات البحث والتحري في الجرائم الإلكترونية

ط.د. عبد النور سعيداني

جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة

د. ليندة بومحراث

جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة

مقدمة:

لقد تطورت الجريمة بتطور وسائل الاتصال الحديثة، خصوصا أنها أصبحت تقع في العالم الافتراضي، مما زاد الأمر تعقيدا وصعوبة على الجهات القضائية هذا من جهة، ومن جهة أخرى أن هذا النوع من الجرائم يتطلب تقنيات عالية من أجل فك ملامسات ارتكابها، وفي ظل الخروقات التي ترتبت عن تهديد الحياة الخاصة للأفراد، والخسائر الناجمة عن ولوج برامج وأنظمة الشركات والأشخاص المعنوية العمومية وخاصة منها الاقتصادية، كان لا بد من وضع إجراءات قانونية خاصة في مرحلة البحث والتحري، تمنع أو تقلص من ارتكاب الجرائم الإلكترونية، هذا ما جعلنا نطرح الإشكال الرئيسي التالي:

هل إجراءات البحث والتحري الخاصة بالجرائم التقليدية استطاعت معالجة الجرائم الإلكترونية أم أن هذه الأخيرة تتطلب نوع خاص من الإجراءات من أجل التعرف على مرتكبيها؟

وتندرج تحت هذه الإشكالية الرئيسية مجموعة من التساؤلات الفرعية أهمها:

- ما مفهوم الجرائم الإلكترونية؟.
 - ما هي الجهات المختصة بإجراء البحث والتحري في الجرائم الإلكترونية؟.
 - ما هي آليات المتابعة الإجرائية في مرحلة البحث والتحري للكشف عن الجرائم الإلكترونية؟.
- خطة البحث:

المطلب الأول: مفهوم الجرائم الإلكترونية.

المطلب الثاني: الاجراءات العامة للبحث والتحري في الجرائم الالكترونية.

المطلب الثالث: الاجراءات الخاصة للبحث والتحري في الجرائم الإلكترونية.

1. مفهوم الجرائم الإلكترونية:

نظرا لحدثة الجرائم الإلكترونية وارتباطها بوسائل الاتصال الحديثة كان لا بد من إيجاد مفهوم لها، وبما أن مثل هذه الجرائم تقع على عدة أشياء مادية ومعنوية مما جعلها تصنف إلى عدة أنواع حسب ما تقع عليه، كما اتسمت بمجموعة من الخصائص تميزها عن غيرها من الجرائم، بالإضافة إلى أن المشرع حدد الأركان التي تقوم عليها الجرائم الإلكترونية.

1.1. تعريف الجرائم الإلكترونية:

لقد اختلفت التسميات المطلقة على الجرائم التي ترتكب بواسطة أجهزة الإعلام الآلي بين الفقهاء فمنهم من يطلق عليها جرائم الحاسب الآلي، والبعض يطلق عليها جرائم الكمبيوتر فيما يطلق عليها آخرون الغش المعلوماتي.



1.1.1.1. التعريف الضيق والموسع للجرائم الإلكترونية:

لقد اختلف فقهاء القانون حول تعريف الجرائم الإلكترونية فمنهم من ركز على الجانب المعنوي والذي يقصد به البرامج التي تنفذ عن طريق الحاسب الآلي، وهناك من ركز على الجانب موسع والذي يعني جميع السلوكيات غير المشروعة المرتكبة بواسطة الحاسب الآلي أيضا.

1.1.1.1.1. التعريف الضيق للجرائم الإلكترونية:

اختلف الفقه في تعريف الجريمة الإلكترونية من جهة نظر ضيقة، فمنهم من اعتمد معيار الوسيلة المستعملة، ومنهم من اعتمد معيار توافر المعرفة بتقنية الحاسب الآلي ومنهم من يرى أن الجريمة الإلكترونية هي التي يكون موضوعها المال المعلوماتي المعنوي¹.

1.1.1.1.1.1. معيار وسيلة ارتكاب الجريمة:

يرى البعض أن الحاسب الآلي هو أساس هذه الجريمة ويميزها عن غيرها من الجرائم بوسيلة ارتكابها. ومن أنصار هذا الرأي "مارو" الذي عرف الجريمة الإلكترونية بأنها: " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"ⁱⁱ.

2.1.1.1.1. معيار توفر المعرفة بتقنية المعلوماتية:

يستند أصحاب هذا الاتجاه إلى معيار شخصي يستوجب أن يكون الفاعل ملما بتقنية المعلومات واستخدام الحاسب الآليⁱⁱⁱ. ولذا عرفها دافيد تومسون بأنها: " أية جريمة يكون مطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"^{iv}. وقد عرفها سترين سكجوبر (STRIN SCKJOBR) بأنها: " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمركبه"^v.

3.1.1.1.1. معيار موضوع الجريمة:

يرى آخرون أن تعريف الجريمة الإلكترونية إنما يرجع إلى موضوعها وغير متعلق بالوسيلة المستعملة أو الفاعل، حيث يرى هؤلاء أن الجريمة هي التي يكون موضوعها المال المعلوماتي المعنوي، دون النظر فيها إذا كان الحاسب هو الأداة المستعملة في ارتكابها من عدمه^{vi}. وعرفها فريق آخر من الفقه بأنها: " كل فعل متعمد أي كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالجني عليه أو كسب يحققه الفاعل"^{vii}.

2.1.1.1. التعريف الموسع للجرائم الإلكترونية:

يوسع البعض مفهوم الجريمة المعلوماتية لتشمل إساءة استخدام الحاسب (Computer abuse) التي عرفوها: " أي فعل متعمد مرتبط بأي وجه بالحسابات، يتسبب في تكبد أو إمكانية تكبد الجاني عليها لخسارة، أو الحصول أو إمكانية حصول مرتكبه على مكسب"^{viii}. ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها: " كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر"^{ix}.

2.1.1. تعريف الجرائم الإلكترونية في التشريع الجزائري:

المشرع الجزائري لم يعرف الجريمة الإلكترونية وإنما تبنى للدلالة على الجريمة الإلكترونية، مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة، حيث يمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لا بد من تحققه حتى يمكن توافر أركان الجريمة، كما لم يتطرق قانون العقوبات الجزائري المعدل والمتمم لتعريف جرائم الإنترنت، بل اكتفى بالعقاب على بعض الأفعال تحت عنوان الجرائم الماسة بنظام المعالجة الآلية للمعطيات^x.



فقد تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجرمية لقمع الاعتداءات الواردة على المعلوماتية^{xii}. وهذا يظهر واضحا من خلال نص المادة الثانية (02) الفقرة الأولى من القانون رقم 04-09 الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي جاء فيها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"^{xiii} فقد جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، وهذا ما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات والذي أفرد القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 8 مواد من المادة 394 مكرر وحتى المادة 394 مكرر 7^{xiii}. كما استحدث المشرع الجزائري القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و المتخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها^{xiv}. ويقصد بمفهوم هذا القانون بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال^{xv}.

2.1. أنواع الجرائم الإلكترونية:

توجد عدة تصنيفات للجرائم الإلكترونية وأبرز هذه الجرائم، الجرائم الواقعة على الأموال، أو على الأشخاص، أو على أمن الدولة.

1.2.1. الجرائم الواقعة على الأموال:

تنقسم الجرائم الواقعة على الأموال باستعمال الأنظمة المعلوماتية إلى ثلاث جرائم وهي: جرائم غسل الأموال والمخدرات، جرائم التجارة الإلكترونية، جرائم السرقة والنصب أو الاحتيال.

1.1.2.1. جرائم غسل الأموال و المخدرات:

سنفصل في جرائم غسيل الأموال أولا ثم جرائم المخدرات.

1.1.1.2.1. جرائم غسل الأموال:

توجد عدة أساليب يلجأ إليها المجرمون فيما يخص غسيل الأموال، وتختلف حسب نوعية الأموال المقصود غسلها ومن بين هذه الأساليب نجد ما يلي:

- شراء الأصول مثل الطائرات، السيارات، القطارات و القوارب وتسجيلها بأسماء آخرين.
- النقود الإلكترونية وتعتبر هذه التقنية نتيجة التطور الهائل في المجالات الإلكترونية والمصرفية، حيث تمكن من استخدام البطاقات الذكية (Smart Carde)، دون مخاطرة أو تكاليف مرتبطة بعملية التبادل دون وسيط كما تتميز بسرعة الحركة والتغيير^{xvi}.

2.1.1.2.1. جرائم المخدرات:

تختلف جرائم المخدرات على شبكة الأنترنت والحواسب الآلية حسب طريقة الاستعمال، فهناك من يستعمل الأنترنت للإنتاج وآخرون للبيع أو الاستخدام عبرها، ونذكر كالاتي:

1.2.1.1.2.1. إنتاج المخدرات على الإنترنت:

يوفر الوصول للإنترنت كميات كبيرة من المعلومات تتعلق بإنتاج المخدرات بما في ذلك من عمليات ووصفات ومكونات ومقادير، وهذه المعلومات متوفرة لصغار السن والمراهقين والمتعاطين. وإن هذه المعلومات ليست بالضرورة أن تكون دقيقة وصحيحة فالمعلومات



الخاطئة قد تقود إلى اصابات خطيرة أو أمراض أو حتى أحيانا قد تؤدي للوفاة. كما أن أدوات الانتاج متوفرة عبر الإنترنت والمواد الكيميائية اللازمة لإنتاج المادة المخدرة متوفرة أيضا، وحتى أن هذه المواد والمعدات رخيصة الثمن^{xvii}.

2.2.1.1.2.1. استخدام المخدرات على الإنترنت:

تحتوي الإنترنت كميات هائلة من المعلومات تتعلق بآثار استخدام المخدرات وطرائقها والتحذيرات حولها، وعن أي نوع يفكر فيه المتعاطي أو أي فرد على الإنترنت حيث أن هناك العديد من المواقع تشجع على خلق ثقافة استخدام المخدرات و إغواء الشباب بمثل هذا الاستخدام خاصة عند ربطها بموضوع الإثارة الجنسية.

3.2.1.1.2.1. بيع المخدرات على الإنترنت:

تباع المخدرات سواء القانونية منها أو غير القانونية بشكل واسع على الإنترنت، وغالبا ما تتم الصفقات للمخدرات غير الشرعية عبر لوحات النقاش وغرف الدردشة بلغة مشفرة، وترسل المخدرات إلى عنوان المعني كما أنه يمكن تقديم المعلومات اللازمة لإنتاجها في المنزل^{xviii}.

2.1.2.1. جرائم التجارة الإلكترونية:

تتعدد وتنوع الجرائم الواقعة على التجارة الإلكترونية، وينحصر أغلبها في:

- الاعتداء على التوقيع الإلكتروني.
- السطو على أرقام البطاقات الائتمانية.
- الاعتداء على حقوق الإنترنت^{xix}.

3.1.2.1. جرائم السرقة والنصب والاحتيال:

تتم جرائم النصب والاحتيال الإلكتروني بطرق وأشكال متنوعة ومدروسة للنصب والاستلاء على أموال الآخرين ولعل أبرزها ما تم عن طريق مواقع التواصل الاجتماعي خاصة (فيسبوك و تويتر) كونه أداة سهلة للتلاعب بالآخرين لسرقة أموالهم، وهذا ما أدى إلى وقوع الكثير من مستخدمي هذه المواقع فريسة الاحتيال والنصب عليهم، ومن أشهر حالات النصب عبر مواقع التواصل الاجتماعي الاحتيال في التسويق الإلكتروني، الاحتيال في عروض الوظائف، الاحتيال عبر التسول الإلكتروني، الاحتيال عبر أسئلة الامتحان^{xx}.

2.2.1. الجرائم الواقعة على الأشخاص:

من أبرز الجرائم الواقعة على الأشخاص بواسطة البرامج المعلوماتية، جرائم الاعتداء على حياة الخاصة عبر الإنترنت، وجرائم الدم والقذف والتحقيق عبر الأنترنت.

1.2.2.1. جرائم الاعتداء على حياة الخاصة عبر الإنترنت:

لقد حاول بعض الفقهاء وضع تعريف للحق في الحياة الخاصة فقد عرف الفقيه (Martin) الحق بالحياة الخاصة بأنه: "الحق بالحياة الأسرية والشخصية والداخلية والروحية لشخص عندما يعيش وراء باب مغلق"^{xxi}.

وتعتبر الخصوصية من المبادئ العامة التي تقرها الدساتير أيضا لتضمن حماية حرمة الحياة الخاصة للمواطن، فجميع الأشخاص الحق في أن تظل أسرار حياتهم الخاصة مصانة عن العلن وتدخلات الغير وعلمه، و اعتداءاته عليها، وزادت أهمية حماية الحياة الخاصة إزاء تطور وسائل التواصل وانتشارها ل يتم استخدام الوسائل المعلوماتية في هذا الجانب^{xxii}.

2.2.2.1. جرائم الدم والقذف والتحقيق عبر الإنترنت:



تعد جريمة السب والقذف والتعرض للحياة الشخصية للأفراد بغرض التشهير والخوض في أعراضهم، من أكبر الجرائم التي تم تجريمها في كافة القوانين، سواء في الدول العربية أو الدول الأجنبية، وترجع أسباب التجريم إلى تحريج الأشخاص في أعراضهم ومبادئهم وشرفهم ونسب أمور غير صحيحة إليهم بغرض التشهير بهم والخوض في أعراضهم وفي حياتهم الخاصة^{xxiii}.

والجرائم تتم إما عبر البريد الإلكتروني أو عن طريق شبكة الويب حيث ترتكب جريمة الدم والقذف إذا قام المعتدي بإسناد مادة للعلنية، أو بإسناده حكما أو صفة عامة في القذف إلى المعتدى عليه في أحد مواقع الشبكة الإلكترونية أو عن طريق مجموعات الأخبار كما يلاحظ أن صور الدم والقذف يمكن أن تمارس من خلال مجموعات الأخبار في نشر التعليقات والمشاركة على مواضيع منشورة، وتحقق علنية الدم والقذف إذا كانت رؤية ما يرد في الرسائل والتعليقات متاحة للجميع في مجموعات الأخبار أو عبر غرف الدردشة والمحادثة.

3.2.1. الجرائم الواقعة على أمن الدولة:

لقد أصبحت عدة دول أمنها مهدد بفعل التطور التكنولوجي الحاصل، وتنوعت الجرائم في هذا المجال بحسب طبيعتها، ومن بين أهم الجرائم الواقعة في على أمن الدولة، جريمة التجسس، جرائم الإرهاب، الجريمة المنظمة.

1.3.2.1. جريمة التجسس:

التجسس هو الاطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر وليس مسموحا لغير المخولين بالاطلاع عليها. وقد سهلت شبكة الإنترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية و الوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاث أهداف رئيسية وهي: التجسس العسكري، التجسس السياسي، والتجسس الاقتصادي، كما تستخدم العديد من الدول التجسس باستخدام التقنية المعلوماتية، وهذه الأنشطة تمارس من قبل دولة على دولة أو دول أخرى، أو من قبل الدول على مواطنيها، أو من قبل شركة على شركات أخرى منافسة^{xxiv}.

2.3.2.1. جرائم الإرهاب:

يتم بث ثقافة الإرهاب عبر الإنترنت والوسائل الحديثة عن طريق تأسيس مواقع افتراضية تمثل المنظمات الإرهابية وهي مواقع آخذة في الازدياد مع ازدياد المنظمات الإرهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى الهجمات التي ارتكبت، أو بيانات تنفي أو تعلق على أخبار صادرة من منظمات أو جهات دولية أخرى. وتجنّد الجماعات الإرهابية من خلال الإنترنت عبر وسائل وأنظمة الحواسيب الآلية عناصر إرهابية جديدة تساعدهم على تنفيذ أعمالهم الإجرامية، وهم في ذلك يعتمدون على فئة الشباب خصوصا ضعاف العقل والفكر^{xxv}.

3.3.2.1. الجريمة المنظمة:

الجريمة المنظمة ليست وليدة التقدم وإن كانت استفادت منه، فالجريمة المنظمة بسبب تقدم وسائل الاتصال والتكنولوجيات الحديثة أصبحت غير محدودة لا بقيود الزمان ولا بقيود المكان، وأصبح انتشارها على نطاق واسع وكبير كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة على وسائل الإنترنت في تخطيط وتمويل وتوجيه المخططات الإجرامية بسهولة، فقد اكتشفت هذه الجماعات أن استخدام شبكات الإنترنت والتكنولوجيا تستطيع أن تؤمن فرص جديدة وفوائد حية لأعمالهم وأرباح غير مشروعة عما يقومون به^{xxvi}.

3.1. خصائص الجرائم الإلكترونية:



تتميز الجريمة الإلكترونية بخصائص جعلتها تختلف عن الجريمة التقليدية، وذلك لتعلقها وارتباطها بشبكة الأنترنت ومن بين هذه الخصائص نجد مايلي:

1.3.1. صعوبة اكتشاف الجريمة:

الجريمة الإلكترونية من الجرائم التي ترتكب في الخفاء مما يزيد صعوبة، حيث يتم نقل البيانات والمعلومات في شكل نبضات إلكترونية. كما أن هذه الجرائم في الغالب الأعم تكون منظمة، وترتب وتنفذ وتقس إقليم أكثر من دولة واحدة لاستخدامها شبكة الاتصالات العالمية (الإنترنت)، أضف إلى ذلك امكانية تدمير الدليل في مدة قياسية، ومن بين الأسباب التي تؤدي إلى صعوبة اكتشافها صعوبات تعود الى الجاني وأخرى إلى المجني عليه^{xxvii}.

1.1.3.1. صعوبات تعود إلى الجاني:

قد يكون المجرم في الجريمة الإلكترونية شخصا طبيعيا يعمل لحسابه الخاص ويهدف إلى تحقيق مصلحة شخصية له، ولكن في الغالب يقوم بهذا الفعل لحساب أحد الأشخاص المعنوية (شركة عامة أو خاصة) تستند في عملها على تكنولوجيا المعلومات، بغية السطو على أحد الأنظمة المعلوماتية أو اضرار بالغير^{xxviii}.

2.1.1.3.1. صعوبات تعود إلى المجني عليه:

المعتدى عليه في الجريمة الإلكترونية هو من يكون ضحية الاعتداءات غير المشروعة على مكونات الحاسوب، وقد يكون شخصا طبيعيا أو شركة أو مؤسسة تتعامل بمجال الحاسوب أثناء ممارسة الأعمال التجارية، والاقتصادية والسياسية التي ينبغي أن تستغل الحاسوب في إدارة أعمالها^{xxix}.

توجه هذه الجرائم بصفة خاصة إلى البنوك والمواقع الإلكترونية للمؤسسات المالية، لأن القطاعات المستهدفة من الجريمة الإلكترونية هي التي تعتمد أكثر من غيرها على أجهزة الحاسوب وملحقاته وتعتبر تلك البنوك من أهم القطاعات وأكثرها تضررا^{xxx}.

2.3.1. صعوبة إثبات الجريمة:

الجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة. ما يجعل فكرة مسرح الجريمة في الجريمة الإلكترونية يتضاءل دوره في الافصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين:

- الأول: أن الجريمة المعلوماتية لا تخلق أثارا مادية.

- الثاني: أن كثيرا من الأشخاص يترددون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي فترة طويلة نسبيا، الأمر الذي يعطي مجالا للجاني أو للآخرين، أن يغيروا أو يتلفوا ويعبثوا بالأثار المادية إن وجدت، الأمر الذي يولد الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية^{xxxi}.

2. الاجراءات العامة للبحث والتحري في الجرائم الالكترونية:

يختص وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها^{xxxii}.

إن الجريمة الإلكترونية كغيرها من الجرائم تتطلب إجراءات قانونية عامة من أجل فك ملامساتها، والتي تتمثل في الإجراءات المادية، والإجراءات الشخصية بالإضافة إلى إجراءات تقنية.



1.2. الإجراءات المادية:

تتضمن الإجراءات المادية المعاينة التقنية للوقوف على كيفية ارتكاب الجريمة، وكذا التفتيش المعلوماتي من أجل الحصول على الأدلة الكافية المتعلقة بالجريمة في حد ذاتها.

1.1.2. المعاينة التقنية:

نصت المادة 79 من الأمر رقم 66-155 المتضمن ق.إ.ج.ج والتي نصت على أنه: "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها...".^{xxxiii}

كما يقصد بالمعاينة فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، كمعاينة مكان ارتكاب الجريمة أو أدواتها، والمعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على ما يقتضيه إجرائها من مساس بحقوق الأفراد، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال، وإذا اقتضت دخول مسكن له حرمة خاصة كانت إجراء تحقيق.^{xxxiv}

1.1.1.2. إجراءات المعاينة التقنية:

تتمثل إجراءات المعاينة التقنية في الانتقال إلى مسرح الجريمة لمعاينته وتأمينه.

1.1.1.1.2. الانتقال إلى مسرح الجريمة:

تتم المعاينة في الجريمة الإلكترونية المرتكبة عبر الإنترنت أو بواسطة الحاسب الآلي كأى جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية، إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني.^{xxxv}

ومن بين التدابير الفنية والتحفظية التي تساعد المحقق على المعاينة الإلكترونية هي كالاتي:

- الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد وموقع الأجهزة الإلكترونية وشبكاتها وسائر ملحقاتها والنهائيات الطرفية المتصلة بها المتوقع مدامتها.
- توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتأمين وحفظ المعلومات.
- التحفظ على محتويات سلة المهملات ومستندات الادخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.

- إعداد فريق من المتخصصين وأهل الخبرة في مجال تكنولوجيا الإعلام الآلي للاستعانة بهم عند الحاجة.^{xxxvi}

2.1.1.1.2. تأمين مسرح الجريمة:

من أجل ضمان حماية وتأمين لمسرح الجريمة الواجب مراعاة بعض الضوابط التالية:

- تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.
- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف، حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها وتأمينها.
- إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.
- أن تقتصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر فيهم الكفاءة العملية والخبرة الفنية في مجال الحواسيب.^{xxxvii}



2.1.2. التفتيش:

التفتيش هو: "إجراء من إجراءات التحقيق تقوم به سلطة مختصة حددها القانون، يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحزمة^{xxxviii}."

التفتيش في الجريمة الإلكترونية إجراء يحتاج إلى تقنيات خاصة، لأن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات الحاسوب ومجال إخفاء المعلومات فيها لأنه يسهل إتلافها جزئيا أو كليا، ويصعب تحديد مكان الدليل من حيث أنه داخل النظام أم على دعامة خارجية، وقد تكون الملفات مشفرة لا يظهر محتواها إلا بفك التشفير، وقد تكون البيانات التي تثبت حصول الفعل جزءا من نظام حاسوب يقع خارج الحدود في دولة أخرى، كل هذه الحقائق وغيرها يجعل تحديد السبب الموجب للتفتيش أمرا صعبا، ويجعل من تقديم وصف محدد لمحل التفتيش أمرا أكثر صعوبة^{xxxix}.

1.2.1.2. الشروط القانونية للتفتيش في الجرائم الإلكترونية:

من أجل القيام بعملية التفتيش في الجرائم الإلكترونية لا بد من توافر مجموعة من الشروط الشكلية والموضوعية.

1.1.2.1.2. الشروط الشكلية:

وهي شروط ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء حفاظا على الحريات الفردية من التعسف أو الانحراف في استخدام السلطة^{xl} وهي كالآتي:

1.1.1.2.1.2. الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في البيئة الإلكترونية:

يعتبر هذه الإجراء من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم، حيث أن المتهم هو الشخص الذي يستوجب القانون حضوره عند إجراء التفتيش، إذ أن الإجراء المتخذ بمسه هو، غير أنه قد لا يتسنى للمتهم الحضور في حال كان محل التفتيش مسكنه، فمن أجل ذلك أجاز القانون له أن يُنيب عنه غيره ليجري التفتيش في حضوره، وإلا وجب استدعاء شاهدين في بعض الأحوال، كما يحق للمتهم أن يستعين بمحاميه عند إجراء التفتيش، ومن ثم يجوز للمحامي الحضور أيضا، كذلك إذا جرى التفتيش لدى غير المتهم وجب إتاحة الفرصة لحائز المكان في الحضور رعاية لمصالحه، ويجوز للمشرع للنيابة العامة أيضا حق الحضور أثناء التفتيش الذي يجريه قاضي التحقيق^{xli}.

2.1.1.2.1.2. موعد إجراء التفتيش في الجرائم الإلكترونية:

اختلفت التشريعات الإجرائية في وضع مبدأ موحد يخص الميعاد الزمني للتفتيش لنظم المعلوماتية، فمنها من حظر القيام بهذا الإجراء في أوقات معينة في الليل مثلا، وهنالك من قرنه بوقت معين حرصا على تضيق نطاق الاعتداء على الحرية الفردية وحرمة المساكن، وهنالك من تركه على مطلقه يتم في أي ساعة من ساعات الليل والنهار وترك السلطة التقديرية في ذلك للقائم أو للسلطة المكلفة بالتفتيش^{xlii}.

أما عن المشرع الجزائري فقد تطرق إلى هذه الجزئية من خلال نص المادة 47 من ق.إ.ج.ج.، والتي جاء فيها: "عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".



3.1.1.2.1.2. محضر التفتيش في الجرائم الإلكترونية:

باعتبار أن التفتيش عمل من أعمال التحقيق، فينبغي تحرير محضر يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما، ثم ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسوب والإنترنت يرافقه للاستعانة به في صياغة مسودة محضر التفتيش^{xliv}

2.1.2.1.2. الشروط الموضوعية:

وهي الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاث شروط أساسية هي السبب، المحل، والسلطة المختصة بالقيام بالتفتيش^{xliv}.

1.2.1.2.1.2. سبب التفتيش في البيئة الإلكترونية:

فالسبب هو وقوع الجريمة جناية أو جنحة، وتوافر أمارات قوية وقرائن على وجود دليل يفيد في كشف الجريمة لدى المتهم أو غيره وهذا السبب لا ينشأ إلا بعد وقوع الجريمة، واتجاه قرائن الاتهام ضد شخص، أو وجود أمارات قوية ضد آخر على حيازته ما يفيد في كشف الحقيقة^{xliv}.

2.2.1.2.1.2. محل التفتيش:

يشترط كذلك لصحة ومشروعية التفتيش في الجريمة الإلكترونية أن ينصب على محل بحيث يشترط أن يكون محددا أو قابلا للتحديد ويكون مشروعا يرد على محل جائز قانونا. كالمكونات المادية والمعنوية للكمبيوتر وملحقاته وبرامجه، الهاتف الذكي وشبكات الاتصال عن بعد، كما نشير إلى استثناء بعض الأشخاص والأماكن من التفتيش مثل أشخاص ومسكن وسيارات أعضاء السلك الدبلوماسي وأعضاء المجالس النيابية، ومكاتب المحامين لتمتعهم بالحصانة، وعليه فأى تفتيش لها يعد منافيا للقانون ومآله البطلان^{xlvi}.

3.2.1.2.1.2. السلطة المختصة بالقيام بالتفتيش:

إن التفتيش إجراء قاصر على السلطة المختصة به وهي قاضي التحقيق والنيابة العامة، فالنيابة العامة توجه الاتهام وقاضي التحقيق يباشر الإجراءات بما فيها التفتيش. كما أنه يجوز لقاضي التحقيق القيام بإجراء التفتيش في أي مسكن يرى أنه توجد به أشياء من شأنها أن تفيد التحقيق وإظهار الحقيقة. وزيادة على ذلك له الحق في إنابة أحد ضباط الشرطة القضائية للقيام بهذا التفتيش (بشروط حددتها المواد من 138 إلى 142 من ق.إ.ج.ج) إذا استحال على قاضي التحقيق تنفيذه بنفسه^{xlvi}.

2.2.1.2. إجراءات التفتيش:

يقع التفتيش على جانبيين في الجرائم الإلكترونية على الجانب المادي وعلى الجانب المعنوي، وذلك من أجل فك ملابسات الجريمة.

1.2.2.1.2. تفتيش منظومة الحاسب الآلي المادية:

يتكون الحاسوب من كيانات مادية، تتمثل في وحدة المدخلات، ووحدة الذاكرة الرئيسية، ووحدة الحاسوب والمنطق، ووحدة التحكم، وحدة المخرجات، ووحدات التخزين الثانوية، وفي الواقع أغلب الجرائم المعلوماتية تقع على معدات الحاسب، وشاشة العرض ومفاتيح تشغيلها وغيرها، وإن الولوج إلى هذا النوع من الكيانات للبحث عن شيء يفيد في كشف الحقيقة، والبحث عن مرتكبها بشأن جريمة معلوماتية وقعت يخضع لإجراءات قانونية خاصة بالتفتيش ولا يثير أية صعوبة^{xlvi}.

2.2.2.1.2. تفتيش مكونات الحاسب الآلي المعنوية:

يقصد بها أنظمة الكمبيوتر والبيانات المخزنة فيه التي جرى التلاعب فيها أو تغييرها وغيرها من الوسائط التي تساعد على تخزين المعلومات^{xliv}، فالبيانات والمعلومات المخزنة في الحاسب الآلي تصلح لأن تكون محلا للتفتيش، ويمكن ضبطها واستنساخها على



الورق أو الأقراص، أو على أي دعامة أخرى كالفلاش ميموري (Flash Memory)، بحيث يمكن الاستناد إليها كدليل على ارتكاب المتهم الجريمة في مرحلة المحاكمة¹.

2.2. الإجراءات الشخصية: وهي مجموعة الإجراءات التي تتعلق بالشخص في حد ذاته، وتتمثل في الشهادة والخبرة بحيث يعتبران من أهم الأدلة في المواد الجنائية.

1.2.2. الشهادة: يقصد بالشهادة " إقرار من الشاهد بأمر رآه أو سمعه أو أدركه بأي حاسة من حواسه".^{li}، وللشهادة عدة شروط حتى يحتكم إليها القاضي كدليل إثبات ومن بينها مايلي:

1.1.2.2. التمييز: هي القدرة على فهم ماهية الفعل وطبيعته وتوقع الآثار التي من شأنه أحداثها. وهذه القدرة تنصرف إلى ماديات الفعل فتتعلق بكيانه وعناصره وخصائصه، وتنصرف كذلك إلى آثاره من حيث ما تنطوي عليه من خطورة على المصلحة أو الحق الذي يحميه القانون وما تنذر به من اعتداء عليه.

2.1.2.2. تخليف اليمين: ألزم الشرع الشاهد أن يحلف اليمين قبل أداء الشهادة، وذلك كضمانة تضيي عليها الثقة كي تكون دليلا يستمد منه القاضي اقتناعه، وتعطي لها قيمتها القانونية من جهة، ومن جهة أخرى تجلب هذه المشكلة انتباه الشاهد إلى خطورة ما سيُدلي به، حيث تجعله حريصا على قول الحق.

3.1.2.2. حرية الاختيار: ينبغي أن يكون الشاهد متمتعا بإرادة حرة عند الإدلاء بشهادته بمعنى أن لا تكون أقواله صادرة إثر تهديد أو إكراه وإنما يشترط أن تكون صادرة عنه بمحض إرادته.^{lii}.

2.2.2. الخبرة: تعرف بأنها "استشارة فنية يستعين بها القاضي و المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى دراية علمية لا تتوفر لدى السلطة القضائية المختصة"^{liiii}. فالخبرة في الجريمة الإلكترونية إجراء يهدف إلى استخدام قدرات شخص سواء كانت فنية أو علمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن وقوع الجريمة^{liv}.

3.2. الإجراءات التقنية: الإجراءات التقنية تتطلب جمع المعلومات والبيانات الخاصة بالجريمة أو ما يعرف بمرحلة جمع الاستدلالات التي تعتبر بمثابة المرحلة التمهيديّة، وفي الوقت ذاته التقاط القرائن والأدلة.

1.3.2. جمع الاستدلالات: «ينصرف مفهوم الاستدلال إلى تجميع المعلومات والبيانات الخاصة بالجريمة، وذلك عن طريق التحري والمراقبة والبحث عن الفاعلين بشتى الوسائل القانونية، كما يقصد بها ضبط الواقعة الإجرامية عن طريق التحري عنها، والبحث عن مرتكبيها بكافة الأساليب القانونية المشروعة، وجمع كل ما يمكن جمعه من المعلومات بشأنها^{lv}.

2.3.2. ضبط الدليل الإلكتروني: يعرف الضبط بأنه: "وضع اليد على شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبها، بهدف ضبط الأدلة والوثائق والأشياء التي تفيد في كشف الجريمة". كما يعرف الدليل الإلكتروني بأنه: " الدليل الذي يوجد أساسا في العالم الافتراضي ويقود إلى الجريمة، فهو كل البيانات التي يمكن إعدادها أو تخزينها بشكل إلكتروني، بحيث تمكن الحاسب من إنجاز مهمة ما"^{lvi}.

1.2.3.2. حجية الدليل الإلكتروني:

الدليل الإلكتروني دليل جنائي رقمي وحتى يتم قبوله كدليل إثبات يجب أن يتم الحصول عليه بطريقة مشروعة، وذلك من خلال أن يكون الإجراء المتبع في استخلاص الدليل الجنائي الرقمي مشروعا، عن طريق مراعاة القواعد الموضوعية والشكلية أثناء اتخاذ أي إجراء، حيث تتمثل القواعد الموضوعية في أن يكون الإجراء الذي يستهدف استخلاص الدليل الجنائي الرقمي عملا إراديا صادرا من شخص له صلاحية القيام به بناء على سبب معين، زيادة على ذلك يجب أن يكون المحل الذي يرد عليه الإجراء محددا أو قابل



للتحديد وأن يكون مشروعا، وأما بالنسبة للقواعد الشكلية فيجب الالتزام باحترام كيفية مباشرة تنفيذ هذا الإجراء، ودائما ما تكون القواعد الشكلية محددة بموجب القانون^{lvii}.

3. الإجراءات الخاصة لمرحلة البحث والتحري في الجرائم الإلكترونية:

لقد استحدثت المشرع الجزائري جملة من الإجراءات الخاصة بمرحلة البحث والتحري، وهذا تماشيا مع الأساليب المستجدة لارتكاب الجرائم.

1.3. اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

تعتبر عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من الأساليب التي اتخذها المشرع الجزائري من أجل حماية الأشخاص والممتلكات، وذلك كونها تتميز بطابع السرية.

1.1.3. اعتراض المراسلات:

يقصد بعملية اعتراض المراسلات والتي أشار إليها المشرع الجزائري من خلال نص المادة 65 مكرر 05 من ق.إ.ج.ج أنها: "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض".

وبالتالي المراسلات حصرتها المشرع الجزائري في الشكل الكتابي فقط، إلى أن جاء القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، والذي جاء فيه من خلال نص المادة الثانية الفقرة السادسة "أي ترسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"^{lviii}. لذا يمكننا القول أن المراسلات تعني كل رسالة مكتوبة بأي شكل من الأشكال سواء مادية أو إلكترونية، وسواء كانت على دعامة ورقية أو رقمية، مرسله بأي وسيلة لعدد معين ومحدد من المرسل إليهم، باستثناء الكتب والمجلات والجرائد والحوليات التي لا تعتبر من قبيل المراسلات الخاصة^{lix}.

2.1.1.3. خصائص اعتراض المراسلات: من بين خصائص اعتراض المراسلات نجد مايلي:

1.2.1.1.3. اعتراض المراسلات يتم خلسة بدون رضا وعلم صاحب الشأن:

اعتراض المراسلات هو إجراء يتم دون رضا وعلم صاحب الشأن، فلو كان صاحب الشأن عالم بالإجراءات المطبقة عليه لا تطبق بذلك خاصية الاعتراض، وكذا عند وضع الخط الهاتفي تحت المراقبة، لا يمكننا القول بأننا أمام إجراء الاعتراض، لهذا فهو سري^{lx}.

2.2.1.1.3. تستهدف عملية اعتراض المراسلات الحصول على دليل غير مادي:

إن ضرورة البحث والتحري عن الجرائم تقتضي الوصول إلى شتيين وهما الحصول على أدلة مادية أو غير مادية. فالأدلة المادية هي التي تنبعث من عناصر مادية ناطقة بنفسها وتؤثر في اقتناع القاضي بحكم العقل والمنطق، في حين الأدلة القولية هي التي تنبعث من عناصر شخصية تشمل فيما يصدر عن الغير من أقوال وتؤثر في اقتناع القاضي بطريق غير مباشر بتأكده من صدق هذه الأقوال^{lxi}.

3.2.1.1.3. استناد اعتراض المراسلات على أجهزة قادرة على التقاط الأحاديث:

أصبح استخدام الوسائل الحديثة الحصول على معلومات وأخذ نسخة منها دون الانتقال إلى مكان وجودها، كما أنها تستطيع أن تفصل الأصوات المسموعة وتميزها عن بعضها من أجل الوصول إلى الصوت المراد سماعه من بين تلك الموجودة في ذلك المكان، ويمكن للقائمين بها أن يجعلوا منها عملية فعالة ومفيدة، بالإضافة إلى إمكانية استنتاج الأدلة المادية على ارتكاب الجريمة وعلى كيفية أدائها دون علم وملاحظة المجرم بذلك^{lxii}.



2.1.3. تسجيل الأصوات:

يقصد به النقل المباشر والآلي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمله من عيوب في النطق إلى شريط تسجيل بحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي، بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه^{lxiii}. والمشرع الجزائري لم ينص في قانون الإجراءات الجزائية على تعريف التسجيل الصوتي، لكن أشار إلى ذلك من خلال نص المادة 65 مكرر 05 حيث جاء فيها: "وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية"^{lxiv}

1.2.1.3. طرق تسجيل الأصوات: التسجيل الصوتي لا يتم إلا بطريقتين: يكون إما عن طريق التسجيل المباشر أو التسجيل غير المباشر.

1.1.2.1.3. التسجيل المباشر:

يتم تسجيل الصوت مباشرة من المصدر دون وسيط في ذلك، مثال وجود جهاز التسجيل في نفس المكان الذي به الشخص، بحيث يتم رصد الصوت مباشرة فور خروجه من الشخص على شريط التسجيل.

2.1.2.1.3. التسجيل غير المباشر:

يقصد به إجراء التسجيل عن طريق وسيط ينقل الصوت من مصدره إلى المسجل، أو بالأحرى عدم وجود مصدر الصوت أمام جهاز التسجيل، أو آلة التقاط الصوت (الميكروفون) مباشرة، بل إن الصوت هنا ينقل عبر الهاتف، مثلا ليلتقطه جهاز التسجيل أو نقل الصوت، أو أن يتم التسجيل من تسجيل صوت آخر^{lxv}.

3.2.3. التقاط الصور:

لم يشر المشرع الجزائري إلى مفهوم التقاط الصور وإنما أشار إلى ذلك في نص المادة 65 مكرر 09 من ق.إ.ج.ج بمصطلح "الالتقاط"، في حين عرفها البعض بأنها: "تمثيل لشخص أو شيء عن طريق أحد الفنون من نقش أو نحت أو تصوير فوتوغرافي أو فيلم، ولم تقف الصورة عند حد تجسيد المادة لشخص ما بل تعدت ذلك إلى عكس شخصيته وانفعالاته"^{lxvi}. أما فيما يخص إجراءات التقاط الصور فالمشرع الجزائري لم ينص على شروط وإجراءات خاصة بهذه العملية، وهذا ما يفسر رغبة المشرع في الربط بين إجراء عملية التقاط الصور والأحكام المتعلقة باعتراض المراسلات وتسجيل الأصوات.

2.3. التسرب:

عرف المشرع الجزائري التسرب من خلال نص المادة 65 مكرر 12 من ق.إ.ج.ج. والتي جاء فيها: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهاهم أنه فاعل معهم أو شريك أو خاف".

1.2.3. صور التسرب:

للتسرب عدة طرق نص عليها المشرع الجزائري في نص المادة 65 مكرر 12 من ق.إ.ج.ج، ويتم ذلك من خلال الصور التالية:

1.1.2.3. المتسرب كفاعل:

الفاعل هو ما جاء بيانه في نص المادة 41 من قانون العقوبات كالتالي: "يعتبر فاعلا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو اساءة استعمال السلطة الولائية أو التحليل أو التدليس الإجرامي"^{lxvii}.



2.1.2.3. المتسرب كشريك:

لقد جاء في نص المادة 42 من ق.ع.ج تعريف الشريك بأنه: "يعتبر شريكا في الجريمة من لم يشترك اشتراكا مباشرا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك" فالعلم بالجريمة يشكل عنصرا أساسيا في الاشتراك.

3.1.2.3. المتسرب كخاف:

عرف المشرع الجزائري الاخفاء في المادة 387 من قانون العقوبات على أنه: "كل من أخفى عمدا أشياء مختلسة أو مبددة أو متحصلة من جناية أو جنحة في مجموعها أو جزء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر".

4.1.2.3. التسرب في نطاق الجرائم الالكترونية:

يمكن تصور عملية التسرب في الجرائم الإلكترونية من خلال دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، كالمشاركة في غرف محادثات الدردشة أو حالات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو انخراطه في مجموعات ونوادي الهاكر، مستخدما في ذلك أسماء وصفات مستعارة وهمة ظاهرا فيها وكأنه واحد مثلهم قصد استدراجهم وللكشف عنهم وعن أعمالهم الإجرامية، كما يمكن تكييف عمل المتسرب على أنه شاهد.^{lxviii}

2.2.3. شروط عملية التسرب:

تتمثل شروط عملية التسرب فيما يأتي:

1.2.2.3. تقرير ضباط الشرطة القضائية:

يقوم ضباط الشرطة القضائية قبل مباشرة عملية التسرب بكتابة تقرير إلى وكيل الجمهورية، وهذا كمبدأ عام على أعمال الشرطة القضائية. كما نصت المادة 65 مكرر 13* من ق.إ.ج.ج صراحة أن ضباط الشرطة القضائية المكلف بتنسيق عملية التسرب هو المسؤول عن تحرير التقرير.

2.2.2.3. الحصول على الإذن:

لا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات المختصة والمتمثلة في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه، ولا يكفي صدور الإذن من الجهة المختصة فحسب، بل لابد أن يكون مكتوبا وإلا كان هذا الإجراء باطلا^{lxix}.

3.2.2.3. السرية في عملية التسرب:

أوجب المشرع الجزائري في عملية التسرب وأحاطها بالسرية الكاملة والمشددة وهذا ما نصت عليه المادة 65 مكرر 16 من ق.إ.ج.ج و التي تنص على: " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشرُوا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات"^{lxx}.



3.3. المراقبة الإلكترونية:

عرف الفقه إجراء المراقبة الإلكترونية على أنه: "مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر^{lxxi}. والمراقبة الإلكترونية تشمل مراقبة الاتصالات الإلكترونية أو مراقبة الأشخاص والأشياء والأموال.

1.3.3. مراقبة الاتصالات الإلكترونية:

لم يتطرق المشرع الجزائري إلى المقصود من مراقبة الاتصالات الإلكترونية، لكنه عرف الاتصالات الإلكترونية ويقصد بها: "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال^{lxxii}.

2.3.3. حالات اللجوء إلى المراقبة الإلكترونية للاتصالات:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة^{lxxiii}.

2.2.3. مراقبة الأشخاص والأشياء والأموال:

مراقبة الأشخاص أو ما يعرف بملاحظتهم وتتبعهم، تعني وضع هؤلاء تحت أعين رجال الضبطية القضائية لترصد تحركاتهم وتنقلاتهم والأماكن التي يتردد عليها المشتبه بهم واتصالاتهم بالأشخاص الآخرين، وكذلك يمكن مراقبة حتى نمط معيشتهم إن تطلب الأمر، وفي سبيل الكشف عن أفراد هذه الشبكات الإجرامية، يقوم رجال الضبطية القضائية بمراقبة وترصد حركة الأموال، وتتبع وجهتها مثل ما هو الحال في جريمة تبييض الأموال، وذلك بهدف المساهمة في الكشف عن عمليات إعادة توظيف الأموال الناتجة عن الجرائم وتمويل النشاطات الإرهابية بالجزائر والوقاية منها والردع عنها.

كما تنصب المراقبة على أشياء قد تستغل في ارتكاب الجريمة، حيث تكون هذه المواد محل تتبع وملاحظة رجال الضبطية القضائية لمعرفة الوجهة الحقيقية لهذه المواد بغية وضع اليد على التنظيم الإجرامي وتفكيكه^{lxxiv}.

خاتمة:

أولا: النتائج: من خلال هذه الورقة البحثية توصلنا إلى النتائج التالية:

- يرتبط مفهوم الجريمة الإلكترونية بكل الأفعال الغير مشروعة التي لها علاقة مع البيئة الرقمية، والتي تهدد حياة الإنسان أو ممتلكاته أو المؤسسات العمومية أو الخاصة.
- تختلف الجريمة الإلكترونية على الجريمة التقليدية، كونها تقع في عالم افتراضي يصعب الاحاطة بها وفك جميع ملباساتها.
- يتميز الجاني في الجريمة الإلكترونية بالذكاء العالي، وسرعة التنفيذ، ومسح آثار الفعل الغير مشروع.
- يشترط في مرحلة البحث والتحري اتخاذ كافة الإجراءات القانونية اللازمة والتي حددها المشرع الجزائري، والتي تتناسب مع طبيعة الجريمة الإلكترونية، وخاصة عنصر الخبرة.
- إجراءات البحث والتحري الخاصة بالجرائم الإلكترونية تتطلب وسائل تقنية حديثة، كتسجيل الأصوات والتقاط الصور والتسرب.



ثانيا: التوصيات: من جملة ما يمكن طرحه كتوصيات ما يأتي:

- ضرورة تكوين محققين مختصين في الجرائم الإلكترونية، يتمتعون بالكفاءة والمهارة اللازمة من أجل فك ملابسات مثل هذا النوع من الجرائم.
- تعزيز أساليب الرقابة على الشبكة المعلوماتية، حتى يضيق على كل من تسول له نفسه الاعتداء على حرمة الأشخاص أو ممتلكاتهم، أو تخريب واختراق الأنظمة والبرامج الخاصة بالأشخاص المعنوية.
- سن قوانين أكثر ردة على الجناة تصل عقوبتها إلى المؤبد أو الإعدام، لأن مثل هذه الجرائم لها آثار جسيمة على الفرد والمجتمع والدولة، وحتى على الأمن العالمي.

قائمة المراجع

- i - غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية، د.ط، الجزائر، 2015م ص14.
- ii - محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة، ط.1، عمان الأردن، 2007، ص08.
- iii - سميرة معاشي، ماهية الجريمة الإلكترونية، مجلة المنتدي القانوني، ع7، جامعة بسكرة، ص276.
- iv - عائشة بوبخزة، الحماية الجزائرية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2013م، ص21.
- v - سميرة معاشي، ماهية الجريمة الإلكترونية، مرجع سابق، ص277.
- vi - غنية باطلي، الجريمة الإلكترونية، مرجع سابق، ص17.
- vii - أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)، دار الجامعة الجديدة، دط، الإسكندرية، مصر، 2007م، ص86.
- viii - سامي علي حامد عياد، الجريمة المعلوماتية واجرام الإنترنت، دار الفكر الجامعي، دط، الاسكندرية، مصر، 2007م، ص43.
- ix - فريال لعافل، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر، كلية الحقوق، جامعة أكلي محمد اولحاج، البويرة، الجزائر، 2015م، ص10.
- x - فضيلة عاقل، الجريمة الإلكترونية و إجراءات مواجهتها من خلال التشريع الجزائري، مركز جيل البحث العلمي، www.jilrc.com، 2022.02.12، 16.30.
- xi - فريال لعافل، الجريمة المعلوماتية في ظل التشريع الجزائري، مرجع سابق، ص12.
- xii - المادة 02 الفقرة 1 من القانون 04-09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، ع47، ص05.
- xiii - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، دط، مصر، 2002م، ص01.
- xiv - الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق ل 25 غشت 2021 المتتم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية.
- xv - المادة 211 مكرر 22 الفقرة الثالثة من قانون الإجراءات الجزائية.
- xvi - ينظر: عبد الله بن مرزوق العتيبي، جريمة غسل الأموال وعلاقتها بالجرائم الحديثة، جامعة نايف للعلوم الأمنية، دط، الرياض، السعودية، 2009م، ص04-05.
- xvii - ذياب موسى البدائية، الشباب والإنترنت والمخدرات، مركز الدراسات والبحوث، ط1، الرياض، المملكة العربية السعودية، 2011م، ص46.
- xviii - ذياب موسى البدائية، الشباب والإنترنت والمخدرات، مرجع نفسه، ص47.
- xix - نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الإنترنت، دار نور، دط، د.م، 2017م، ص72.



- xx - زينب شاكر السماك، جرائم الاحتيال الإلكتروني www.annaba.org/arabic، 14 فيفري 2022م، 18:40.
- xxi - أمنة بوشاقور، جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية، مذكر ماستر في القانون الجنائي للأعمال، كلية الحقوق، جامعة العربي بن مهيدي، أم البواقي، الجزائر، 2015م/2016م، ص23.
- xxii - حنان ربحان مبارك المضاحكي، الجرائم المعلوماتية (دراسة مقارنة)، منشورات الحلبي الحقوقية، ط1، سوريا، 2014م، ص322.
- xxiii - ليلي لفويلي، الجريمة الإلكترونية، مذكرة ماستر في قانون العقوبات والعلوم الجنائية، كلية الحقوق، جامعة قسنطينة01، قسنطينة، الجزائر، 2012م، ص37.
- xxiv - محمد أمين بالبحري، زينب بو العام، الجريمة الإلكترونية كجريمة منظمة عابرة للحدود، مذكرة ماستر، كلية الحقوق، جامعة منتوري، قسنطينة، 2014م/2015م، ص53.
- xxv - يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2012م/2013م، ص55.
- xxvi - يوسف صغير، الجريمة المرتكبة عبر الإنترنت، المرجع نفسه، ص56.
- xxvii - غنية باطلي، الجريمة الإلكترونية، مرجع سابق، ص34.
- xxviii - محمد عبد الله أبو بكر، موسوعة جرائم المعلوماتية - جرائم الكمبيوتر والإنترنت -، المكتب العربي الحديث، دط، الإسكندرية، مصر، 2007م، ص49.
- xxix - فاطمة الزهراء بختي، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، 2013م، ص18.
- xxx - فاطمة الزهراء بختي، إجراءات التحقيق في الجريمة الإلكترونية، المرجع نفسه، ص19.
- xxxi - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص59.
- xxxii - المادة 211 مكرر 25 من قانون الإجراءات الجزائية.
- xxxiii - المادة 79 من الأمر رقم 66-155، المؤرخ في 18 صفر 1386هـ الموافق لـ 08 جوان 1966م المتضمن قانون الإجراءات الجزائية، ج.ر، ع84، ص38.
- xxxiv - عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة الدكتور طاهر مولاوي، سعيدة، الجزائر، 2016م، ص28.
- xxxv - ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة ماستر في القانون الجنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، الجزائر، 2015م/2016م، ص63.
- xxxvi - ينظر: بشير حماني، خصوصية التحقيق في الجريمة الإلكترونية، مذكرة ماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2019م، ص64-65.
- xxxvii - ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، المرجع السابق، ص65.
- xxxviii - عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، دار الثقافة، ط1، الأردن، 2010م، ص500-501.
- xxxix - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، ط1، عمان، الأردن، 2011م، ص151.
- xl - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، دط، الإسكندرية، مصر، 2010م، ص108.
- xli - ينظر: عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية أو الاستثنائية، المرجع السابق، ص515-516.
- xlii - عائشة بوخبة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، وهران، الجزائر، 2013م، ص194.



- xlili- ينظر: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، المرجع السابق، ص112-113.
- xliv- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، المرجع نفسه، ص99.
- xlv- عبد الله ماجد العكايبة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، مرجع سابق، ص512-513.
- xlvi- ينظر: جمال براهيم، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018م، ص58.
- xlvi- ينظر: المواد 81.82.83.84 من ق.إ.ج.ج.
- xlvi- راضية بن جاب الله، إجراءات التفتيش على ضوء قانون الإجراءات الجزائية الجزائري، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، المسيلة، الجزائر، 2013م، ص72.
- xlxi- خالد عباد الحلي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، ط1، عمان، الأردن، 2011م، ص159.
- ¹ - أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، ع58، م29، الرياض، المملكة العربية السعودية، ديسمبر 2013م، ص90.
- li- عماد محمد ربيع، حجية الشهادة في الإثبات الجزائي، دار الثقافة، ط1، عمان، الأردن، 1999م، ص109.
- lii- ينظر: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، مرجع سابق، ص133.
- liii- يسعد رويبو، فرحات بابا، الخبرة القضائية ودورها في الإثبات، مذكرة ماستر في المهن القانونية والقضائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، 2019م، ص12.
- liv- ينظر: عبد الله ماجد العكايبة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، المرجع السابق، ص383.
- lv- عبد الله ماجد العكايبة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، المرجع نفسه، ص197.
- lvi- خالد عباد الحلي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، المرجع السابق، ص229.
- lvii- عبد المطلب طاهري، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، 2015م، ص20.
- lviii- القانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009م المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر، ع47.
- lix- عبد المطلب طاهري، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، 2015م، ص20.
- lx- نصر الدين مروك، محاضرات في الإثبات الجنائي، دار هومة، ط3، الجزائر، 2009م، ص132.
- lxi- فوزي لواتي، التحقيق في جرائم المخدرات على ضوء أساليب التحري الخاصة، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر1، الجزائر، 2015م، ص18.
- lxii- ليدية سعدلي، كاهنة العيدي، تعزيز مكانة ضباط الشرطة القضائية ضمن استراتيجية مكافحة الفساد، مذكرة ماستر في القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، 2018م، ص09.
- lxiii- عبد القادر رويس، أساليب البحث الخاصة وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية، ع3، جوان 2017م، ص40.
- lxiv- ينظر: المادة 65 مكرر 05 الفقرة 02 من الأمر رقم 66-155، مرجع سابق، ص29.
- lxv- وسام عواس، مشروعية وسائل البحث الجنائي الحديثة، شهادة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2014م، ص104.
- lxvi- رشيد شمشيم، الحق في الصورة، مجلة العلوم الانسانية، ع3، 2008م، ص127.
- lxvii- المادة 41 من الأمر 66-156 المؤرخ في 18 صفر 1386هـ الموافق لـ 08 جوان 1966م المتضمن قانون العقوبات المعدل والمتمم بالقانون رقم 82-04 المؤرخ في 13 فيفري 1982م، ج.ر، ع07، ص318.



- lxviii- ينظر: لامية وعلي، كاهنة سعودي، إجراءات مكافحة الجريمة الالكترونية، مذكرة ماستر في القانون الجنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، 2019م، ص 99-100.
- lxix- ينظر: جمال براهيم، التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 85-86.
- lxx- ينظر المادة 65 مكرر 16 من ق.إ.ج.ج.
- lxxi- بشير حماني، خصوصية التحقيق في الجريمة الالكترونية، المرجع السابق، ص 73-74.
- lxxii- ينظر: المادة 05 من المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015م الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، ع 53، ص 17.
- lxxiii- ينظر: سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية، مجلة الباحث للدراسات الأكاديمية، ع 9، جوان 2016م، ص 394.
- lxxiv- ينظر: ميليسة سليمان، نصيرة خلوات، خصوصيات المعاينة في الجرائم المستحدثة، مذكرة ماستر في القانون الجنائي والعلوم الإجرامية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2017م، ص 53.54.55.



جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني

ط.د. بن عبد القادر أسماء

جامعة الأمير عبد القادر للعلوم الإسلامية

أ.د. حفيظة مبارك

جامعة الأمير عبد القادر للعلوم الإسلامية

مقدمة:

تطور عالم الجريمة بتطور الحياة وبظهور التكنولوجيا، فظهرت الجريمة الالكترونية، وظهر معها صنف جديد من الجناة يتصفون بمواصفات تختلف عن المواصفات التقليدية في الجرائم العادية، لأن مقتري الجرائم الإلكترونية يتصفون بالذكاء وقد يكونون خبراء ومختصين في مجال الإعلام الآلي وتكنولوجيا الإعلام والاتصال، لذلك ورغم إيجابيات التجارة الإلكترونية، فالجرائم والاعتمادات التي تقع في إطارها تلحق بالمتعاملين بها خسائر تزعزع ثقتهم بها، فظهرت أنظمة حماية كالتوقيع والتصديق الإلكترونيين، ورغم ما تحققه من هذه الأنظمة من أمان إلا أنها لم تسلم، ولحقها الجناة بارتكاب جرائم الكترونية حولها كجريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني. وهذا ما يقودنا الى طرح الإشكالية التالية:

ماهي جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني في حماية التوقيع الإلكتروني؟

– ما هو نظام التوقيع الإلكتروني؟

– ماهي جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني؟

ونجيب عن هذه الإشكالية وفق الخطة الآتية:

قسمنا بحثنا إلى جزئين الأول فصلنا فيه ماهية التوقيع الإلكتروني، من خلال التفصيل في مفهوم التوقيع الإلكتروني، ثم في أنواع وأهمية التوقيع الإلكتروني، ويليه شروط التوقيع الإلكتروني. أما الجزء الثاني فخصصناه للتفصيل في الجريمة محل الدراسة، من خلال تعريفها وأركانها وأخيرا عقوبتها.

1. ماهية التوقيع الإلكتروني:

إن وضع التوقيع على أية محرر يهدف إلى ترتيب آثار قانونية معينة. فمن خلال هذا التوقيع يمكن تحديد هوية الموقع ومعرفة صلاحيته. كذلك فإن توقيع أصحاب الشأن على المحرر يعد إقرارا منهم لمضمون ما ورد به،^{lxxiv} فإن السؤال الذي يجب بحثه هو ماذا يقصد بالتوقيع الإلكتروني؟ في **المطلب الأول** وماهي أنواعه وشروطه؟ وهذا ما سنعالجه في **المطلب الثاني**، وكذلك بما أن التوقيع التقليدي له أهمية كبيرة وحجية على المحرر الموجود فيه خاصة في المعاملات التجارية، ما الأهمية التي يكتسبها التوقيع الإلكتروني في منظومة التجارة الإلكترونية؟ وما حججه في إثبات محررات ومعاملات التجارة الإلكترونية؟ وهذا ما سنجيب عنه في **المطلب الثالث**.

1.1 مفهوم التوقيع الإلكتروني:

لتوضيح ماهية التوقيع الإلكتروني وجدنا أنه من الأنسب الخوض في جزئيتين مهمتين تفي بالغرض المنشود كل منهما خصصنا لها فرع محدد: الأول يخصص لتعريف التوقيع الإلكتروني، والثاني لكيفية عمل تقنية التوقيع الإلكتروني.



1.1.1 تعريف التوقيع الإلكتروني:

عرف التوقيع الالكتروني تعريفات عدة على نطاقات كثيرة فمنها التعريفات التشريعية ومنها التعريفات الفقهية لذا فصلنا في هذا الفرع في التعريفات التشريعية، ثم في التعريفات الفقهية، ولتوضح صورته أكثر تعرضنا إلى كيفية عمل تقنية التوقيع الإلكتروني:

1.1.1.1 التعريفات التشريعية: تنوعت التعريفات التشريعية بتنوع وتعدد التشريعات فمنها الدولية كقانون اليونسترال ومنها الداخلية كالقانون الجزائري:

1.1.1.1.1 قانون اليونسترال بشأن التوقيعات الإلكترونية لعام 2001: عرفت المادة الثانية من هذا القانون التوقيع الالكتروني بأنه: "بيانات في شكل الكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات".^{lxxiv}

2.1.1.1.1 المشرع الجزائري: يعد التوقيع الإلكتروني حديثا بالنسبة للمشرع الجزائري إذ لم يعتد به إلا في المادة 2/327 من القانون المدني في تعديل 2005 والتي تنص على: "ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323^{lxxiv} مكرر 1 أعلاه" ثم في المرسوم التنفيذي 162-07 المؤرخ في 30-05-2007 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، فقد عرف فيه التوقيع الإلكتروني في المادة الثالثة منه كالاتي: "التوقيع الإلكتروني هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر، 323 مكرر 1"

إلى أن خصه بتنظيم قانوني منفرد متمثل في القانون 04-15 المؤرخ في 01-02-2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين. لكن باستقراء نصوص هذا القانون نجد أنه حسب المشرع الجزائري هناك نوعان من التوقيع الإلكتروني التوقيع الإلكتروني العادي والتوقيع الإلكتروني الموصوف، فعرف التوقيع الإلكتروني العادي في المادة 1/2 من القانون 04-15^{lxxiv} بأنه "بيانات إلكترونية في شكل الكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق"، في حين عرفت المادة 7 منه التوقيع الإلكتروني الموصوف بأنه: "التوقيع الإلكتروني الموصوف هو التوقيع الذي تتوفر فيه المتطلبات الآتية:

- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.

- أن يرتبط بالموقع دون سواه.

- أن يمكن من تحديد هوية الموقع.

- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.

- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.

- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات".

2.1.1.1.1 التعريفات الفقهية: واخترنا منها تعريفين فقط لأنها جميعها تصب في معنى واحد وأغلبها بتعبير واحد:

أ- " طريقة اتصال مشفرة تعمل على توثيق المعاملات التي تتم عبر الإنترنت. بشكل أساسي فإن الفكرة الكامنة وراء التوقيعات الالكترونية هي نفسها كما في التوقيع المكتوب بخط اليد. إنك تستخدمه للتصديق أو لتوثيق الحقيقة بأنك وعدت بشيء ما ولا تستطيع التراجع عنه فيما بعد".^{lxxiv}



أ- "يتمثل التوقيع الإلكتروني في استخدام رمز أو شفرة أو رقم بطريقة موثوق بها تضمن صلة التوقيع بالوثيقة الإلكترونية وتثبت- في ذات الوقت- هوية شخص الموقع. فوسيلة التوقيع الإلكتروني إذن رمز أو شفرة أو رقم، ودعامته وثيقة إلكترونية، وضمانته إجراءات توثيق تقنية تحقق قدرا معقولا من الأمان والثقة".^{lxxiv}

2.1.1. كيفية عمل تقنية التوقيع الإلكتروني:

يتم إنشاء التوقيعات الإلكترونية وكذلك التثبيت من صحتها من خلال التشفير وهو فرع من الرياضيات التطبيقية المختصة بتحويل الرسائل إلى أشكال تبدو وكأنها لا يمكن فهمها وإعادة تأمل مرة أخرى كما كانت.^{lxxiv} أي يتم إنشاؤه بآلية إنشاء خاصة بالتوقيع الإلكتروني وقد عرفها المشرع الجزائري في الفقرة الرابعة من المادة الثانية من القانون 04-15 بأنها: "جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني"، وكما عرف بيانات إنشاء التوقيع الإلكتروني في الفقرة الثالثة من المادة ذاتها كالآتي: "بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني".

2.1. أنواع وأهمية التوقيع الإلكتروني:

وأما في هذا المطلب سنوضح نقطتين مهمتين، بحيث كل نقطة نخصص لها فرعاً مستقلاً، الفرع الأول ندرس في أنواع التوقيع الإلكتروني، والفرع الثاني نتناول فيه أهمية التوقيع الإلكتروني.

1.2.1 أنواع التوقيع الإلكتروني:

توجد أنواع كثيرة من التوقيع الإلكتروني نذكر أشهرها وأكثرها شيوعاً واستخداماً:

1.1.2.1. التوقيع الرقمي أو الكودي: هو عدة أرقام يتم تركيبها لتكون في النهاية كود يتم التوقيع به، ويستخدم هذا في المعاملات البنكية والمراسلات الإلكترونية التي تتم بين التجار أو بين الشركات وبعضها، ومثال له بطاقة الائتمان التي تحتوي على رقم سري لا يعرفه سوى العميل.

2.1.2.1. التوقيع الشخصي: يقوم على أساس التحقق من شخصية المتعامل بالاعتماد على الصفات الجسدية للأفراد مثل البصمة الشخصية، مسح العين البشرية أو التعرف على الوجه البشري، خواص اليد البشرية، التحقق من نبرة الصوت. ويتم التأكد من شخصية المتعامل عن طريق إدخال المعلومات للحاسب الآلي أو الرسائل الحديثة مثل التقاط صورة دقيقة لعين المستخدم أو صورته أو يده ويتم تخزينها بطريقة مشفرة في ذاكرة الحاسب الآلي ليقوم بعد ذلك بالمطابقة، ويعتري هذا النظام العديد من المشاكل منها أن صورة التوقيع يتم وضعها على القرص الصلب للحاسب الآلي ومن ثم يمكن مهاجمتها أو نسخها بواسطة الطرق المستخدمة في القرصنة الإلكترونية.^{lxxiv}

3.1.2.1. التوقيع بالقلم الإلكتروني: هنا يقوم مرسل الرسالة بكتابة توقيع شخصي باستخدام قلم إلكتروني خاص على شاشة الحاسب الآلي عن طريق برنامج معين ويقوم هذا البرنامج بالتقاط التوقيع والتحقق من صحته، ويستخدم هذا التوقيع للتحقق من الشخصية. ورغم بساطة هذا النوع من التوقيع، وسهولة استخدامه، إلا أنه لم يعرف على نطاق واسع في مجال التجارة الإلكترونية التي تفضل التوقيعات الرقمية، هذا فضلاً عن أن التوقيع بالقلم الإلكتروني يحتاج جهاز كمبيوتر بمواصفات خاصة تمكنه من التقاط التوقيع والتأكد من صحته ومطابقته للتوقيع المخزن في الذاكرة.^{lxxiv}

2.2.1 أهمية التوقيع الإلكتروني:

للتوقيع الإلكتروني أهمية كبرى في شتى المجالات، منها:



- هو وسيلة إثبات للمحررات الإلكترونية تغطي عليها طابع الرسمية وتعبّر عن صدق رغبة الموقع في تنفيذ ما جاءت به الدعامة الإلكترونية، مما يجعلها تعادل الدعامة الورقية الرسمية من حيث الحجية وقوة الإثبات.
- تحويل المعلومات الشخصية بصورة سرية ومضمونة لكل مواطن.
- يمكن الاعتماد اعتمادا كليا على التوقيع الإلكتروني ضمن الإجراءات القانونية والقضائية في المنازعات بين الأشخاص والشركات الخاصة أو المؤسسات والهيئات الحكومية.
- توفير الهوية الرقمية لكل مواطن.
- التوفير في جميع إجراءات إرسال البيانات إلى المواطن والحصول على المعلومات منه (التوفير في الورق، الطلبات، الطباعة، الخبر... إلخ)

- توفير عامل الوقت الثمين للمواطن والتجار وفي هذه الحالة لن يضطرا إلى التنقل للقيان بالمعاملات فيما بينهم.^{lxxiv}

3.1. شروط التوقيع الإلكتروني وحجيته:

أما هذا العنصر فقسمناه إلى فرعين الأول يتحدث عن الشروط الواجب توافرها في التوقيع الإلكتروني، والثاني عن حجية التوقيع الإلكتروني في التشريع الجزائري.

1.3.1. شروط التوقيع الإلكتروني:

يجب أن تتوفر في التوقيع الإلكتروني الشروط التالية:

- 1.1.3.1. أن يرتبط بالموقع دون سواه: أي أن يكون لصاحب التوقيع الإلكتروني بيانات وشفرة خاصة به عن باقي الموقعين، ذلك أنه عندما تصدر بيانات إنشاء التوقيع لشخص ما فلا يمكن أن يتم إصدار نفس التوقيع لشخص آخر
- 2.1.3.1. أن يمكن من تحديد هوية الموقع: فقد نص المشرع الجزائري على هذا الشرط من خلال نص المادة 1/323 من ق.م.ج والتي تنص على أنه: "..... بشرط إمكانية التأكد من هوية الموقع التي أصدرها." إذن فالمشرع قد أقر بالاعتداد بالتوقيع الإلكتروني في الإثبات متى كان كفيلا بالتعريف عن هوية الموقع والتحقق من نسبة التوقيع إليه. كما نصت على هذا الشرط المادة 6 من القانون 04-15.

3.1.3.1. إنشاء التوقيع الإلكتروني بواسطة وسائل خاصة تكون تحت سيطرة الموقع: ليتصف بالحجية في الإثبات أما إذا فقد الموقع تلك السيطرة لأي سبب فإن بيانات التوقيع تفقد طابعها السري مما يفقد التوقيع الإلكتروني حجتيته في الإثبات، لأن تمييز هويته وتحديد شخصيته يكون مشكوكا فيه.

4.1.3.1. أن يكون التوقيع مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التعبيرات اللاحقة بهذه البيانات: ومفاد هذا الشرط هو عدم إمكانية إحداث تغيير في المحرر الإلكتروني دون معرفة التوقيع الإلكتروني نفسه، لأنه يمكن الوصول إلى المحرر الإلكتروني دون معرفة التوقيع الإلكتروني، ويقصد بهذا الشرط حماية التوقيع والمحرر معا.

5.1.3.1. وجوب توثيق التوقيع لدى جهة معينة: تختص بالتحقق من مدى مصداقيته، والتأكد من الشخص العائد له ليتم منحه شهادة توثيق يؤكد صحة التوقيع.^{lxxiv}

وقد حدد المشرع الجزائري شروط التوقيع الإلكتروني الموصوف في المادة 7 من القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين: " التوقيع الإلكتروني الموصوف هو التوقيع الذي تتوفر فيه المتطلبات الآتية:
- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.



- أن يرتبط بالموقع دون سواء.
- أن يمكن من تحديد هوية الموقع.
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.
- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات".

1.3.2. حجية التوقيع الإلكتروني:

لا يمكن للقواعد التقليدية للقانون المدني من استيعاب التصرفات التي ترم في الشكل الإلكتروني، وهذا ما دفع بالمشروع الجزائري إلى التدخل بتعديل هذه القواعد حتى يمنح بموجبها حجية لهذه التصرفات. لذا بحجية التوقيع الإلكتروني صراحة في القانون 04-15 المتضمن للتوقيع والتصديق الإلكترونيين، وذلك ضمن المادة السابعة منه-السابقة الذكر- حيث وضع له فيها شروطا كي يعتد به ويكون حجة في الإثبات، بأن فرق بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني الموصوف بأن ألزم في الثاني أن تصادق عليه جهة تصديق وطنية تحل محل الضابط العمومي في الدعامات الورقية. كما وقد نص في المادة الثامنة من القانون 04-15 على: "يعتبر التوقيع الإلكتروني الموصوف وحده ماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي" وقد اعترف المشروع الجزائري بالتوقيع الإلكتروني غير الموصوف بنصه في المادة 9 من القانون 04-15 على: "بغض النظر عن أحكام المادة 8 أعلاه، لا يمكن تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب:

- شكله الإلكتروني أو،
 - أنه لا يعتمد على شهادة تصديق إلكتروني موصوفة، أو،
 - أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني".
- بمعنى أنه يتعين قبول التوقيع الإلكتروني البسيط كدليل للإثبات. ولكن يجب أن نأخذ في الاعتبار أنه عند حدوث ازدواجية في هذه الحالة بين توقيعين إلكترونيين: أحدهما بسيط، والآخر موصوف، فتكون الأولوية لهذا الأخير حيث إنه يتمتع بعناصر أمان يمكن أن تمنحه هذه الأولوية. ^{lxxiv}

2. جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني:

كأي جريمة إذا أردنا دراستها نتعرف عليها أولا في مطلب مستقل، ثم نحلل أركانها في المطلب الثاني وفي المطلب الأخير نتطرق للعقوبات المقررة قانونا.

1.2. تعريف جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني:

تتمثل الجريمة عند قيام شخص بإعداد توقيع إلكتروني دون موافقة صاحبه بل ومجرد حيازة أو إفشاء أو استعمال، والفاعل هنا قد يقوم بصناعة برنامج أو النظام المعلوماتي، بمعنى خلقه من العدم أي تصميمه حسب مواصفات فنية وتقنية معينة بذات الأدوات التي يعد بها البرنامج أو النظام المعلوماتي المشروع، كي يتوصل في النهاية إلى عمل ذلك التوقيع الإلكتروني. ^{lxxiv} أي امتلاكه لبيانات تمكنه من إنشاء توقيع الكتروني.

ويمكن أن يكون الفاعل شخص معنوي أو طبيعي مرخص له بالعمل في هذا المجال أو غير مرخص لهم طالما لم يتحصلوا على إذن الموقع في استخراج هذا التوقيع من صاحبه.



إذن محل التجريم هنا هو صنع أو الاحتفاظ أو استعمال أو اختراق أو إفشاء توقيع الكتروني أو بيانات إنشاءه من أشخاص غير مرخص لهم بفعل ذلك.

وهذه الجريمة تعد جنحة حسب المشرع الجزائري الذي جرمها بنص المادة 68 من القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين

2.2. أركان جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني:

كباقي الجرائم فإن لقيام هذه الجنحة يجب توافر ركنين:

1.2.2. الركن المادي:

الركن المادي في هذه الجريمة يتخذ عدة صور أو أفعال وهي:

الصورة الأولى: حيازة بيانات إنشاء توقيع الكتروني.

الصورة الثانية: إفشاء بيانات إنشاء توقيع إلكتروني.

الصورة الثالثة: استعمال بيانات إنشاء توقيع الكتروني.

وتمثل السلوك الإجرامي في هذه الجريمة هي قيام الجاني بأحد الأفعال المذكورة سابقا، ويعد القيام بأحد هذه الأفعال كافيا لقيام الجريمة وهي تعد من جرائم السلوك أي لا يشترط تحقق نتيجة جرمية لاستحقاق العقوبة بل يكفي القيام بالفعل، وفي هذه الحالة حتى ولو لم ينشأ توقيع الكتروني لكن بمجرد الاعتداء على بيانات إنشاءه يتحقق الركن المادي في الجريمة طالما لم تكن تلك الأفعال مبنية على ترخيص صاحب التوقيع.

أما الوسيلة التي يستخدمها الجاني في الجريمة هي عبارة عن مجموعة من الأجهزة والأدوات التي يختلص بها معلومات عن توقيعات قائمة بالفعل ليحصل لي نسخة منها دون موافقة أصحابها، أو عمل برنامج معلوماتي جديد غير النظام القائم وذلك حتى يساعده في تحقيق غرضه الإجرامي غير المشروع، لا تقوم الجريمة إذا لم يكن للنظام أو البرنامج القدرة الفنية على عمل التوقيع الإلكتروني، لذلك يجب توفر الشروط الثلاثة لقيام الجريمة، أما الصورة الثانية للركن المادي في هذه الجريمة فهي حيازة برنامج لإعداد توقيع الكتروني دون موافقة صاحبه، والفرض هنا حيازة الجاني للبرنامج المعلوماتي غير المشروعة، أي غير مالك له أو مستأجرا.^{lxxiv} وتتحقق الجريمة باستعمال الجاني ذاته للبرنامج أو مجرد حيازته أو إفشاءه بمنحه لشخص آخر غير صاحبه بمقابل أو بدونه.

2.2.2. الركن المعنوي:

الركن المعنوي فيها هو القصد الجنائي العام بعنصرية العلم والإرادة، وذلك بأن يعلم الجاني بحقيقة سلوكه الإجرامي، وإذا تحقق من وقوع الركن المادي فلا بد من توافر ركنها المعنوي في حق الفاعل، وصورته هو القصد الجنائي بعنصرية العلم والإرادة، فالجريمة عمدية ولا يتصور قيامها بطريق الخطأ، وصياغة نص المادة 68 القانون 04-15 تقع بضرورة وقوع الجريمة بطريق العمد بعنصرية العلم والإرادة، وذلك بأن يعلم الجاني بكافة الوقائع المكونة لسلوكه الإجرامي ويعلم بمخالفة ذلك للقانون لأن يفترض فيه الاحترافية، ومع ذلك تنصرف إرادته إلى الفعل الإجرامي مع قبول النتيجة الإجرامية المترتبة عليه.^{lxxiv}

3.2. عقوبة جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني:

بالنسبة لعقوبة هذه الجريمة في التشريع الجزائري أقرت بموجب القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين في المادة 68 منه حيث تنص على: "يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث سنوات (3) سنوات وبغرامة من مليون دينار



(1.000.000 دج) إلى خمسة ملايين دينار (5.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير." ويلاحظ أن المادة تذكر عقوبة التوقيع الإلكتروني الموصوف دون العادي.

كذلك تبين هذه المادة ومن خلال العقوبة أن الجريمة جنحة حسب المشرع الجزائري. أما المشرع المصري فقد اهتم في مشروع التجارة الالكترونية بجريمة الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الإلكتروني فقد نص في المادة 27 من مشروع القانون المصري على أنه " يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه أو بإحدى هاتين العقوبتين، كل من صنع أو حاز أو حصل على نظام معلومات أو برنامج لإعداد توقيع إلكتروني" من هذه المادة نستنتج أن المشرع المصري عاقب على هذه الجريمة بالحبس والغرامة على اعتبار التدخل غير المشروع وجعل الحبس جوازيا،^{lxxiv} وهنا المشرع المصري لم يخص عقوبة هذه الجريمة بالتوقيع الإلكتروني المقدم (الموصوف)، أو البسيط (العادي) مما يجعل تطبيقها على كليهما ممكنا.

خاتمة:

من خلال دراستنا توصلنا إلى النتائج التالية:

- التوقيع الإلكتروني هو بيانات رقمية تتم عبر أجهزة رقمية على محركات الكترونية تعبر عن إرادة الموقع في تنفيذ أو في تحقيق آثار ذلك المحرر، أي أنه وسيلة إثبات.
- أول ما تطرق المشرع الجزائري للتوقيع الإلكتروني سنة 2005 في القانون المدني إلى أن خصه بتشريع خاص سنة 2015 وهو القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين.
- المشرع الجزائري أحاط التوقيع الإلكتروني بحماية جنائية من خلال تشريع جرائم والمعاقبة عليها بنصوص في القانون 04-15 كجريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني، وهي حماية تعتبر غير كافية خاصة مع التطور الكبير التي يلحق مثل هذه الأنظمة، وخاصة مع الإقبال الكبير عليها في الواقع العملي والتجاري.
- تتمثل جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني عند قيام شخص بإعداد توقيع إلكتروني دون موافقة صاحبه بل ومجرد حيازة أو إفشاء أو استعمال.
- تعد جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني من جرائم السلوك أي لا يشترط تحقق نتيجة جرمية لاستحقاق العقوبة بل يكفي القيام بالفعل، وفي هذه الحالة حتى ولو لم ينشأ توقيع إلكتروني لكن بمجرد الاعتداء على بيانات انشاءه يتحقق الركن المادي في الجريمة طالما لم تكن تلك الأفعال مبنية على ترخيص صاحب التوقيع.
- بالنسبة لعقوبة هذه الجريمة في التشريع الجزائري أقرت بموجب القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين في المادة 68 والتي اعتبرتها جنحة.

توصيات:

- تعديل القانون 04-15 بما يتماشى مع العصر.
- تشريع مختلف الجرائم التي تقع على التوقيع الإلكتروني التي يطرحها الواقع وتبين عقوباتها بوضوح.
- استحداث حماية تقنية أكبر للتوقيع الإلكتروني تحميه من الاختراق.



قائمة المراجع والمصادر:

1. القانون 15-04 مؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر 06، الصادرة في 2015/02/10.
2. الجمعية العامة للأمم المتحدة: القانون النموذجي بشأن التوقيعات الإلكترونية، الجلسة العامة 85، 12 ديسمبر 2001.
3. عبد الفتاح بيومي حجازي: التجارة الالكترونية وحمايتها القانونية، دار الفكر الجامعي، الاسكندرية-مصر، 2006، د.ط.
4. لالوش راضية: أمن التوقيع الإلكتروني، مذكرة لنيل الماجستير في القانون، تخصص قانون الأعمال، كلية الحقوق، جامعة مولود معمري، تيزي /- وزو-الجزائر، 2012.
5. بوعمر آسيا: النظام القانوني للتجارة الإلكترونية، دراسة مقارنة، أطروحة دكتوراه للعلوم، تخصص قانون الملكية الفكرية، كلية الحقوق، جامعة بن عكنون، الجزائر، 2012.
6. وسف حسن يوسف: العقود التجارية الإلكترونية الدولية، منشورات المركز القومي للإصدارات القانونية، القاهرة- مصر، ط1.
7. سعيد السيد قنديل: التوقيع الإلكتروني، دار الجامعة الجديدة للنشر، الإسكندرية- مصر، 2004، د ط.
8. لزه بن سعيد: النظام القانوني لعقود التجارة الإلكترونية، منشورات دار الفكر الجامعي، الإسكندرية-مصر، 2010م، ط 1.
9. حمد المرسي زهرة: الحماية المدنية للتجارة الالكترونية، منشورات دار النهضة العربية، القاهرة-مصر، ط3.
10. حمد خالد جمال رستم: التنظيم القانوني للتجارة والإثبات الإلكتروني في العالم، منشورات الحلبي الحقوقية، بيروت- لبنان، 2006م، ط1.



إثبات الجنائي بالوسائل المستحدثة للجرائم (دليل رقمي) نموذجاً

سماحي سمية

جامعة طاهري محمد بشار

Soumi.smahi@gmail.com

مقدمة:

أصبحت الجريمة الإلكترونية أكثر انتشاراً في الآونة الأخيرة وذلك يعود الى كافة التعاملات التي أصبحت بالعالم التكنولوجي الافتراضي والذي لجأ له العديد من الأشخاص لتعامل عبر هذا المجال، لكن استغله البعض بالجانب السلبي بارتكاب الفعل الإجرامي الإلكتروني وذلك لسهولة وسرعة ارتكاب الفعل مع طمس آثاره بالمحو أو إلغاء أو التلاعب بالمعطيات.

ولمكافحة الجريمة الإلكترونية أصبح من الضروري إيجاد وسائل تختلف عن الوسائل التقليدية التي كانت تستعمل في الجرائم التقليدية وذلك لحدثة الجرائم الإلكترونية التي تسبح في عالم افتراضي واسع لا يستطيع تقييده أو الحد من وقوع الفعل الإجرامي الإلكتروني داخله، لذلك سعت العديد من النظم في البحث عن وسائل وأدلة تساعد في الكشف عن الجريمة الإلكترونية وحقيقة ارتكابها، ومن بين أهم الوسائل الحديثة التي ساعدت في الحد من الجرائم الإلكترونية نوعاً ما، الدليل الرقمي الذي تميز لخصوصيته كبيرة في إثبات الجرائم الإلكترونية وذلك لاعتباره دليل قطعي يقيني بأخذ في جميع مراحل التحقيق الجنائي ومن خلال هذا نطرح الإشكالية التالية: ما مدى حجية الدليل الرقمي في اكتشاف الجرائم الإلكترونية؟.

مع طرح بعض التساؤلات:

- ما هو الدليل الرقمي؟.
- ما هي خصائصه وأنواعه؟.
- كيف يتم الحصول عليه؟.
- ما هي الإجراءات التي يجمع لها الدليل الرقمي؟.
- وما مدى حجية الدليل الرقمي في مختلف الأنظمة وما حجته أمام القاضي الجنائي؟.

وللإجابة على هذه التساؤلات قسمنا مداخلتنا عبر الخطة التالية:

1. مفهوم الدليل الرقمي.
- 1.1. تعريف الدليل الرقمي وخصائصه:
 - 1.1.1. تعريف الدليل الرقمي.
 - 2.1.1. خصائص الدليل الرقمي.
 - 2.1. أنواع وأشكال الدليل الرقمي.
 - 1.2.1. أنواع الدليل الرقمي.
 - 2.2.1. أشكال الدليل الرقمي.
 - 3.1. إجراءات والبرامج المختصة بجمع الدليل الرقمي.
 - 1.3.1. الإجراءات التقليدية.
 - 2.3.1. الإجراءات الحديثة.



3.3.1. برامج جمع الدليل الرقمي.

2. حجية الدليل الرقمي في الإثبات الجنائي مختلف الأنظمة وأمام قاضي الجنائي

1.2. حجية الدليل الرقمي في الإثبات في مختلف الأنظمة.

2.2. حجية الدليل الرقمي أمام القاضي الجنائي.

1. مفهوم الدليل الرقمي:

هو عبارة عن معلومات يقلها المنطق والعقل ويعتمدها العلم يتم الحصول عليها بالإجراءات قانونية وعلمية بترجمة البيانات الحاسوبية المخزنة في الأجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شخص له علاقة بجريمة أو الجاني أو المجني عليه (الشيري، 2004، صفحة 88).

ينقسم مصطلح الدليل الرقمي الى شقين:

الشق الأول: الدليل: يعرف على انه الوسيلة التي يتعين بها القاضي في تكوين قناعته القضائية للوصول الى الحقيقة (بن قارة، 2010، صفحة 51).

ويعرف الدليل أيضا على أنه ما يلزم من العلم به علم شيء آخر، وغايته يتوصل العقل الى التصديق اليقيني بما كان يشك في صحته أي التوصل به الى معرفة الحقيقة (أبو قاسم، 1991، صفحة 174).

الشق الثاني: الدليل الرقمي أو الإلكتروني، وهو الدليل الذي يجد أساسا في العالم الافتراضي ويعود الى الجريمة (بن يونس، 2006، صفحة 5).

ومن خلال هذا المنطق الدليل الرقمي الذي تعددت لتعريفاتها على النحو التالي:

1.1. تعريف الدليل الرقمي وخصائصه:

1.1.1. تعريف الدليل الرقمي:

الدليل الرقمي أو الإلكتروني مأخوذ من أجهزة الكمبيوتر ويكون في شكل نبضات كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور والأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون (عبد المطلب، 2006، صفحة 88).

2.1.1. خصائص الدليل الرقمي:

1.2.1.1. صعوبة إثبات جرائم الأنترنت:

تعتبر هذه الخاصية من أهم الخصائص المميزة لجرائم الأنترنت ومن قبل الشخص ذي دراية وما ينجم عن ذلك من سهولة إخفاء معالم الجريمة والتخلص من أثارها وبالتالي صعوبة التحقيق فيها وتتبع مرتكبيها والقبض عليهم أو تعود أيضا صعوبة إثبات جرائم الأنترنت الى:

- صعوبة الاحتفاظ الفني بآثارها.

- تعتمد على قمة الذكاء والمهارة في ارتكابها.

- تعتمد على الخداع في ارتكابها والتظليل في التعرف على مرتكبيها، فإن هؤلاء يعتمدون على التخفي عبر دروب الأنترنت تحت قناع في (هروال، 2007، صفحة 40).



2.2.1.1 تنوع وتطور الدليل الرقمي:

إن الأدلة الرقمية ذات طبيعة ديناميكية فائقة السرعة والقدرة على الانتقال من مكان لأخر عبر شبكات الاتصال غير معترفة لحدود المكان والزمان، فمن خلال الدليل الرقمي يرى البعض ان هناك مرونة في التعامل مع مختلف القضايا الجنائية. خلافا للأدلة التقليدية التي تكون أكثر عرضة للتلف خاصة إذا كان موجود على دعامة ورقية (زروقي، 2018، صفحة 366) .

3.2.1.1 الدليل الرقمي دليل علمي:

إن استخلاص الدليل الجنائي الرقمي وتحليله يتطلب طرقا غير تقليدية بحيث يتم إجراء تجارب عملية وتقنية على جهاز الحاسب الأولي الذي استخدم في جريمة معينة.

وعليه يتم البحث عن الدليل الجنائي الرقمي، يجب ان تكون هذه العملية في إطار جغرافيا نظام افتراضي، الخاضعة لقوانين الإعلام الآلي أو البيئة المعلوماتية ككل (بن يونس، 2006، صفحة 5) .

ومن خلال هذه الخاصية يتبين أنه لا يمكن الحصول على الدليل الجنائي الرقمي او الاطلاع عليه إلا بالوسائل والأساليب العلمية وهذا يعود الى المنشأ الذي تكون منه وفيه هذا الدليل.

4.2.1.1 السعة التخزينية العالية للدليل الرقمي:

يمتاز الدليل الرقمي بقدرة استيعاب كبيرة في التخزين، فأجهزة المعلوماتية المعدة للتخزين الملفات تمتاز بذاكرة كبيرة جدا، وقدرة استيعاب واسعة كآلة الفيديو الرقمية مثلا يمكنها تخزين مئات الصور، والأفلام وديسك صغيرة يمكنه تخزين مكتبة صغيرة، ناهيك عن بطاقات الذاكرة التي تتسع لعشرات الجيغات (بن قارة، 2010، صفحة 63).

5.2.1.1 الدليل الإلكتروني غير ملموس:

وذلك يعني ان ترجمته وإخراجه في شكل مادي ملموس لا يعني ان هذا التجمع يغير دليل بل ان هذه العملية تعتبر عملية نقل تلك البيانات عن مجالها الى شكل ملموس يمكن الاستدلال بها (خليفة، 2007، صفحة 33).

6.2.1.1 الدليل الرقمي للضحية دور فيه:

وذلك إذا كان الجاني يعمل لحساب الضحية لا سيما إذا كان عارفا بأنظمة الحسابات والثغرات الأمنية فيها، او كان مؤتمنا على ذلك كأن يكون هو المسؤول عن المركز المعلوماتي فيشغل مركز الثقة الذي يحوزه (خليفة، 2007، صفحة 38) .

2.1 أنواع الدليل الرقمي وأشكاله:

إن التعريف بالدليل الرقمي يتحتم علينا تحديد أنواعه وأشكاله حتى يسن فهم الهياكل التي يتخذها للحكم قيمته القانونية فيما بعد ولذا سنتناول أنواعه وتحدد أشكاله التي يبدو عليها هذا الدليل وذلك على النحو التالي:

1.2.1 أنواع الدليل الرقمي:

1.1.2.1 أدلة تعتبر وسيلة إثبات:

– السجلات التي يتم إنشاؤها بواسطة الحاسوب تلقائيا، وتغير هذه السجلات من مخرجات الحاسوب التي لا يساهم الأفراد في إنشائها مثل سجلات الهاتف وفواتير البطاقة البنكية.

– سجلات يتم حفظ جزء منها بالإدخال وجزء منها تم إنشاؤه بواسطة الحاسوب مثل رسائل غرف المحادثات المتبادلة على الأنترنت ووسائل البريد الإلكتروني (فرغلي و سعيد ، 2007، صفحة 14) .



2.1.2.1. أدلة لاتعد لتكون وسيلة إثبات:

وهذا النوع من الأدلة الإلكترونية نشأ من دون إدارة الفرد، أي أنها يتركه الجاني دون أن يكون راغبا في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وفيها يمكن تسميته أيضا بالآثار المعلوماتية الرقمية، وتتجسد في الآثار التي يتركها مستخدم شبكة الأنترنت بسبب تسجيل الرسائل المرسله منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسوب وشبكة الأنترنت حيث أن هذا النوع من الأدلة لم يعد أساسا للحفظ من قبل من صدر عنه غير أن الوسائل الفنية الخاصة التي تجرى عبر الأنترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها كلما يمكن ضبطها بواسطة تقنية خاصة (خلف و حمداني، 2016، صفحة 65).

2.2.1. أشكال الدليل الرقمي:

يتخذ الدليل الإلكتروني أو الرقمي ثلاثة أشكال رئيسية هي الصورة الرقمية، التسجيلات، النصوص المكتوبة، وتتناول هذه الأشكال على النحو التالي.

1.2.2.1. الصورة الرقمية: هي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقديم الصورة إما في شكل ورقي أو شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تتمثل في التكنولوجيا البديلة للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطورا ولكنها ليست بالصورة الأفضل من الصور التقليدية.

2.2.2.1. التسجيلات الصوتية: وفي التسجيلات التي يتم ضبط تخزينها بواسطة الألة الرقمية وتشمل المحدثات الصوتية على الأنترنت... إلخ.

3.2.2.1. النصوص المكتوبة: وتشمل النصوص التي يتم كتابتها بواسطة الألة الرقمية، ومنها الرسائل عبر البريد الإلكتروني، الهاتف المحمول، البيانات المسجلة بأجهزة الحاسب الألي... إلخ (عبد المطلب، ممدوح عبد الحميد، 2005، صفحة 10).

3.1. الإجراءات والبرامج المختصة بجمع الأدلة الرقمية:

1.3.1. الإجراءات المختصة بجمع الأدلة الرقمية:

لجمع الدليل الرقمي الذي يكشف عن حقيقة ارتكاب الجرائم المعلوماتية يجب أن يمر على إجراءات تقليدية التي تتميز بها باقي الجرائم التقليدية بالإضافة إلى إجراءات حديثة وذلك لحداثة وتطور الجرائم المعلوماتية التي تقع داخل العالم الافتراضي لذلك سوف نفصل هذا في ما يلي:

1.1.3.1. الإجراءات التقليدية في البيئة الرقمية:

1.1.1.3.1. المعاينة في البيئة الرقمية:

يقصد بالمعاينة رؤية المكان أو الشخص المشتبه فيه وأي شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة (بن قارة، 2010، صفحة 86)، وتمت المعاينة التقنية في البيئة الرقمية من خلال انتقال ضباط الشرطة القضائية إلى محل الدليل الرقمي والتي يوجد مكانه في جهاز الحاسب الألي وتحديد ذلك البيانات الرقمية في ذاكرة الجهاز، في إطار ذلك تتم الاستعانة في ذلك بمختصين وخبراء في الإعلام الألي (بوعتاد، 2013، صفحة 67).

وتعرف المعاينة في علم التحقيق الجنائي ب"مشاهدة المكان الذي ارتكبت فيه الجريمة وعمل وصف شامل له، سواء لكتابة أو بالرسم التخطيطي أو بالتصوير لإثبات حالته بالكيفية التي تركها بها الجاني (خالد ممدوح، 2009، صفحة 149).



2.1.1.3.1. صلاحية المعاينة في كشف وضبط الدليل الجنائي الرقمي:

البعض يرى ان دور المعاينة يتضاءل في الكشف عن الجريمة المعلوماتية، وسبب ذلك ان الجريمة التقليدية تجرى غالبا على مسرح جريمة يخلف آثار مادية، وهذا المسرح يعطي المجال أمام جهة البحث والتحري في الكشف عن غموض الجريمة، على عكس مسرح الجريمة المعلوماتية التي يتضاءل فيه دور المعاينة، بسبب ان الجريمة المعلوماتية قلما تخلف آثار مادية بالإضافة الى إمكانية التلاعب في الأدلة الجنائية الرقمية عن بعد عن طريق محوها أو إتلافها (هروال، 2007، صفحة 217).

وعليه ولنتجاوز هذا الإشكال، ينبغي على الفنيين القائمين على عملية المعاينة، التعامل مع المسرح الجريمة المعلوماتية على انه مسرحان -مسرح تقليدي(مادي): ويشمل هذا المسرح جميع المكونات المادية للحاسب الآلي، ويمكن ان يحتوي على آثار مادية مثل بصمات الجاني أو وسائط تخزين رقمية، أو أوراق.

-مسرح افتراضي (رقمي): ويقع داخل العالم الافتراضي (الرقمي) الجهاز الحاسب الآلي وتحتوي على جميع المعلومات والبيانات الرقمية المخزنة فيه والتي تفيد التحقيق (بوعتاد، 2013، صفحة 68).

3.1.1.3.1. إجراءات المعاينة التي تتم أمام مسرح الجريمة للعالم الافتراضي:

-لقيام بتصوير الجهاز الحاسب الآلي، وكل ما يتصل به من أجهزة ظرفية ومحتوياته الذي بواسطته ارتكاب الجرائم (رستم، 1994، صفحة 60).

-العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والأثار الإلكترونية التي يخلقها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية، التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم على طريقة الولوج الى النظام أو الموقع أو الدخول معه في الحوار (حجازي، 2006، صفحة 104).

-الاستعانة بأهل الخبرة عند الضرورة.

-تأمين التيار الكهربائي من الانقطاع المفاجئ، لأن ذلك يسبب العديد من المخاطر تتمثل في محو المعلومات في الذاكرة من جراء غلق جهاز الكمبيوتر وبالتالي فقدان كافة العمليات التي كان يتم تشغيلها واتصالات الشبكة والأنظمة الثابتة (عبد المطلب، ممدوح عبد الحميد، 2005، صفحة 115).

4.1.1.3.1. التفتيش في البيئة الرقمية:

-يعد إجراء التفتيش من إجراءات التحقيق التي تهدف الى البحث عن الحقيقة في مستودع السر، تبرز الغاية من هذا الإجراء هو الوصول الى الأدلة التي تساهم بشكل كبير في إظهار الحقيقة واكتشافها، يعرف التفتيش في البيئة الرقمية بأنه إجراء يسمح باستخدام الوسائل الإلكترونية لجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني وهذا يشمل محل التفتيش في البيئة الرقمية الحاسب الآلي والمزود الآلي للخدمة وملحقات التقنية (النيل، 2012، صفحة 39).

-وبين المشرع الجزائري موقفه من خلال القانون رقم 09-04 المتعلقة بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها، إذ ينص صراحة على تفتيش أنظمة الحاسب الآلي، وذلك بموجب نص المادة 05 منه، بحيث يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانوني الإجراءات الجزائية الدخول لغرض التفتيش ولو عن بعد



الى المنظومة المعلوماتية او جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، وكذا منظومة تخزين المعلوماتية (المادة 5 من قانون رقم 04-09 المتعلق بالقواعد الخاصة للرقابة من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال ومكافحتها) .

- وإضافة الى ذلك نشير الى المشرع الفرنسي الذي نص على تفتيش أنظمة الحاسب الألي من خلال المادة 94 من قانون الإجراءات الجزائية، إذا انه نص على: يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها الى أشياء او معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة، وذلك طبعاً بعد تعديل هذه المادة بموجب المادة 42 من قانون رقم 545-204 المؤرخ في 2004/06/21، المتعلق بالثقة مع الاقتصاد الرقمي والذي أضاف لنص المادة عبارة المعطيات المعلوماتية (سعيداني، 2013، صفحة 106) .

5.1.1.3.1 الخبرة في البيئة الرقمية:

الخبرة القضائية هي الإشارة الفنية التي يستعين بها القاضي او المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها الى معرفة او دراية عملية خاصة، إذن فالخبرة وسيلة لتحديد التفسير للأدلة للاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلاً مستقلاً وإنما هي تقييم في هذا الدليل (بوعتاد، 2013، صفحة 71).

يستوجب وجود خبير ذو دراية عالية للاستعانة به في مجال الجريمة المعلوماتية ضروري وذلك لسبب ان عملية استخلاص الأدلة الجنائية الرقمية تتطلب مهارة ودراية كبيرة في مجال الحاسب الألي، ولهذا كان لزاماً ان يتم اللجوء الى خبير فني ومختصين (ثنيان، 2012، صفحة 156) .

6.1.1.3.1 ضوابط التي تحكم عمل الخبير في مجال المعلومات:

تطبق على الخبير ضوابط المنصوص عليها في المادة 145-144 التي نص عليها قانون الإجراءات الجزائية خلال ذكره لضوابط التي يجب ان تتوفر في الخبير أثناء أداء خبرته في الجرائم التقليدية أما بالنسبة لضوابط الفنية يتوجب على الخبير ان يكون ملماً بكل ما يتعلق بالحاسب الألي وملحقاته، ووجوب تمكنه وفهمه البيئة التي يعمل فيها والقدرة على أداء المهام الموكلة له دون ان يترتب على ذلك ضرراً للدليل الجنائي الرقمي المراد استخلاصه (حجازي، 2006، صفحة 331) .

2.1.3.1 الإجراءات الحديثة في البيئة الرقمية:

1.2.1.3.1 حفظ المعطيات:

الزام المشرع الجزائري مقدمي الخدمات بحفظ المعطيات، وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في الأرشيف ووضعها في ترتيب معين، في حين اتخاذ الإجراءات القانونية أخرى، المحتملة الأخرى كالتفتيش وغيره، وقد حصر المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة، وهي المعطيات المتعلقة بحركة السير (معطيات المرور) وهي عرفتها المادة 2 من قانون رقم 04-09 تلك المعطيات المتعلقة بالاتصال عن طريق المنظومة المعلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة الاتصالات توضح مصدر الاتصال، الوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم مدة الاتصال ونوع الخدمة (سعيداني، 2013، صفحة 61) .

وقد حصر المشرع الجزائري معطيات المرور التي ألزم بحفظها في المادة 11 من قانون 04-09 ويتضمن ما يلي:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

- المعطيات المتعلقة بالتجهيزات الظرفية المستعملة للاتصال.

- الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال.



- معطيات متعلقة بالخدمات التكميلية المطلوبة او المستعملة ومقدميها المعطيات التي تسمح بالتعرف على المرسل إليه، الاتصال وكذا عناوين المواقع المطلع عليها، وبما ان حفظ المعطيات إجراء فني، واختراقا للحق في الخصوصية، فان المشرع الجزائري فرض على مزودي الخدمات يعتبرون مصدر الجهات التحقيق وللحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها، وفي نفس الوقت ملزمين بوضعها تحت تصرف هذه الجهات إذا ما تم طلبها (المادة 11 من قانون 09-04).

1.3.1.2.2. التسرّب:

إن التطور الهائل الذي عرفه العالم مؤخرا بصفة عامة وللمجتمع الجزائري بصفة خاصة أدى الى ظهور بعض الجرائم المستحدثة الخطيرة التي تهدد استقراره وكيانه، ومحاربتها اعتمد المشرع الجزائري منظومة قانونية جديدة بتعديله لقانون الإجراءات الجزائية بموجب القانون (06-22)، المؤرخ في 20/12/2006 أدخل فيها تقنيات جديدة للبحث والتحري عنها ومن بينها التسرّب.

والتسرّب يعتبر إجراء خطير لكونه يعد اختراقا في أوساط المجموعات الاجرامية وكذا المساس بخصوصية الأفراد وحرياتهم عن طريق استعمال هوية مستعارة للعون المتسرب دون علمهم بهدف إثبات والكشف عن الجرائم ومركبيها، وبالتالي تم تغليب مصلحة المجتمع على المصلحة الخاصة للفرد، ويبقى الدليل المستمد من هذا الأسلوب غير كاف في غياب أدلة اخرى تدعمه (بوعتاد، 2013، صفحة 69).

وهذا وفقا لما جاء في نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية الذي يعطي الحق لضباط او عون الشرطة التنكر وباستعمال هوية مستعارة للتعامل مع المجرمين او المخترقين وذلك للكشف عن الحقيقة.

1.3.1.3.2. شروط صحة التسرّب: حسب المادة 65 مكرر 12 من قانون إجراءات الجزائية:

- صدور إذن من وكيل الجمهورية، او قاضي التحقيق بعد إخطار وكيل الجمهورية.

- ان يكون الإذن مكتوبا ومسببا.

- يذكر في الإذن الجريمة التي تبرر اللجوء الى هذا الإجراء وهويته ضابط الشرطة.

- مدة إجراء التسرّب: لا تتجاوز 6 أشهر ولكن يمكن تجديد المدة (المادة 65 مكرر 11 من قانون رقم 22/06).

1.3.1.4.2. اعتراض المراسلات الإلكترونية:

يقصد بهذا الإجراء مراقبة الاتصالات الإلكترونية أثناء بثها وليس الحصول على الاتصالات الإلكترونية مخزنة، وقد استحدث المشرع الجزائري هذا الإجراء من خلال القانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال حيث حددت الحالات التي يجب فيها اللجوء الى المراقبة الإلكترونية كالأفعال الموصوفة لجرائم الإرهاب، او التخريب، او جرائم الماسة بأمن الدولة، او في حالة توفير معلومات عن أعمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام او مؤسسات الدولة او في إطار تنفيذ طلبات مساعدة قضائية، وتستخدم المراقبة الاتصالات التي تكون مباشرة وسرية ومخزنة في وسائط مادية قابلة للنقل كدليل في إثبات الجريمة الواقعة (بوعتاد، 2013).

1.3.1.5.2. المراقبة الإلكترونية:

تم استحداث هذا الإجراء بموجب قانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (الجريدة الرسمية رقم 47، الصادرة بتاريخ 16-08-2009 بلا تاريخ).



6.2.1.3.1. تعريف المراقبة الإلكترونية:

بالرجوع الى قانون رقم 04-09 السابق ذكر، لم يعرف المشرع الجزائري بإجراء المراقبة الإلكترونية بل تلك أمر تعريفها للفقهاء ومنه تعرف بأنها عمل أمني أساس له نظام معلومات إلكترونية، يقوم فيه المراقب بمراقبة المراقب بواسطة الأجهزة الإلكترونية وعبر شبكة الأنترنت، لتحقيق غرض محدد، وإفراغ النتيجة في ملف إلكتروني وتحرير تقارير بالنتيجة (موسى، 2005، صفحة 192). يمكن القول أن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه (هروال، 2007، صفحة 199). يقوم ضابط الشرطة القضائية ذو الكفاءة تقنية عالية الذي يعد كمراقب إلكتروني، والمراقبة الإلكترونية لا ليست للحد من الوقوع في الجرائم الإلكترونية فقط بل تعد أيضا كوسيلة وقائية تدرج ضمن التدابير الوقائية من الجريمة المعلوماتية (سعيداني، 2013، صفحة 184).



2.3.1. طرق الجمع والحصول على الدليل الرقمي:

مصادر الحصول على الدليل الرقمي	البرامج المتقدمة في جمع الدليل الرقمي	الأجهزة والأنظمة الواجب فحصها للحصول على الدليل الرقمي	الحصول على الدليل الرقمي من البروتوكولات الأنترنت
1 الكمبيوتر الخاص بالمشتبه فيه: وذلك بفحص جهاز الكمبيوتر المتهم المشتبه فيه، وخاصة وحدة التخزين الدائمة، القرص الصلب، Hardisk والوحدات الفرعية الملحقة وتشمل على القرص المرن وأقراص الليزر أو أي وحدة تخزين أخرى من الممكن استعمالها مثل جهاز flash Memory، كل تلك الأجهزة يمكن فحصها وبيان الطريقة التي قام بها المتهم في ارتكاب الجريمة. 2- جهاز الكمبيوتر الجني عليه: مما لا شك فيه انه الجني عليه هو المصدر الكاشف والنتيجة التي يترتب عليها ما قام به المشتبه فيه من جرائم والجني عليه قد يكون شخص طبيعي أو مؤسسة مالية، أو هيئة حكومية وغيرها. وبالتالي فعلى فحص مثل تلك الأجهزة يمكن للمحقق من معرفة الدخول وتتبع مصادر المشتبه فيه. 3. مقدم خدمة الانترنت : يمكن الاستعانة أيضا في كشف الأدلة الإلكترونية بعدة جهات أخرى مثال: مقدم خدمة الانترنت مثل شركة yahoo، جوجل google، او sms فان مثل تلك الشركات تنفع في مساعدة معرفة هوية المجرمين والمشتبه فيهم بالإضافة الى البريد الإلكتروني يساعد على معرفة موقع وهوية المجرم.	برامج إذن التنفيذ: Computer schorch warrant program قرص بدء تشغيل الكمبيوتر. Bootable diskette برنامج النسخ مثل. Lab Link برنامج معالجة الملفات. Xtree pro gold برامج كشف الديسك: مثل Amadisk, new disk برامج الاتصالات: La ntastic (الغافري، 2019، صفحة 419)	فحص نظام الاتصال بالانترنت: وذلك بفحص الانترنت الذي يشكل الحركة التراسلية للنشاط الممارس من خلال الانترنت فحص النظام الأمني للشبكة: وذلك خلال ربط بشبكة الانترنت او بدون الربط شبكة الانترنت. نظام فحص البروتوكول الانترنت: فحص الخادم او الملقم وهو الذي يترصّد تحركات المستخدم خلال الاتصال بالمواقع والصفحات التي يتم استضافتها على هيئة رقمية فيه. فحص مكونات الكمبيوتر : -فحص القرص الصلب -فحص البرمجيات فحص النظام المعلوماتي: فحص نظام الذاكرة التخزين caching فحص الطابعة فحص لوحة المفاتيح.	الحصول على الدليل من البروتوكولات الأنترنت. T.C.P. Transmission control porotocl بروتوكول التحكم بالنقل، او بروتوكول التحكم بالإرسال، او مفاق التحكم بالنقل، هو بروتوكول مهم وأساسي في بروتوكولات الأنترنت يؤمن نقلا موثوقا خالي من الأخطاء. IP. Internet Protocol : بروتوكول الانترنت (هال، 1997، صفحة 11) وهو المعرف الرقمي لأي جهاز مرتبط بالأنترنت.

2. حجية الدليل الرقمي في بعض الأنظمة والتشريعات وأمام القاضي الجنائي من ناحية الإثبات الجنائي:

1.1.2. حجية الدليل الرقمي في النظم الإجرائية للإثبات:

لقد اختلفت النظم الإجراءات الجنائية وتنوعت تبعا لاختلاف الأوضاع الاجتماعية والسياسية للشعوب، هذه الأوضاع التي فرضت على التشريعات الجنائية على ان تنتهج نظاما إجرائيا معيناً من أجل العمل على إثبات الجريمة، فمنها ما يأخذ بنظام الإثبات الحر



وان أي دليل يكون مقبولا للإثبات، ومنه ما جعل الدليل مقيدا في نصوص قانونية على سبيل الحصر إذا لا يجوز الخروج عنها، ومنها من أخذ بالنظامين معا، او بما يعرف بالنظام المختلط للإثبات الجنائي، وعليه سوف نحاول إسقاط قواعد النظم الإجرائية للإثبات الجنائي على الدليل الرقمي.

2.1.2. حجية الدليل الرقمي في النظام الإثباتي المقيد:

يقوم نظام الإثبات المقيد على مبدأ أساسيا يتمثل في ان المشرع الجنائي يعد سلفا الوسائل ومختلف الطرق التي يعتمد عليها في إقامة الدليل الجنائي على مرتكبي الجرائم، فوفقا لهذا الاتجاه فإن المشرع هو الذي يحدد الأدلة التي يجوز للقاضي اللجوء إليها ويقدر قيمتها الإقتناعية (هلال، عبد الاله أحمد، 1997، صفحة 22).

حيث يقتصر دور القاضي في هذا النظام على مجرد فحص الدليل والتأكد من توافر الشروط التي حددها القانون، فلا سبيل للاستناد على دليل ينص عليه القانون صراحة ضمن أدلة الإثبات، كما لا دور للقاضي في تقدير القيمة الاستدلالية للدليل، حيث ان القانون يقيد القاضي بقائمة الأدلة التي حددت قيمتها الإثباتية (هلال، عبد الاله أحمد، 1997، صفحة 22).

3.1.2. حجية الدليل الرقمي في نظام إثبات الحر:

يسود نظام الإثبات الحر في القوانين الإجرائية اللاتينية بحيث يتمتع القاضي بموجب هذا النظام بالحرية المطلقة في إثبات الوقائع المفروضة عليه ولا يلزمه القانون بأدلة معينة للاستناد عليها في تكوين قناعته الشخصية، وإن حجية الأدلة الإلكترونية لا تثير أي صعوبات متعلقة بمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة، وباعتبارها أدلة إثبات في المواد الجنائية ام لا، بل ان العنصر الأساسي وفق هذا المدة هو مدى حرية قاضي الموضوع في تقدير هذه الأدلة، ومدى قبول الأدلة الناشئة عن الآلة او الأداة العلمية مثل أجهزة التصوير وأجهزة التنصت والتسجيل وغيرها من الوسائط الرقمية، كدليل قائم بذاته كاف لإثبات الإدانة او البراءة (بالهادي، 2009، صفحة 27).

فالقاضي في هذا النظام يتمتع بدور إيجابي في مجال الإثبات وبالمقابل تقييد دور المشرع، وعليه ففي هذا الاتجاه لا تتور مشكلة مشروعيتها الدليل الرقمي من حيث وجود على اعتبار ان المشرع لم يعهد إليه مهمة تحديد قائمة أدلة الإثبات وكذلك فمسألة قبول الدليل لا ينال منها سوى مدى اقتناع القاضي به (بالهادي، 2009، صفحة 28).

4.1.2. حجية الدليل الرقمي في النظام للإثبات المختلط:

يقوم النظام المختلط على أساس الجمع بين خصائص النظام المقيد ونظام الإثبات الحر، وقد حاول تفادي أوجه النقد الى وجهت للنظامين السابقين، وهو الاتجاه الذي يجمع بين النظامين اللاتيني والأنجلوساكسوني، إذا يعتمد أساسا ان القانون يحدد أدلة معينة لإثبات وقائع دون بعضها الآخر، وقد يحدد قبول الدليل بشروط معينة في بعض الحالات، كما يعطي للقاضي الحرية في تقدير الأدلة القانونية على غرار القانون الجزائري الذي حدد الأدلة التي يمكن للقاضي اعتمادها للوصول الى الحقيقة، أما بالنسبة للأدلة الرقمية فيرى الفقه بأن السجلات الإلكترونية مغناطيسية تكون غير مرئية، لذلك لا يمكن ان تطرح كدليل أمام جهات القضاء إلا إذا تم تحويلها الى صورة مرئية عن طريق الطباعة وبالتالي يمكن قبول الدليل (هلال، عبد الاله أحمد، 1997، صفحة 29).

5.1.2. فيما يخص حجية الدليل الرقمي في الجزائر:

المشرع الجزائري قد أخذ بنظام الإثبات الحر شأن المشرع الفرنسي فمن خلال استقراء نصوص قانون الإجراءات الجزائية، نلاحظ مدى تكريسه لمبدأ اقتناع الشخصي للقاضي، حيث نص المادة 212 منه على: "يجوز إثبات الجرائم بأي طريقة من الطرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي ان يصدر حكمه تبعا لاقتناعه الخاص ...". كما نصت المادة 307 من نفس القانون على ان القانون لا يطلب من القضاة ان يقدموا حساب عن وسائل التي بها قد وصلوا الى تكوين قناعته ولا



يرسم لهم قواعد بما يعين عليهم ان يخضعوا لها على الأخص تقديراتهم، ولكن يأمرهم بأن يسألوا أنفسهم في صمت وتدبير وان يبحثوا بإخلاص ضمائرهم في أي تقييم للأدلة وهنا ترى ان قانون الجزائري اعطى الحرية في اقتناع القاضي خلال سلطته التقديرية للدليل الرقمي (المادتين 212 و 307 من ق.إ.ج.ج).

2.2. حجية الدليل الرقمي أمام قاضي التحقيق:

1.2.2. اقتناع القاضي بالدليل الرقمي:

حرصت الكثير من التشريعات والأنظمة على جعل مبدأ الاقتناع القاضي عنوانا لإثبات الجزائي، حيث يستند اليها القاضي في حكمه وذلك بإعطائه الحرية في الاقتناع بالدليل الرقمي بشرط ان يكون للقاضي الإيمان العميق بالركون الى صحة الوقائع التي يأخذ بها اقتناعه ويجب ان يكون حكمه خاضع لضميره دون تقييد، ما عدا ما يضبطه من قيود وضوابط التي وضعها القانون (مروان، 1999، صفحة 427).

2.2.2. سلطة القاضي في تقدير الأدلة الرقمية:

القاضي الجنائي الحرية في ان يستعيد الدليل ويطرحه إن لم يطمئن اليه، بأخه كاملا او يأخذ بالجزء الذي يطمئن إليه ويقتنع بصحته وهو الأمر الذي يتطبق على الدليل الرقمي سواء كانت في بيئتها الرقمية، إما على شكل مخرجات طباعة او اتخذت على شكل صور او مقاطع فيديو (عبد الغني، 2007، صفحة 85).

1.2.2.2. حرية القاضي الجنائي في استبعاد الدليل الرقمي:

للقاضي ان يستبعد في مجال تقديره للدليل مالم يطمئن اليه عندما يمارس سلطة في الدعوى موضوعيا، ويعود عدم اطمئنان القاضي لقيمة الدليل الذي يطرحه تكمن في ضعف الدليل المستبعد في الدلالة على حقيقة التي يسعى الحكم في جعلها عنوانا له في ذلك القضاء. او لأن هناك أدلة أقوى منه في الإثبات وكافية في تكوين قناعته المحكمة (زكي، 2010، صفحة 158).

2.2.2.2. حرية القاضي الجنائي في الأخذ بالدليل الرقمي:

هذه الحرية لها صورة عديدة فالقاضي يأخذ بمبدأ الاقتناع القاضي فيما يتعلق بالدليل، فللقاضي ان يأخذ به كاملا او يأخذ بجزء منه دون الجزء الآخر وان يأخذ به المتهم دون شريكه وان يأخذ بالدليل في حالة تعدد التهم دون التهم الأخرى (زكي، 2010، صفحة 159).

3.2.2.2. ضوابط قبول اقتناع القاضي بالدليل الرقمي:

إن الأدلة المتحصلة عن الآلة تنير إشكالية عدم قبولها لدى القضاء نتيجة عدم تعبيرها عن الحقيقة نظر لما يمكن ان تخضع له طرق الحصول عليها من التعرض للتزييف والتحريف والأخطاء المتعددة وسرعة إتلافها او تغييرها ولم يفيد المشرع الجزائري بشروط وضوابط خاصة بل تركها للقاضي.

لذلك يتعين على القاضي لقبول هذه الأدلة كأساس تستفيد إليه الحقيقة في الدعوى العمومية سواء كان الحكم فيها بالإدانة او البراءة توافر بعض الشروط والضوابط أهمها:

1.3.2.2.2. الضوابط التي تتعلق بمصدر الاقتناع: تتمثل في:

- ضابط مشروعية الدليل الرقمي وذلك ان يكون الدليل الإلكتروني مقبولا فعلى القاضي ان يستمد اقتناعه من أدلة مقبولة ومشروعة وتحترم الإنسان وحرية (مروك، 2003، صفحة 519).



-ضابط ضرورة طرح الدليل الإلكتروني في جلسة المناقشة، يجب على القاضي ان يستمد قناعته من أدلة طرحت بالجلسة وخصصت للمناقشة بين الخصوم تبعا لمبدأ الشفافية المذكورة في المواد 300، 304، 353 من قانون الإجراءات الجزائية ومبدأ العلنية بحسب مواد 285، 342، 355، 399 من نفس القانون "قانون الإجراءات الجزائية الجزائري" (عبد الحميد، 2020، صفحة 488).

2.3.2.2. الضوابط التي تتعلق بالاقتناع ذاته:

وجب على القاضي ان يصدر حكمه على اقتناع يقيني بالإضافة الى ضابط ملائمة الاقتناع القضائي لمقتضيات العقل والمنطق أي أنه على القاضي استنتاج الحقيقة الواقعة وما كشف عنها من أدلة لا يخرج عن مقتضيات العقل والمنطق من غير تعسف في الاستنتاج، بالإضافة الى ضرورة توفر ضابط مهم حتى لا يشيد القاضي في حكمه وهو مراقبة المحكمة العليا لسلطة القاضي الجنائي (عبد الحميد، 2020، صفحة 488).

الخاتمة:

في ختامنا لدراسة الموضوع نلاحظ ان الدليل الرقمي يعد من أهم الوسائل التي تكشف عن الجرائم الإلكترونية، وله حجية في الإثبات الجنائي، وهذا بمعنى أنه دليل يستعمل لإثبات الجرائم الإلكترونية الواقعة له مميزات وخصائص، وبمر هذا الدليل على إجراءات خلال مرحلة الجمع للحصول عليه مثل أي دليل آخر يستعمل في الجرائم التقليدية إلا أنه اعتمد على أدلة أخرى وهي حديثة وذلك لحداثة الجرائم الإلكترونية الواقعة في العالم الافتراضي، ولكن قد يعرض هذا الدليل إشكالية نوعا ما وهو التعدي على الخصوصية المعلوماتية للأفراد لكن الإشكال في ذلك إن كان هذا التعدي له ضوابط وحدود للكشف عن الجرائم الإلكترونية، ويستمد هذا الدليل حجتيه ويقينته من السلطة التقديرية للقاضي الذي يحكم في الدليل باقتناعه الشخصي الذي يكون بضمير ونزاهة وطبعا بعد ما يتأكد من مبدأ مشروعيته هذا الدليل ومن خلال هذا سوف نتطرق الى بعض الاقتراحات والتوصيات.

1- يستوجب على القاضي إتباع كل الضوابط التي نص عليها المشرع خلال مرحلة تقييمه للدليل وذلك لحماية الخصوم وحماية الحرية الشخصية لكل طرف منهم.

2- يجب تأسيس مخبر تقنية وتكنولوجية تحليلية ذات كفاءة عالية لتتمكن من فك الشفرات الصعبة التي يستخدمونها المتمرسون المتميزون بالذكاء الخارق وأيضا لتحقيق العبء على الشرطة القضائية العلمية من كثرة المعطيات والبيانات التي يتحصلون عليها خلال استخدام الدليل الرقمي.

3- يجب تشريع خاص وتمثل بالجرائم المعلوماتية الإلكترونية وذلك ليشمل دراسة معمقة ومفصلة من كل النواحي والجوانب المتعلقة بهذه الجرائم وخاصة بعدما استفحلت هذه الأخيرة على كافة المجتمعات والعالم بأسره.

4- ضرورة الالتزام بالأحكام الدستورية التي تحمي الخصوصية والحرية الشخصية خلال القيام بالإجراءات التي يجمع فيها الدليل الرقمي.

قائمة المراجع

أبو قاسم، أ. (1991). الدليل الجنائي ودوره في إثبات جرائم الحدود والقصاص. الرياض: منشور بالمركز العربي للدراسات المنية والتدريب.

1. الجريدة الرسمية رقم 47، الصادرة بتاريخ 2009/08/16.

2. الغافري، ح. (2019). السياسة الجنائية في مواجهة جرائم الانترنت. جامعة أسبوط: كلية الحقوق.

3. المادة 11 من قانون (s.d.). 04-09 المتعلق بالقواعد الخاصة بالرقابة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.



4. المادة 5 من قانون رقم 04-09 المتعلق بالقواعد الخاصة للرقابة من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها (s.d.).
ج. ر. عدد 47 المؤرخ في 16 أوت 2009.
5. المادة 65 مكرر 11 من قانون رقم 06/22 المؤرخ 20 ديسمبر 2006، المعدل والمتمم لقانون الإجراءات الجزائية، ج، عدد 84 الصادر بتاريخ 24 ديسمبر 2006، الجزائر.
6. المادتين 212 و 307 من ق.إ.ج.ج.
7. النيل، ع. (2012). إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية. العراق: دار الكتب والوثائق القومية.
8. الشيربي، م. (2004). التحقيق في الجرائم المستحدثة. الرياض: جامعة فائق العربية للعلوم الأمنية.
9. بالهادي، ح. (2009). حجية الدليل الرقمي في الإثبات الجنائي. مجلة البحوث والدراسات القانونية والسياسية، المجلد التاسع، العدد الأول.
10. بن قارة، ع. (2010). حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دون طبعة. الاسكندرية: دار الجامعة الجديدة الإسكندرية.
11. بن يونس، ع. (2006). مذكرة الإثبات الجنائي عبر الانترنت. مصر: ندوة الدليل الرقمي بمقر جامعة الدول العربية.
12. بوعتاد، ف. (2013). مكافحة الجريمة الإلكترونية في تشريع الجزائري. جامعة الجيلالي اليابس، سيدي بلعباس: مجلة الندوة الدراسية للقانون، العدد 01.
13. ثنيان، ن. (2012). إثبات الجريمة الإلكترونية، دراسة تأصيلية تطبيقية، رسالة ماجستير. السعودية: جامعة فائق العربية للعلوم الأمنية، كلية الدراسات العليا.
14. حجازي، ع. (2006). مبادئ الجنائية في جرائم الكمبيوتر والانترنت. الاسكندرية: دار الفكر الجامعي، الإسكندرية، ط. 1.
15. خالد ممدوح، ا. (2009). فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى. مصر: دار الفكر الجامعي.
16. خلف، م. &، حمداني، ح. (2016). مشروعية الأدلة الإلكترونية في الإثبات الجنائي. القاهرة: مجلة البحوث والدراسات العليا العربية، العدد 65 المجلد 16.
17. خليفة، م. (2007). الحماية الجنائية لمعطيات الحاسب الألي في قانون الجزائري والمقارن. الاسكندرية: دار الجامعة الجديدة.
18. رستم، ه. (1994). الجوانب الإجرامية للجرائم المعلوماتية (دراسة مقارنة) أسبوط: مكتبة الآلات الحديثة.
19. زروقي، ع. (2018). طرق الإثبات في ظل قانون الإجراءات الجزائية الجزائري. جامعة سعيدة: أطروحة دكتور في الحقوق، كلية الحقوق والعلوم السياسية.
20. زكي، أ. (2010). الإثبات في المواد الجنائية. الإسكندرية: الفنية للطباعة والنشر.
21. سعيداني، ن. (2013). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية. باتنة، الجزائر: جامعة الحاج لخضر.
22. عبد الحميد، ع. (2020). الدليل الرقمي كحجية لإثبات أمام القاضي الجزائري في المعاملات الإلكترونية. الجزائر: مجلة الصوت، المجلد السابع، العدد 10 ماي.
23. عبد الغني، ش. (2007). الحماية الجنائية للمعاملات الإلكترونية. الاسكندرية: دار الجامعة الجديدة.
24. عبد المطلب، م. (2006). البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت. الاسكندرية: دار الكتب القانونية.
25. عبد المطلب، ممدوح عبد الحميد. (2005). أدلة الصور الرقمية في الجرائم عبر الكمبيوتر. دبي: مركز الشرطة.
26. فرغلي، ع. &، سعيد، و. (2007). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة مقارنة. جامعة نايف العربي للعلوم الأمنية، الرياض: المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي.



27. مروان م. (1999). نظام الإثبات في المواد الجنائية في القانون الرقمي. حلب: ديوان المطبوعات الحلبية.
28. مروت ن. (2003). محاضرات في الإثبات الجنائي. دار هومة، الجزائر: نظرية العامة لإثبات الجنائي، الجزء الأول.
29. موسى م. (2005). المراقبة الإلكترونية عبر شبكات الأنترنت (دراسة مقارنة بين المراقبة الامنية التقليدية والإلكترونية) مصر: دار الكتب القانونية.
30. هروال ن. (2007). الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة) الجزائر: دار الفكر الجامعي، ط.1.
31. هلال ع. (1997). تقنيتين نظام الحاسب الآلي وضمانات المتهم المعلوماتية. القاهرة: دار النهضة العربية.
32. هلال عبد الله أحمد. (1997). حجية المخرجات الكمبيوترية. القاهرة: دار النهضة العربية.



سلطة القاضي الجنائي في تقدير الدليل الرقمي

بن حليلة سعاد

souad.benhalima@univ-relizane.dz

كلية الحقوق و العلوم السياسية جامعة غليزان

مخبر التشريعات الدولية للبحار وأثرها على المنظومة القانونية البحرية في الجزائر

مقدمة

مبدأ حرية القاضي في الاقتناع بالدليل الرقمي هو أساس الإثبات بالوسائل العلمية في المواد الجزائية، ومفاد هذا المبدأ أن القاضي الحر في تكوين اقتناعه الشخصي القائم على فكري قبول الدليل و تقييمه حتى يكون حكمه مبنيا على الجرم و اليقين. كون أن القاضي الجنائي حر في الاستعانة بكافة طرق الإثبات المتوصل لكشف الحقيقة فلا يجوز أن يكتفي بفحص الأدلة المقدمة من أطراف الدعوى، بل يجب عليه أن يتحرى بنفسه عن الأدلة و يستعين بالأشخاص المؤهلة أكثر منه لفهم الدليل أو تقديره. وبالتالي فان القاضي الجنائي له حرية وسلطة واسعة في مجال الإثبات الجنائي، ولكن لا تعتبر هذه السلطة المطلقة، وإنما في الحقيقة أن المشرع وضع لهذه السلطة ضوابط جعلها بمثابة صمام أمان في مواجهة انحراف القضاة عند ممارستهم لها، و كذلك لضمان عدم اختلال الأحكام.

ونظرا إلى أن الجريمة المعلوماتية أصبحت تستفحل المجتمعات نظرا للتطور التكنولوجي الذي يشهده العالم مما يجب اللجوء إلى الدليل الإلكتروني الذي له أهمية كبيرة لما يتمتع به من خصائص تجعله يسمو على الأدلة الكلاسيكية كون هذه الأخيرة أصبحت لا تواكب مقتضيات البحث والتحري وخاصة التحقيق النهائي مما جعل الأحكام تفقد مصداقيتها وثقة الأفراد فيها ولطريقة استنباط الدليل الإلكتروني دور كبير في تكوين قناعة القاضي الجنائي فهو يدرس الدليل المقدم إليه دراسة دقيقة منظمة حتى لا يصدر أحكاما تتنافى و المنطق القضائي وتعرض أحكامه للنقض.

أسباب اختيار الموضوع

الأسباب التي دفعتنا لمعالجة الموضوع هو أن الأدلة الإلكترونية تتميز بعدة خصائص ما يؤهلها لتصدر قائمة الأدلة التقليدية لذلك يجب إعطاؤها قيمة قانونية دون إهمال السلطة التقديرية للقاضي الجنائي في تقديرها كون الفرد يتمتع بحقوق وحرية يجب عدم انتهاكها إضافة إلى أن الأدلة الإلكترونية في ميدان الإثبات الجنائي تحتاج إلى قدرة ومهارة فنية كبيرة للتعامل معها ونظرا لتنوع الأدلة الإلكترونية فعلى المشرع أن يوضح بدقة المقبولة منها وغير المقبولة ولا يجوز الاعتماد على أدلة غير مشروعة حتى ولو كانت علمية.

أهمية الموضوع

تكمن أهمية موضوع في السلطة التقديرية للقاضي الجنائي في تقدير الدليل الرقمي نظرا للدور الذي يلعبه القاضي الجنائي أثناء إصدار الحكم أو القرار من خلال الأدلة المتوفرة لديه فيجب عليه أن يعمل سلطته التقديرية بما يتماشى ومبدأ اقتناعه الشخصي دون التعسف في استعمال هذه السلطة بما لا يضر مصلحة الفرد والمجتمع، إضافة إلى القيمة العلمية و العملية للدليل الإلكتروني والذي لا يعني التعامل معه كدليل قاطع الدلالة فلو تم التعامل معه بهذا المنطق والشكل سيتم القضاء على سلطة القاضي الجنائي في تقديره.

أهداف الموضوع

نهدف من خلال دراستنا لهذا الموضوع الوصول إلى تحقيق النقاط التالية:

— معرفة الضوابط التي يعتمد عليها القاضي الجنائي في تكوين قناعته



__ معرفة أهم القواعد التي يستند عليها القاضي الجنائي في تقدير الدليل الرقمي .

الإشكالية

تتمحور إشكاليه المداخلة في

فيما تكمن سلطة التقديرية للقاضي الجنائي في تقدير الدليل الرقمي؟

وتتفرع على الإشكالية الرئيسية الإشكالات الفرعية

ما المقصود بمبدأ الاقتناع الشخصي للقاضي الجنائي في تقدير الدليل الرقمي؟

فيما تتجلى ضوابط الاقتناع الشخصي للقاضي الجنائي؟

المنهج المستخدم

للإجابة على هذه الاسئلة اعتمدت في دراستنا على المنهج الوصفي والتحليلي وذلك بتحليل الإطار المفاهيمي للدليل الإلكتروني

ومعرفة الضوابط اقتناع القاضي الجنائي في تقدير الدليل الرقمي.

معتمدة في ذلك على الخطة التالية

المحور الأول: مبدأ حرية الاقتناع الشخصي للقاضي الجنائي في تقدير الدليل الرقمي

المحور الثاني: ضوابط اقتناع القاضي الجنائي بالدليل الرقمي

المحور الأول: مبدأ حرية الاقتناع الشخصي للقاضي الجنائي في تقدير الدليل الرقمي:

إن مبدأ الاقتناع الشخصي يمنح القاضي دورا فعالا حيال الدليل الذي يوضع أمامه، كما يمنحه الحرية الكاملة في أن يستعين بكافة الطرق للبحث على الحقيقة و الكشف عنها، كما يمنحه كافة الصلاحيات التي تمكنه من اتخاذ ما يراه يخدم إظهار الحقيقة، و يخوله أيضا حرية تقدير ووزن قيمة كل دليل وضع بين يديه، بالإضافة إلى التنسيق بين الأدلة المقدمة و استخلاص نتيجة منطقية إما بالإدانة أو البراءة، وهو في ذلك يختلف عن القاضي المدني الذي يكون دوره سلبيا في الدعوى المنظورة أمامه، حيث يقتصر على الموازنة بين أدلة الخصوم دون أن يبحث بنفسه فيما يعتقد انه مفيد في إظهار الحقيقة. (تومي، حدود السلطة التقديرية للقاضي الجزائري، 2021، صفحة 13_14)

1. مفهوم مبدأ حرية القاضي في الاقتناع بالدليل الرقمي:

يعد مبدأ حرية القاضي الجزائري في الاقتناع بالدليل المطروح أمامه، من أهم المبادئ التي المادة الجزائية على غرار باقي المبادئ الأخرى، وقد استقر الفقه و القضاء الجنائي على الأخذ بهذا المبدأ، إذ لا يخلو أي منظومة قانونية لأي دولة من النص على هذا المبدأ و تبنيه. (بوراس، 2017، صفحة 458)

و نجد أن المشرع الجزائري أخذ بنظام الإثبات الحر، وهو ما يعني أنه حدد الأدلة المقبولة في الإثبات، إلا أن قوة الإثبات لكل دليل متروك أمر تقديره للقاضي. (أحمد، 1987، صفحة 303)

وتتجلى حرية القاضي في الاستعانة بكافة وسائل الإثبات من خلال نصوص المواد المحددة لهذه الوسائل، حيث تنص عليها المادة 212 من قانون الإجراءات الجزائية. (قانون، 1966)

وتنوعت وسائل الإثبات الجنائي و نظرا لتفاهم الجريمة الالكترونية التي استفحلت المجتمعات مما ينبغي الاعتماد على الأدلة الرقمية لهذه الأخيرة و عليه يمكننا تعريف الدليل الرقمي: " الدليل المأخوذ من أجهزة الحاسب الآلي و يكون في شكل موجات او نبضات مغناطيسية او كهربائية يمكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة و يتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، وهو مكون رقمي لتقديم المعلومات في أشكال متنوعة مثل النصوص المكتوبة و الصور و الأصوات و الأشكال



و الرسوم وذلك من اجل الربط بين الجريمة و المجرم و المجني عليه بشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ القانون. (فرغلي و المسماي، صفحة 13)

1.1. تعريف مبدأ حرية القاضي الجنائي في الاقتناع بالدليل العلمي:

يقول الفقه في ضبط المعنى الفني الدقيق لهذا المبدأ انه يسمح للقاضي الجنائي بأن يقدر قيمة الأدلة المعروضة عليه تقديرا عقلانيا منطقيا مسببا كيفما إليه اقتناعه، مستهدفا الحقيقة بوزن دقيق و تمحيص أكيد الدليل، يساعده في ذلك تكوينه الثقافي القانوني وحنكته و ذكاؤه، هكذا فمن تحصيل الحاصل أن نقول بأن الفقه سعى إلى تعليق هذه الحرية على القناعة الداخلية " الذهنية و النفسية للقاضي الجنائي. (اغليس، 2010، صفحة 113)

فمبدأ حرية القاضي الجنائي في الاقتناع معناه تلك الحرية المعترف بها له في تكوين اقتناعه الشخصي، بما يستقر في ضميره ووجدانه، من خلال حريته في تقديره وموازنة ما يعرض عليه من أدلة ووقائع في الدعوى، ليسقط حكم القانون الذي يراه مناسبا عليها بتكليفها، لتقرير الحكم المناسب إما بالبراءة او الإدانة. (العبادي، 2010، صفحة 17)

2.1. شروط قبول الدليل الرقمي في الإثبات:

المشرع الجزائري و على غرار أغلبية التشريعات المقارنة قد أخذ بنظام الإثبات الحر في المواد الجزائية، وتعني هذه الحرية انه قد حدد الأدلة المقبولة في الإثبات إلا أن قوة الإثبات لكل دليل متروكة للسلطة التقديرية للقاضي الجنائي. (بوراس، 2017، صفحة 173) بحيث يعتبر الدليل الرقمي تطبيقا للدليل العلمي بل أكثر الأدلة العلمية حجية في الإثبات وذلك لما يتميز به من موضوعية و حياد وكفاءة وهو محكم وفق قواعد علمية حساسية لا تقبل التأويل مما يقوي من يقينية و يساعد القاضي في التقليل من الأخطاء القضائية و الاقتراب أكثر إلى تحقيق العدالة و التوصل بدرجة أكثر إلى الحقيقة، ذلك أن التقنية العلمية قد توفر طرقا دقيقة لجمع الأدلة تتمتع بقوة علمية يصعب إثبات عكسها لكن إذا كان صحيحا أن الدليل الرقمي و بحكم طبيعته العلمية يمثل نقلا و أخبارا صادقا للواقع باعتبار علميته و موضوعيته وحياده و كفاءته، إلا أن هذا لا ينفي استبعاد كونه موضع شك من حيث سلامته من العبث من ناحية و صحة الإجراءات المتبعة من ناحية أخرى، إذ يمكن التشكيك في صحة الدليل من ناحيتين: (نعيم، 2013، صفحة 215)

— إمكانية العبث به على نحو يخالف الحقيقة إذ يقدم هذا الدليل معبرا عن واقعة معينة صنع أساسا من اجل التعبير عنها خلافا للحقيقة دون أن يكون في استطاعته غير المتخصص إدراك ذلك العبث، ذلك أن التقنية الحديثة تمكن العبث بالدليل الرقمي بسهولة بحيث يظهر وكأنه نسخة أصلية في تغييره عن الحقيقة؛

— أما الثانية فتتعلق بنسبة الخطأ في الحصول على الدليل الرقمي وذلك راجع إما للخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي كالحلل في شيفرة الدخول المستخدمة او في معطيات معينة، وقد يكون الخطأ في استخلاص الدليل بسبب استخدام أداة نسبة صواب نسبية.

ومن هنا فان الشك في الدليل الرقمي لا يتعلق بمضمونه ولكن بعوامل مستقلة عنه لكنها تؤثر في مصداقيته لذلك فان الأمر يتطلب توفر مجموعة من الشروط في الدليل الرقمي لتقريبه من الحقيقة وقبوله كدليل إثبات تبنى عليه أحكام البراءة و الإدانة:

— يجب الحصول على الدليل بطريقة مشروعة " مبدأ مشروعية المخرجات الالكترونية"؛

— يجب أن تكون الأدلة الالكترونية غير قابلة للتغيير أي يقينية " مبدأ يقينية الدليل الرقمي "

— إمكانية مناقشة الأدلة الالكترونية المستخرجة من الحاسوب و الانترنت. (سامية، 2021، صفحة 685_686_687)



2. ضوابط اقتناع القاضي الجنائي بالدليل الرقمي:

إن سلطة القاضي في تقدير الأدلة يحكمها مبدأ السلطة التقديرية للقاضي إلا أنه مع تطور العلوم و اعتماد الوسائل العلمية و التكنولوجية طرح التساؤل حول ما إذا كان نظام الإثبات العلمي سيحل محل الأدلة الاقناعية وهل يتمتع الدليل العلمي بقيمة في الإثبات تتجاوز الدليل الجنائي العادي؟ وفي الحقيقة رغم ما أحدثه العلم من تطور إلا أنه لم يؤثر على مبدأ القناعة الوجدانية للقاضي، فرغم أن الوسائل العلمية قد تعطي نتائج لها قدر عالي من الثقة إلا أنها لا تغني عن العملية الذهنية التي يقوم بها القاضي بهدف الوصول إلى الحقيقة. (لاغية، 2012، صفحة 130)

وتتباين الضوابط التي تحكم قناعة القاضي الجنائي في الأخذ بالدليل العلمي أو رده بين ضوابط متعلقة بدرجة الاقتناع، و أخرى متعلقة بالدليل الجنائي العلمي في حد ذاته. (بوراس، 2017، صفحة 175)

1.2. الضوابط المتعلقة بدرجة الاقتناع:

تحكم القناعة الوجدانية للقاضي بالدليل الرقمي ضوابط لا بد من توافرها حتى تكون هذه القناعة موضوعية و لا لبس عليها، ويعد بناء الاقتناع الشخصي على الجرم و اليقين و كذا صلاحية الدليل في حد ذاته ليكون إما دليلا للإثبات و للنفي أهم ضابطين يحكمان هذه القناعة.

1.1.2. بناء الاقتناع الشخصي على الجرم و اليقين:

إن الأصل في الإنسان البراءة وهذا يقين لا يزول إلا بيقين مثله أو أقوى منه و لذلك فإن الأحكام الصادرة عليها بالإدانة و التي يترتب عليها هدم هذه القرينة، يجب أن يكون مبناها اليقين الذي يقوى على إثبات عكس هذا الأصل، فالشك و الاحتمال إذا ما تطرق إلى اقتناع قاضي الموضوع و عجز عن الوصول في قضائه إلى اليقين، فانه يجب عليه أن يفسر ذلك لصالح المتهم و يحكم بالبراءة، فالدلائل و القرائن غير القاطعة، يحوطها الشك، ومن ثم فلا تصلح منفردة لان تكون دعامة لأحكام الإدانة و التي يجب أن يكون مبناها اليقين، و لا يعني بهما الجرم و اليقين المطلقين، فذلك لا سبيل إلى تحقيقه بالنسبة للأدلة الاثباتية القولية لان اليقين او الجرم المطلق إنما هو شئ يتحقق فقط في الأمور التي لها تكييف مادي بالترقيم او التحليل او الإحصاء، إما المعنويات كالإيمان و العدل وما إليها فإنها لا تكون إلا بالنسبة فقط ومن ثم لا يطلب أن يكون يقين القاضي مطلقا.

وإنما يكفي أن يكون نسبيا، بمعنى آخر المطلوب أن تبني عقيدة القاضي بناء متجها نحو عدم الشك او الرجحان، وإنما يكون بناؤها على أساس من الاحتمالات ذات الدرجة العالية من الثقة. (بوراس، 2017، صفحة 175)

وبما أن القاضي الجنائي حر بكافة وسائل الإثبات للبحث عن الحقيقة و كشفها، فلا يجوز له أن يقتنع بفحص الأدلة التي يقدمها له الأطراف، بتقديم عناصر الإثبات اللازمة لإظهار الحقيقة، و هكذا فان للقاضي الجنائي سواء بناء على طلبات الخصوم او من تلقاء نفسه أن يتخذ أي إجراء يراه ضروريا و لازما للفصل في الدعوى كما يتعين عليه التحقيق من عدم وجود البراءة، او قرينة براءة الظاهر حتى ولو لم يدفع بها المتهم، فللقاضي أن يحكم من تلقاء نفسه بالبراءة إذ يتبين له أن المتهم كان في حالة من حالات الدفاع الشرعي، او توفير مانع من موانع المسؤولية أو العقاب. (سلامة، صفحة 15)

2.1.2. صلاحية الدليل لتكوين عناصر إثبات او نفي:

إن الدليل الذي يكون منه القاضي الجنائي قناعته في عملية الإثبات يجب أن يكون مثبتا او نفيا لوقائع معينة في الدعوى المعروضة على القضاء، وهذا لا يكون إلا إذا استند القاضي في هذه العملية إلى وقائع المكونة للجريمة و كانت منطقية و غير متنافية مع العقل لتكون صالحة لتكوين عناصر وقائع معينة او إثباتها، و تكون كذلك مسارية للأدلة التي تتجه لتحقيق الغاية نفسها، فمثلا: لا يمكن أن يحكم القاضي بإدانة متهم إلا إذا اطمأن ضميره إلى دليل يثبت صحة ما نسب إلى المتهم



من وقائع، مع وجوب أن يكون هذا الاطمئنان مستمدة من أدلة قائمة في الدعوى يتقبلها العقل و المنطق السليم لتؤدي إلى ما اقتنع به القاضي.

و القانون لا يشترط في أدلة الإثبات التي تقام عليها الأحكام أن تكون مباشرة، بل يكفي أن تؤدي إلى نتائج حقيقية بعملية منطقية، كما لا يشترط في الدليل أن يكون صريحا على الواقعة بل يكفي أن يكون استخلاص ثبوتها عن طريق الاستنتاج ليكتشف للمحكمة الظروف و القرائن التي ترتب النتائج. (الدين، محاضرا في الاثبات الجنائي، 2009، صفحة 621)

2.2. طرح الدليل العلمي للمناقشة أثناء المرافعة:

إن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الانبثاقية التي طرحت في جلسات المحاكمة، وخضعت لحرية مناقشة أطراف الدعوى، وهذا ما تناوله المشرع في المادة 212 الفقرة 02 من قانون الإجراءات الجزائية. (الجابري، 2005، صفحة 360) لا يسوغ للقاضي أن يبنى قراره إلا على الأدلة المقدمة في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه " و بمعنى انه لا يجوز للقاضي أن يبنى اقتناعه إلا على الأدلة التي طرحت أمامه و خضعت لمناقشة من أطراف الخصومة، فاستناده إلى أدلة لم تطرح للمناقشة في الجلسة موجب للبطلان، و القاعدة أن القاضي لا يحكم إلا بناء على التحقيقات التي حصلت في مواجهة الخصوم وشفهيا، إذ يجب أن يكون الدليل الذي يستند عليه قاضي الموضوع موجودا ضمن أوراق الدعوى الموضوعة تحت بصره أي أن الدليل الذي يتبنى عليه المحكمة حكمها له أصل ثابت في ملف الدعوى و أن يكون قد طرح للمناقشة دون تفرقة بين دليل الإدانة او دليل البراءة، والتي أتيح للخصوم الاطلاع عليها و مناقشتها في الجلسة و إبداء رأيهم فيها وعدم مناقشته بأدلة إثبات استعملت كدليل و لا علم لهم بها أصلا، وذلك لان الدليل لا يعرض على الخصوم لمناقشة لا يجوز الأخذ به، و لا بناء الحكم عليه مادام لا سند له في أوراق الدعوى، ونفس الشيء بالنسبة للقاضي الموضوع إذا استند على أوراق و عثرت عليها النيابة العامة دون أن يثبت أن هذه الأوراق قد عرضت على الخصوم لمناقشتها، او كان مبنيا على تحقيق جنائي لم تناقشه الخصوم، لان حيده القاضي توجب عليه أن لا يقيم قضاؤه إلا على ما طرح أمامه و كان موضع الفحص و التحقيق وهذا ما نصت عليه المادة 212 من قانون الإجراءات الجنائية.

من الملاحظ أن المشرع الجزائري في المادة 302 من قانون الإجراءات الجزائية استخدم عبارتي " إن لزم الأمر " و " إن كل ثمة محل ذلك بمعنى أن عرض الأدلة أمر جوازي رهبن بسلطة تقديرية للقاضي متى رأى انه من اللازم أن يفعل ذلك و أن لم يعرضها من تلقاء نفسه يمكن للمتهم او محاميه طلب عرضها هنا لا يجوز له أن يستند إليها في حكمه إلا إذا كان قد عرضها على المتهم، وفي حالة إذا ما سكت الأطراف و لم يطلب عرضها جاز له الاستناد إليه أي تسليم بوجود هذه الوسائل. (مراد، دون سنة النشر، صفحة 477)

الخاتمة

خلصنا في هذه الدراسة إلى القول بأن مبدأ العام الذي يحكم سلطة القاضي الجزائي في تقدير الأدلة هو مبدأ حرية القاضي في تكوين قناعته، هذا الاقتناع الذي يبدد من جانبيين هما حرية القاضي في أن يستمد قناعته من أي دليل يطمئن إليه، دون أن يتقيد فيه تكوين قناعته بدليل معين، و حريته في تقدير الأدلة المطروحة عليه، دون أن يكون ملزما بإصدار حكم بالإدانة او البراءة لتوفير دليل معين طالما انه لم يقتنع به، فله أن يأخذ بالدليل الذي يطمئن إليه وجدانه و يطرح الدليل الذي لا يطمئن إليه.

وعليه يمكن أن نستنتج بأن تطور أدلة الإثبات في العصر الراهن خلق تباينا واضحا في حجية الدليل، بين قطعيته في المجال العلمي و خضوعه للسلطة التقديرية أمام القضاء الجنائي، مما يمنح القاضي في المواد الجزائية سلطة واسعة في تقدير الأدلة العلمية. غير أن هذه السلطة محاطة بمجموعة من الضوابط القانونية، على رأسها طرح الدليل العلمي للمناقشة أثناء المرافعة و إخضاع الدليل العلمي لقاعدة للمناقشة أثناء المرافعة و إخضاع الدليل العلمي لقاعدة تساند الأدلة و تضافرها.



و خلصت الدراسة الى عدة نتائج متنوعة بعدة توصيات

النتائج:

- __ القاضي له سلطة و حرية الكاملة في الأخذ بالدليل الرقمي نظرا للجرائم المستحدثة المرتكبة من طرف المجرمين.
- __ مهما اتسعت هذه السلطة التقديرية للقاضي الجزائري فان لها حدود، ذلك أن المشرع لن يتركها مطلقة بل قيدها، وذلك بأن أورد عليها بعض الاستثناءات التي لا يملك القاضي إزاءها أي حرية في تقدير الأدلة، كما انه أخضعها لبعض الضوابط التي يتعين على القاضي الالتزام بها حيث إعماله لهذه السلطة.

أما بخصوص التوصيات

- __ على المشرع أن يحدد الأدلة العلمية التي هي مشروعة و ذلك من اجل تفادي الخوض في مدى مشروعية دليل مطروح أمام القضاء ولا وجود لنص قانوني بشأنه.
- __ إبراز سلطة القاضي الجزائري وحدودها فيما يخص تقدير الدليل العلمي في حد ذاته و ليس فقط في كيفية الحصول عليه.
- __ إحداث تقنيات من اجل خلق التواصل بين القاضي الجنائي و ما يستحدث من أدلة علمية.

المراجع

- 1- الاجراءات الجزائية قانون. (08 جويلية، 1966). قانون رقم 66_155 المتعلق بالقانون الاجراءات الجزائية. الجزائر.
- 2_ الدين م. ن. (2009). محاضرات في الاثبات الجنائي. الجزء 01، الجزائر: دار الهومة.
- 3_ إيمان علي الجابري. (2005). يقين القاضي الجنائي. مصر: منشأة المعارف.
- 4_ بلجراف سامية. (2021). سلطة القاضي الجزائري في قبول و تقدير الدليل الرقمي. المجلد رقم 07، العدد 01، جامعة محمد خيضر بسكرة، الجزائر.
- 5_ بن لاغية. (2012). حجية ادلة الاثبات الجنائية الحديثة. مذكرة لنيل شهادة الماجستير، الجزائر.
- 6_ بوزيد اغليس. (2010). تلازم مبدأ الاثبات الحر بالاقتناع الذاتي للقاضي الجزائري. الاردن: دار الهدى للنشر و التوزيع.
- 7_ تومي جمال. (19 01، 2021). حدود السلطة التقديرية للقاضي الجزائري. الجزائر، جامعة مولود معمري تيزي وزو، الجزائر.
- 8_ سعيداني نعيم. (2013). اليات بحث و التحري عن الجريمة المعلوماتية في القانون الجزائري. رسالة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة مولود معمري تيزي وزو.
- 9_ عبد الفتاح مراد. (دون سنة النشر). التحقيق الجنائي التطبيقي. مصر، جمهورية مصر العربية: دون دار النشر
- 10_ عبد الناصر محمد محمود فرغلي، و محمد عبيد سيف سعيد المسموي. (بلا تاريخ). الاثبات الجنائي بالادلة الرقمية من الناحيتين القانونية و الفنية دراسة تطبيقية مقارنة. نايف للعلوم الامنية، الامارات العربية المتحدة.
- 11_ مأمون سلامة. (بلا تاريخ). الاجراءات في التشريع المصري. دار الفكر العربي: القاهرة.
- 12_ محمد عبد الكريم العبادي. (2010). القناعة الوجدانية للقاضي الجزائري و رقابة القاضي عليها. الاردن: دار الفكر.
- 13_ مروت نصر الدين. (2009). محاضرات في الاثبات الجنائي. الجزائر: دار هومة الجزائر.
- 14_ منير بوراس. (2017). سلطة القاضي في تقدير الدليل العلمي. الجزائر، المجلة الاكاديمية للبحث القانوني، المجلد 15، العدد 01، الجزائر.
- 15_ هلاي عبد الله أحمد. (1987). النظرية العامة للاثبات في المواد الجنائية. مصر: دار النهضة العربية.



مراقبة الاتصالات الالكترونية في التشريع الجزائري وتأثيرها على الحقوق والحريات

ط.د فاطمة ضيف الله

diffallahazhar@gmail.com

ط.د محمد الأبيض

labiad.mohamed@gmail.com

مقدمة

تمثل الحقوق والحريات محورا أساسيا كرسته النصوص الدستورية، فالدستور الجزائري على غرار باقي دساتير العالمية يكفل جميع الضمانات التي تضمن ممارسة هذه الحقوق والحريات، ويتجلى ذلك في تكريس حق كل فرد في إضفاء السرية على كافة مظاهر حياته الخاصة وسرية مراسلاته واتصالاته الخاصة في أي شكل كانت وهذا ما أكدته المادة 47 من الدستور الجزائري، فالأصل العام عدم جواز المساس بالحقوق والحريات للأفراد وينبغي احترامها من قبل الأفراد والسلطات وأن تكفل هذه الأخيرة حماية دستورية وقانونية ضد انتهاكها غير المشروع.

إلا أنه يقع استثناء على هذا الحق لضرورات تفرضها ظروف قانونية معينة مرتبطة باعتبارات المصلحة العامة، لذا فقد أجاز القانون للسلطة العامة خروجاً عن الأصل العام مراقبة الاتصالات والمراسلات في الحالات التي حددها، ويقصد بهذه المراقبة تجميد وتسجيل محتوى الاتصالات الالكترونية ومن ثم الاطلاع عليها والكشف عنها، كما ينصب إجراء المراقبة على الاتصالات الالكترونية وفقاً لما نص عليه القانون 04/09^{lxxiv}، والتي عرفها في المادة 02 بند (و) منه بأنها "كل ترأسل أو إرسال أو استقبال علامات وإشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".

حيث يعد إجراء مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية من أخطر الإجراءات مساساً بالحقوق والحريات العامة، باعتباره تهديداً للحق في حرمة الحياة الخاصة ففي كثير من الأحيان تحتوي هذه الاتصالات الالكترونية على ما يمس حياة الشخص الخاصة بوصفها مستودع سر لصاحبها، إلا أنه في نفس تلك النصوص التي خولت للسلطات العامة هذا الحق، قد أوردت أيضاً الضوابط والضمانات التي يجب على السلطات العامة احترامها والالتزام بها، مما يكفل حماية لهذا الحق، ويقصد بضمانات وقواعد اللجوء إلى مراقبة الاتصالات الالكترونية تلك الضوابط والقيود التي يجب على السلطة المختصة أثناء مباشرتها لإجراء تسجيل وتجميع محتوى الاتصالات والبحث في منظومة معلوماتية احترامها، لذلك فإن الهدف من تقرير ضوابط اللجوء إلى هذه الإجراءات الحديثة هو خلق توازن بين حقوق وحريات الأفراد وبين المصلحة العامة للدولة في تعقب الجرائم الخطيرة أو العابرة للحدود الدولية والكشف عن مرتكبيها.

وعليه فبقدر ما تكون هذه الضوابط كافية ومحددة وواضحة فإنها تحقق كفالة للحريات الفردية وأهمها الحق في حرمة الحياة الخاصة وسرية الاتصالات والمراسلات، وعلى العكس من ذلك فإن عدم وضع ضوابط وضمانات يفسح المجال للسلطة التقديرية للسلطة المختصة في اللجوء إلى هذه الإجراءات دون رقابة مما يشكل خطراً كبيراً على حقوق وحريات الأفراد.

أهمية الموضوع:

تبرز أهمية الموضوع في التعرف على إجراءات اللجوء إلى استعمال تقنية مراقبة الاتصالات الالكترونية بشأن الجرائم الماسة بتكنولوجيات الإعلام والاتصال وذلك بعد الثورة التي عرفها العالم في السنوات الأخيرة في مجال المعلوماتية وعلاقته بالحقوق والحريات العامة للأفراد،



بالإضافة تسليط الضوء على الضمانات والشروط القانونية لمراقبة الاتصالات الالكترونية التي أوردها المشرع الجزائري في القانون 04/09 لحماية حقوق وحرية الأفراد.

إشكالية الدراسة:

المداخلة تناقش إشكالية رئيسية تتمحور حول ماهية الضمانات القانونية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية التي أوردها المشرع الجزائري في القانون 04/09 لحماية حقوق وحرية الأفراد؟

منهج الدراسة :

اعتمدنا في هذه الدراسة على المنهج التحليل الوصفي الذي يتركز على تجميع و تحليل المعلومات، بالإضافة إلى منهج المقارنة كلما استدعى البحث ذلك.

تقسيم الدراسة

للإجابة على الإشكالية المطروحة يمكن تقسيم المداخلة إلى محورين رئيسيين:

1. الضمانات الموضوعية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية
2. الضمانات الشكلية والإجرائية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية

1. الضمانات الموضوعية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية:

يقصد بالضمانات الموضوعية تلك الإجراءات التي أوجب المشرع مراعاتها عند إجراء عملية مراقبة والهدف من وضع هذه الضمانات من قبل المشرع هو إحاطة عملية المراقبة بإجراءات موضوعية تضمن صحة ودقة النتائج التي يصل إليها القائم بالمراقبة وإحاطة المتهم بضمانات كافية للحفاظ على حريته الفردية لضمان عدم تعسف الجهات القائمة بالمراقبة، يمكن إجمال الضوابط الموضوعية التي أقرها القانون لمراقبة الاتصالات الالكترونية في مجموعة من الضمانات أهمها:

1.1. تحقق الغرض من عملية اللجوء إلى مراقبة الاتصالات الالكترونية والتفتيش:

تعرف مراقبة الاتصالات الالكترونية بأنها استخدام التقنية الالكترونية لجميع بيانات أو معلومات عن المشتبه فيه سواء أكان شخص أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أممي أو لأي غرض آخر^{lxxiv}، واكتفى بتعريف الاتصالات الالكترونية في الفقرة (و) من المادة 02 من القانون 04/09 ، بأنها " كل تراسل أو إرسال أو استقبال علامات وإشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".

هو نفس التعريف الذي جاءت به المادة 5 فقرة أولى من المرسوم التنفيذي 15-261 المحدد لتشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.^{lxxiv}

كما يقصد بتفتيش المنظومات الالكترونية بالإجراء الذي استحدثه المشرع الجزائري بموجب المادة 05 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أجاز للسلطات القضائية المختصة وكذا الشرطة القضائية في إطار قانون الإجراءات الجزائية ، وفي الحالات المنصوص عليه في المادة 04 من ذات القانون.

لم يحدد المشرع المقصود بتفتيش المنظومات، إلا أنه عرفه المجلس الأوروبي بتفتيش المنظومات المعلوماتية بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل قانوني^{lxxiv}، كما يقصد بالمنظومات المعلوماتية على أنها نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها أو البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.^{lxxiv}



لقد اعتمد المشرع الجزائري على إجراء اللجوء إلى المراقبة الاتصالات الالكترونية وتفتيش المنظومة المعلوماتية في حالات استثنائية فقط لما لها من تأثير مباشر على حق الإنسان في سرية حياته الخاصة واتصالاته الشخصية وذلك بهدف اكتشاف الجريمة والوصول إلى مرتكبيها خلال مرحلتي جمع الاستدلالات والتحقيق الابتدائي بسبب عجز الإجراءات التقليدية التوصل إلى الحقيقة ، وهو ما أقره المشرع الجزائري في نص المادة 03 من القانون 04/09 بأن يتم اللجوء إلى هذا الإجراء متى تطلبت مستلزمات التحريات والتحقيقات القضائية الجارية.

كما أن المشرع الجزائري لم ينص على إمكانية اللجوء إلى المراقبة بعد ارتكاب الجريمة والبحث عن حقيقة الوصول إلى مرتكبيها فقط، بل أقر أيضا اللجوء إلى استعمال هذه التدابير قبل حدوث الجريمة كوسيلة وقائية استباقية للحماية من وقوع جرائم معينة هي الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة والاعتداء على منظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني وفقا لما نصت عليه المادة 04 فقرة (أ) و (ب).

بالإضافة إلى تعزيز التعاون الدولي في مجال مكافحة الإجرام المنظم في مجال المعلوماتية ذلك أن هذه الجرائم تعد من الجرائم العابرة للحدود الوطنية ولا ترتبط في كثير من الأحيان بمكان معين ويكون ذلك في إطار المساعدة الدولية المتبادلة وفقا لما نص عليه القانون والاتفاقات الدولية في هذا الشأن.

في حين أن المشرع الفرنسي اشترط في نص المادة 100-1 من قانون الإجراءات الجزائية الفرنسي، بأن يكون اللجوء إلى المراقبة ضروري لمصلحة التحقيق وتحقيق حالة الضرورة حين يكون من الصعب معرفة الجناة وضبط أدلة الجريمة بوسائل البحث والتحري العادية.

2.1 الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الالكترونية

لقد قام المشرع الجزائري باستحداث نصوص قانونية تتضمن جملة من المفاهيم التقنية تتلاءم مع ضبط الرسائل الالكترونية في حالة التلبس أو التحقيق الابتدائي بصدد عدد من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وتتميز عن النصوص التقليدية في كونها تضمنت جوانب تقنية تسمح بمقتضاها لقاضي التحقيق أو ضابط الشرطة القضائية المناب أو المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

لقد أباح المشرع الجزائري مراقبة الاتصالات في 5 جرائم محددة على سبيل الحصر وفقا لنص المادة 65 مكرر 5 ق 1 ج إلا أنه وسع نطاقها في نص المادة 03 من قانون 04/09، وجعلها مطلقة على كافة الجرائم ولكن في حالات محددة وهي في حالة المساس بالنظام العام، أو لمستلزمات التحريات، أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وكذا قانون 04/09 هذا مع عدم المساس بجملة من الضمانات.

لقد نص القانون 04/09 على الحالات التي تسمح باللجوء إلى المراقبة الالكترونية أو دخول منظومة معلوماتية أو منظومة تخزين معلوماتية بغرض التفتيش وهي الحالات التي جاءت على سبيل الحصر متمثلة في ما يلي:

1.2.1 الوقاية من ارتكاب الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة:

الملاحظ هنا أن المشرع الجزائري أباح اللجوء إلى مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية في مرحلة سابقة على ارتكاب هذا النوع من الجرائم وتفتيش المنظومات المعلوماتية أي بمجرد وصول العلم إلى السلطة القضائية المختصة باحتمال ارتكاب جريمة من جرائم الإرهاب والتخريب أو جريمة من الجرائم الماسة بأمن الدولة، وحتى في حالة توافر شكوك ولو بسيطة أن هناك احتمال قيام شخص أو مجموعة من الأشخاص بالتحضير لإحدى الجرائم سألغة الذكر^{lxxiv}.



فترى أن السبب في ذلك راجع إلى خطورة هذه الأفعال على الدولة وعلى حياة الأفراد وممتلكاتهم، يضاف إلى ذلك صعوبة الكشف عن هذه الجرائم بسبب تطور التقنيات المستعملة فغالبا ما تتم عن طريق أجهزة اتصالات أو تحكم عن بعد.

2.2.1 حالة توفر عن احتمال وجود اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة و الاقتصاد الوطني:

تتعلق هذه الحالة أيضا باللجوء إلى إجراءات المراقبة أو التفتيش قبل وقوع جريمة الاعتداء المعلوماتي على منظومة معلوماتية وذلك بمجرد وصول معلومات إلى السلطة القضائية بشرط أن تكون هذه المعلومات تهدد النظام العام والدفاع الوطني في هذه الحالة فإن لهذه الإجراءات دورا وقائيا بمجرد توافر معلومات عن احتمال اعتداء على منظومة معلوماتية تمس بالمصالح السابقة يجعل إجراء الرقابة الالكترونية فعلا مشروعا ويستوي أن تتوفر هذه المعلومات من قبل السلطات ذاتها أو من قبل البلاغات والشكاوي التي ترد إلى السلطات من قبل المواطنين^{lxxiv}، التي من شأنها الحيلولة دون وقوع مثل هذه الجرائم الخطيرة والتي تستهدف على وجه الخصوص أمن الدولة.

3.2.1 مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية

يتم اللجوء إلى المراقبة أو التفتيش بعد ارتكاب الجريمة وأثناء مرحلة جمع الاستدلالات أو التحقيق القضائي ويكون الغرض من ذلك هو التوصل إلى معرفة مرتكبي الجريمة وذلك في حالة عدم جدوى الإجراءات التقليدية في الوصول إلى الحقيقة ويجب الإشارة هنا على أنه براءة أولية للبند (ج) من الفقرة الأولى لنص المادة 04، وعند استقراء المادة السابقة نلاحظ أن المشرع لم يحدد ما هي الجرائم المقصودة، وهل يسري هذا الإجراء على جميع الجرائم، وهناك رأي من الفقه يرى أنه طالما لم يحدد نوع معين من الجرائم على النحو الذي أشارت إليه البنود السابقة من نفس الفقرة، فإن المراقبة يلجأ إليها بمناسبة جميع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال طالما أن هذا القانون يهدف فقط إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ويتعلق الأمر خاصة بالجريمة المنظمة أو العابرة للحدود الوطنية^{lxxiv}.

4.2.1 في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة:

يتعلق الأمر بالتعاون الدولي لمكافحة الجريمة العابرة للحدود، خاصة الجرائم التي ترتكب خارج الإقليم الوطني، ومن شأن عملية مراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية في الإقليم الجزائري أن تفيد دولة أخرى بنتائج تتعلق بمعاينة هذه الجرائم الماسة بتكنولوجيات الإعلام والاتصال وكشف مرتكبيها، بشرط أن يتم ذلك في إطار تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة أي أن يكون ذلك في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل^{lxxiv}.

2. الضمانات الشكلية لمراقبة الاتصالات الالكترونية و تفتيش المنظومات المعلوماتية:

من القواعد الشكلية التي جاء بها المشرع الجزائري أن يكون هناك إذن باللجوء إلى مباشرة مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية صادر من السلطة المختصة، وهذا ما تضمنه المادة 65 مكرر 05 من ق.إ.ج^{lxxiv}، كما نصت عليه المادة 04 من قانون 04/09^{lxxiv}، للجوء لهذا الإجراء يجب أن تتوافر فيه شروط معينة فيجب أن يشمل بيانات خاصة وأن يرتبط بمدة معينة.

1.2. ضرورة صدور إذن من السلطة القضائية المختصة باللجوء إلى مراقبة الاتصالات الالكترونية والتفتيش:



يعد هذا الإجراء إجراء استثنائيا لا يتم اللجوء إليه إلا إذا دعت إلى ذلك ضرورات التحري والتحقيق الابتدائي في جرائم محددة على سبيل الحصر وهذا ما أكدته القانون 04/09 بأنه لا يتم اللجوء إلى مراقبة الاتصالات الالكترونية إلا إذا استدعت ذلك مقتضيات ومستلزمات التحريات والتحقيقات الجارية وفقا للقواعد المنصوص عليها في القانون الإجراءات الجزائية^{lxxiv}، يعتبر الحصول على إذن من السلطة القضائية المختصة لمراقبة الاتصالات الالكترونية من أهم الضمانات التي وضعها المشرع الجزائري للأفراد، فيمكن اللجوء لهذا الإجراء في مرحلتين التحريات الأولية والتحقيق القضائي الابتدائي ويتعلق الأمر بقاضي التحقيق أو وكيل الجمهورية حسب الأحوال أو النائب العام لدى مجلس قضاء الجزائر إذا تعلق الموضوع بمراقبة جرائم الإرهاب والتخريب وأمن الدولة وفقا لما نصت عليه صراحة نص المادة 04 فقرة 2 و 3 من القانون 04/09 و جب على القضاء قبل أن يصدر الإذن أن يقدر توافر حالة من الحالات الواردة على سبيل الحصر في الفقرة 1 من نص المادة 04 السابق عرضها منعا للتعسف من أي جهة أخرى.

من ثم فإذا قام ضابط الشرطة القضائية من تلقاء نفسه بهذا الإجراء باطلا وبالتالي يبطل الدليل المستمد من المراقبة ومتى وقع باطلا بطلت معه جميع الإجراءات التي بنيت عليه^{lxxiv}.

أما بالنسبة لمباشرة إجراء تفتيش المنظومات المعلوماتية وفقا لما نصت عليه المادة 05 من القانون 04/09 والذي ذكر فيه أن هذا الإجراء محمول للسلطة القضائية وضابط الشرطة القضائية ولا يطرح الإشكال بالنسبة للسلطة القضائية التي يجوز لها القيام بالإجراء بنفسها أو تنيب عنها ضابط الشرطة القضائية للقيام بهذا الإجراء، لكن يطرح الإشكال بالنسبة لضابط الشرطة القضائية هل يحول لهم القانون إجراء تفتيش المنظومات المعلوماتية من تلقاء أنفسهم دون صدور إذن من السلطة القضائية المختصة^{lxxiv}.

عند استقراء نص المادة 05 نجد أن المشرع الجزائري سكت ولم ينص على وجوب صدور إذن من السلطة القضائية المختصة مثلما اشترط ذلك بالنسبة لإجراء مراقبة الاتصالات الالكترونية صراحة ومن ثم وفقا للتفسير الضيق لنص هذه المادة فإنه يشترط صدور إذن من السلطة القضائية المختصة لمباشرة ضابط الشرطة القضائية التفتيش .

كما أنه في حالة ما إذا وجدت أسباب تؤدي إلى الاعتقاد بأن المعطيات محل البحث مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك^{lxxiv}.

الملاحظ أن المشرع الجزائري بمناسبة تمديد التفتيش لم يشترط وجوب صدور إذن من السلطة القضائية المختصة بل يكفي مجرد إخطار هذه السلطة أنه سيتم تمديده إلى منظومة معلوماتية أخرى، بشرط أن يتم الدخول إليها بواسطة المنظومة المعلوماتية الأولى الصادر بشأنها الإذن بالتفتيش، ويجب أن تدعى الضرورة لذلك أي توافر حالة الاستعجال أي الخوف من محو المعطيات المخزنة أو حذفها أو تعديلها ونحن نرى أن هذا التمديد يجب أن يكون بموافقة السلطة القضائية وتحت إشرافها المباشر ومسؤوليتها حتى لا يتعسف ضابط الشرطة القضائية في قيامه بإجراء التفتيش وفي ذلك خطر كبير على الحق في الحياة الخاصة للأفراد.

1.1.2 بيانات الإذن بمراقبة الاتصالات الالكترونية والتفتيش:

لم يحدد القانون 04/09 بيانات الإذن بمراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية، لكن بالرجوع إلى القواعد العامة في قانون الإجراءات الجزائية التي أحالت إليها نصوص هذا القانون فينطبق عليه ما ينطبق على غيره من الأوامر التي تصدرها الجهات القضائية، وهذه البيانات تختلف من حيث الأهمية بين البيانات الجوهرية التي يترتب على عدم وجودها بطلان الإذن، والبيانات غير الجوهرية التي يترتب على عدم وجودها بطلان الإذن و لبيانات الجوهرية.



سنتناول فيما يلي البيانات التي يجب أن تتوفر في الإذن بمراقبة الاتصالات الالكترونية أو التفتيش حسب القواعد العامة الواردة في التشريع الجزائري كما التالي:

1.1.1.2. أن يكون الإذن بمراقبة الاتصالات الالكترونية أو التفتيش مكتوبا وصريحا

من الشروط التي يجب توافرها في الإذن بالمراقبة أو التفتيش أن يكون مكتوبا طبقا لما نصت عليه صراحة المادة 04 فقرة 2 من القانون 04/09^{lxxiv}، وهذا ما قال به المشرع الجزائري في المادة 65 مكرر 7 ق.إ.ج بمناسبة جميع إجراءات التحقيق تطبيقا للقاعدة العامة المعمول بها فيجب أن تثبت دائما بالكتابة لكي تكون النتائج المتوصل إليها صحيحة. إضافة إلى شرط الكتابة يجب أن يكون الإذن صريحا يستفاد منه مباشرة نية السلطة القضائية المختصة في اللجوء إلى هذا الإجراء، وبالتالي يجب أن يذكر في الإذن صراحة أن الإذن يتعلق بمراقبة الاتصالات الالكترونية أو يرد في الإذن عبارة الأمر بتفتيش منظومة معلوماتية معينة فهنا يقع الإذن صحيحا^{lxxiv}، فكلما تم مراعاة هذه الضمانات التي أقرتها العديد من التشريعات المقارنة تم التأكيد على احترام الحريات الفردية للأشخاص وخاصة حرمة الحق في الحياة وسرية الاتصالات والمراسلات.

2.1.1.2. أن يكون الإذن بمراقبة الاتصالات الالكترونية أو التفتيش مؤرخا وموقعا

لم ينص قانون الإجراءات الجزائية على هذا الشرط صراحة لكن يفترض ذلك في أي أمر مكتوب يصدره قاضي التحقيق يشمل التاريخ اليوم والشهر والسنة والساعة.

ترجع الفائدة من تحديد تاريخ الإذن إلى معرفة ما إذا كان مصدر الإذن السلطة المختصة به محليا وقت إصداره فعلا أو كانت غير مختصة فعليا بذلك كما يفيد أيضا في حساب المدة التي يجب خلالها تنفيذ عملية المراقبة طالما أن الإذن بالمراقبة يصدر لمدة معينة لارتباطه بالحياة الخاصة للأفراد التي يجب عدم انتهاكها إلا بالقدر اليسير الذي يجيز الكشف عن حقيقة الجريمة والتوصل إلى مرتكبيها، كما يفيد تاريخ الإذن حساب مدة تقادم الدعوى العمومية إذا كان آخر الإجراءات التي تم اتخاذها بمناسبة الدعوى العمومية ولم تتبعه إجراءات أخرى كما أنه يقطع تقادم الدعوى الجنائية.

يجب أيضا على مصدر أمر اللجوء إلى مراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية سواء كان وكيل الجمهورية أو قاضي التحقيق أو النائب العام أن يوقع عليه، والغرض من هذا الإجراء بطبيعة الحال التعرف على من أصدر هذا الأمر للتأكد من اختصاصه أو عدم اختصاصه بإصداره، ولا يشترط شكل معين في التوقيع مادام موقعا عليه فعلا ممن أصدره.

كما يجب أيضا أن يتضمن الإذن باللجوء إلى مراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية بطبيعة الحال اسم مصدره وصفته أي كونه قاضي التحقيق أو وكيل جمهورية أو النائب العام حتى يتمكن من التحقق من أن هذا الإذن قد صدر عن السلطة المختصة بإصداره.

3.1.1.2. تحديد الشخص المراد مراقبة اتصالاته الالكترونية وتفتيش منظومته المعلوماتية:

يجب أن يتضمن الإذن اسم الشخص المراد مراقبة اتصالاته الالكترونية ويجب أن لا يصدر الإذن عاما لأن في ذلك مساس بحريات الأفراد، وكما يجب أن يتخذ الإجراء ضد هذا الشخص فقط دون غيره فإذا امتدت المراقبة إلى غير المذكورين في الإذن عد باطلا. يتم تحديد الشخص المراد مراقبة اتصالاته الالكترونية ببيان اسمه ولقبه ومحل إقامته وكل ما يفيد تعيينه ونفي الجهالة عنه، ومن أهم الشروط التي يجب مراعاتها في الإذن ضرورة ارتباط الشخص بالجريمة، وهناك من الفقه من يرى أنه يمكن تمديد إجراء المراقبة لأي شخص متى كان في تلك المراقبة فائدة في إظهار الحقيقة.^{lxxiv}

إلا أن القانون لم يستثن أشخاصا معينين من الرقابة إلا أنه في المادة 65 مكرر 6 فقرة 1 نص على ضرورة عدم المساس بالسر المهني إذا تعلق بتنفيذ هذه العمليات في أية أماكن يوجد بها أشخاص ملزمون بالسر المهني مثل السر المهني للمحامي والطبيب والموثق،



وهو نفس الاتجاه الذي كرسه القانون 04/09 في المادة 03، بعكس القانون الفرنسي بحيث يكون إجراء اعتراض المراسلات تحت طائلة البطلان إذا خالف أحكام هذه الحماية مثل حماية المحامين وحقوق الدفاع، وأعضاء البرلمان.^{lxxiv} كما يقع إجراء التفتيش صحيحا بتحديد المنظومة المعلوماتية المراد تفتيشها بدقة ومكان وجودها سواء كان مكانا عاما أو خاصا دون حاجة لذكر صاحبها إذا لم يتم التعرف عليه.

4.1.1.2. بيان طبيعة الاتصالات الالكترونية المطلوب مراقبتها:

ينصب الإذن بإجراء مراقبة الاتصالات الالكترونية على محل معين يتمثل في اتصالات الشخص الالكترونية، وتبعا لذلك فيجب أن يحدد الإذن كل العناصر التي تسمح بالتعرف على الاتصالات الالكترونية المطلوب تجميعها وتسجيلها والذي يجب أن يحدد بدقة طبيعة هذه الاتصالات^{lxxiv}، هل هي مراسلات الكترونية تتعلق برسائل تصل بريده الالكتروني أو أحاديث خاصة تتم عن طريق شبكة الانترنت، وعلة ذلك أن نطاق الإذن من حيث تنفيذه يتحدد بمحله فإذا صدر الإذن بمراقبة اتصالاته الالكترونية لم يتعداها إلى تفتيش منظومته المعلوماتية إلا ما تعلق منها ببريده الالكتروني والذي يرتبط باتصالات الشخص الالكترونية^{lxxiv}.

يشترط أيضا أن تبقى الإجراءات المتخذة سواء المتعلقة بمراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية في إطار المعلومات المبحوث عنها، وهو الشرط الذي نص عليه المشرع صراحة في نص المادة 04 الفقرة الأخيرة من القانون 04/09 والتي أوجبت على أن تكون الترتيبات التقنية الموضوعة للأغراض الموجهة للحماية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة موجهة حصرا لتجميع وتسجيل معطيات ذات صلة بالحماية منها وعدم الالتزام بذلك يترتب عليه توقيع العقوبات المتعلقة بالمساس بالحقوق في حرمة الحياة الخاصة، ويكون المشرع قد قصد تطبيق المادة 203 مكرر 3 وما يليها من قانون العقوبات الجزائري.

وإذا تضمن الإذن مراقبة الاتصالات الالكترونية لشخص في مكان خاص معين فقط، فإن هذا الإذن يستدعي اتخاذ التدابير التقنية اللازمة لذلك في هذا المكان دون غيره، وتبعا لذلك فيجب أن يتضمن الإذن هذه الأماكن سواء كانت سكنية أو عامة وتحديد عنوانها تحديدا دقيقا نافيا للجهالة.

5.1.1.2. تحرير محضر بالعمليات التقنية التي تم القيام بها:

تكتسي المحاضر أهمية كبيرة من حيث قيمتها في الإثبات على وقوع الجريمة ونسبتها لفاعلها، فقد عرفها المشرع الجزائري بأنها الوثائق التي يحررها ضابط الشرطة القضائية أثناء ممارسته مهامه ويضمنها ما عاينه أو تلقاه من صلاحيات أو قام به من عمليات تدخل في اختصاصه^{lxxiv}، ما كان اللجوء إلى مراقبة الاتصالات الالكترونية والتفتيش عملا من أعمال التحقيق فإنه يجب تحرير محضر بها يثبت فيه ما تم من إجراءات بشأنها وما أسفرت عنه من أدلة حتى لو لم يشترط ذلك صراحة في نصوص القانون 04/09 ومن ثم فيجب على ضابط الشرطة القضائية المأذون له والمناوب من طرف القاضي المختص تحرير محضر عن كل عمليات وضع التدابير التقنية لمراقبة للاتصالات الالكترونية وما أسفرت عنه، كذلك عمليات التفتيش التي تم القيام بها وأسفر عنها من أدلة.

ويجب أن يذكر في المحضر أيضا تاريخ وساعة بداية هذه العمليات والانتهاؤها منها وجميع الشروط الشكلية العامة في جميع المحاضر كلما يجب أن يكون محررا باللغة العربية.^{lxxiv}

6.1.1.2. محضر العمليات:

يحرر المحضر من قبل ضابط الشرطة القضائية المكلف بها، يدرج في ملف الإجراءات، ويمكن لمحامي المتهم الخاضع للمراقبة الاطلاع عليه من أجل مناقشته والتأكد من مضمونه والمطالبة بإجراء خبرة على الصوت المسجل أو الصور الملتقطة حيث يدون في هذا المحضر جميع مجريات سير عملية وضع الترتيبات التقنية، وكل مرحلة من مراحل العمليات الالتقاط والتثبيت والتسجيل الصوتي أو المرئي وفيه تاريخ وساعات بداية التسجيل ونهاية الإجراء^{lxxiv}.



للإشارة فإن عمليات الاعتراض والتسجيل والالتقاط لا يتم انتظار بلوغ مرحلتها النهائية لتحرير محضر بشأنها فعلى قاضي التحقيق أو وكيل الجمهورية بحكم مراقبته المباشرة للعمليات وضابط الشرطة القضائية المنتدب لإجراء العمليات تحرير محاضر عن كل مرحلة على حدة، إذ يحضر بشكل منفصل محضر الترتيبات التقنية ومحضر الدخول إلى المساكن ومحضر الالتقاط ومحضر تثبيت ومحضر تسجيل الصوتي أو محضر تسجيل السمع البصري، ومحضر الاعتراض ومحضر تسجيل المراسلات وإذا كانت المكالمات التي تم اعتراضها أو التسجيلات الصوتية والسمعية البصرية بلغة أجنبية تتم ترجمتها بمساعدة مترجم يتم تسخيرها لهذا الغرض^{lxxiv}.

كما تسجل الاتصالات الالكترونية التي تكون موضوع مراقبة وتحرر وفقا للشروط والإشكال المنصوص عليها في ق.ا.ج وتسلم التسجيلات والمحركات إلى مصالح الشرطة السلطات القضائية المختصة التي تحتفظ دون سواها بهذه المعطيات أثناء المدة القانونية.^{lxxiv}

7.1.1.2. محضر النسخ والوصف: طبقا لنص المادة 65 مكرر 1/10 من ق.ا.ج يقوم ضابط الشرطة القضائية بانتقاء من التسجيلات كل ما هو مفيد في إظهار الحقيقة وينسخه ويفرغه بنقله إلى معطيات كتابية ويجري في محضر مستقل عن هذا النقل ويكون ملخصا ومختصا لمضمون التسجيلات ويودع المحضر بدوره في ملف الإجراءات، في حالة كانت الاتصالات بلغة أجنبية تترجم وجوبا إلى اللغة العربية بمساعدة ترجمان مسجل بجدول المقبولين لدى المحاكم كما يجوز الاستعانة بخبراء وذوي الاختصاص في حالة اشتغال التسجيلات على رموز وألغاز.

8.1.1.2. حماية المعطيات المتحصل عليها:

حيث نص المادة 09 من قانون 04/09 أنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا قانون إلا في الحدود الضرورية للتحريات والتحقيقات القضائية وهذا تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به في حالة استعمال هذه المعطيات خارج هذه حدود التحريات والتحقيقات القضائية.

9.1.1.2. مساءلة ضباط الشرطة القضائية في حالة مساسهم بالحرية الشخصية للفرد:

يعتبر أعضاء الشرطة القضائية موظفون منحهم القانون صفة الضبطية القضائية و خولهم بموجبها حقوق و فرض عليهم واجبات في إطار البحث عن الجرائم و مرتكبيها و جمع الاستدلالات عنها فيبدأ دورهم بوقوع الجريمة و ينتهي عند فتح التحقيق القضائي أو إحالة المتهم إلى جهة الحكم و تتميز الشرطة القضائية عن الشرطة الإدارية في أن المهمة الرئيسية لهذه الأخيرة تتمثل في تنفيذ تدابير الشرطة العامة الصادرة من السلطات المختصة و مراقبة نشاط الأفراد و الجماعات قبل وقوع الجريمة قصد المحافظة عن الأمن العمومي و منه أسباب الاضطرابات و إزالتها إذا وقعت فأعمال الشرطة الإدارية إجراءات وقائية و مانعة في حين أعمال الشرطة القضائية عبارة عن إجراءات رادعة.

حيث جاء في نص المادة 107 من قانون العقوبات الجزائري بأنه "يعاقب الموظف العمومي بالسجن من 5 سنوات إلى 10 سنوات إذا أمر بعمل تحكيمي أو ماس بالحرية الشخصية للفرد أو بالحقوق الوطنية لمواطن أو أكثر"، ونشير هنا إلى أن ضابط الشرطة القضائية ملزم بالإجراءات التي وضعها القانون حماية لحقوق الأفراد وحرقاتهم الشخصية كما أنه ملزم بالتقيد بالإذن المقدم له سواء قبل قاضي التحقيق أو وكيل الجمهورية وأي خروج عن فحوى الإذن ينتج عنه مساس بالحرية الشخصية يعرض ضابط الشرطة القضائية إلى العقوبة سالفه الذكر

10.1.1.2. خضوعها لسلطة القضاء:

يعتبر خضوعها لسلطة القضاء المشار إليها سابقا ضمانة الضمانات وذلك لأنها تقع تحت إشراف رقابة القضاء مما لا يدع مجالا للقول بمساس الضبطية القضائية بحقوق الأفراد.



11.1.1.2. سرية الإجراءات:

تتم العملية بسرية عامة في مواجهة الأشخاص، حيث تتم بدون علمهم ودون رضاهم كما أنها تتم بالسرية في مواجهة كافة احتراماً لمبدأ السر المهني، المقرر في المادة 45 فقرة 4 من ق.ا.ج.

12.1.1.2. التسخير:

حيث يجوز لوكيل الجمهورية أو لقاضي التحقيق أو لضباط الشرطة القضائية أن يسخر عون مؤهل لدى هيئة مكلفة بالاتصالات سواء كانت عامة أو خاصة للقيام بهذا الإجراء كما يمكنه طلب المساعدة من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، لأن من ضمن مهامها قانوناً هي مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال.

قد نص القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لمكافحتها في الفصل الخامس منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المعلوماتية، حيث نصت المادة 13 منه على أن " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحته.. تحدد تشكيلة الهيئة و تنظيمها وكيفية سيرها عن طريق التنظيم"، تعمل تحت سلطة وزارة الدفاع الوطني حدد مقرها تعد الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي بالجزائر العاصمة مع إمكانية نقلها أي مكان آخر بموجب قرار من وزارة الدفاع الوطني، و يتضمن المرسوم الرئاسي 172/19 تعديلاً في الهيكل التنظيمي للهيئة، حيث أصبحت تضم مجلس توجيه ومديرية عامة

2.1.2. تسبب الإذن باللجوء إلى مراقبة الاتصالات الالكترونية والتفتيش المنظومات المعلوماتية:

يقصد بتسبب الإذن بالمراقبة بيان الأسانيد الواقعية والقانونية التي أدت إلى إصداره ومن ثم يجب على السلطة القضائية المختصة ذكر الأسباب التي دفعت بها إلى إصدار الإذن بمراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية، بالرجوع لقانون 04/09 نرى أن المشرع لم ينص صراحة على ذلك، بعكس المشرع الفرنسي الذي نص عليه في المادة 706-1/97 من ق.ا.ج^{lxxiv}، وهو الأصل المعمول به بمناسبة معظم الأوامر التي تصدر عن السلطة القضائية لكن يمكن أن يؤسس الإذن على إحدى الحالات التي نصت عليها المادة 04 من القانون 04/09 أي أن يكون سببه الوقاية من الوقوع جرائم إرهابية أو جرائم ماسة بأمن الدولة أو احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو تكون ضرورات التحري أو التحقيق الابتدائي هي التي دفعت إلى اللجوء إلى هذه الإجراءات أو كان الإجراء في إطار تنفيذ طلبات مساعدة دولية متبادلة.

في هذا الصدد فقد ذهب المشرع الجزائري إلى ضرورة أن يرافق الإذن بمراقبة الاتصالات الالكترونية للوقاية من الأفعال الإرهابية والتخريبية والماسة بأمن الدولة تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها وفقاً لما نصت عليه المادة 04 فقرة 3 ومن شأن هذا التقرير أن يوضح الأسباب والدوافع التي دفعت بالسلطة القضائية اتخاذ الأمر بمراقبة الاتصالات الالكترونية وما هو الغرض الذي يراد الوصول إليه وهذا هو المقصود بعنصر التسبب ويجب التأكيد على أن هذا التقرير يجب أن يصحب جميع حالات مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية. قد أكدت المادة 05 فقرة 2 من هذا القانون على ضرورة توافر أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأنه يمكن الدخول إليها من المنظومة المعلوماتية الأولى لتمديد التفتيش إلى منظومة معلوماتية أخرى الأمر الذي يستتف منه ضرورة توافر الأسباب لإصدار الإذن من البداية.



يجب أن تكون أسباب اللجوء إلى إجراءات المراقبة والتفتيش جدية وكافية، وفي هذا الصدد يكفي الإشارة إلى الدلائل والقرائن التي تسوغ إصدار الإذن.

يرجع سبب اشتراط أن يكون الإذن الصادر عن القضاء باللجوء إلى المراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية مسببا، إلى أنها تعد من أخطر الإجراءات الماسة بحريات الأفراد وانتهاك حقهم الطبيعي في السرية ولكونه إجراء استثنائيا يرد على الأصل العام المنصوص عليه في الدستور والمتمثل في حرمة الحياة الخاصة للمواطنين وحقهم في سرية اتصالاتهم وهذا الاستثناء تبرره المصلحة العامة من الوقاية من الجرائم المذكورة أعلاه قبل وقوعها أو بقصد التوصل إلى كشف الحقيقة والقبض على الجناة.

2.2. مدة الإذن بمراقبة الاتصالات الالكترونية:

حرص المشرع الجزائري على تحديد مدة معينة لمباشرة إجراء المراقبة منعا من تعسف وإساءة استعمال السلطة وحماية الحق في حرمة الحياة الخاصة للأفراد، وقد حددها المشرع في المادة 65 مكرر 7 ق.1. ج بمدة أربعة أشهر قابلة للتجديد، أما بالنسبة إلى القانون 05/09 نجد أن المادة 04 فقرة 3 منه حددت مدة الإذن الذي يمنحه النائب العام لدى مجلس قضاء الجزائر لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته بشأن وضع الترتيبات التقنية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة لمدة ستة أشهر قابلة للتجديد، والملاحظ أن إطالة المشرع الجزائري لمدة المراقبة نوعا ما في القانون 04/09 مقارنة بقانون الإجراءات الجزائية يمكن أن يرجع سببه إلى خطورة هذا النوع من الإجرام الذي يمس أمن الدولة بالدرجة الأولى، إلا أنه لم يجعلها قابلة للتجديد بعكس قانون الإجراءات الجزائية لذا على المشرع الجزائري تدارك هذا النقص بتحديد عدد مرات التجديد بشكل واضح .

يلاحظ التباين في مدة الإذن بين المادة 4 من القانون 04/09 و المادة 65 مكرر 5 من ق.1. ج يخلق نوع من اللبس بأي المدين يمكن الأخذ، لكن عند التمعن في نص الفقرة الأخيرة من المادة 4 نلاحظ أن مدة 6 أشهر متعلقة بالحالة (أ) من المادة 4 أما باقي الحالات فيمكن فيها الرجوع إلى القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية و هي مدة 4 أشهر.

الخاتمة:

لقد أحدث التطور المستمر لوسائل الإعلام والاتصال أشكالا جديدة من الإجرام وثورة في قانون الإجراءات الجزائية ووسائل الإثبات التقليدية والتي لم تعد كافية للكشف على الجريمة ومرتكبيها في البيئة الرقمية، لذا أصبح من الضروري استخدام تقنيات الاتصال بمهارات عالية الكفاءة، الأمر الذي تطلب ضرورة وضع نصوص قانونية تتلاءم مع خصوصيتها.

لذا أباح المشرع الجزائري في القانون 04/09 اللجوء إلى استعمال تقنية مراقبة الاتصالات الالكترونية بشأن الجرائم الماسة بتكنولوجيات الإعلام والاتصال، كما تم من خلال هذا القانون النص على قواعد إجرائية خاصة بالتفتيش والحجز في مجال جرائم المتصلة بتكنولوجيات الإعلام والاتصال مع مراعاة القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية.

غير أن اللجوء إلى لهذا الإجراء يعد مساسا بمبادئ الحرية التي كفلها الدستور الجزائري، ويتعارض مع حق الفرد في خصوصية حياته وسرية اتصالاته ومراسلاته، لذا وجب تقييد هذا الإجراء بعدم اللجوء إليه إلا في حالات استثنائية وفقا لما حدده القانون 04/09، ولا يتأتى ذلك إلا من خلال وضع ضمانات وضوابط معينة بحيث إذا ما تركت هذه الضمانات كلها أو بعضها كان اللجوء إلى هذه الإجراءات باطلا، وتقسم هذه الضمانات كما سبق تناوله إلى ضمانات موضوعية تتصل بالجريمة والمجرم، وأخرى شكلية إجرائية تتصل بكيفيات الترخيص ومدته والسلطات المختصة بذلك.

إلا أن الملاحظ أن القانون 04/09 لم يوضح بدقة الإجراءات الشكلية الواجبة الإتيان، وأخضعها للقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية دون أن يحددها بدقة، مما يتطلب إعادة صياغة بعض مواد هذا القانون.



من أهم الملاحظات التي خرجنا بها من هذه الدراسة:

- ضرورة النص على ضمانات تسبب الأمر الصادر من الجهات القضائية المختصة في حالة اللجوء إلى المراقبة الالكترونية للمراسلات والاتصالات.
- ضرورة إحاطة الإذن بالمراقبة الالكترونية للمراسلات والاتصالات بضمانات شكلية محددة تمكن الأشخاص المسخرين من إثبات مشروعية الأعمال.
- ضرورة النص على حضور المتهم أو محاميه إجراءات الاطلاع على المراسلات والمكالمات الهاتفية بعد تسجيلها وذلك للاطمئنان إلى سلامة الإجراء وضمان حقوق الدفاع أيضا.
- ضرورة النص على إجراء إتلاف تسجيلات المراقبة ومحضر الإتلاف بعد استخدامها.
- ضرورة تحديد عدد المرات التي يمكن فيها تجديد الإذن باللجوء إلى المراقبة الالكترونية على أن يكون الأمر مسببا.
- ضرورة النص على بطلان إجراء اللجوء إلى إجراء مراقبة الاتصالات الالكترونية أو تفتيش منظومة المعلوماتية صراحة إذا لم تراعى الضمانات المنصوص عليها قانونا.

المراجع باللغة العربية:

المقالات:

1. ثابت دنيازاد، مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية.
2. جبار فطيمة، مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، العدد 3، سنة 2016.
3. حلليم رامي، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاير البحوث العلمية، المجلد 9، العدد 1، سنة 2001.
4. روابح فريد، ضمانات حرمة الحياة الخاصة أثناء إجراء مراقبة الاتصالات الالكترونية، مجلة الأبحاث القانونية والسياسية، المجلد 2، العدد 2، سنة 2020.

القوانين والتشريعات:

1. قانون رقم 04/09 المؤرخ في 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، سنة 2009.
2. المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 8 أكتوبر 2015، الجريدة الرسمية العدد 53، سنة 2015.
3. الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية المعدل والمتمم، الجريدة الرسمية عدد 48، سنة 2021.

المراجع باللغة الفرنسية:

Lois et Legislations:

1. Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF n°59 du 10 mars 2004, France.

البعد الأمني

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني



المؤسسة الأمنية ومكافحة الجريمة الإلكترونية: أمن ولاية تمنراست بالمرصاد للتهديدات السيبرانية

الدكتورة: نجية هبوب
nadjiba_h2005@yahoo.fr

ط.د. شبيب شنيقي
chenikichouaib@gmail.com

مقدمة

يظهر العالم مع التطور التكنولوجي بعيدا عن العنف الجسدي والحروب العسكرية وقريب من عنف آخر ذو طيبة خاصة يعتمد على الفكر والمقدرة العقلية والذهنية، عنف يستطيع الجاني فيه تدمير أي دليل يمكن أن يستخدم لإدانتته، ذلك لأنه يرتكب في بيئة افتراضية، يحجم الكثير ممن تعرض لها عن الإبلاغ مخافة تأثير ذلك على أعمالهم وحياتهم الاجتماعية. ورغم أن هذا النوع من الجرائم يتطلب إلماما كافيا بالمهارات والمعارف التقنية ذات الصلة بالحاسب وأنظمتها، إلا أنه تم استحداث وتكوين فرق خاصة ومؤهلة بإمكانيات وأجهزة متطورة قادرة على حماية معلومات الأفراد وبياناتها والبنية التحتية للمؤسسات العامة والخاصة، واكتشاف مرتكبي هذه الجرائم.

1. الإشكالية :

كثرت في الآونة الأخيرة مع ازدياد استخدام الانترنت الجرائم الإلكترونية بمختلف أشكالها، كجرائم إتلاف وتدمير المعطيات، الاحتيال المعلوماتي وغيرها من الجرائم التي يصعب حصرها، وقد يصعب التعامل معها كونها ظاهرة عالمية وهذا يتطلب وجود أجهزة متخصصة لفك شفرتها والتعامل معها. كل هذا جعل الأجهزة الأمنية مضطرة لمتابعة هذه الجرائم وحل القضايا المرتبطة بها من أجل الحفاظ على مصالح الأفراد والدولة، لحماية المعلومات والنظم الإلكترونية والتصدي لمخاطر الهجمات السيبرانية. وعليه نحاول من خلال هذه الدراسة البحثية تسليط الضوء على الأجهزة الأمنية وقدرتها على مجابهة الجريمة الإلكترونية مستدلين في ذلك بعدد القضايا المعالجة حول الجرائم الإلكترونية ونوعها لأمن ولاية تمنراست لسنوات 2018-2019-2020-2021.

2. أهداف الدراسة :

تسعى الدراسة الراهنة المتعلقة بالمؤسسة الأمنية ومكافحة الجريمة الإلكترونية: أمن ولاية تمنراست بالمرصاد للتهديدات السيبرانية إلى تحقيق الأهداف الآتية:

- 1- تشخيص واقع الجريمة الإلكترونية بالمجتمع الجزائري.
- 2- تحديد أنواع الجرائم الإلكترونية المرتكبة في المجتمع التمنراستي.
- 3- تحديد أهمية واحترافية المؤسسات الأمنية في الكشف عن الجرائم الإلكترونية.
- 4- معرفة الطرق الأمنية اللازمة للحماية من الجرائم الإلكترونية.



3. ضبط المفاهيم :

1.3. المؤسسة الأمنية و

الأمن حاجة أساسية من حاجات البشر. وقد أخذ المفهوم العديد من المعاني بتعدد وتفاوت الإيديولوجيات السائدة في المجتمع، وإلى الاعتبار الاقتصادية والاجتماعية التي يحققها. فقد عرف بأنه "مجموعة من التدابير والقوانين التي يتبعها الإنسان لتحقيق الحماية لنفسه وماله، أو عرضه أو أي شيء ثمين يخاف عليه". (الدوكات. 2018)

وهو "قدرة الدولة على حماية قيمها الداخلية من التهديدات الخارجية، والتي كانت في الأغلب والأعم تهديدات عسكرية. غير أن الأمر اختلف بمرور الزمن فلم تعد القوة العسكرية مصدر التهديد الوحيد والأساسي بل ظهرت قوى جديدة إلى جانبها تمثلت في التهديدات الاجتماعية والاقتصادية والسياسية وغيرها" (سالم. 2003. ص18).

مع رجا كما يعرف الأمن بأنه "قدرة المجتمع على مواجهة الأحداث والوقائع الفردية للعنف وكذلك جميع المظاهر المتعلقة بالطبيعة المركبة والمؤدية للعنف" (بن عيسى. 2001. ص14).

أما اصطلاح المؤسسة الأمنية فيعني "منظومة اجتماعية هدفها الأول مراعاة نشر الأمن والأمان في المجتمع وذلك من خلال قوانين تسن في دستور الدولة تحدد عمل الأفراد وحقوقهم وواجباتهم" (دور المؤسسات الأمنية في المجتمع. 2020).

المؤسسات الأمنية هي "هيئة دورها حماية حقوق المواطنين في الحياة والحرية والأمن، لذا فإن أي فعل لهذه المؤسسات الأمنية يجب أن يهدف إلى ضمان السلامة العامة، ومنع الاضطرابات والجريمة وحماية حقوق الآخرين" (المبادرة المصرية للحقوق الشخصية. 2011).

وعليه فالمؤسسة الأمنية في الجزائر هي قوة نظامية تابعة لوزارة الداخلية لا تستطيع أداء مهامها دون تظافر جهود أفراد المجتمع ل الأمن والشرطة للقيام بمهامها للحد من انتشار الجريمة وتوفير الأمن والاستقرار.

2.3. الجريمة الإلكترونية

الجريمة الإلكترونية أو ما يطلق عليها باسم الغش المعلوماتي، جرائم الحاسب الآلي، جرائم الكمبيوتر والانترنت أو مهما كان اسمها هي جريمة مستحدثة ناتجة عن الاستخدام غير المشروع للكمبيوتر وقد ساهم الارتباط بشبكة الانترنت في تفاقمها.

لقد جاء في توصيات المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته المنعقد في فيينا سنة 2000 تعريف الجريمة الإلكترونية بأنها "جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" (بوضياف. 2018. ص252).

أما المشرع الجزائري فقد اصطلح على الجرائم الإلكترونية تسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وقد جاء تعريفها في المادة الثانية من القانون 09-04 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات". (الجريدة الرسمية. سبتمبر 2009. ص5).

عليه فالجريمة الإلكترونية هي كل فعل ينشأ عن الاستخدام غير المشروع لتكنولوجيا الاتصال والمعلومات وتشمل الاعتداءات الأجهزة والوسائل، البرامج، المعلومات المستخرجة، إضافة إلى الاتصالات، يتعرض لها الأشخاص والمؤسسات في حال عدم وجود برامج وأجهزة لحماية المعلومات من السرقة والتلاعب والاختراق.



4. الأمن الوطني والجريمة الإلكترونية: تصدي ومواجهة :

تحصي الجزائر سنويا التبليغ عن قضايا متعلقة بالجرائم الإلكترونية وهذا ما جعل مصالح الأمن تتجند لحماية مستخدمي الانترنت بإنشاء فرق متخصصة لمواجهة هذا النوع من الجرائم على مستوى المصالح الولائية للشرطة القضائية والمنصبية على مستوى 58 ولاية.

إذ تم التبليغ عن 567 جريمة إلكترونية خلال 8 أشهر الأولى من سنة 2016، عولجت منها 385 جريمة إلكترونية من قبل الفرق المتخصصة إلى جانب تسجيل 57 قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية وهذا ما توضحه المعطيات الواردة في الجدول الآتي:

الجدول رقم (1): عدد القضايا المسجلة سنة 2016

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الانترنت	430	289	365	68
جرائم الاعتداء على سلامة الأنظمة المعلوماتية	57	31	39	55
جرائم الاحتيال عبر الانترنت	25	17	32	68
جرائم التحريض والتطرف عبر الانترنت	14	14	31	100
الجرائم المخلة بالحياة	12	08	22	67
جرائم بيع السلع المحظورة عبر الانترنت	06	05	15	84
جرائم مختلفة (نسخ البرامج دون حق، القرصنة)	23	21	39	92
المجموع	567	385	543	68

المصدر المديرية العامة للأمن الوطني، 2017

أما بالنسبة لسنة 2017 فقد كشفت مصالح الدرك الوطني والشرطة الجزائرية في إحصائيات مشتركة عن تسجيل 2500 جريمة إلكترونية تتعلق بالقرصنة والابتزاز والتشهير والتحرش الإلكتروني والاحتيال (بورنان، 2018)، كما أكد نفس المصدر أن 80% من الجرائم المرتكبة تمت عن طريق مواقع التواصل الاجتماعي فيسبوك من خلال استعمال الابتزاز والتهديد بنشر صور أو أسرار شخصية أو التشهير، والجدير بالذكر أن المصالح الأمنية المختصة اكتشفت أنه كثيرا من الصور التي هدد بها أصحابها مغيرة وأخرى تتعلق بصور وفيديوهات مخلة بالحياة أو وثائق ورسائل نصية.

في حين تم معالجة أزيد من 1100 قضية خلال 2018 على المستوى الوطني (وكالة الأنباء الجزائرية)، حسب إحصائيات مقدمة من المصلحة المركزية لمكافحة الإجرام السيبراني للدرك الوطني، 30% منها تتعلق بالابتزاز والتشهير. وقد قفزت سنة 2020 الجرائم المرتكبة بوسائل تكنولوجيا الإعلام والاتصال إلى 6525 جريمة إلكترونية حسب ما سجلته مصالح الدرك والشرطة منها 5163 جريمة سجلتها مصالح الأمن الوطني، تم معالجة 4135 منها، 80% من الجرائم المرتكبة تمت عن طريق الفايسبوك، تعرض من خلالها البرلمانيين والوزراء وإطارات عليا في الدولة إلى ابتزاز وتهديد بنشر الأسرار الشخصية، وجرائم التهديد بالتشهير عبر الفايسبوك من خلال قيام محترفي الجريمة الإلكترونية باستغلال صور الأشخاص، خاصة المخلة بالحياة وكذا الفيديوهات وحتى الوثائق والرسائل



النصية، وجعلها وسيلة ضغط وتهديد للأشخاص والعائلات وتأثي النساء في الدرجة الأولى (باشوش، 2021)، وهذا بالمقارنة بسنة 2019 التي وصل عددها 4210 قضية.

وفي هذا الصدد نجد أيضا تعرض عدة مواقع إلكترونية جزائرية تتبع جهات حكومية ومؤسسات اقتصادية وخدماتية خاصة، لهجمات قراصنة انترنت من بينها الموقع الإلكتروني لوكالة النفط وذلك سنة 2020، كما أطلقت المديرية العامة لسوناطراك تحذيرا لموظفيها ضد برمجيات ضارة Ransomware، التي مست بعضا من الحسابات الشخصية للمستخدمين في الشركة، مرفقا بجملة من التعليمات والإرشادات لمجابهة الخروقات والتي قد تمس قواعد بياناتها، هذا وقد تعرضت سوناطراك للعديد من محاولات الاختراق لمواقعها قام بها هاكرز مؤجرين والتي كانت تركز بالأساس على استثمارات الشركة الوطنية للمحروقات، بالإضافة إلى أشغال استكشاف آبار البترول وآبار الغاز.

5. بطاقة فنية عن أمن ولاية تمنراست :

تقع ولاية تمنراست في أقصى جنوب البلاد، تتربع على مساحة تشغل ربع (1/4) مساحة الوطن والمقدرة بحوالي: 557.906.25 كلم مربع وهذا قبل التقسيم الإداري الجديد، تقدر الكثافة السكانية لولاية تمنراست بـ 242.852 نسمة، هذا العدد الكبير من النسمة يسهر على حمايته من كل أنواع الجرائم والمجرمين أجهزة ومؤسسات أمنية يتمتع موظفوها بأعلى مستوى من الكفاءة وهذا لضمان الخصوصية الفردية، والأرواح من أي فعل إجرامي.

ونظرا لخصوصية المنطقة كونها منطقة حدودية ومنطقة عبور، وبها كل من قنصليتي جمهورية النيجر ومالي، ومنطقة صناعية بامتياز بها العديد من المؤسسات الاقتصادية الأجنبية والعمومية (أنظر الجدول رقم 2) ويتوافد عليها العمال الأجانب والإطارات العاملة بالشركات وعمال من كل ربوع الوطن، فالتعرض للهجمات السيبرانية بكل أنواعها أمر وارد قد يمس الأشخاص أو المؤسسات.

جدول رقم (2): عدد الشركات العاملة بتمنراست

عدد المؤسسات	مجال العمل
28	المؤسسات الأجنبية
17	المؤسسات الخدماتية القطاع الخاص
281	البناء والأشغال العمومية
92	الصناعة
351	المجموع

إحصائيات مقدمة من المديرية العامة للأمن الوطني "أمن ولاية تمنراست"

6. المديرية العامة للأمن الوطني "أمن ولاية تمنراست": كفاءات بشرية لمواجهة الجريمة الإلكترونية :



لمحاربة الجريمة الإلكترونية التي اكتسحت المجتمع الجزائري تباشر مصالح الشرطة القضائية من خلال فرقة مكافحة الجريمة الإلكترونية المدعمة بأفراد وأعوان تلقوا تكوينا خاصا في كيفية الوصول إلى المجرم الإلكتروني، وباستخدام أحدث تكنولوجيا البحث والتحري عن هذا النوع من الجرائم، فور تقديم شكاوي تتعلق بجرائم الانترنت، ومن بين المؤسسات الأمنية التي تسعى إلى تحقيق أمن واستقرار الأفراد نجد أمن ولاية تلمسان.

أجريت الدراسة الراهنة بأمن ولاية تلمسان التي تقع بوسط المدينة بحي آمشون الذي يضم أمن دائرتين هما: أمن دائرة سيرت وأمن دائرة تازروك، إضافة إلى وجود 5 أمن حواضر موزعة عبر كل من حي بامون، سرسوف، أنكوف، تقيارت، قطع الواد. ويضم أمن ولاية تلمسان حوالي 7 مصالح ولأئمة من بينها المصلحة الولائية للشرطة القضائية، التي بدورها تنقسم إلى فرقة من بينها فرقة مكافحة الجريمة المعلوماتية والتي تضم إطارات ورتباء وأعوان يسهرون على مكافحة والتصدي للجرائم الإلكترونية عبر آليات وبرامج مختصة، وفيما يلي إحصائيات حول نشاطات هذه الفرقة في مجال الجريمة الإلكترونية:

خلال سنة 2018 قامت المصالح العملياتية للشرطة القضائية بتمناسات بتسجيل 1278 قضية جزائية منها 20 قضية تتعلق بجرائم المعلوماتية أي ما معدله 1.56% من إجمالي عدد الجرائم تورط فيها 12 شخص والجدول الآتي يوضح ذلك:

المجدول رقم (3): إحصائيات سنة 2018

أنواع الجرائم	القضايا المسجلة	الأشخاص المتورطون	المودعون رهن الحبس المؤقت
المساس بحرية الأشخاص	08	04	01
النصب و الاحتيال	04	02	00
السب و الشتم	03	01	00
التهديد	01	//	//
انتحال هوية الغير	02	02	00
جرائم أخرى	02	03	00
المجموع	20	12	01

إحصائيات مقدمة من المديرية العامة للأمن الوطني "أمن ولاية تلمسان"

هذه الإحصائيات تجلي الغموض عن الجرائم الإلكترونية المسجلة سنة 2018، والتي تتنوع بين جرائم المساس بحرية الأشخاص وكانت أعلى القضايا المسجلة بـ 8 قضايا، النصب والاحتيال 4 قضايا، السب والشتم 3 قضايا، انتحال هوية الغير قضيتين، التهديد سجلت خلال نفس السنة قضية واحدة فقط، انتحال هوية الغير قضيتين وغيرها من الجرائم بنسب متفاوتة، التي تتعدد أنواعها حسب الزمان والمكان، كما أن تسجيل تورط 12 شخص ليس من باب الصدفة وإنما نتيجة التحريات والمجهودات التي قامت بها فرقة مكافحة الجريمة الإلكترونية والتي أفضت إلى إبداع شخص واحد رهن الحبس المؤقت.

أما سنة 2019 سجلت نفس المصالح 1325 قضية جزائية منها 13 قضية تتعلق بجرائم المعلوماتية أي ما معدله 0.98% من إجمالي عدد الجرائم، تورط فيها 14 شخص والجدول رقم (4) يوضح ذلك

المجدول رقم (4): إحصائيات سنة 2019



أنواع الجرائم	القضايا المسجلة	الأشخاص المتورطون	المودعون رهن الحبس المؤقت
المساس بحرمة الأشخاص	01	01	00
النصب و الاحتيال	05	05	00
السب و الشتم	01	01	00
التهديد	01	01	00
القذف	04	05	01
استعمال تكنولوجيا الإعلام والاتصال (الفايسبوك)	01	01	01
المجموع	13	14	01

إحصائيات مقدمة من المديرية العامة للأمن الوطني "أمن ولاية تمنراست"

الإحصائيات المسجلة سنة 2019 تظهر تناقص عدد الجرائم الإلكترونية وهذا لتراجع عدد المبلغين عنها، رغم تسجيل نفس الجرائم المسجلة سنة 2018، المتعلقة بالمساس بحرمة الأشخاص وتسجيل قضية واحدة قيد المعالجة، النصب والاحتيال مع تسجيل 5 قضايا وتورط 5 أشخاص، السب والشتيم قضية واحدة، القذف سجلت 4 قضايا، إضافة إلى جريمة جديدة مبلغ عنها تتعلق باستعمال تكنولوجيا الإعلام والاتصال (الفايسبوك) أين تم تسجيل قضية واحدة مع تورط شخص واحد في القضية، أما أكبر القضايا المبلغ عنها هي جريمة النصب والاحتيال فقد تم تسجيل 5 قضايا مع تورط 5 أشخاص بعدها جريمة القذف وتورط 5 أشخاص فيها تم الكشف عنهم من قبل مصالح فرقة مكافحة الجرائم المعلوماتية، كما أن تسجيل تورط 14 شخص دليل على احترافية مصالح الأمن وبالأخص فرقة مكافحة الجريمة المعلوماتية.

في حين سجل من طرف نفس المصالح سنة 2020، 1433 قضية جزائية منها 51 قضية تتعلق بجرائم المعلوماتية أي ما يعادل نسبة 3.55 % من إجمالي الجرائم والجدول رقم (5) يوضح ذلك



أنواع الجرائم	القضايا المسجلة	الأشخاص المتورطون	المودعون رهن الحبس المؤقت
المساس بجريمة الأشخاص	05	05	00
النصب و الاحتيال	13	15	00
السب و الشتم	01	01	00
التهديد	00	00	00
القفذ	11	10	00
الدخول والبقاء عن طريق الغش في منظومة المعالجة الآلية للمعطيات	04	03	00
استخدام الانترنت لأغراض إجرامية	07	08	04
أنواع أخرى	10	08	02
المجموع	51	50	06

إحصائيات مقدمة من المديرية العامة للأمن الوطني "أمن ولاية تلمسان"

ما يلاحظ على الجرائم الإلكترونية المسجلة سنة 2020 هو الارتفاع النسبي في عدد القضايا المسجلة والذي بلغ 51 قضية في مقابل 13 قضية سنة 2019، تورط فيها 50 شخص، وتعتبر جريمة النصب والاحتيال من أعلى القضايا المسجلة والمقدرة بـ 13 قضية مع تسجيل 15 شخص متورط فيها، بالإضافة إلى ذلك نلاحظ زيادة تعدد أنواع الجرائم الإلكترونية كجريمة الدخول والبقاء عن طريق الغش في منظومة المعالجة الآلية للمعطيات وقد تم تسجيل 4 قضايا متعلقة بها، وكذا جريمة استخدام الانترنت لأغراض إجرامية أين تم تسجيل 7 قضايا مع تورط 8 أشخاص بخصوصها، وهذا خصوصا مع استفحال الوضعية الوبائية عالميا ومحليا، ارتفاع عدد القضايا المسجلة يقابله ارتفاع في الكشف عن المتورطين.

خلال سنة 2021 سجلت مصالح الشرطة القضائية 70 قضية حول الجرائم الإلكترونية من إجمالي 1410 قضية، حيث بلغت نسبة حل القضايا 50 % ، كما سجلنا 54 شخص متورط، تم إيداع 06 أشخاص الحبس المؤقت، والجدول رقم (6) يوضح ذلك:

الجدول رقم (6): إحصائيات 2021



أنواع الجرائم	القضايا المسجلة	الأشخاص المتورطون	المودعون رهن الحبس المؤقت
المساس بالأشخاص عبر الانترنت (السب والشتيم ، القذف، المساس بالحياة الشخصية)	18	50	//
النصب و الاحتيال عبر الفايسبوك	27	//	//
الدخول والبقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات	03	//	//
جرائم أخرى	22		
المجموع	70	50	//

إحصائيات مقدمة من المديرية العامة للأمن الوطني "أمن ولاية تلمسان"

خلال سنة 2021 نلاحظ الارتفاع المستمر للقضايا المسجلة مع تعددها، وهذا يعبر عن زيادة وعي الأفراد بضرورة التبليغ عن هذا النوع من الجرائم التي يصعب الكشف عنها بالرغم من ذلك تم تسجيل 50 شخص متورط فيها ولا زالت جرائم النصب والاحتيال عبر الفايسبوك في ارتفاع مستمر مقارنة بباقي الجرائم أين سجلنا 27 قضية في مقابل 18 قضية مسجلة حول المساس بالأشخاص عبر الانترنت (السب والشتيم، القذف، المساس بالحياة الشخصية).

من خلال قراءة هذه الجداول الإحصائية لسنوات 2018، 2019، 2020، 2021 نشير إلى تعدد أنواع الجريمة الإلكترونية التي تحقق فيها مصالح الشرطة القضائية ومن خلالها فرقة مكافحة الجريمة الإلكترونية لأمن ولاية تلمسان وتتمثل في جرائم المساس بحرية الأشخاص، النصب والاحتيال، السب والشتيم، التهديد، انتحال هوية الغير، استعمال تكنولوجيا الإعلام والاتصال (الفايسبوك)، الدخول والبقاء عن طريق الغش في منظومة المعالجة الآلية للمعطيات، استخدام الانترنت لأغراض إجرامية.

وما يلاحظ على هذه الإحصائيات للأربع سنوات الأخيرة هو ارتفاع عدد القضايا المعالجة حول الجرائم الإلكترونية، وذلك يرجع لزيادة استخدام الانترنت، بالتالي الوقوع وتعرض الأفراد والمؤسسات لهذا النوع من الجرائم، إضافة إلى زيادة وعي الأفراد بأهمية التبليغ عن ذلك، وأهم شيء هو قدرة الإطارات والرتباء وأعاون الأمن على حل هذه القضايا بفضل القدرات الذهنية، والقدرة على استخدام التجهيزات التكنولوجية المساعدة على الكشف عن الجناة بفضل الدورات التكوينية والتدريبية التي يخضع لها بصفة دورية ومستمرة المعنيين بالأمر، وهذا ما يوضح الأهمية البالغة التي توليها الدولة لحماية الأفراد وحياتهم الشخصية إضافة إلى حماية المؤسسات من الاختراقات والقرصنة.

وينبغي الإشارة في هذا الإطار أن وجود ظاهرة إجرامية مستجدة يفرض وجود نصوص قانونية لتجريم مرتكبيها وفرض عقوبات مناسبة لها، لهذا عمد المشرع الجزائري إلى وضع نصوص قانونية خاصة بهذا النوع من الجرائم لحماية الخصوصية الشخصية للأفراد في مجتمع يعتز كثيرا بمبادئه وقيمه الفاضلة.

7. توصيات واقتراحات :



خلصت الدراسة الراهنة إلى التوصيات والاقتراحات التالية:

- ضرورة إعادة النظر في التشريعات الإجرائية في الجزائر المتعلقة بحماية الحرية الشخصية وحرية الحياة الخاصة من الوسائل الإلكترونية.
- ضرورة وجود اتفاق دولي حول تعريف الجريمة الإلكترونية والأنواع التي تندرج تحتها مع مراعاة التطور التكنولوجي الحاصل.
- ضرورة التوافق الدولي في وضع قوانين لمحاربة الجريمة الإلكترونية بكل أنواعها.
- توقيع اتفاقيات دولية لتكوين فرق بحث وتحري حول الجريمة الإلكترونية لحماية الأفراد والبنية التحتية للدول ومؤسساتها من أي هجوم إلكتروني محتمل.
- الاستنجاد بشركات متخصصة في مجال تكنولوجيا الإعلام والاتصال للمشاركة في رصد وتحليل الجرائم المتعلقة بالانترنت

خاتمة

خصوصية الجرائم الإلكترونية وارتباطها بالحاسب الآلي جعلها تتميز عن الجرائم التقليدية، وانعكاس ذلك على إجراءات المتابعة المنتهجة من قبل السلطة المختصة بالتحري والكشف عن مرتكبي هذه الجرائم. فالجرائم المعلوماتية تتميز بالخبرة المكتسبة في مجال تكنولوجيا المعلومات، قد تكون دوافعه مادية كالنصب والاحتيال عبر مواقع التواصل الاجتماعي أو دوافع معنوية الغرض منها الانتقام أو إلحاق الضرر بالأفراد، أو تبين قدرة ذهنية إزاء كل تقنية تظهر. ولكن مهما تعددت وتنوعت هذه الجرائم ومهما كان الدافع إليها، لجأت السلطات المعنية بتطوير أساليب لحماية الأفراد والمؤسسات من الهجمات السيبرانية وتحقيق حماية استباقية ضد أي تهديدات متقدمة، قد تؤدي إلى خسائر مالية فادحة، بالاعتماد على كفاءات بشرية مؤهلة لفك لغز الغش والاحتيال والقرصنة، خاضعين لتدريبات على أعلى مستوى في مجال تكنولوجيا الإعلام والاتصال ومواكبين لكل جديد فيها مثل ما هو موجود على مستوى مديرية الأمن لولاية تلمسان.

قائمة المراجع

- 1- الدوكات، سناء. (2018). تعريف الأمن متاح على الرابط <https://mawdoo3.io/article/19125> تاريخ الاسترجاع 2021/12/12.
- 2- سالم، صلاح. (2003). تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع. ط1. مصر: عين للدراسات والبحوث الإنسانية والاجتماعية.
- 3- بن عيسى. محسن محمد العجمي. (2001). الأمن والتنمية. ط1. المملكة العربية السعودية: جامعة نايف العربية للعلوم الأمنية.
- 4- (دور المؤسسات الأمنية في المجتمع. (2020) متاح على الرابط <https://mafahem.com> تاريخ الاسترجاع 2021/11/23.
- 5- المبادرة المصرية للحقوق الشخصية. (2011). قواعد حفظ الأمن في المظاهرات والاضطرابات العامة. متاح على الرابط https://eipr.org/publications_%D8 تاريخ الاسترجاع 2021/12/31.
- 6- بوضياف. إسمهان. (2018). الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر. مجلة الأستاذ الباحث للدراسات القانونية والسياسية. ع11. جامعة محمد بوضياف. الجزائر. (ص 348-375).
- 7- قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية. ع47. صادرة بتاريخ 2009/08/16.
- 8- المديرية العامة للأمن الوطني. (2017). مصالح شرطة مكافحة الجرائم الإلكترونية تسجل 567 قضية تتعلق بجرائم الانترنت. متاح على الرابط <https://www.algeriepolice> تاريخ الاسترجاع 2017/02/11.
- 9- بورنان، يونس. الجزائر.. 2500 جريمة إلكترونية في 2017. العين الإخبارية. متاح على الرابط <https://al-ain.com/article/algeria-2500-electronic-crime-2017> تاريخ الاسترجاع 2021/11/11.



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها

رمز I05L02UN260120190001

- 10- وكالة الأنباء الجزائرية. (2018). الجريمة الالكترونية: معالجة أزيد من 1100 قضية خلال 2018 على المستوى الوطني. متاح على الرابط <https://www.aps.dz/ar/sante-science-technologie/63173-1100-2018>
- 11- باشوش، نواره. (2021). الإجرام الإلكتروني.. أرقام مرعبة. متاح على الرابط <https://www.echoroukonline.com/2021/11/22> تاريخ الاسترجاع



دور الأجهزة الأمنية في محاربة الجريمة السيبرانية في الجزائر

عائشة عبد الحميد

draicha614@gmail.com

مقدمة:

إن التطور المتسارع الذي تشهده الجزائر في مجال التكنولوجيات الجديدة للإعلام والاتصال والاستخدام المتنامي للتطبيقات المتصلة بالإنترنت و الوسائط الإلكترونية والرقمية الجديدة لحفظ الملفات والصور وغيرها، يستدعي إرساء قاعدة قانونية وتوفير الأجهزة والهياكل الضرورية لمكافحة الجريمة السيبرانية العابرة للأوطان .

حيث تواجه البشرية تهديدات رقمية جديدة أكثر تعقيدا و أشد فتكا وضررا، تتسبب في إتلاف منظومات شبكات الكمبيوتر لمؤسسات كبيرة وحساسة داخل الدول التي لا زالت غير آمنة، بالإضافة إلى وجود هجمات إلكترونية موجهة ومعقدة، حيث ينتج تعقيد هذه الهجمات الإلكترونية من كون أنه قد لا يبرز أثرها على الفور، فأغلبية ضحايا هذه الهجمات يجهلون بادئ الأمر تعرضهم للقرصنة ولا يكتشفوا ذلك إلا بعد مرور الوقت.

وحسب آخر الإحصائيات، فإن 40 % فقط من الدول الإفريقية هي التي تملك اليوم إطارا قانونيا يعاقب الأعمال المتعلقة بالجرائم السيبرانية، وحتى وإن وجدت هذه القوانين الساعية لتطوير مجال الأمن السيبراني إلا أنها لا تواكب الوتيرة المتسارعة للابتكارات المتجددة في مجال التكنولوجيا الرقمية.

وتعد الجزائر من الدول التي تحارب الإجرام السيبراني حفاظا على مراسلاتها الإلكترونية و أمنها المعلوماتي. مع مرور الزمن و تسارع التطور التكنولوجي، غلبت ثقافة العولمة في أرجاء المعمورة فتحول العالم إلى قرية صغيرة وأصبح تبادل المعلومات والأفكار متاح بضغطة زر.

وعليه: ما هو مفهوم الإجرام السيبراني ؟ وما هو دور مرفق الدفاع الوطني في التصدي لهذا النوع وتحقيقي الأمن المعلوماتي.

من خلال هذه الإشكالية سنقسم هذه المداخلة إلى العناصر التالية :

1. الإطار المفاهيمي للجريمة السيبرانية في نظر التشريع الجزائري وتطورها.

2. الأجهزة الأمنية المتكلفة بمحاربة الجريمة السيبرانية.

1. الإطار المفاهيمي للجريمة السيبرانية في نظر التشريع الجزائري وتطورها :

1.1 تعريف الجريمة السيبرانية (الإلكترونية):

تعتبر الجريمة المعلوماتية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية، لتطورها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية بـ " إساءة استخدام الكمبيوتر " ثم " احتيال الكمبيوتر "، " فالجريمة المعلوماتية " بعدها " جرائم الكمبيوتر"، جرائم التقنية العالية إلى " جرائم الهاكرز " فجرائم الإنترنت " وأخيرا " السبركرام"¹

وقد وصفت هذه الجريمة بأنها مقاومة للتعريف، لكثرة ما تناولته الكتابات عنها شرحا و توضيحا، فمنهم من نظر إليها من خلال وسيلة ارتكابها، و منهم من خلال موضوعها، و منهم من خلال توافر المعرفة بتقنية المعلومات.

¹ أنظر مليكة عطوي ، الجريمة المعلوماتية ، حوليات جامعة الجزائر ، عدد 21 ، ص 08



حيث يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها " الجريمة التي تلعب فيها البيانات الحاسوبية، والبرامج المعلوماتية دورا رئيسيا¹ أو كل " فعل إجرامي متعمد أيا كانت صلتها بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه ، أو كسب يحققه الفاعل²

وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي و التنمية (OCDE) للجريمة المعلوماتية في اجتماع باريس عام 1983 بأنه :

"كل سلوك غير مشروع أو غير أخلاقي ، أو غير مصرح به يتعلق بالمعالجة الآتية للبيانات أو نقلها"³.

1.1 مراحل تطور الجريمة السيبرانية:

مرت الجريمة السيبرانية بتطور تاريخي، بدأ من اختراع الحاسوب و إنشاء الشبكة العنكبوتية، وصولا إلى الثورة العالمية في الاتصالات والتكنولوجيا، وبحكم هذا التطور تطورت هذه الجريمة بشكل عام وخاص، و يمكن ملاحظة ثلاث مراحل لتطورها:

1.2.1 مرحلة شيوع استخدام الكمبيوتر في الستينات ثم السبعينات : بظهور استخدام الكمبيوتر و ربطه بالشبكات في الستينات إلى السبعينات ظهرت أول معالجة لنظام الكمبيوتر وتدمير أنظمة الكمبيوتر فبقيت محصورة في البداية في إطار السلوك الغير أخلاقي دون النطاق القانوني، ومع توسع الدراسات تدريجيا وخلال السبعينات بدأ الحديث عنها كظاهرة إجرامية جديدة⁴.

2.2.1 مرحلة الثمانينات: في هذه المرحلة، ظهر نوع جديد من الجرائم ارتبط بعمليات اقتحام نظام الحاسوب عن بعد، ونشر الفيروسات عبر شبكات الكمبيوتر أين شاع اصطلاح "الهاكرز" و كانوا مرتكبوها من العباقرة صغار السن لإظهار التفوق التقني، وبعد ذلك تحولت الجريمة من مجرد مغامرة إلى أفعال تستهدف التحسس والاستيلاء على البيانات الاقتصادية والاجتماعية و السياسية والعسكرية.⁵

3.2.1 مرحلة التسعينات: شهدت هذه المرحلة تناميا هائلا ، في حقل الجرائم التقنية و تغييرا في نطاقها و مفهومها، فظهرت أنماط جديدة كأنشطة إنكار الخدمة، كما نشطت جرائم نشر الفيروسات عبر مواقع الانترنت، كما ظهرت أنشطة الرسائل والمواد الكتائبة المنشورة على الانترنت، أو المراسلة عبر البريد الإلكتروني المنطوية على إثمه الأحقاد أو المساس بالكرامة.⁶

3.1 خصائص الجريمة السيبرانية:

تعد الجرائم السيبرانية إفرازا ونتاجا لتقنية المعلومات وهذا ما أكسبتها طابعا قانونيا خاص يميزها عن غيرها من الجرائم التقليدية بمجموعة من الخصائص:

1.3.1 الجرائم السيبرانية هي جرائم عابرة للحدود: إن الجريمة المعلوماتية هي شكل من أشكال الجرائم العابرة للحدود، فمسح الجريمة لم يعد محليا بل أصبح عالميا، إذ أن العامل لا يتواجد ماديا على مسرح الجريمة، فالفاعل يستطيع القيام بجريمته بالدخول إلى

¹ أنظر مليكة عطوي ، الجريمة المعلوماتية ، حوليات جامعة الجزائر ، عدد 21 ، ص 08

² نحلة عبد القادر المومني ، الجرائم المعلوماتية ، الأردن ، دار الثقافة للنشر و التوزيع ، ط1 ، ص 49.

³ سميرة معاشي ، ماهية الجريمة المعلوماتية ، مجلة المنتدى القانوني ، عدد 7 ، جامعة محمد خيضر ، بسكرة ، أفريل 2010 ، ص 278.

⁴ - يونس عرب، جرائم الكمبيوتر و الانترنت، إيجاز في المفهوم و النطاق و الخصائص و الصور و القواعد الإجرائية للملاحظة و الإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات و البحوث الجنائية، أبو ظبي، 2002، ص 08.

⁵ - عبد الفتاح مراد ، د.ت.ن ، دور الكمبيوتر في مجال ارتكاب الجرائم الالكترونية بشرح جرائم الكمبيوتر و الانترنت ، مصر ، دار الكتب و الوثائق المصرية، ص 43.

⁶ - يونس عرب، مرجع سابق،



ذاكرة الحاسوب الموجود في بلد آخر وهذا الفعل ليلقى شخصا ثالثا موجود في بلد آخر.¹ وهذا ما يثير مسألة الاختصاص القضائي في محاكمة الجاني.

2.3.1 صعوبة اكتشاف و إثبات الجرائم السيبرانية: تتميز هذه الجرائم بصعوبة الاكتشاف والإثبات وذلك لعدم ترك الجاني آثار تدل على إجرامه، فالجريمة تتم عن طريق إدخال رموز وأرقام دقيقة يصعب اكتشافها وإثباتها، لهذا عادة ما يتم اكتشافها بالصدفة، وغالبا ما يصعب معاقبة المجرم وذلك لعدم وجود أدلة قائمة في حقه.²

3.3.1 فالجريمة المعلوماتية لا تترك آثار ملموسة، وبذلك لا تترك شهود تمكن الاستدلال بأقوالهم، ولا أدلة مادية يمكن فحصها، لأنها تقع في بيئة افتراضية، يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية.³

4.3.1 ارتفاع الخسارة الناتجة عن الجريمة المعلوماتية: وذلك مقارنة بالجريمة التقليدية، فقطاعات الأعمال العالمية يتكبد خسائر تصل إلى 400 مليار دولار أمريكي، وقد خسر مصرفين في الخليج 45 مليون دولار في ساعات قليلة وأعلنت الهند عن تعرض 308371 موقعا الكترونيا للاختراق بين عامي 2011 و 2013،⁴ قلة الإبلاغ عن وقوع الجريمة الإلكترونية راجع إلى الخشية والخوف من التشهير والإساءة للسمعة.

4.1 موقف المشرع الجزائري من الجريمة السيبرانية:

بالموازاة مع منافعها وخدماتها الجمّة، أضحت التكنولوجيا والانترنت بصفة خاصة تستخدم لارتكاب الجرائم والإضرار بالأفراد والمؤسسات وممتلكاتهم، وبالتالي أصبح من واجب الدولة اتخاذ الإجراءات اللازمة لإحباط أي هجوم من شأنه تهديد سيادة الدولة ومؤسساتها وأمن مواطنيها.

لقد أبدت الجزائر التي تعتبر دولة رائدة إقليميا في مجال الأمن المعلوماتي استعدادها منذ سنوات لمكافحة الجرائم السيبرانية والمعلوماتية بشكل حازم، لذا عكفت على إعداد النصوص القانونية القادرة على إنشاء منظومة دفاعية وقائية يتم على أساسها مكافحة الأعمال الإجرامية المتعلقة بالانترنت و متابعة مرتكبيها قضائيا، كما تسمح بتقفي آثار المجرمين والجناة الذين يستغلون التكنولوجيا وتطبيقاتها لارتكاب أعمالا إجرامية وغير قانونية.

- فكيف ساهمت النصوص المختلفة في مكافحة و محاربة الإجرام السيبراني أو الإجرام المعلوماتي ؟

- وبعبارة أخرى كيف واجه التشريع الجزائري الجرائم السيبرانية ؟

حاول المشرع الجزائري إصدار قوانين عامة وخاصة وهيكل و أجهزة للجرائم الالكترونية ومن بينها :

كفل الدستور الجزائري الصادر في 06 مارس 2016 حماية الحقوق الأساسية والحريات الفردية وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان منها المواد 38، 44 من الدستور.

وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات وقانون الإجراءات الجزائية والتي تحظر كل مساس بهذه الحقوق.

¹ - معتوق عبد اللطيف ، 2011 ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن ، مذكرة ماجستير جامعة العقيد الحاج لخضر ، باتنة ، كلية الحقوق ، 2012 ، 2011 ، ص 24.

² - معتوق عبد اللطيف، المرجع نفسه، ص 24.

³ - سعيد علي نعيم ، آليات البحث و التحري عن الجرائم المعلوماتية في القانون الجزائري ، مذكرة ماستير ، جامعة العقيد الحاد لخضر ، باتنة ، كلية الحقوق، 2013 ، 2012 ، ص 24.

⁴ - سعيد علي نعيم، المرجع نفسه، ص 34.



1.4.1 قانون العقوبات :

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي حيث عدل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات، ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 7.

2.4.1 قانون الإجراءات الجزائية :

قام المشرع الجزائري بتمديد الاختصاص المحلي لوكيل الجمهورية في مجال الجرائم الالكترونية، طبقا للمادة 37 فقرة 02 من قانون الإجراءات الجزائية.¹

حيث يمتد الاختصاص المحلي إذا تعلق الأمر بجرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد والتهريب.² كما تعد هذه الجرائم أيضا من الجرائم الموصوفة طبقا للتشريع الجنائي الجزائري.

كما نص على التفتيش في المادة 45 فقرة 7 من نفس القانون المعدل حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعرف عليه من حيث القواعد الإجرائية العامة والشروط الشكلية والموضوعية، وبالتالي لا تطبق عليه المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية ونص على توقيف النظر في جريمة المساس بأنظمة معالجة المعطيات طبقا للمادة 51 فقرة 06 من القانون .

كما نص أيضا قانون الإجراءات الجزائية بموجب المادة 65 مكرر 3 فقرة 5 أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن وكيل الجمهورية المختص يقوم بوضع الترتيبات التقنية دون موافقة المعني، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة .

وفي عام 2006، أدخل المشرع تعديل آخر على قانون العقوبات بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2004، من هذا التعديل القسم السابع مكرر و الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال.

وبعد التعديل الأخير لقانون العقوبات الجزائري بموجب القانون رقم 16-02 المؤرخ في 19 يونيو 2016³، ضمن القسم السابع مكرر من قانون العقوبات بموجب المواد من 394 مكرر إلى المادة 394 مكرر 8.

وضمن نطاق الفصل الثالث الخاص بالجنايات و الجنح ضد الأموال .

من بين هذه الجرائم: الغش أو الشروع فيه في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات، حذف أو تغيير للمعطيات المنظمة، إدخال أو تعديل في نظام المعطيات، تصميم أو بحث أو تجميع أو توفير أو نشر أو حيازة أو إفشاء أو نشر أو استعمال المعطيات، تكوين جمعية الأشرار.

3.4.1 صدور قانون رقم 09-04:

¹ - أنظر المادة 37 من قانون الإجراءات الجزائية ، بموجب الأمر 15-02 المؤرخ في 23 يوليو سنة 2015.

² - عبد الله أوهابيه ، 2018 ، شرح قانون الإجراءات الجزائية ، الجزء الأول ، الجزائر ، دار هومة، ص 358.

³ - أنظر الجريدة الرسمية عدد 37 المؤرخ في 22 يونيو 2016.



عمليا، سعت الجزائر إلى استدراك الفراغ القانوني من خلال تعزيز منظومتها التشريعية خاصة منذ 2009، بحيث سن المشرع الجزائري القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بتاريخ 05 أوت 2009¹.

يحتوي هذا القانون على 19 مادة موزعة على 06 فصول مستمدة من الاتفاقيات الدولية. كما جاء مطابقا للتشريعات الوطنية لاسيما تلك المتعلقة بمحاربة الفساد و تبييض الأموال وتمويل الإرهاب. حيث نص القانون رقم 09-04 وبموجب الفصل الخامس منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات والوقاية ومساعدة الجهات التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام ببحرث قضائية في حالة الاعتداءات على المنظومة المعلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

وذلك بالتعاون مع جهات قضائية أخرى منها المعهد الوطني للأدلة الجنائية و علم الإجرام والمديرية العامة للأمن الوطني لمكافحة الجريمة الإلكترونية ذات البعد الدولي من خلال انضمامها للمنظمة الدولية للشرطة الجنائية INTERPOL.

علاوة على ذلك يجب التنويه بالجهود التي تقوم بها الجزائر منذ جانفي 2015 من أجل تكيف إطارها التشريعي والتنظيمي من خلال تبني مجموعة من القوانين الهامة منها الخاصة بالتوقيع والمصادقة الالكترونية التي من شأنها تطوير الخدمات المقدمة عبر الانترنت مثل الإدارة الالكترونية، التجارة الالكترونية وكذا البنوك الالكترونية، فضلا عن سعي الجزائر الحثيث إلى إرساء قاعدة قانونية لاستخدام التكنولوجيات الجديدة للإعلام والاتصال في تطوير قطاع العدالة.

2. الأجهزة الأمنية المتكيفة بمحاربة الجريمة السيبرانية:

لقد وضعت قيادة الدفاع الوطني الأمن السيبراني أحد أولوياتها، على غرار باقي دول العالم التي سارعت إلى مراجعة سياساتها الأمنية، وإدراجها لآليات وميكانيزمات جديدة تعني بهذه المسائل بالموازاة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي. ويفرض مطلب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية، ولهذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي للأطر القانونية و التكنولوجية الملائمة، وتأخذ بعين الاعتبار دقة الهجمات الالكترونية وتعقيدها والتي يزداد خطرها مع التطور التكنولوجي واستخداماتها اليومية.

وتجسيدا لذلك باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية والحد من انتشارها، وإن شاء أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال، إذ أصبحت الحماية السيبرانية جزءا مهما في أي منظومة للدفاع، وقد استطاع الجيش الشعبي الوطني المضي قدما ومسايرة التطورات التكنولوجية والإعلامية الحاصلة في العالم، ومن ثمة تأمين وحماية نطاقه المعلوماتي، وتأمين الفضاء المعلوماتي لكل الناشطين فيه.²

1.2. الهياكل المنشأة لتقصي الجريمة السيبرانية:

¹ - أنظر المادة نص القانون رقم 09-04، الجريدة الرسمية، عدد 47 الصادرة في 05 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

² - سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر، الدور والتحديات الملتقى الدولي حول سياسات الدفاع الوطني، جامعة قاصدي مرباح، ورقلة، كلية الحقوق، 2017/01/31.



1.1.2 مركز الوقاية من جرائم الإعلام الآلي و جرائم المعلوماتية للدرك الوطني:

أنشئ هذا المركز في 2008، يوجد مقره بئر مراد رابح، أهدافه تأمين منظومة المعلومات لخدمة الأمن العمومي، وهو بمثابة مركز توثيق، ويقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية المرتكبة، ومحاولة تحديد هوية أصحابها، مما يضمن الأنظمة المعلوماتية للمؤسسات والبنوك والبيوت والشركات ... الخ، ويعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى، والجدير بالذكر أن المركز استطاع معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يفوق 500 قضية رقمية خلال سنة 2015، وهذا بفضل التركيبة البشرية المؤهلة التي اكتسبها الجهاز من التكوين المستمر والمتلقيات الوطنية والدولية وتبادل الخبرات مع الدول الأخرى.

2.1.2 المعهد الوطني للأدلة الجنائية وعلم الإجرام:

أنشأ المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والاتصال الإلكتروني، أنشأ بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004 وعدل نظامه الأساسي بموجب المرسوم الرئاسي رقم 09-118 المؤرخ في 14 أبريل 2004.

يتكون هذا الجهاز من "11" إحدى عشر دائرة متخصصة في عدة مجالات متباينة، تضمن جميعها الخبرة و التكوين والتعليم، وتقديم جميع المساعدات التقنية، تقوم دائرة الإعلام الآلي والالكتروني المكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة مع تقديم المساعدة للمحققين، يتكون من عدة تجهيزات تتمثل في محطة ترميم وتصليح الأجهزة والحوامل المعطلة، الشبكات الإعلامية والتجهيزات البيانية، محطة محمولة وثابتة لإجراء خبرات الإعلام الآلي، ويحتوي سبع قاعات، هي: كتب التوجيه، فصيلة الأنظمة المشحونة، فصيلة تحليل المعطيات، فصيلة الهواتف، اقتناء المعطيات، قاعة موزع و قاعات تخزين.

حيث يعد مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بالمهام التالية: إجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية وهذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجرح.

- ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.
- المشاركة في الدراسات و التحاليل المتعلقة بالوقاية و التقليل من كل أشكال الإجرام.
- تصميم وإنجاز بنوك المعطيات.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة و إجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام و الأدلة الجنائية على الصعيدين الوطني و الدولي.

- المشاركة في كل المتلقيات والمحاضرات والندوات على الصعيدين الوطني والدولي لتطوير مستوى مستخدمي المعهد.
- المساهمة في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية.
- ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها:

- **مصلحة البصمات:** يتم على مستوى هذه المصلحة مقارنة البصمات للتعرف على الجثث وتحدد الإشارة إلى أن الدرك الجزائري مجهز بأنظمة التعرف الآلي على البصمات (THE AFIS AutomatedFingerprint Identification System).



– **مصلحة الوثائق:** في هذه المصلحة يتم التأكد من صحة الوثائق والإمضاءات والتحقق من النقود وكذلك التأكد من صحة الوثائق السرية.

– **مصلحة الإعلام الآلي:** على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية.

– **مصلحة البيئة:** تشرف هذه المصلحة على عمليات البحث في أسباب تلوث المياه والتربة وكذا الكشف عن المواد السامة المتواجدة في المحيط أو أماكن العمل.¹

3.1.2 المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الالكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.

4.1.2 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261 وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يرأسها وزير العدل وتضم أساسا أعضاء من الحكومة معينين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء. وتضم الهيئة قضاة وضباط وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام القانون الإجراءات الجزائية.

وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات و التزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الالكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

وهي سلطة إدارية تشكلت بمرسوم رئاسي رقم 15-261 تعمل تحت إشراف لجنة يديرها وزير العدل، تضم أعضاء من الحكومة ومسؤولي مصالح الأمن وقضاة وأعوان الشرطة القضائية تابعين للاستعلامات العسكرية والدرك الوطني والأمن الوطني. تعمل على الكشف عن الجرائم الإرهابية الالكترونية وجرائم المساس بأمن الدولة.²

2.2 دور الجيش الوطني الشعبي في تحقيق الأمن المعلوماتي :

¹ – سمير بارة ، الأمن السيبراني في الجزائر ، السياسات و المؤسسات ، المجلة الجزائرية للأمن الانساني ، العدد الرابع ، جويلية 2017 .

² – يوسف بوغرة ، الأمن السيبراني ، الإستراتيجية الجزائرية للأمن و الدفاع في القضاء السيبراني ، مجلة الدراسات الإفريقية و حوض النيل ، المركز الديمقراطي العربي ، المجلد الأول ، العدد الثالث ، سبتمبر 2018.



يقصد بالدفاع الالكتروني في الاستراتيجيات العسكرية: " مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثير الهجمات الالكترونية، والتخفيف من حدتها والتعافي منها بسرعة"، فقد اعتبرت الإستراتيجية النمساوية مصطلح الدفاع الالكتروني " جميع التدابير اللازمة للدفاع عن الفضاء الالكتروني بالوسائل المناسبة لتحقيق الأهداف العسكرية الإستراتيجية "، أما بخصوص الإستراتيجية العسكرية البلجيكية، اعتبرت الدفاع الالكتروني " تطبيق التدابير الوقائية الفعالة للحصول على مستوى مناسب من الأمن الالكتروني، وتقليل المخاطر الأمنية إلى مستوى مقبول، " و فيما يتعلق بالإستراتيجية العسكرية الفرنسية: " مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع عن نظم المعلومات الحرجة في الفضاء الالكتروني "، وفيما يتعلق بالإستراتيجية العسكرية الجزائرية، فقد اعتبرت الدفاع الالكتروني "مراقبة الأنظمة التي تحمي الدولة من كافة التهديدات، ومتابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومة الأسلحة للجيش"¹

حيث أصبحت الحروب المستقبلية حروب الانترنت، كما أبرزت مجلة الجيش في العدد 676 لشهر نوفمبر 2019 على أهمية المركز الوطني للإشارة للجيش الوطني الشعبي.²

1.2.2 الدفاع السيبراني في الجيش الوطني الشعبي :

قررت القيادة العليا للجيش الوطني إحداث "مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة " على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، بهدف تأمين و حماية المنظومات والمنشآت الحيوية لقواتنا المسلحة ضد التهديدات السيبرانية. وعيا منها بالتحديات التي بات يحملها هذا الواقع الجديد وقصد الإلمام بكافة التهديدات التي يشكلها الدفاع السيبراني على الأمن وحتى على سيادة الدول والحكومات. قامت قيادة الجيش الوطني الشعبي بوضع إستراتيجية دفاع سيبراني، تغطي كل الجوانب التي لها صلة بتحقيق نظام دفاع سيبراني متكامل وفعال بهدف تأمين وحماية المنظومات و المنشآت الحيوية للدولة الجزائرية، حيث تم في هذا الصدد وبتاريخ 6 نوفمبر 2015 إحداث على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة "، تكلف أساسا بتخطيط وإدراج و متابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لتحقيق بفعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومات الأسلحة للجيش الوطني الشعبي.

تتمحور إستراتيجية الدفاع السيبراني للجيش الوطني الشعبي حول سبعة محاور وهي:

- **جانب وظيفي و تنظيمي:** تكون أعمال الدفاع السيبراني ضمن الجيش الوطني الشعبي موجهة و منفذة في إطار وظيفة و / أو تنظيمية مكرسة لضمان تجانس وفعالية هذه الأعمال .
- **جانب قانوني :** تحيين وتعزيز باستمرار الإطار القانوني المتعلق باستعمال تكنولوجيايات الإعلام والاتصال عموما وتأمين منظومات الإعلام خصوصا.
- **جانب الموارد البشرية :** تعد جاهزية مورد بشري تقني معتبر و ذوي كفاءة عالية في مجال الدفاع السيبراني هدفا أساسيا لكي تضمن نجاح إدخال هذا المجال في النشاطات العملية والتسيير للجيش الوطني الشعبي.

¹ - نورة باشوش ، الجيش يدخل حرب الفضاء الالكتروني و مكافحة الجوسسة ، على الموقع التالي :

www.echoronkonlire.com/arar/articles/536554.html تاريخ دخول الموقع 2019/11/25.

² - عزاري عبد الغني ، الفريق أحمد قايد صالح ي دشّن المركز الوطني للإشارة ، الحروب المستقبلية هي الأساس حروب الكترونية ، مجلة الجيش ، العدد 676 لشهر نوفمبر 2019.



- **جانب تقني:** تقوية و تكييف القدرات التقنية للحماية، الكشف و الرد على الهجمات السيبرانية باستمرار، مع ضمان يقظة دائمة فيما يخص الطرق والوسائل المستعملة من طرف المهاجمين
 - **جانب الوقاية و التحسيس:** الوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنجز عن استعمال تكنولوجيا الإعلام والاتصال في الإطار المهني أو الشخصي بطريقة مستمرة
 - **جانب البحث و التطوير:** تعد درجة معتبرة من الاستقلالية التكنولوجية، باستعمال وسائل تقنية خاصة أو مشخصة من طرف هياكل البحث والتطوير للجيش الوطني الشعبي، لاسيما تلك المستعملة للحماية ضد التهديدات السيبرانية، عنصرا حاسما في إستراتيجية الدفاع السيبراني.
 - **جانب التعاون :** تعزيز التعاون في مجال الدفاع السيبراني مع جيوش الدول الشريكة من أجل السماح للجيش الوطني الشعبي من الاستفادة من الخبرات والوسائل التكنولوجية المتقدمة جدا.
- في سياق ذي صلة و تعزيزا لإستراتيجية الدفاع الوطني لمكافحة التهديدات السيبرانية، وقصد الإلمام بكافة المستجدات في هذا المجال، وبخاصة تلك التي تعالج موضوع الأمن السيبراني والدفاع كرهان للأمن والدفاع الوطنيين وحماية المنشآت الحساسة ضد الهجمات السيبرانية، تعكف مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لدائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي دوريا على تنظيم ملتقيات محاضرات وورش عمل تطبيقية، كان آخرها ملتقى بعنوان: " الدفاع السيبراني: مكون أساسي للأمن والدفاع الوطني " يومي 15 و 16 ماي 2017 ، والذي أكد من خلاله رئيس دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي اللواء شريف زراد في كلمة افتتاحه، أن تنظيم مثل هذا الملتقى يأتي من أجل خلق فضاء نقاش بين مختلف الفاعلين في الفضاء السيبراني على المستوى الوطني، لفهم أفضل لرهانات الأمن والدفاع السيبرانيين، والتحسين وإثراء المعارف في مجال الوقاية ومكافحة التهديدات السيبرانية وكذا تحديد أثرها على الأمن الوطني.¹
- **مهام مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:** مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة هي تركيبة ملحقة بدائرة التحضير والاستعمال لأركان الجيش الوطني الشعبي، فاستحدثتها في نوفمبر 2015، يندرج ضمن نهج إرساء السياسة الشاملة المسطرة من قبل القيادة العليا و الهادفة إلى حماية مؤسستنا ضد المخاطر والتهديدات السيبرانية، وباعتبارها جهازا للتوجيه والخبرة من المستوى الاستراتيجي، تحرص هذه المصلحة أساسا على وضع وتطبيق السياسة العامة للدفاع السيبراني في الجيش الوطني الشعبي وأيضا إلى تقييم و تعزيز مستوى أمن الأنظمة المستغلة وكذا إلى تهيئة وتطبيق الإطار التنظيمي المسير لمجال الدفاع السيبراني.
 - على الصعيد العملياتي: تتمثل مهام المصلحة التي تعد طرفا فاعلا في العمليات العسكرية في تعزيز قدراتنا في مجال الدفاع السيبراني، على نحو يسمح بتأمين أنظمة السلاح والإعلام والاتصال .
 - طبقا لتوجيهات القيادة العليا، وباعتبارها هيئة تابعة لوزارة الدفاع تساهم هذه المصلحة مع الهيئات الوطنية المعنية في إعداد ووضع السياسة الوطنية المتعلقة بالدفاع السيبراني، مع ضمان التنسيق مع مختلف الهيئات في مجال تأمين المنشآت الرقمية الحساسة.

2.1.3 الأمن و الدفاع السيبراني للجيش الوطني الشعبي:

تحت تأثير الفضاء الالكتروني أو ما أصبح يعرف بالقوة السيبرانية، دفعت العديد من الدول إلى تبني استراتيجيات في مجال دفاعها السيبراني وتدعيم مراكز قوتها بطريقة تشابه الاستراتيجيات الدفاعية التقليدية، خاصة في ظل توزيع القوة السيبرانية بين عدد من

¹ - بوكبشة محمد ، الأمن و الدفاع السيبراني أولوية قصوى ، مجلة الجيش ، العدد 651 ، أكتوبر 2017.



الفاعلين من غير الدول و بروز التهديدات التي أصبحت تطل أمان و استقرار الدول موازاة مع تغيير منطق الحروب حاليا نحو الاتجاه اللاتماثلي.

شهد القرن الحالي ثورة منفردة في عالم تكنولوجيا الإعلام والاتصال، إلى الحد الذي أعدها بعض الخبراء والمختصين الميدان الخامس للنزاعات، بعد الأرض، البحر، الجو والفضاء، ويعود ذلك إلى درجة الانتشار والتطور السريعين لهذه التقنية، حيث يكاد لا يخلو مجال من مجالات الحياة إلا و ارتكز عليها، وبالخصوص مع ارتباط معظم الخدمات وقواعد البيانات والبنى التحتية والأنظمة المالية و المصرفية بشبكة الانترنت، وكذا اتجاه معظم الدول و الحكومات لتبني نماذج الحكومات الذكية و التحول نحو الخدمات الالكترونية التي قلصت الجهد، الوقت والتكلفة، وساهمت بسرعتها ومرونتها في تلبية الاحتياجات، ولذا فإن الحفاظ على هذا البنى من أي هجمات الكترونية يدخل في صميم الأمن القومي للدول، لأن تعرض أحد هذه الأنظمة لهجوم الكتروني يمكن أن يولد آلاف الضحايا في دقائق معدودة، فمثلا قد يؤدي اختراق نظام المواصلات كأنظمة ملاحاة الطيران والسفن وسكك الحديد إلى تصادمها، وعليه فإن خلق نظام دفاع الكتروني فعال يعمل بمثابة حائط صد للهجمات الالكترونية يعد أمرا حيويا للأمن القومي للدول.

على الرغم من الايجابيات التي حملتها الانترنت والتي جعلت من عصرنا الحالي عصر فضاء الكتروني بامتياز، وأضحى فيه (الانترنت) الإطار العام الحاكم لتفاعلاته كافة ، سواء كانت شخصية أو عامة، عسكرية أو سياسية، اقتصادية أو اجتماعية، إلا أنها جلبت معها العديد من التهديدات والمخاطر والأخطار على الأمن القومي للدول، فإذا كان العدو في عهد الحرب الباردة معروفا وواضحا ، ويمكن تعقبه والتنبؤ بسلوكه، فإن الأمر يختلف تماما في حالة العصر السيبراني، فالعدو ليس بالضرورة دولة، ولا يتقاسم بالضرورة جوارا جغرافيا، كما أن استهداف المناطق و الخدمات الإستراتيجية قد يكلف أقل من الحرب التقليدية، وفي أحيان أخرى قد يكون أكثر تدميرا إذا كان الأمر يتعلق بالسيطرة على البنى التحتية والخدمات اللوجستية، سواء كانت مدنية أو عسكرية.

● طبيعة وأشكال التهديدات السيبرانية :

هناك العديد من أنواع الهجمات السيبرانية، نذكر منها على سبيل المثال لا الحصر:

✓ **تخريب المواقع:** الهجمات التي تشوه صفحات على الانترنت أو تدمرها أو تغير طبيعتها، وهذا النوع من الهجمات عادة ما يرد بسرعة ويكون ضرره محدودا.

✓ **الدعاية السلبية:** رسائل سياسية يمكن نشرها لأي شخص يستخدم الانترنت.

✓ **جمع البيانات:** بمعنى أن المعلومات السرية غير المحفوظة بأمان يمكن اعتراضها والتقاطها، بل وتعديلها، مما يجعل التأمر في هذه الحالة ممكنا.

✓ **تعطيل المعدات العسكرية :** الأنشطة العسكرية التي تستعمل الحواسيب والأقمار الاصطناعية للتنسيق هي في خطر من هذا النوع من الهجمات، حيث يمكن اعتراض الأوامر و الاتصالات أو استبدالها، مما يعرض حياة الجنود للخطر.

✓ **مهاجمة البنى التحتية الحساسة:** شبكات الكهرباء والماء والوقود والاتصالات والمواصلات كلها معرضة لحروب الانترنت، ويمثل هذا التدمير الاقتصادي الأشد وطأة في الحالات القصوى .

ويمكن لهذه الهجمات السيبرانية، أن تستعمل بالموازاة مع أعمال أخرى غير تقنية مثل الاستعلام والاستغلال والتخريب.

نتيجة لهذا التطور التكنولوجي أصبحت الدول في حاجة إلى استراتيجيات جديدة لإدارة أمن الفضاء الالكتروني تنطلق من مبدأ رئيسي هو القابلية للاختراق خاصة أن الفضاء الالكتروني مجال عام لا يعترف بالحدود، وعليه فإن منطلق الأمن "السيبراني" لأي دولة يبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الأمن "السيبراني" والحاجة لإجراءات وطنية وإلى التعاون الدولي، بل ويتعدى ذلك إلى



تطوير مخطط وطني لتحفيز الأمن السيبراني بهدف تقليص مخاطر وأثار التهديدات السيبرانية و كذا المشاركة في الجهود الدولية و الإقليمية لتحفيز الوقاية الوطنية والتحضير والاستجابة للتعاين من الحوادث السيبرانية، فعلى سبيل المثال سنت الولايات المتحدة الأمريكية على مدار السنوات الخمسة الماضية فقط ولوحدها 34 قانونا و 5 أوامر تنفيذية لتحسين الأمن السيبراني. وفقا للمؤشر العالمي للأمن السيبراني GCI في نسخته الثانية الذي أصدرته وكالة الأمم المتحدة للإتصالات في 5 جويلية 2017 ، فإنه لا يزال هناك حاجة إلى بذل المزيد من الجهود في هذا المجال الحرج، خاصة أن الحكومات تعتبر المخاطر الرقمية ذات أولوية عالية، كما أصبح الأمن السيبراني مصدر قلق كبير للدفاع القومي، وأظهرت الدراسة وجود فجوات كبيرة في الأمن السيبراني بين الدول الأكثر قوة في العالم.

يعتمد الأمن السيبراني بناء على توصيات الإتحاد الدولي للاتصالات على مزيج مركب من التحديات التقنية والسياسية، الاجتماعية والثقافية، وحصص المختصون صلاحياته في:

- تطوير إستراتيجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة.
- إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات.
- ردع الجريمة السيبرانية.
- خلق قدرات وطنية لإدارة حوادث الحواسيب الآلية.
- تحفيز ثقافة وطنية للأمن السيبراني.¹

خاتمة

يغطي الدفاع السيبراني باهتمام بالغ من قبل السلطات العليا للبلاد، التي يجب أن تشرك كل الفاعلين المعنيين. فمن الضروري إرساء إطار مناسب يتضمن كل العناصر التنظيمية والقانونية والتقنية يسمح بتبادل المعلومات بين مختلف المؤسسات والهيئات لصالح الدفاع السيبراني. في هذا الخصوص، لا يمكن أن يقتصر العمل على نشاط للتعاون أحادي الجانب، بل يجب أن يندرج ضمن مقاربة شاملة ودائمة تسعى إلى تحقيق التنسيق والتجانس بين مختلف مؤسسات الدولة المعنية . في هذا السياق بادرت وزارة الدفاع الوطني بوضع آلية لتنسيق و تبادل المعلومات المتعلقة بالدفاع السيبراني، وهي محل مشاورات بين مختلف الأطراف المعنية.

الحقيقة أنه في عالم الأمن السيبراني لا يمكن الحديث عن ضمان تأمين مطلق للأنظمة، لأن الأمر يتعلق باتباع مسار للتطوير المستمر للأمن، وعليه فإن كسب رهان الأمن السيبراني يستلزم تحديد مقاربة استباقية وتفاعلية، تهدف إلى تعزيز وتدعيم أمن وسلامة أنظمتنا الأمنية لمواجهة أي تهديد سيبراني محتمل .

ومن هذا المنطلق نحن بصدد تكتيف الجهود لتحقيق الأهداف المرجوة.

في هذا الخصوص، يجب التنويه بالدعم الدائم والمستمر للقيادة العليا للجيش الوطني الشعبي من خلال تسخيرها كل الإمكانيات المادية والبشرية الضرورية لإنجاز هذه المهمة بفعالية ونجاعة ومن ثم التحكم في التكنولوجيا المستعملة في هذا المجال.

قائمة المراجع :

I. النصوص القانونية:

¹ - بوكبشة محمد مرجع سابق، العدد 651 ، أكتوبر 2017.



1. الجريدة الرسمية عدد 37 المؤرخ في 22 يونيو 2016.
2. المادة 37 من قانون الإجراءات الجزائية ، بموجب الأمر 15-02 المؤرخ في 23 يوليو سنة 2015.
3. المادة نص القانون رقم 09-04 ، الجريدة الرسمية، عدد 47 الصادرة في 05 أوت 2009 ، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها .

II. الكتب القانونية:

1. عبد الفتاح مراد ، د.ت.ن ، دور الكمبيوتر في مجال ارتكاب الجرائم الالكترونية بشرح جرائم الكمبيوتر والانترنت، مصر، دار الكتب و الوثائق المصرية.
2. عبد الله أوهائية ، 2018 ، شرح قانون الإجراءات الجزائية ، الجزء الأول ، الجزائر ، دار هومة.
3. محمد عبيد الكعبي ، 2009 ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت ، القاهرة ، دار النهضة العربية، ط2 .
4. ثملة عبد القادر المومني ، الجرائم المعلوماتية ، الأردن ، دار الثقافة للنشر و التوزيع ، ط1.

III. المقالات والمدخلات:

1. بوكبشة محمد ، 2017، الأمن و الدفاع السيبراني أولوية قصوى ، مجلة الجيش ، العدد 651 ، أكتوبر.
2. سمير بارة ، 2017 ، الأمن السيبراني في الجزائر ، السياسات و المؤسسات ، المجلة الجزائرية للأمن الإنساني ، العدد الرابع ، جويلية.
3. سمير بارة ، 2017، الدفاع الوطني و السياسات الوطنية للأمن السيبراني في الجزائر ، الدور و التحديات الملتنقى الدولي حول سياسات الدفاع الوطني ، جامعة قاصدي مرباح ، ورقلة ، كلية الحقوق ، جانفي.
4. سميرة معاشي ، 2010، ماهية الجريمة المعلوماتية ، مجلة المنتدى القانوني ، عدد 7 ، جامعة محمد خيضر ، بسكرة ، أفريل.
5. عزارمي عبد الغني ، 2019، الفريق أحمد قايد صالح يدين المركز الوطني للإشارة ، الحروب المستقبلية هي بالأساس حروب الكترونية، مجلة الجيش ، العدد 676 لشهر نوفمبر.
6. مليكة عطوي ، الجريمة المعلوماتية ، حوليات جامعة الجزائر ، عدد 21 .
7. يوسف بوغرة ، 2018، الأمن السيبراني ، الإستراتيجية الجزائرية للأمن و الدفاع في القضاء السيبراني ، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي ، المجلد الأول ، العدد الثالث ، سبتمبر.
8. يونس عرب، 2002، جرائم الكمبيوتر و الانترنت، إنجاز في المفهوم و النطاق و الخصائص و الصور و القواعد الإجرائية للملاحظة و الإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات و البحوث الجنائية، أبو ظبي.

IV. الرسائل والمذكرات:

1. سعيد علي نعيم ، 2013 ، 2012، آليات البحث و التحري عن الجرائم المعلوماتية في القانون الجزائري ، مذكرة ماستير ، جامعة العقيد الحاد لخضر ، باتنة ، كلية الحقوق.
2. معنوق عبد اللطيف ، 2011 ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن ، مذكرة ماجستير جامعة العقيد الحاد لخضر ، باتنة ، كلية الحقوق .

V. المواقع الإلكترونية:

نواة باشوش ، الجيش يدخل حرب القضاء الالكتروني و مكافحة الجوسسة ، على الموقع التالي :

www.echoronkonlire.com/arar/articles/536554.html تاريخ دخول الموقع 2019/11/25.



الجريمة الإلكترونية وتهديداتها للأمن الاجتماعي في الجزائر

أ/ كمال عمتوت⁽¹⁾

جامعة طاهري محمد - بشار، مخبر الدراسات الاجتماعية والنفسية والأنتروبولوجية - جامعة غليزان،

amttout.kamel@gmail.com

أ.د. عبد العزيز ديلملي⁽²⁾

جامعة حسينة بن بوعلي - الشلف، مخبر المجتمع ومشاكل التنمية المحلية في الجزائر - جامعة الشلف

azizdilmi@gmail.com

مقدمة

يشكل الأمن الاجتماعي هدفاً أساسياً للدول، وقد سعت إلى تحقيقه في جميع المراحل التاريخية التي مرت بها المجتمعات البشرية، من خلال مجموعة من الأنظمة والقوانين التي تم سنّها من أجل الحفاظ على نظام المجتمع وضمان استقرار أفراده، فالأنظمة منذ عصر الحضارة اليونانية والحضارات والمسيحية واليهودية...، وعلى الرغم من الاختلافات الجوهرية بين هذه الحضارات من حيث طبيعة الدين وطرق التفكير، إلا أن نظرهم كانت موحدة في اعتبار ظاهرة الجريمة تهديداً يجب مواجهته بمختلف الأساليب والوسائل.

ومع التقدم العلمي والتكنولوجي الذي عرفته المجتمعات، أصبح تحقيق الأمن المجتمعي أمراً صعباً بسبب التحديات العديدة التي تقف في طريقه، في المجتمع الذي شهد ثورة صناعية كبيرة، وإذا قارنا هذين المجتمعين وطبيعة الأساليب المتبعة في الجريمة بمجتمع المعلومات اليوم، نجد أن الخطر قد تضاعف، حيث أنه لم يعد مرتبطاً بمجتمع معين، أو بمكان وأدوات معينة كما كان الأمر في الحقبة التقليدية، مما يؤكد أن المجتمعات المعاصرة تواجه ثورة معلوماتية نتجت عنها أساليب جريمة جديدة قائمة على التكنولوجيا.

ففي عام 2011، نجد أن ما لا يقل عن (2.3) مليار شخص، أي ما يعادل أكثر من ثلث الإجمالي العالمي للسكان، لديهم إمكانية الوصول إلى الإنترنت. وبحلول عام 2017، يقدر أن اشتراكات الأجهزة المحمولة ستقترب من (70%) من الإجمالي العالمي للمليارات السكان. وبحلول عام (2020)، [قدر حينها] أن عدد الأجهزة المتصلة بالشبكة "إنترنت الأشياء" (The internet of things) يفوق عدد الأشخاص بنسبة ستة إلى واحد، مما يؤدي إلى تغيير المفاهيم الحالية للإنترنت. ففي عالم الغد شديد الاتصال، سيكون من الصعب تخيل "جريمة كمبيوتر"، وربما أية جريمة أخرى لا تنطوي على أدلة إلكترونية مرتبطة باتصال بروتوكول الإنترنت (IP). (United Nations Office on Drugs and Crime in Vienna 2013, 18).

وعليه أصبح تناول الأمن المجتمعي في ظل انتشار جرائم جديدة ضرورة علمية، تتطلب من الباحثين والمتخصصين عرض مشاكله وتشخيص أسبابها وتحديد طبيعتها.

وانطلاقاً من هذا التحدي الخطير جاءت هذه الدراسة لتتناول تهديدات الجرائم الإلكترونية للأمن المجتمعي، من خلال عرض بعض أنواع الجرائم التي مست خصوصية المجتمع، وخصوصية أفراده، وانعكاسات هذا الأمر على الاستقرار الأسري والمجتمعي. وبناء على هذا نطرح الإشكالية التالية: ما هي أهم التهديدات التي تواجه الأمن المجتمعي في ظل انتشار الجرائم الإلكترونية في الجزائر؟

أهداف الدراسة:

تهدف هذه الدراسة إلى رصد العلاقة بين الجريمة الإلكترونية والأمن المجتمعي وأهم التحديات التي تطرحها، كما تسعى إلى الكشف عن أسرار الجريمة الإلكترونية المستحدثة وانتهاكها لخصوصية الأفراد، خاصة في ظل الاستعمال الواسع لمواقع التواصل الاجتماعي والمواقع الإلكترونية، ومن أهدافها أيضاً تقديم الرؤى الجديدة للحفاظ على الأمن المجتمعي في ظل هذا التهديد الخطير الذي يواجهه.



منهج الدراسة:

اعتمدنا في هذه الدراسة المنهج الوصفي، باعتباره يعتمد على توصيف الظواهر وتفسير جميع الظروف التي تحيط بها. ومنه وجدناه مناسبة لطبيعة هذا الموضوع، بحيث عملنا على التعرف على ظاهرة الجريمة الإلكترونية كتحدٍ يواجه الأمن المجتمعي، لأجل وضعها في إطارها الصحيح، من خلال تحديد طبيعتها وأسبابها، وانعكاساتها على الفرد والمجتمع.

1. الجريمة الإلكترونية: المفهوم والمضمون ;

1.1. في مفهوم الجريمة الإلكترونية ;

الجريمة الإلكترونية في ظاهرها العام هي عبارة عن مركب لغوي بين الجريمة والمعلوماتية (الإلكترونية)، التي تعني علوم الحاسوب، بمعنى أنها تلك الجرائم التي تعتمد في ممارستها على هندسة النظم المعلوماتية التي يهتم بنقل المعلومة وتحويلها وتشغيلها، لكن في جزئياتها نجد اختلافا بين العلماء في تعريفاتها، وهذا الأمر «يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، حيث أدت الحداثة التي تتميز بها الجرائم الإلكترونية، واختلاف النظم القانونية والثقافية بين الدول في التعامل معها، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها، وعدم الاتفاق، هذا انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، وذلك خشية حصرها في مجال ضيق». (عسال و عماد 2020، 153).

أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد عرفها على أنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية. والجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية." (الموني 2010، 50) مثل جرائم انتحال شخصية على المواقع، والتهديد والابتزاز الإلكتروني، وجرائم السرقة المصرفية والاستخدام المزور لبطاقات الائتمان وغيرها من الجرائم المعلوماتية التي يمكن أن تمس بأمن الأشخاص وبأموالهم.

ويعرفها الأستاذ عبد الفتاح بيومي الحجازي على مستويين: الفني والقانوني، فالتعريف الفني ينظر إليها من حيث أنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة، كوسيلة أو كهدف لتنفيذ الفعل الإجرامي المقصود. أما التعريف القانوني فيقتضي تصنيف صورها ويتطلب تعريف المفردات المتعلقة بأركان الحاسوب الآلي وهي: الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول، الخدمات، الخدمة الحيوية." (معاشي 2018، 406). وعليه تُبنى الجريمة الإلكترونية على ثلاثة شروط أساسية، من حيث أنها تتطلب استخدامات الحاسب الآلي كوسيلة ضرورية في تحقيق هذا الفعل، كشرط أول، كما تتطلب إلماما جيدا بتقنيات الشبكة الحاسوبية كشرط ثاني، من أجل القدرة على الوصول إلى المعلومات الخاصة، كشرط ثالث لها. ومن جملة المخاطر التي تشكلها هذه الجريمة على أمن المجتمع، أنها لا يمكن معرفة نطاقها، فهي تتعلق بعالم افتراضي لا ترسمه حدود معينة، وربما هذا ما يؤكد افتراضية أن "هذه الجرائم هي صورة صادقة من صور العوامة." (العادي 2006، 08)، التي استطاعت أن تخدر العديد من العقول نتيجة الانكفاء على المواقع الإلكترونية، ووسائل التواصل الاجتماعي كل اليوم. وهي بهذا التأثير بوسعها أن تستقطب حالات عديدة من فئات المجتمع في جعلتها، وتزرع في داخلهم خلايا الإجرام.

وطابعها الافتراضي هذا ساعدها على التحرر من الزمان والمكان فغالبا "ما يرتكب هذه الجريمة في مكان ما يختلف عن المكان الذي تعرضت فيه الضحية للضرر أو مكان حدوث الضرر." (Glenn 2009, 03). وهذا يعد عاملا قويا على تشجيع الإجرام داخل المجتمع، لأن المجرمين لا يجدون صعوبة كبيرة في إنقاذ أنفسهم، وبهذا من العسير الوصول إلى مرتكبيها، ذلك أنهم "يمكنهم بسهولة إخفاء الهوية الحقيقية على الإنترنت." (European Crime Prevention Network 2016, 11) فهي لا تتطلب ارتباطا ماديا بين الجاني والمجني عليه، يكفي فقط عمليات بيانية عن بعد ومن شتى الدول.



كما تزيد صعوبة كشفها إذا تعلق الأمر بمسألة البحث عن أدلة الجريمة من حيث أنها "جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداول البصمات الإلكترونية غير المرئية ولا توجد مستندات ورقية." (إبراهيم 2011، 03). وهذه الخاصية ساعدتها على قابلية التوسع والتكرار، وهنا نستنتج أن كل هذه الميزات وغيرها للجريمة المعلوماتية يعتبر تحديدا واضحا للأمن المجتمعي، وخطر محقق على اختراق الأسس القيمية والثقافية للمجتمع.

2.1. الجريمة الإلكترونية كشكل جديد للجريمة المستحدثة :

يصعب إيجاد تعريف محدد للجرائم المستحدثة نتيجة للطبيعة التي تتميز بها، لذا فتعريفها دائما يقتصر بالجرمة التقليدية من حيث الاختلافات بينهم على مستوى التطبيق والأدوات المستخدمة، لذا أي تعريف لها لا بد له أن يتناول تلك المقارنات بينهما، وفي هذا الميدان فرق المتخصصون بين الجريمة المستحدثة والجريمة التقليدية من حيث أن هذه الأخيرة "تتمثل في تلك الجرائم المتعارف عليها قانونا بالعقاب نتيجة مساسها بالمصلحة." (قدادة 2019، 13) مثل السرقة وجرائم القتل والاختطاف، في حين أن الجرائم المستحدثة هي تلك الجرائم التي ارتبطت بالتطورات التكنولوجية المعاصرة ولا يشملها نص قانوني محدد.

إن هذا النوع من الجرائم يركز على استخدام طرق تقنية حديثة تختصر المسافات والوقت وحتى التكلفة المالية، بشكل دقيق يصعب على الأبحاث الجنائية وأمن الشرطة كشفها نتيجة الانتشار الواسع التي عرفته، خاصة في الآونة الأخيرة مع الثورة الرقمية التي تخللت جميع ميادين الحياة المعاصرة بما فيها الاجتماعية والاقتصادية والسياسية. وهي تتنوع ما بين جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجريمة المعلوماتية، جرائم تبييض الأموال، جرائم الإرهاب، جرائم الصرف وجرائم الفساد.

أما عن خصائص الجريمة المستحدثة فهي تتعدد وتنوع، فإن أهم ميزة يمكن البدء بها هي ارتباطها بالتقنية "فالتسهيلات المختلفة التي ترتبت على تطور الاتصالات بعيدة المدى في كافة المجالات فتحت المجال على مصارعه لارتكاب عدد واسع من الجرائم باستخدام تلك التقنية الحديثة." (اليوسف 2014، 77) مثل الحاسوب والهواتف المحمولة، والشبكة الحاسوبية، وهذا الأمر ساعدها على التحرر من حدود الزمان والمكان، فهي "ترتكب وتمارس في أبنية اجتماعية مختلفة عن الأبنية التي ظهرت فيها وارتبطت بها بادي ذي بدئ." (اليوسف 2014، 77).

وهذا عكس الجرائم التقليدية، التي كانت ترتبط بوسائل مادية معينة، في إطار مكان وزمان محددين. مثل سرقة الأموال، ففي القديم كانت المسألة تتطلب الذهاب إلى بنك معين، وفي زمان معين من أجل السطو عليه، لكن حديثا أصبحت هذه العملية تسيرها مجموعة من الأزرار، فقط عن طريقها يتم اختراق حسابات الأشخاص المالية في المكان غير الذي يتواجد فيه المجرم. وهذا ما أضفى عليها خصوصية التحرر من الحدود الوطنية "بحيث أصبحت الجماعات المتورطة في الجرائم المستحدثة خاصة الجرائم المنظمة والجرائم عابرة الدول، أصبحت جماعات متعددة الجنسيات تقوم بها، الأمر الذي يجعل ضبطها وملاحقتها خارج السلطة السياسية والتشريعية لأية دولة من الدول أمرا صعبا جدا." (اليوسف 2014، 77).

بمعنى أنها دولية، فالجناة قد تجدهم متعددي الجنسيات ومن مختلف البلدان، يتواصلون عن طريق المواقع الإلكترونية من أجل تحقيق مخططاتهم الإجرامية دون أي حاجة إلى لقاءات جسدية، وهذا ما يزيد من خطورة هذه الجريمة من حيث أنه يسهل على الجاني الفرار وعدم ترك أي أثر يدل على جنائته. مما يصعب على القوى الأمنية ملاحقته والقبض عليه، إلا في حالات نادرة بعد بذل مجهود كبير جدا.

ومن بين الميزات الأخرى التي تشترك في هذا النوع من الجرائم "غياب الأبنية القانونية وآليات الضبط الاجتماعي الرسمي الخاصة بمكافحة هذه الجرائم على الصعيدين المحلي والدولي. فالقانون الجنائي والهيئات القائمة على تنفيذه لا يزال يأخذ طابعا إقليميا." (اليوسف 2014، 77)، لان المتابعة التشريعية للجريمة تتطلب الركن المادي والمعنوي الذين من خلالهما تعرف الروابط السببية



لافتعال الجريمة، وتتبع آثار المجرم من خلال البصمات مثلا، لكن الجريمة المستحدثة تفتقد لكل هذه الأركان، مما يسهل على الجناة استغلال هذه الثغرات القانونية لصالحهم، خاصة إذا كانت أساليبهم احترافية متقدمة، وهذا طبعا يكون معيقا أمام إحصائها وضبط نسب انتشارها، مما يقف حائلا أمام اتخاذ التدابير الوقائية تجاهها من طرف الجهات المسؤولة عن حماية امن الدولة والمجتمع، وهذا يساهم في انتشارها وزيادة خطورتها أكثر، فقد تدفع الحكومات إلى دفع تكلفة عالية نتيجة الآثار الناجمة عنها، بالأخص إذا تعلق الأمر بالأمن المجتمعي والجرائم المعلوماتية التي تهدده.

3.1 إحصائيات حول الجريمة الإلكترونية في الجزائر :

إن الانتشار الواسع للوسائل الإلكترونية، وسهولة الوصول إليه من طرف مختلف فئات المجتمع، تسبب في تطور وتنامي عدد الجرائم المرتكبة باستعمال تكنولوجيا الإعلام والاتصال، وذلك ما تمت ملاحظته من خلال عدد القضايا المسجلة على مستوى المصالح المختصة في محاربة الجريمة الإلكترونية التابعة للأمن الوطني.

وفي نفس السياق، وفي إطار العمل الاستباقي الهادف إلى حماية الأنظمة المعلوماتية الوطنية، تمكنت مصالح مكافحة الجرائم الإلكترونية للأمن الوطني من تحقيق إنجازات متتالية وعمليات أمنية نوعية، والتي تعمل في إطار منظومة شرطية متكاملة، للحفاظ على أمن الأفراد ومواجهة كل تهديدات الأمن الاجتماعي ومحاربة كل أشكال الإجرام، وفي حصيلة سنوية سجلتها سنة (2021)، يمكن تسليط الضوء على بعضها من خلال الجدول رقم 01 الموالي:

الجدول رقم (01): الحصيلة السنوية للجريمة الإلكترونية في الجزائر سنة 2021

تصنيف الجرائم		عدد القضايا		نسبة المعالجة	
		2021	2020	2021	2020
المساس بالأشخاص		2146	2816	76.28%	72.15%
المساس بالأنظمة المعلوماتية		371	330	59.83%	53.74%
النصب والاحتيال		500	238	89.40%	89.49%
الإرهاب الإلكتروني		71	51	91.36%	100%
إباحية الأطفال		39	110	89.74%	93.64%
نشر محتويات مخالفة للنظام		994	1366	90.84%	97.50%
بيع سلع محظورة		118	175	90.52%	90.80%

المصدر: (الشرطة الجزائرية جانفي 2022، 19) بالتصرف

2. الأمن الاجتماعي وأسس النظرية :

لأجل التعرف على مفهوم الأمن الاجتماعي كمركب لغوي بين كلمتي الأمن والمجتمع، يتطلب منا معرفة مدلولات مفردة الأمن، في القواميس وفي الدراسات الأمنية. حتى يسهل علينا استنتاج تلك العلاقة التداخلية بين الأمن والمجتمع، والأبعاد المختلفة لها.



1.2 مفهوم الأمن:

الأمن من الكلمات التي يصعب تحديدها نتيجة تنوع مجالاتها، فحسب ما أجمع عليه الباحثون في الدراسات الأمنية والعلاقات الدولية أن مفهوم الأمن "ليس من المفاهيم المتفق عليها بصورة عامة، وأنه من الصعب تقديم تعريف محدد لما تعنيه كلمة الأمن، شأنها في ذلك شأن الكثير من الكلمات المتداولة التي تفتقر إلى تعريف محدد يمكن تقديره بشكل قاطع." (قسوم بلا تاريخ، 17) وعليه سنحاول تناول هذه المفردة على مستوى المفهوم اللغوي، وبعض المفاهيم الاصطلاحية.

المفهوم اللغوي للأمن حسب بن منظور هو "ضد الخوف، والأمن: الأمن ورجل أمانة - بالفتح - الذي يصدق كل ما يسمعه، ولا يكذب بشيء، ورجل أمانة إذا كان يطمئن إلى كل الناس ويثق بهم، واستأمن إليه: دخل في موضع الأمن، والأمن: المستجير ليأمن نفسه، الأمانة والأمانة، نقض الخيانة لأنه يؤدي ذاته." (منظور 1979، 140، 141).

أما على مستوى التعريف الاصطلاحي فإن مفهوم الأمن هو عبارة عن استراتيجيات أمنية تلجأ لها الدولة لتحقيق حماية الفرد وحماية حقوقه، ويعرفه الهيئتي بأنه "مجملة الإجراءات الأمنية التي تتخذ لحفظ أسرار الدولة، وتأمين أفرادها، ومنشأتها، ومصالحها الحيوية، ويعني الطمأنينة والهدوء، والقدرة على مواجهة الأحداث والطوارئ دون اضطراب" (علي التميمي و علي التميمي 2012، 05) وجاء في الموسوعة الفقهية الكويتية أن "الأمن عند فقهاء المسلمين ما به يطمئن الناس على دينهم وأنفسهم وأموالهم وأعراضهم، ويتجه تفكيرهم إلى ما يرفع شأن مجتمعهم وينهض بأمتهم." (علي التميمي و علي التميمي 2012، 05)، ويحاول محمد عمارة تقديم تعريف آخر للأمن بقوله: "الطمأنينة المقابلة للخوف والفرع والروع في عالم الفرد والجماعة، وفي الحواضر ومواطن العمران، وفي السبل والطرق، وفي العلاقات والمعاملات، وفي الدنيا والآخرة جميعا." (عمارة 1998، 11).

وإذا تأملنا في هذه التعريفات نجد أن مفهوم الأمن يرتبط دوما بمعاني الطمأنينة والاستئناس كما ذهب إليه التعريفات اللغوية، وهذا المعنى لا يختلف كثيرا عن المفهوم الاصطلاحي من حيث أن التعريفات فيه تتفق في عمومها على أن الأمن هو الشعور بالطمأنينة على مستوى الفرد والجماعة، من حيث حماية احتياجاتهم المادية والمعنوية وعلاقاتهم الاجتماعية المختلفة. لكن هذا المفهوم يأخذ معنا آخر إضافيا، إذا تعلق الأمر بالأمن القومي وحماية سياسات الدول من أي هجمات مضادة، وعليه فهو يرتبط ارتباطا وثيقا بالإمكانات العسكرية وقوة الردع من أجل الحفاظ على قيم الدولة، إذ يعرفه "والتر ليمبان" بقوله: "إن الأمة تبقى في وضع آمن إلى الحد الذي لا تكون عرضة لخطر التضحية بالقيم الأساسية إذا كانت ترغب في تفادي وقوع حرب، وتبقى قادرة لو تعرضت للتحدي على صون هذه القيم عن طريق انتصارها في حرب كهذه." (جراية 2014، 20).

2.2 مفهوم الأمن الاجتماعي :

يعرفه أسامة السيد في كتابه الأمن الاجتماعي في الإسلام بقوله: "أن يعيش الفرد ويحيا حياة اجتماعية آمنة مطمئنة مستقرة على نفسه وورقه ومكانه الذي يعيش فيه هو ومن يعول." (أسامة السيد بلا تاريخ، 19) محققا في هذا الشأن اكتفاء الذاتي على مستوى الحياة الاقتصادية وما يتخللها من تحقيق الإشباع اليومي، ومحققا أيضا استقراره الشخصي من حيث التحرر من كل خوف، وفي هذا تعمل الدولة على حمايته من الحروب والجرائم.

ولهذا المصطلح عدة رؤى فكرية عبر التاريخ، اهتمت بشروط بناء المجتمعات، وسن القوانين اللازمة لتنظيم العلاقات بين الأفراد وحفظ حقوقهم وضمان استمرارية الدولة، وتطور الحضارات الإنسانية، ذلك أن كل خطوة نحو التقدم في الركب، ترتبط بمدى استتباب أمن مجتمعات هذه الدول ومراعاتها لحقوق الإنسان. قد تختلف هذه الشروط من رؤية لأخرى ومن عصر إلى عصر، ومن حضارة لحضارة أخرى تتحكم فيها الروابط الدينية والثقافية والقيمية، لكن يبقى هدف الأمن هو الذي يوجهها.



ففي المرحلة اليونانية كما مثلتها الفلسفة اليونانية، وفي المحاورة التي كانت تدور بين سقراط وتراسيماخوس حول فضيلة العدل في كتاب الجمهورية لأفلاطون، فكانت النظرة تتفق على أن بناء المجتمعات يحتاج إلى تحقيق هذه الفضيلة بين الأفراد، من أجل تفادي كل تفرقة، ذلك "أن الظلم يخلق الانقسامات والكراهية والفتن، والعدل يوزع التناسب والصدقة." (أفلاطون 1994، 79) وعليه فالظلم حيث ما كان في المدينة أو الدولة أو الجيش أو يورث العصيان، ورغم حاجة المدينة إلى الدولة لحماية الأفراد يفضل العدل هو من يحافظ على النظام العالم واستتباب الأمن فيها.

أما في فترة الفكر الإسلامي فيعتبر ابن خلدون أكبر أمودج في التنظير لبناء المجتمع والدولة من خلال كتاب المقدمة، رأى من خلاله أن استمرارية المجتمعات وتحقيق أمنها يرتبط بشكل وثيق بنظام الدول وقوته، ذلك أن ضرورة الاجتماع البشري تتطلب الحكم والوازع الذي يرجعون إليه، لكن بشرط "أن يكون مستندا إلى شرع منزل من عند الله يوجب انقيادهم إليه إيمانهم بالثواب والعقاب عليه الذي جاء به مبلغه، وتارة إلى سياسة عقلية يوجب انقيادهم إليها ما يتوقعونه من ثواب ذلك الحاكم بعد معرفته بمصالحهم." (ابن خلدون 2002، 278) وعليه فالدول التي تنهار وتقرم، وتفشل في تحقيق أمنها المجتمعي هي التي يخللها الانحلال الخلقي بظلم حكامها وفسادهم وانشغالهم بالملذات فقط، وخلو نظامها من كل عدل.

ومع تيارات الفكر الحديث تطور هذا المفهوم مع جان جاك روسو في كتابه العقد الاجتماعي، يرى فيه أن الأمن المجتمعي يتحقق من خلال اتفاق جماعة على عقد يحوي جملة من القوانين التي تضمن حقوق الأفراد، شرط أن تكون نابعة من إرادة الفرد، من أجل تفادي الفوضى والانحلال الاجتماعي الناجمة عن تضارب المصالح والملكيات الخاصة، فحسب تصوره "أن الناس، إذا كانوا لا يستطيعون إنتاج قوى جديدة، بل توحيد القوى القائمة وتوجيهها، عاد لا يكون لديهم وسائل للبقاء غير تأليفهم بالتكتل." (روسو 2012، 37).

بناء على هذه التصورات يبدو أن الأمن المجتمعي كان هاجس الحضارات الإنسانية منذ القدم، كل منها قدمت تنظيرا بشأنه يتناسب مع واقعها الاجتماعي والاقتصادي والثقافي الذي تعيشه، لكن هذا المفهوم عرف تطورا كبيرا في القرن العشرين، مثلته العديد من المواثيق الدولية التي تدافع عن حقوق الإنسان، وتضمن له حرياته وسلامه، ويعد ميثاق أو إعلان (1948) من أهم المواثيق الدولية التي لها روابط بين حقوق الإنسان والأمن البشري في كل صوره وأشكاله، سواء من حيث "الأمن الذي يتخذ صورة الأمن الشخصي (مثل الحماية من الحبس التعسفي)، والأمن الاجتماعي مثل توفير الاحتياجات الأساسية كتوفير الغذاء، والأمن الدولي (الحق في العيش ظل نظام دولي آمن)." (بينديك و البرغوثي 2014، 25)، ولكن السؤال الذي يطرح في هذا السياق: إلى أي مدى تتحقق هذه المبتغيات في ظل التطورات العلمية المعاصرة، وفي ظل الجرائم الإلكترونية الناتجة عنها.

3. تهديدات الأمن المجتمعي في ظل الجرائم الإلكترونية :

القصد بالتهديدات هي مجموعة المخاطر والتحديات التي تواجه الأمن المجتمعي، وتزعزع استقرار أفراد وجماعاته، على المستوى الاجتماعي والاقتصادي والثقافي والصحي والتعليمي، ومع تطور التكنولوجيا المعاصرة تضاعفت هذه التهديدات، وتنوعت أساليب الجرائم ضد الإنسانية مما انعكس سلبا على أمن المجتمعات، وفي هذا السياق سنتناول البعض منها من أجل تحديد معدل هذه التهديدات على مستقل أمن الأفراد والأسرة والمجتمع ككل.

1.3. اختراق الحسابات الشخصية وتهديدها للكرامة الإنسان :

تعد عملية الاختراق التي تتعرض لها حسابات الأشخاص، وبياناتهم الخاصة، من أهم مظاهر الجريمة الإلكترونية التي تمس بحقوق الإنسان، بحيث يلجأ فيها المجرم الإلكتروني إلى الدخول غير القانوني لهذه الحسابات، وبطرق احترافية، يجمع فيها بين المهارة العالية في استخدام الكمبيوتر، وفهم عميق لأسرار الشبكة العنكبوتية، بهدف انتهاك السرية.



وهذا النوع من الجرائم يدخل في نطاق التصيد الاحتيالي الذي أصبح يعرف انتشارا واسعا بين الدول، فقد "لاحظ روديوناساكين، في دراسته للاستخدام غير القانوني للمعلومات الشخصية في روسيا، النمو السريع للتصيد الاحتيالي منذ عام (2000)، حيث نجح المخادعون في خداع العملاء للكشف عن كلمات المرور وأرقام التعريف الشخصية، وبالتالي تمكين الوصول إلى الحسابات المصرفية وبطاقات الائتمان." (Glenn 2009, 3).

كما "يشير تقرير عام 2008 الصادر عن وكالة إدارة الطوارئ السويدية إلى أن هذا التصيد قد أزعج البنوك السويدية منذ عام 2006." (Glenn 2009, 3).

2.3. انتهاكات في حق الأطفال :

أصبح من السهل جدا الوصول إلى المواد الإباحية والصور الفاحشة، نتيجة الاستخدام السيئ لمواقع التواصل الاجتماعي والإنترنت، فالجناة يستغلون عن طريقها الأطفال والقصر في تحقيق مآربهم، ومحاولو الاعتداء عليهم جنسيا، وأديتهم جسديا ونفسيا. وسبيلهم في هذا القيام بإنتاج "مواد إباحية ثم يتم مشاركتها وبيعها على الإنترنت." (Veli Acar 2016, 111) تكون بدايتها بإقامة علاقة صداقة سواء بالرسائل النصية، أو التواصل الصوتي، مع إتباع أسلوب الإطراء وتقديم الهدايا، وهذا بهدف الاستمالة، لكن بمجرد حصول المعتدي على المواد الجنسية، فإنه يهدده بإساءة استغلالها ما لم يمثل الطفل له". وفي دراسة أجريت سنة (2009)، "على 155 من الجناة كانوا يقدمون شروطاً لاستخدام الأطفال في المواد الإباحية عبر الإنترنت، فاكشفوا أنه على الرغم من أن (26%) من هؤلاء الرجال لديهم سجلات جنائية رسمية تتعلق بالجنس، وجرائم ضد القاصرين، (85%) من هؤلاء الرجال من اعترف بارتكابهم في الواقع جنائية اتصال واحدة على الأقل ضد قاصر أثناء العلاج." (Keith and Ronald N.D, 800).

إلى جانب الابتزاز الجنسي، يستغل الجناة هذه المواقع في عملية الاختطاف من حيث التحضير والتنفيذ، فحسب بعض الإحصائيات في أمريكا في عام (2011) "شملت عمليات الاختطاف (9%) من الأطفال الضحايا." (Finkelhor and J 2016, 11) وهنا "لعبت التكنولوجيا دوراً في الاتصال المسبق بين الجاني والضحية التي أدت إلى الاختطاف، أو استخدام الجاني الأجهزة الإلكترونية، مثل الهواتف المحمولة أو أجهزة الكمبيوتر، للاستغلال الجنسي للضحية المخطوفة." وفي بعض الحالات، يستغل الوالدين هذه الوسائل في استغلال أطفالهم مثلما أثبتت البحوث أن الأم استخدمت "الإنترنت لبيع ابنتها لممارسة الجنس لرجل كان لديه طفل أسير." (Finkelhor and J 2016, 11).

وفي سياق هذا الحديث نجد أن الجرائم الإلكترونية المنتهكة لحقوق الإنسان، تتعدد مظاهرها، وتتنوع أساليبها، فهي لا تتوقف إلى حد الاختراق، والابتزاز والاختطاف، بل تتجاوز إلى الاتجار بالبشر، واستغلال الأطفال في الأعمال الدنيئة.

3.3. تقييد الحقوق الرقمية وتضييق نطاق حرية التعبير :

يطرح الموضوع هنا على مستوى علاقة الجريمة الإلكترونية بالحقوق الرقمية، والحق في حرية الكلام المتعلق بمحتوى الإنترنت، وحقوق التعبير الإلكتروني. فبسبب التوظيف السلبي لمواقع الإنترنت تحول هذا المحتوى إلى شكل من أشكال التحريض الإلكتروني، أو ما يعرف بجريمة الترويح لخطاب الكراهية، ويكون هذا عن طريق نشر العداوة بين الدول والطوائف والأشخاص والسكان، من خلال إرسال رسائل وهمية تحمل في طياتها كل أنواع الشتم والتمييز العنصري والإشاعات، بهدف تفعيل كل آليات الحرب، وهذا الأمر "يتسبب في أعمال عنف تعسفية ضدهم، عن طريق الإهانة أو التحقير بطريقة خبيثة أو تشويه سمعة أجزاء من السكان بطريقة يمكن تعكير صفو السلم العام." (United Nations 2013, 113) ويستخدم الجناة الاختلافات العرقية، والدينية، كأداة أساسية في تشجيع هذا النوع من الخطابات، مثلما يجري اليوم في بعض الدول العربية التي وقعت ضحية هذا الفعل الإجرامي.



4.3. تهديدات الجرائم المنظمة العابرة للحدود الوطنية:

عرفت هذه الجريمة انتشارا واسعا خاصة في القرن الواحد والعشرين، وهي تتميز بالدقة في العمل والتخطيط على أشكال هرمية منظمة كل قسم له عمل خاص به، ومن التعاريف المتداولة في تحديد تعريف ليندا سميث إذ تعرفها على أنها "جريمة مهنية تشمل نطاق من العلاقات المحددة بالتزامات وميزات متبادلة." (زين 2017، 11) وفي تعريف آخر هي "ارتباط لجماعة صغيرة من المجرمين لتنفيذ أنماط معينة من الجريمة." (زين 2017، 11) أما التعريف القانوني فيعتبرها "ممارسة جماعة منظمة لنشاط إجرامي بقصد تحقيق كسب مال." (زين 2017، 11، 12).

الواضح من هذه التعريفات أن الجريمة المنظمة هي عبارة عن سلوك إجرامي تنظمه جماعة معينة، تتميز بالقوة والتنظيم والاحترافية، هدفها تحقيق الربح المالي السريع، بالاعتماد على جملة من الوسائل الممكنة، و تختلف تسمياتها في الاستخدام اللغوي، بحيث "يستخدم الباحثون مصطلحات متباعدة للإشارة إلى الإجرام المنظم فوجد مصطلح الجريمة المنظمة (CrimeOrganized) كما نجد مصطلح الجريمة الاحترافية (Professional Crime) والجريمة المتقنة (Sophisticated Crime) وأيضا الجريمة المخططة (Planned Crime)." (زين 2017، 11).

أما من حيث خطورة هذه الجريمة فهي واسعة الانتشار، وتتميز بالقوة الكبيرة، خاصة أنها لا تعترف بالحدود الوطنية، فهي ترتكب في العديد من الدول ويمتد تأثيرها حتى إلى الدول المجاورة، كما أنها تستقطب في بنيتها العديد الأشخاص، وهذا ما يهدد مستقل الأفراد خاصة الشباب الذين يستهويهم الربح المالي السريع، وتحقيق الذات والنفوذ. والأخطر من هذا أنها "أصبحت اليوم تشكل جزءا من الثقافة الإجرامية لشعوب الأرض قاطبة. فكما أصبح تبادل الثقافات المجتمعية سمة عصرية للقرية الكونية، فإن تبادل الثقافات الإجرامية يشكل من هذا النقل الثقافي العصري خطرا محققا." (أديبة 2009، 65).

ومن المخاطر الكبيرة لهذه الجريمة أنها تهدد تماسك المجتمع، وتهدد أمنه الاقتصادي، بسبب الأساليب الاحترافية التي تستخدمها في سرقة المال العام، والاعتداء على الممتلكات الخاصة، والقتل والتفكيك، فهي بهذه الطرق تستهدف "عناصر التماسك الاجتماعي فيه، وتفتت النسيج الاجتماعي من خلال أنشطتها الإجرامية مثل الاتجار بالمخدرات، وتكوينها قيما خاصة معاكسة لقيم المجتمع وأخلاقياته." (أديبة 2009، 65)، مما يتسبب في التقاعس عن العمل النبيل، والتوجه إلى الربح السريع الذي تفتح أبوابه التجارة بالمخدرات، والتجارة بالبشر، وتبييض الأموال وغسلها... إلخ بشكل خيالي، وهذا بدوره يؤثر على الحالة الاقتصادية للمجتمع والدولة. كما أنها ستكون محفزا كبيرا لنمو الخلايا الإرهابية وهذا خطر كبير يواجه الأمن المجتمعي.

خاتمة

يمكن القول في خاتمة هذه الدراسة أن التحول من الأسلوب التقليدي للعملية الإجرامية الذي كان يفتقر إلى المعلوماتية والمنهجيات العلمية الدقيقة مقارنة بالأسلوب الإلكتروني المعاصر، الذي أصبح هاجسا يُطرح بشكل قوي على مستوى البحث العلمي المتخصص، نظرا للتحديات التي بات يعيشها العالم اليوم.

ومن هذا المنطلق، وبناء على هذه التحليلات للجريمة الإلكترونية وتهديداتها للأمن المجتمعي في الجزائر بمختلف أبعاده، بما فيها الأمن الصحي، والاقتصادي، والأسري، والشخصي، يمكننا أن نلتم ببعض النتائج على النحو الآتي:

1. الجريمة الإلكترونية خطر كبير يهدد مستقبل المجتمعات الإنسانية، وهي سبب من أسباب التخلف التي تعاني منها بعض الدول، نتيجة الاستنزاف الكبير لثرواتها الثقافية والفكرية والمادية لعجزها عن مكافحة هذا النوع من الجرائم.

2. الخصائص التي تتميز بها الجرائم الإلكترونية، يجعل منها جرائم مستعصية يصعب مكافحتها، إلا بتكاتف مجتمعي ودولي.



3. الأمن الاجتماعي ضرورة حضارية، بما تبنى الأمم وتستمر، وكان ومازال من أكبر الاهتمامات التي أولتها الدول في وقتنا الحاضر، وعليه لا يمكن الحديث عن تطور دولة، إلا بالحفاظ عن هذا البعد، وحمايته من كل الأخطار المحدقة به.

4. في إطار البحث في تهديدات أنواع الجرائم الإلكترونية للأمن المجتمعي، يبدو واضحا أن هذه الجرائم تستهدف بنية المجتمع، وتعمل على تعطيل نظامه، وهدم قيمه، وتخريب عقول أفراد، وبالتالي فتخريب المجتمعات في زمن العالم الافتراضي أصبح من الأمر السهل والخطير.

5. الجرائم الإلكترونية لا تستهدف الأمن المجتمعي فقط، بل تعتدي على الكرامة الإنسانية، وتسقط من مكانته التي خلق لأجلها. فهي تعبير عن اللاإنسانية، بكل أشكالها وصورها، خاصة إذا تم الحديث عن الإرهاب الكيميائي والبيولوجي والإشعاعي والنووي.

6. الجرائم الإلكترونية تتسبب في أذية الإنسان، وانتهاك حقوقه على جميع النواحي، الأخلاقية والسياسية والاقتصادية والاجتماعية والثقافية.

عطفا على هذه النتائج يمكن اقتراح بعض التوصيات نحمل أهما فيما يلي:

1. مكافحة الجرائم بكافة أنواعها المستحدثة وغير المستحدثة مسؤولية الجميع، من الفرد إلى الأسرة إلى المجتمع إلى الدولة، كل له دوره في إصلاح نفسه، وإصلاح أسرته وإصلاح مجتمعه.
2. يبدو واضحا أن التهميش سبب رئيسي في الدخول في عالم الجريمة، وعليه يكون على عاتق الدولة ضرورة التكفل بالفئات التي تعاني من القهر النفسي والاجتماعي، خاصة تلك التي تعاني من متاعب مادية.
3. كما تقع المسؤولية على عاتق الوالدين، في قدرتها على غرس القيم الأخلاقية في نفوس أولادهم، ويبدأ هذا بالتربية بالقُدوة، ومراقبتهم بطريقة ذكية أثناء اتصالهم بعالم الإنترنت، ووسائل التواصل الاجتماعي.
4. انتشار الجرائم في المجتمعات المتطورة التي حققت إشباعها المادي، دليل واضح على أن هذه الجرائم تتمكن من النفوس التي تعاني من فراغ روحي، وبالتالي فتتمة الجانب المعنوي والرضا الداخلي آلية فعالة في مكافحة السلوكيات الإجرامية.

قائمة المراجع:

أولا: المراجع باللغة العربية

1. ابن منظور. (1979). *لسان العرب*. القاهرة: دار المعارف.
2. أفلاطون. (1994). *الجمهورية*. (شوقي داود ترمز، المحرر) بيروت: الاهلية للنشر والتوزيع.
3. بينيديك، البرغوثي. (2014). *فهم حقوق الإنسان: دليل تعليم حقوق الإنسان*. المركز الأوروبي للتدريب والأبحاث في مجال حقوق الإنسان ومركز رام الله لدراسة حقوق الإنسان.
4. جان جاك روسو. (2012). *العقد الاجتماعي*. (عادل زعيتر، المترجمون) القاهرة: مؤسسة هنداوي للتعليم والقراءة.
5. خالد ممدوح إبراهيم. (2011). *حوكة الانترنت*. الاسكندرية: دار الفكر الجامعي.
6. رضا عسال، وعبد الرزاق عماد. (2020). *الجريمة الإلكترونية والجرائم الإلكترونية: مقارنة مفاهيمية*. مجلة بيبليوفيليا لدراسة المكتبات والمعلومات، العدد 05.
7. سالم قسوم. *الاتجاهات الدولية الجديدة في الدراسات الامنية: دراسة في تطور مفهوم الامن في العلاقات الدولية*. مركز الإمارات للدراسات والبحوث الاستراتيجية.
8. سميرة معاشي. (2018). *الجريمة المعلوماتية: دراسة تحليلية لمفهوم الجريمة المعلوماتية*. دار الفكر.



9. الشرطة الجزائرية. (2022) **حصار الشرطة الجزائرية 2021**. مجلة الشرطة الجزائرية، العدد 150.
10. شوقي قدارة. (2019). **أهم الجرائم المستجدة والمستحدثة وآليات مواجهتها**. مجلة المجتمع والرياضة، المجلد 02 العدد 01.
11. الصادق جاية. (2014). **تحول مفهوم الأمن في ظل التهديدات الدولية الجديدة**. مجلة العلوم القانونية والسياسية، ص 17 - 31.
12. طارق زين. (2017). **الجريمة المنظمة العابرة للحدود الوطنية: التعاون الدولي وسبل المكافحة**. بيروت: المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية.
13. عبد الرحمن بن محمد ابن خلدون. (2002). **مقدمة ابن خلدون**. (درويش الجويدي، المحرر) بيروت: المكتبة العصرية.
14. عبد السميع أسامة السيد. **الأمن الاجتماعي في الإسلام ومقارنته بما ورد في اليهودية والمسيحية**. مصر: دار الجامعة الجديدة.
15. عبد الله عبد العزيز اليوسف. (2014). **أساليب تطوير البرامج والمناهج التدريبي لمواجهة الجرائم المستحدثة**. الأردن: دار حامد للنشر والتوزيع.
16. عماد محمد رضا علي التميمي، و إيمان محمد رضا علي التميمي. (2012). **الأمن الاجتماعي: ضبط المصطلح وتاصيله الشرعي. الأمن الاجتماعي في التصور الاسلامي**. كلية الشريعة جامعة آل البيت.
17. محمد صالح أديبة. (2009). **الجريمة المنظمة: دراسة قانونية مقارنة**. مركز كردستان للدراسات الاستراتيجية.
18. محمد عمارة. (1998). **الإسلام والأمن الاجتماعي**. بيروت: دار الشروق.
19. محمود صالح العادلي. (2006). **الجرائم المعلوماتية، ماهيتها وصورها**. ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية. مسقط.
20. نخلا عبد القادر المومني. (2010). **الجريمة المعلوماتية**. عمان: دار الثقافة.

ثانيا: المراجع باللغة الأجنبية

21. European Crime Prevention Network. (2016). **Cybercrime : A theoretical overview of the growing digital threat**. Brussel.
22. Finkelhor, D., & J, A. (2016). Child, Victims of Stereotypical Kidnappings. **Justice Bulletin**, 11.
23. Glenn, C. (2009). **Cybercrime: An Annotated Bibliography**. Library of Congress – Federal Research Division.
24. Keith, F., & Ronald, L. (N.D). **Internet Crimes against Children**.
25. United Nations. (2013). **Étude détaillée sur la Cybercriminalité**. New York.
26. United Nations Office on Drugs and Crime. (2013). **Comprehensive Study on Cybercrime**. New York: UN Documents.
27. Veli Acar, K. (2016). Sexual Extortion of Children in Cyberspace. **Internationnal journal of Cyber Criminology**, 10(02), p. 111.



دوافع وأسباب ارتكاب الجريمة الإلكترونية في المجتمع الجزائري

سهيلة بن دادة

جامعة باجي مختار عنابة

مقدمة

يشهد العالم تنامي في وسائل التواصل الاجتماعي والتكنولوجيا الحديثة مما أدى إلى إنتقال الفرد من العيش في العالم الواقعي إلى العالم الافتراضي حيث أصبحت كل المعاملات تتم من خلال وسائل التواصل الاجتماعي والانترنت، مما أدى إلى تصعيد وتيرة الجرائم وانتقالها إلى العالم الافتراضي أين أصبح يطلق عليها إسم الجرائم الإلكترونية أين أصبح المجرم يقوم بجرمه بسهولة والتأثير على ضحيته والتحكم فيها عن بعد مع صعوبة إمساكه وإثبات الأدلة على جرمه.

والجزائر مثلها مثل باقي الدول ومحاوله منها لمواكبة عصر التكنولوجيا الحديثة أدى إلى إنتشار وسائل التكنولوجيا الحديثة بين مختلف أفراد المجتمع، وبالرغم من الإيجابيات الكثيرة التي تقدمها للفرد وللمجتمع بصفة عامة إلا أن لها سلبيات خطيرة على الفرد وعلى المجتمع، فمن أجل السيطرة عليها ومحاوله لكبحها قبل تفشيها في المجتمع لابد من معرفة أسباب ودوافع إنتشار الجرائم الإلكترونية في المجتمع الجزائري.

أولاً: الجانب التمهيدي

1. الإشكالية:

مع الانتشار الواسع لوسائل التواصل الاجتماعي والانترنت في مختلف نواحي الحياة اليومية فإن البعض أساء إستخدام الحاسوب لتنفيذ الجرائم مستعملا هذه الوسائل الحديثة لتنفيذ أغراضه الإجرامية، حيث تعتبر الجرائم الإلكترونية من الظواهر الإجرامية التي تفرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر الناجمة عنها، وذلك بإعتبارها من الجرائم الذكية التي تنشأ أو تحدث في بيئة إلكترونية، يفترضها أشخاص من ذوي القدرات التقنية والفنية، حيث أصبحت تهدد المجتمعات ككل نظرا لانتشارها الواسع في مختلف مناطق العالم.

ومن خلال هذه الدراسة أردت التعرف على دوافع وأسباب إرتكاب الجرائم الإلكترونية في المجتمع الجزائري، وذلك من خلال طرحي للتساؤل العام المتمثل فيما يلي:

- ما هي دوافع وأسباب إرتكاب الجرائم الإلكترونية في المجتمع الجزائري؟.

2. الفرضيات:

تتجسد فرضيات هذه الدراسة فيما يلي:

- توجد عوامل فردية تساهم في إرتكاب الجرائم الإلكترونية في المجتمع الجزائري.
- توجد عوامل إجتماعية تساهم في إرتكاب الجرائم الإلكترونية في المجتمع الجزائري.

3. أهداف الدراسة:

هدفت هذه الدراسة إلى:

- التعرف على الجرائم الإلكترونية في المجتمع الجزائري وخصائصها.
- التعرف على دوافع وأسباب الجرائم الإلكترونية في المجتمع الجزائري.



4. أهمية الدراسة:

تكمن أهمية الدراسة في أنها تهتم بالجرائم الإلكترونية التي تعتبر من الظواهر الإجرامية التي فرضتها ظروف الحياة الجديدة والمتسارعة وأنه ليس من السهل معالجتها.

5. حدود الدراسة:

يقتصر البحث على دراسة دوافع وأسباب ارتكاب الجرائم الإلكترونية في المجتمع الجزائري، على عينة من الأفراد قدر عددهم بـ 30 فرد.

6. مصطلحات الدراسة:

-الدوافع والأسباب:

ونعني بها ما هي مختلف الأسباب والعوامل التي تساهم في ارتكاب الجرائم الإلكترونية في المجتمع الجزائري.

-الجريمة:

ونعني بها ذلك الفعل الذي يقع بالمخالفة لقانون العقوبات¹.

-الجريمة الإلكترونية:

هي كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على أي مصلحة مشروعة، سواء أكانت مادية أو معنوية².

ثانيا: الإطار النظري:

1. تعريف الجريمة:

ورد في مختار الصحاح للرازي أبو بكر في الجزء الأول أن الجرم والجريمة يعني الذنب ومنه جرم أجرم وإجترم³. فالجريمة ما هي إلا تعبير عن انعدام شعور التضامن الاجتماعي لدى الفرد والذي يفسره عدم تزويد الفرد بالقيم والقواعد والمعايير الاجتماعية اللازمة لصيانة وحماية الجماعة والتي تتمخض عنها فكرة التضامن الاجتماعي⁴.

أما الجريمة من المنظور النفسي عبارة عن "فعل إجرامي للتعبير عن الصراعات النفسية والإضطرابات في قوى الشخصية يؤدي إلى عدم تكيفها مع النظم السائدة في المجتمع"⁵.

أما من الناحية القانونية فهي كل فعل أو امتناع صادر عن شخص مميز يحدث خرقا أو اضطرابا اجتماعيا عاما أو خاصا ويعاقب عليه القانون بعقوبة جزائية أو تدابير احترازية⁶.

2. الجريمة في عصر العولمة:

يمثل مفهوم العولمة أحد المفاهيم الحديثة في الدراسات الاجتماعية ويتمثل مغزاه الحقيقي في مجال دراسات الجريمة والانحراف في أن كثير من صور الجريمة والمشكلات الانحرافية المعاصرة لم يعد من الملائم دراستها في سياق الدولة الواحدة بل أصبح من الضروري دراستها في سياق العمليات الدولية والعالمية.

وما يمكن قوله عن انعكاس العولمة على أشكال الجريمة ما يلي:

- أن الجرائم التقليدية أصبحت أكثر خطورة من خلال استعانة المجرمين بالتقنيات الحديثة والاستفادة من ثورة المعلومات كأحد أبرز إيجابيات ظاهرة العولمة.

- ظهور أشكال جديدة ومستحدثة من الجرائم من بينها الجرائم المعلوماتية أو جرائم الأنترنت.



- توسيع نطاق الجرائم واتخاذها بعدا دوليا واضحا⁷.

3. تعريف الجريمة الإلكترونية :

فيما يتعلق بتعريف الجريمة الإلكترونية فإنه لا يوجد إجماع على تعريف محدد، وأمام قصور التعريفات على معيار محدد سواء القائمة على معيار قانوني موضوعي أو شخصي برز عدد من التعريفات تركز على أكثر من معيار لبيان ماهية جريمة الكمبيوتر، من هذه التعريفات ما يقرره الأستاذ John Carrol ويتبناه الأستاذ Gion Green: "أنها أي عمل ليس له في القانون أو أعراف قطاع الأعمال جزاء، يضر بالأشخاص أو الأموال، ويوجه ضد أو يستخدم التقنية المتقدمة العالية لنظم المعلومات"⁸.

كما أن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين، فقد تبني التعريف التالي للجريمة الإلكترونية بأنها "الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي"⁹.

كما إصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب أحكام المادة 02 من قانون 04-09 المؤرخ في 05-08-2009 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"¹⁰. وهناك البعض من حاول المزاوجة بين هذه التعريفات فقال: "إن الجريمة المعلوماتية هي فعل ضار يستخدم الفاعل، الذي يفترض أن لديه معرفة بتقنية الحاسوب، نظاما حاسوبيا أو شبكة حاسوبية للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة"¹¹.

4. ظهور الجريمة الإلكترونية وتطورها التاريخي¹²:

يمكن تقسيم مراحل ظهور الجريمة الإلكترونية وتطورها التاريخي إلى ستة مراحل وتتمثل فيما يلي:

1.4. المرحلة الأولى: مرحلة الأربعينيات.

فهي مرحلة بداية صناعة الحواسيب وانطلاق ثورة الإلكترونيات مستقلة عن وسائل الاتصال، حيث اقتصر استخدام الحواسيب على المؤسسة العسكرية وفي مجالات ضيقة لدى المؤسسات الكبرى التابعة للدولة.

2.4. المرحلة الثانية: مرحلة الخمسينيات: ويمكن تقسيمها إلى مرحلتين:

1.2.4. مرحلة بدايات الخمسينيات:

ذكر يونس عرب (2002) في: "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية" أنه في البداية وبعد اختراع الحاسب الآلي بدأ الاستخدام التجاري للحواسيب دون تصور في الأذهان للخطر الناجم عن استخدامها وإن وجد فلم يتعلق بالإجرام بل أرجع إلى البطالة.

2.2.4. مرحلة نهاية الخمسينيات:

ذكر نائل عبد الرحمن صالح (2004) في كتابه: "واقع جرائم الحاسب في التشريع الأردني" أن ظاهرة "جرائم الحاسوب" بدأت بالظهور نهاية الخمسينيات من القرن العشرين، ولكن ضمن إطار مفهوم "إساءة استخدام الحاسوب" المؤسس على البعد الأخلاقي. وكان الخطر الناجم عن العبث في الحواسيب محدودا في ذلك الوقت لقلّة استخدام الحاسوب، حيث ذكر يونس عرب (2002) في المرجع السابق ذكره أن أول جريمة إرتكبت بواسطة الحاسوب الآلي عام 1958 وبدا رصد ونشر ما تتوافر بشأنه تقارير من حالات إساءة استخدام الحاسوب في أمريكا حيث صُنفت إلى جرائم العبث أو التخريب الموجه إلى الحاسوب، سرقة المعلومات أو الممتلكات، الإحتيال أو الغش المالي.

3.4. المرحلة الثالثة: مرحلة الستينيات:



تعد مرحلة الستينات مرحلة شيوع استخدام الكمبيوتر، وبدأ بروز مفهوم إساءة استخدام الكمبيوتر والعبث بالبيانات إلى مفهوم جريمة السير التي لا تحدها حدود، حيث ظهرت أول معالجات لجرائم الكمبيوتر كالمقالات والمواد الصحفية التي تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والإستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر وثار الجدل والتساؤل إن كانت مجرد سلوكيات غير أخلاقية أم هي جرائم بالمعنى القانوني.

4.4. المرحلة الرابعة: مرحلة السبعينيات:

في هذه المرحلة تزايد استخدام الكمبيوتر، فظهرت الدراسات المسحية والقانونية التي إهتمت بجرائم الكمبيوتر لتعالج العديد من الجرائم الفعلية وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة. حيث ذكر يونس عرب (2002) انه تم رصد 1600 حالة إساءة استخدام الحاسوب حدثت منذ 1958 وتم تقديم إستبيان من قبل معهد ستانفورد للتحضير لمناقشة مشروع قانون الجريمة الاقتصادية، أما معهد علم الإجرام وقانون العقوبات الإقتصادي في ألمانيا الإتحادية قام بتقديم دراسة تضمنت وصفا لـ 31 جريمة إرتكبت بواسطة الحاسوب.

5.4. المرحلة الخامسة: مرحلة الثمانينيات:

وفيها ظهر مفهوم جديد لجرائم الكمبيوتر متعلقا بعمليات إقتحام نظم الكمبيوتر عن بعد، والفيروسات الإلكترونية والتي تقوم بعملية قرصنة الملفات أو البرامج، وشاع الهاكرز وبدأت عملية تحديد سمات مرتكبي جرائم الحاسب الآلي والانترنت وظهر مصطلح "المجرم المعلوماتي".

6.4. المرحلة السادسة: مرحلة التسعينيات:

أين شهدت هذه المرحلة تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وأحدثت شبكة الانترنت تسهيلات لعمليات دخول الأنظمة وإقتحام شبكات المعلومات، فأصبحت تضم ملايين المستخدمين في كافة المدن حول العالم وشكلت بيئة متكاملة للإستثمار والعمل والإنتاج والإعلام والحصول على المعلومات. وفي الفترة الأخيرة بدأت مجتمعاتنا العربية بالتأثر بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام عبر هذه التقنية التي من الممكن أن يكون خطرها المحتمل في البيئة العربية كبيرا بإعتبار أن الجاهزية التقنية والتشريعية والأدائية لمواجهتها ليست بالمستوى المطلوب إن لم تكن غائبة تماما.

5. طبيعة الجريمة الإلكترونية وخصائصها¹³:

تتميز الجريمة الإلكترونية بخصائص وصفات تميزها عن غيرها من أنواع الجرائم الأخرى، فأول ما يلفت النظر في الجريمة الإلكترونية هو نعومتها وبعدها عن العنف، فحسب كامل فريد السالك (2000) فهي لا تحتاج إلا للمسكات أزرار، كما تمتاز بإمكانية تنفيذها بسرعة، وإمكانية إرتكابها عن بعد وصعوبة إثباتها¹³.

كما أدرج محمود أحمد عبابنة (2004) في كتابه: "جرائم الحاسوب وأبعادها الدولية" أن هذه الجرائم عابرة للحدود بفضل ما أتاحتها وما تتيحه تكنولوجيا الإتصال الحديثة والحاسب الآلي، كما أنها تتطلب وجود حاسب آلي كوسيلة لتنفيذ الجرائم والمعرفة بتقنية إستخدامه.

كما يضيف مفتاح بوبكر المطردي (2012) أن مرتكب الجريمة الإلكترونية - في الغالب - يكون متكيفا اجتماعيا وقادرا ماديا، باعته من ارتكاب جرمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي، في حين أن مرتكب الجريمة التقليدية - غالبا - ما يكون غير متكيف اجتماعيا وباعته من ارتكابه الجريمة هو النفع المادي السريع¹⁴.

6. دوافع إرتكاب الجرائم الإلكترونية وأسبابها:



يمكن تصنيف أسباب ارتكاب الجريمة الإلكترونية حسب مستويين:

1.6. المستوى الفردي¹⁵:

1.1.6. إثبات التفوق العلمي:

وأغلبيتهم من الصبية والشباب المعروفون بصغار نوايغ المعلوماتية فهم يسعون دائما إلى إكتشاف ما هو جديد ومحاولة التعامل مع البرامج الجديدة غير عابثين بما يمكن أن يحدث من مشاكل أو كوارث.

2.1.6. حب الإستطلاع والشغف بالإلكترونيات:

فالشخص المجرم المعلوماتي يتسم بالنشاط والمخاطرة والذهن المنفذ الذي يسعى إلى خداع الآلة.

3.1.6. السعي إلى تحقيق الربح:

فحسب ما جاء به محمود أحمد عابنة(2004) فإن القطاع المالي يعد من أكثر القطاعات إستهدافا من قبل مجرمي الحاسب.

4.1.6. يعتبر دافع التسلية والدعابة:

من الدوافع التي تجعل الشخص يقوم بتصرفات ينتج عنها نتائج تبلغ درجة الجريمة.

5.1.6. المؤثرات الشخصية:

التي تتمثل في إغراءات مالية أو غير ذلك.

6.1.6. حب المغامرة والإثارة:

فهؤلاء المجرمون مغامرون ويتميزون بصفة الإقدام على المخاطر.

7.1.6. شعورهم بالنقص والدونية:

مما يدفعهم إلى محاولة إثبات ذاتهم بإظهار تفوقهم في مجالات أخرى تعويضا عن العجز الذي يملكهم.

8.1.6. دافع الإنتقام:

والذي يعتبر من أخطر الدوافع لأنه غالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة أو الشخص.

2.6. المستوى المجتمعي¹⁶:

1.2.6. التحضر:

حيث أن الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبرى، يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية وكنيجة يجدون أنفسهم في تنافس غير قادرين على مجاراته مما يجعلهم يلتفتون إلى الإستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال وهي مربحة.

2.2.6. البطالة:

ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الإقتصادية الصعبة، فالشباب الذين يملكون المعرفة يستثمرون ذلك في النشاط الإجرامي الإلكتروني.

3.2.6. الضغوط العامة:

تولد هذه الضغوط العامة الصعبة مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الجريمة الإلكترونية.

4.2.6. البحث عن الثراء:



فحسب نظرية الانومي لميرتون فالرغبة في الثراء يواجهها صعوبات بالغة في تحقيقه بالطرق المقبولة إجتماعيا والقانونية، ولذا يلجأ بعض الناس على الجرائم الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.

5.2.6. ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية:

فهناك الكثير من الدول التي لم تطور من تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها.

ثانيا: الإطار التطبيقي

1. المنهج المعتمد:

إنطلاقا من طبيعة الدراسة والبيانات المراد الحصول عليها لمعرفة دوافع وأسباب الجرائم الإلكترونية في المجتمع الجزائري، فقد إعتمدت الدراسة على المنهج الوصفي الذي يعتمد على دراسة الظاهرة كما توجد في الواقع ويقوم بوصفها وصفا دقيقا ويوضح خصائصها عن طريق جمع المعلومات وتحليلها وتفسيرها، ومن ثم تقديم النتائج في ضوءها.

2. عينة الدراسة:

تمثلت عينة الدراسة في 30 فردا تتراوح أعمارهم ما بين 25 و 40 سنة، حيث تم إختيارهم بطريقة العينة العشوائية البسيطة.

3. أداة الدراسة:

تكونت أداة الدراسة من إستبانة تحتوي 9 عبارات تتضمن موضوع الدراسة المتمثل في البحث عن دوافع وأسباب إرتكاب الجرائم الإلكترونية في المجتمع الجزائري.

4. الأساليب الإحصائية المستخدمة في الدراسة:

يعتبر الإحصاء عنصر أساسي في البحث العلمي حيث يستخدم لتحليل النتائج ومعرفة مدى تجمعها وتشتتها وإرتباطها ليصل الباحث إلى العوامل المؤثرة في الظاهرة، وقد إعتمدت الباحثة في تحليل نتائج البيانات المتحصل عليها في هذه الدراسة على التكرارات والنسب المئوية.

5. عرض وتحليل النتائج:

1.5. النتائج المتعلقة بالفرضية الأولى:

"توجد عوامل فردية تساهم في إرتكاب الجرائم الإلكترونية في المجتمع الجزائري".

العبارة رقم 1:

جدول رقم 1: يوضح مدى تأثير إثبات التفوق العلمي في إرتكاب الجرائم الإلكترونية في المجتمع الجزائري:

إثبات التفوق العلمي	التكرار	النسبة
نعم	25	83
لا	05	17
المجموع	30	100

المصدر : الباحثة.



من خلال ما يوضحه الجدول أعلاه نلاحظ أن نسبة 83% من أفراد العينة أكدوا على أن عامل إثبات التفوق العلمي له دور في إرتكاب الجرائم الإلكترونية، وهذا إن دل على شيء فإنه يدل على أن المجرم المعلوماتي يتصف بدرجة عالية من الذكاء العملي في استخدام وسائل التكنولوجيا والقدرة على التحكم بها وتوظيفها لتحقيق أغراضه الإجرامية.

العبارة رقم 2:

جدول رقم 2: يوضح مدى تأثير حب الإستطلاع والشغف بالإلكترونيات في إرتكاب الجرائم الإلكترونية في المجتمع الجزائري.

حب الإستطلاع والشغف بالإلكترونيات	التكرار	النسبة
نعم	27	90
لا	3	10
المجموع	30	100

المصدر : الباحثة.

من خلال الجدول يتضح لدينا أن نسبة 90% من أفراد العينة أكدوا على أن حب الإستطلاع والشغف بالإلكترونيات يدفع بالأفراد إلى إرتكاب الجرائم الإلكترونية، وهذا يشير إلى أن عامل حب الإستطلاع يساهم في إرتكاب الجرائم الإلكترونية وذلك رغبة لإرضاء شغفه.

العبارة رقم 3:

جدول رقم 3: يوضح مدى تأثير السعي إلى تحقيق الربح في إرتكاب الجرائم الإلكترونية في المجتمع الجزائري.

السعي إلى تحقيق الربح	التكرار	النسبة
نعم	18	60
لا	12	40
المجموع	30	100

المصدر : الباحثة.

من خلال الجدول المبين أعلاه نلاحظ أن إستجابات أفراد العينة المؤيدة لفكرة أن السعي من أجل تحقيق الربح له دور كبير في إرتكاب الجرائم الإلكترونية في المجتمع الجزائري بنسبة قدرت بـ: 60% مقارنة بـ: 40% من أفراد العينة، فمن خلال الجرائم الإلكترونية يستطيع الفرد تحقيق أرباح مادية دون أن يبذل جهد بدني.

العبارة رقم 4:

جدول رقم 4: يوضح أن عامل الشعور بالدونية وتحقير الذات يساهم في إرتكاب الجرائم الإلكترونية في المجتمع الجزائري.



النسبة	التكرار	شعورهم بالدونية وتحقير الذات
50	15	نعم
50	15	لا
100	30	المجموع

المصدر : الباحثة.

من خلال الجدول نلاحظ أن 50% من أفراد العينة مع فكرة أن الشعور بالدونية وتحقير الذات يساهم في ارتكاب الفرد للجرائم الإلكترونية، والفرد الذي يشعر بعدم تقدير ذاته يجعله يسلك سلوك عدائي تجاه الآخرين رغبة منه تحقيق ذاته بإيذاء الآخرين فيلجأ إلى ارتكاب الجرائم الإلكترونية باعتبارها جرائم سهلة الحدوث ويصعب إمساكه وأنها لا تكون أدلة كافية على إدانته.

العبارة رقم 5:

جدول رقم 5: يوضح مدى تأثير عامل دافع الإنتقام في ارتكاب الجرائم الإلكترونية في المجتمع الجزائري.

النسبة	التكرار	دافع الإنتقام
70	21	نعم
30	9	لا
100	30	المجموع

المصدر : الباحثة.

من خلال الجدول الموضح أعلاه نلاحظ أن لعامل دافع الإنتقام دور كبير في ارتكاب الجرائم الإلكترونية حيث أكد أفراد العينة ذلك بنسبة قدرت بـ: 70% من الإجابات الكلية، وهذا يدل على أن كل فرد لديه رغبة في الإنتقام فإنه يلجأ إلى ارتكاب الجرائم الإلكترونية لسهولة ارتكابها مقارنة بباقي الجرائم.

العبارة رقم 6:

جدول رقم 6: يوضح مدى تأثير حب المغامرة والإثارة في ارتكاب الجرائم الإلكترونية في المجتمع الجزائري.



حب المغامرة والإثارة	التكرار	النسبة
نعم	22	73
لا	8	27
المجموع	30	100

المصدر : الباحثة.

من خلال الجدول المبين أعلاه نلاحظ أن: 73 % من أفراد العينة أكدوا على أن حب المغامرة والإثارة يساهم في ارتكاب الجرائم الإلكترونية في المجتمع الجزائري، حيث ما يمكن ملاحظته أن أغلب المجرمين الإلكترونيين نجدهم صغارا في السن مقارنة بباقي الجرائم الأخرى، وذلك نظرا لمواكبتهم عصر التكنولوجيا منذ نعومة أظافرهم، حيث يكتسبون مهارات تمكنهم من استخدام وسائل التكنولوجيا والأنترنت بذكاء، وما يميز هذه الفئة من المجتمع هو حب المغامرة والإثارة فبعضهم يقومون بالجرائم الإلكترونية من أجل التسلية.

2.5. النتائج المتعلقة بالفرضية الثانية:

"توجد عوامل إجتماعية تساهم في ارتكاب الجرائم الإلكترونية في المجتمع الجزائري"

العبارة رقم 7:

جدول رقم 7: يوضح مدى تأثير التحضر في ارتكاب الجرائم الإلكترونية في المجتمع الجزائري.

التحضر والعيش في المدن	التكرار	النسبة
نعم	20	67
لا	10	33
المجموع	30	100

المصدر : الباحثة.

من خلال عرضنا لنتائج الجدول المبين أعلاه لاحظنا أن 67% من أفراد العينة أرجعوا سبب تفشي ظاهرة الجرائم الإلكترونية إلى التحضر والعيش في المدن وما تتطلبه من إمكانيات وقدرات وإستعدادات وإمتميازات للعيش فيها والبحث عن مكانة بين الأقران، عكس الريف الذي يتميز بالهدوء وقلة هذا النوع من الانحرافات إلا في بعض الحالات الشاذة.

العبارة رقم 8:

جدول رقم 8: يوضح مدى تأثير البطالة في ارتكاب الجرائم الإلكترونية في المجتمع الجزائري.



البطالة	التكرار	النسبة
نعم	23	80
لا	7	20
المجموع	30	100

المصدر : الباحثة.

من خلال ما يوضح الجدول أعلاه نلاحظ أن 80% من أفراد العينة أكدوا أن من بين أسباب تفشي ظاهرة الجرائم الإلكترونية في المجتمع الجزائري هو إنتشار البطالة، و20% من أفراد العينة أكدوا أنه ليس بالضرورة ففي بعض الحالات نجذ الشخص يقوم بالجرائم الإلكترونية وهو ذو مستوى معيشي جيد وليس بحاجة للمال إنما فقط من أجل المتعة ولفت الإنتباه بين أقرانه.

العبارة رقم 9:

جدول رقم 9: يوضح مدى تأثير ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية في ارتكاب الجرائم الإلكترونية في المجتمع الجزائري.

ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية	التكرار	النسبة
نعم	24	80
لا	6	20
المجموع	30	100

المصدر : الباحثة.

من خلال الجدول الموضح أعلاه نلاحظ أن نسبة 80% من أفراد العينة أكدوا أن ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية سبب أساسي في تفشي ظاهرة الجرائم الإلكترونية في المجتمع الجزائري، فعندما تغيب القوانين التي تسير مثل هذه الجرائم وتتحكم في إنتشارها فإنه يساهم في تفشيها في المجتمع مما يصعب التحكم فيها مستقبلا.

1. الإستنتاج العام:

أظهرت نتائج البحث أن دوافع وأسباب ارتكاب الجرائم الإلكترونية في المجتمع الجزائري يمكن إرجاعها لعدة عوامل فردية وأخرى إجتماعية.

فالعوامل الفردية متمثلة في حب الإستطلاع والشغف للإلكترونيات، فمعظم الشباب وبحكم مواكبتهم لعصر العولمة وإستخدامه لوسائل التكنولوجيا الحديثة منذ نعومة أظافرهم خلق لديهم شعور بحب الإستطلاع على كل ما هو جديد وإستخداماته، إلا أن بعضهم يستغلون الأمر في تنفيذ جرائم إلكترونية.

كما يمكن إرجاع أسباب ارتكاب الجرائم الإلكترونية إلى إثبات التفوق العلمي، فالشخص الذي تكون لديه قدرات عالية من الذكاء وإستخدام أجهزة التكنولوجيا الحديثة، ورغبة منه لإثبات ذاته وقدراته فيقوم بجرائم إلكترونية.



بالإضافة إلى دافع الإنتقام حيث يسعى الكثيرون للإنتقام من بعض الناس من خلال ارتكابهم جرائم إلكترونية سواء إختراق حسابهم أو إبتزازهم وتهديدتهم.

كما يلجؤون لإرتكاب الجرائم الإلكترونية بغرض التسلية، حيث يلجأ الكثير من الشباب الطائش لإبتزاز الآخرين أو تهديدهم أو إختراق أجهزتهم من باب المزاح والتسلية مع الغير.

بالإضافة إلى السعي لتحقيق الربح والبحث عن الثراء، حيث ترى النظرية العامة للجريمة ل"جتفردسون وهيرشي(1990) أن الإنسان يسعى إلى المتعة ويتجنب الألم، في حين ترجعه نظرية الأنومي لميرتون أن الإنسان يسعى إلى الوسائل غير المقبولة إجتماعيا لتحقيق أهداف مقبولة إجتماعيا، فالشخص الذي يرغب في الثراء تواجهه صعوبات بالغة لتحقيق هدفه بطرق مقبولة إجتماعيا وقانونيا، لذا يلجأ بعض الناس إلى الجرائم الإلكترونية لتحقيق هدفه حيث سهولة التنفيذ وسرعة المردود وقلة الخطورة.

أما العوامل الإجتماعية فيمكن إرجاع أسباب الجرائم الإلكترونية إلى:

عامل البطالة فالجريمة الإلكترونية ترتبط شأنها شأن الجريمة التقليدية بالبطالة، والظروف الإقتصادية الصعبة، ونجد أكثر الفئات يعانون من البطالة هم فئة الشباب، فهم يملكون المعرفة خاصة وأنهم واکبوا عصر العولمة وتطور وسائل التكنولوجيا الحديثة وإستخدامها مما يجعلهم يستثمرون ذلك في النشاط الإجرامي الإلكتروني.

والتحضر يعد أحد أسباب الجريمة الإلكترونية عامة، حيث أن الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة، يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية، مما يجعلهم يعيشون في المدن والأحياء الطرفية، وكنتيجة يجدون أنفسهم غير قادرين على مجاراة، مما يجعلهم يلتفتون إلى الإستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير وهو مربح، حيث يرى ميك(2012) أن التحضر سبب رئيسي للجرائم الإلكترونية وأن التحضر بدون جريمة مستحيل.

كما يمكن إرجاع أسباب إرتكاب الجرائم الإلكترونية إلى مختلف الضغوط العامة التي يمر بها الفرد، حيث ترجعها نظرية الضغوط العامة إلى دافع ناجم عن قوى البناء الإجتماعي أو إستجاباته النفس الإجتماعية للحوادث والظروف التي تعمل كضغوط، فهي كفيلة بسلوكه سلوكا إجراميا معتمدا على التقنيات الحديثة لإرتكاب الجريمة بعيدا عن الشبهات خاصة وأنها تتميز بأنها عابرة للحدود ويصعب إمساك المجرم وإدانته.

كما يمكن إرجاع أسباب الجرائم الإلكترونية إلى ضعف إنفاذ القانون وتطبيقه في الجرائم الإلكترونية، فهناك الكثير من الدول والجزائر من بينها التي لم تطور في تشريعاتها وأجهزة العدالة لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها، بالإضافة إلى ضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية.

خاتمة:

هدفت هذه الدراسة لمعرفة دوافع وأسباب إرتكاب الجرائم الإلكترونية في المجتمع الجزائري، حيث طبقت الدراسة على عينة من الأفراد قدر عددهم 30 فرد، وتم الإعتماد على المنهج الوصفي المناسب لهذه الدراسة، وما تم إستخلاصه بأن الجرائم الإلكترونية من الظواهر الإجرامية الخطيرة والحديثة التي تتماشى من التطور التكنولوجي الحديث لوسائل التواصل الإجتماعي وإنتشار إستخدام الأنترنت في المجتمع الجزائري سواء كان الفرد صغيرا أو كبيرا، ومن خصائصها أنها عابرة للحدود وأنه يصعب التحقيق فيها وإدانة الجاني، ومن الأسباب والدوافع التي تدفع بالفرد إلى إرتكاب مثل هذه الجرائم هو حبه للإستطلاع والشغف للإلكترونيات، ورغبة منه لإثبات ذاته وتفوقه العلمي، وكما يلجأ إليها من أجل الإنتقام والسعي لتحقيق أرباح مادية أو معنوية دون أن يبذل جهد بدني، بالإضافة إلى عوامل إجتماعية تساهم في إرتكاب هذه الجرائم نذكر منها البطالة والفرد الذي يفقد مهنة يثبت ذاته من خلالها فيلجأ إلى



الجرائم الإلكترونية رغبة منه في ملأ وقته، بالإضافة إلى العيش في المدن والتحضر يساهم في تفشي مثل هذه الجرائم رغبة في الكسب السريع سواء ماديا أو معنويا، بالإضافة إلى مختلف الضغوط التي يعاني منها الفرد قد تدفع به إلى ارتكاب الجرائم الإلكترونية.

الهوامش:

1. عدلي السمري، طلعت لطفي، أمال عبد الحميد، عائدة عبد الفتاح، محمد محمود الجوهري(2014). علم إجتماع الجريمة والانحراف، ط2، عمان-الأردن-: دار المسيرة للنشر والتوزيع والطباعة، ص16.
2. مفتاح بوبكر المطردي(2012). الجريمة الإلكترونية والتغلب على تحدياتها، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا(النقض، التمييز، التعقيب) في الدول العربية المنعقد في 23-25/09/2012 بجمهورية السودان، ص13.
3. منصور رحامي(2006). علم الإجرام والسياسة الجنائية، عنابة-الجزائر-: دار العلوم للنشر والتوزيع، ص10.
4. عدلي السمري، المرجع السابق ذكره، ص18.
5. منال محمد عباس(2016). الانحراف والجريمة في عالم متغير، الإسكندرية-مصر-: دار المعرفة الجامعية، ص33.
7. محمد عبد حسين أبو سمرة(2010). علم النفس الجنائي، ط1، عمان-الأردن-: دار الراية للنشر والتوزيع، ط1، ص51.
8. منال محمد عباس، المرجس السابق ذكره.
9. يونس عرب(2006). صور الجرائم الإلكترونية وإتجاهات تبويبها، ورشة عمل بعنوان: تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية"، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان الأردن في 2-4 أبريل 2006.
10. مليكة عطوي(2012). الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد21.
11. قانون 04-09 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد47، لسنة 2009.
12. كامل فريد السالك(2000). الجريمة المعلوماتية، ضمن محاضرة ألقيت في مؤتمر للجمعية السورية للمعلوماتية بعنوان ندوة التنمية و مجتمع المعلوماتية في حلب 21-23 تشرين الأول عام 2000.
13. علي جبار الحسيناوي(2009). جرائم الحاسوب والأنترنت، عمان-الأردن-: دار اليازوري العلمية للنشر والتوزيع، ص9-18.
14. كامل فريد السالك، المرجع السابق ذكره.
15. مفتاح بوبكر المطردي، المرجع السابق ذكره، ص17.
16. منال محمد عباس، المرجع السابق ذكره، ص169-173.
17. ذياب موسى البدانية(2014). الجرائم الإلكترونية: المفهوم والأسباب، ورقة علمية ضمن الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من 2 إلى غاية 4 سبتمبر 2014، كلية العلوم الإستراتيجية، عمان، المملكة الأردنية الهاشمية، ص ص 14-15.



تحديات الأمن السيبراني في مكافحة الجرائم السيبرانية في المجتمع الجزائري

ط.د. عبد القادر صواق

جامعة غرداية

د. قريني كمال

جامعة معسكر

مقدمة :

لقد أدت الثورة الكبيرة التي يشهدها العالم حديثا في مجال تكنولوجيا المعلومات والاتصال إلى تزايد وتنوع التطبيقات والخدمات الالكترونية التي تعتمد على فضاء يدعى الفضاء السيبراني الذي جعل العالم مسرحا وقرية صغيرة يتواصل فيها الجميع عن بعد، وهذا التطور السريع في حياتنا اليومية أدى إلى الاعتماد المتزايد على الأنظمة المعلوماتية والأجهزة المتصلة بالشبكة العالمية للإنترنت من أجهزة هواتف نقالة وأجهزة محمولة شخصية وأخرى ثابتة، الأمر الذي زاد من عدد المتصلين بالفضاء السيبراني، ورفع من احتمالات التعرض للجرم السيبراني .

حيث بينت التجارب العالمية أن هذا الفضاء يتعرض باستمرار وتزايد للجرائم السيبرانية، والجزائر من بين الدول التي ليست بمنأى عن تلك الجرائم، مما جعلت من بين أولوياتها في حماية أمن مجتمعتها ومؤسساتها "الأمن السيبراني"، وهو ما يدفعنا للبحث عن مختلف التحديات التي تواجه الجزائر في مكافحة الجرائم السيبرانية في هذا المجال.

وإنطلاقا من هذا الطرح يُطرح الإشكال المعرفي التالي :

فيما تتجلى أهم تحديات الأمن السيبراني في مكافحة الجرائم السيبرانية في المجتمع الجزائري ؟
وتندرج تحت هذه الإشكالية الرئيسية، أسئلة فرعية تتمثل في الآتي :

1. هل هناك نمو متزايد لنسبة الجرائم السيبرانية في المجتمع الجزائري ؟

2. فيما يتمثل أهم تحدي يواجه الجزائر لمجابهة مختلف مخاطر الجرائم السيبرانية ؟

3. ما هو أهم عنصر لبناء الإستراتيجية السيبرانية الوطنية في الجزائر ؟

فرضيات البحث :

- الفرضية الأولى: يشهد المجتمع الجزائري وتيرة متصاعدة لنسبة الإجرام السيبراني .
- الفرضية الثانية: يعتبر تعزيز الوعي الاجتماعي بمخاطر الفضاء السيبراني أهم تحدي يواجه الجزائر لمجابهة مختلف الجرائم السيبرانية.
- الفرضية الثالثة: بناء الإستراتيجية السيبرانية الوطنية في الجزائر يتطلب تظافر جهود جميع الأطراف للحفاظ على الأمن القومي وتوفير بيئة مناسبة من خلال تعزيز آليات للتعاون وتقليل المخاطر.

أهداف البحث :

تهدف الدراسة من خلال الإجابة عن تساؤلات مشكلة الدراسة إلى ما يلي:

- إثراء المعرفة العلمية في مجال الأمن السيبراني .
- التعرف على التطور السريع لنسبة الإجرام السيبراني في الجزائر .



- تسليط الضوء أهم التحديات التي تواجه الجزائر لمجابهة مختلف مخاطر الجرائم السيبرانية .
- إقتراح حلول ميدانية لردع الجريمة السيبراني وإطار عمل للأمان السيبراني لخفض المخاطر .

أهمية البحث:

يكتسي الموضوع أهمية بالغة نظرا لما يلي :

- أهمية الأمن السيبراني في الوقت الراهن، حيث يمثل أهم عامل لبناء مجتمع رقمي قوي ومتين خاصة وأن العديد من المعاملات والخدمات والاتصالات أضحت إلكترونية .
- أهمية موضوع الجرائم السيبرانية التي أضحت تهدد الأفراد والمؤسسات والدول
- جاءت هذه الدراسة بمثابة دعوة إلى إقتراح حلول ميدانية لردع الجريمة السيبراني وإيجاد إطار عمل للأمان السيبراني لخفض المخاطر .

منهجية البحث :

من أجل الإجابة على التساؤلات المطروحة وبغية إختبار الفرضيات إعتدنا في البحث على المنهج الوصفي الذي يتناسب مع موضوع الدراسة، حيث أنه في بعض أجزاء البحث قمنا بتكوين القاعدة النظرية المستقاة من مختلف المراجع مع محاولة الوصول إلى تحليل وتفسير واقعي، ولهذا الأسلوب الوصفي يعتبر مناسبا لتقرير الحقائق والتعريف بمختلف المفاهيم ذات الصلة بالموضوع.

1. مفهوم الأمن السيبراني :

يعد مصطلح الأمن من المفاهيم القديمة بإعتبار عودة أصوله إلى إمتداد تاريخي عميق، حيث إتضحت معالم أصوله الفلسفية عند اليونان، فأصل كلمة "Securita" في اللاتينية هو مرادف لغياب العناية، ف "Sine" معناها "بلا" و "Cura" تعني "عناية"¹ (مراد، 2014، ص 2).

الأمن في الجانب اللغوي هو نقيض الخوف أي بمعنى السلامة وكلمة "الأمن" لغة مصدر الفعل أمن وأمانا وأمنة ، أي إطمئنان النفس وسكون القلب وزوال الخوف، ويقال : أمن من الشر أي سلم منه² (قسوم، 2010، ص ص 17-18)، وقد وردت كلمة الأمن في مواضع كثيرة في القرآن الكريم أبرزها قوله تعالى : "الذي أطعمهم من جوع وآمنهم من خوف" قريش³ (سورة قريش، الآية 4)

أما بالنسبة لمصطلح الأمن السيبراني "Cyber Security" فهو واحد من المصطلحات التي تعرف تعددا في التعريفات المقدمة له، فمصطلح سيبير "Cyber" هو لفظ يوناني الأصل، مشتق من كلمة "Kybernetes" ، بمعناها القيادة أو التحكم، مصدرها "Cybernetics" يعني: "علم الإتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية"⁴ (Lehto et al, 2015, p. 8).

1.1. تعريف المشرع الجزائري للأمن السيبراني :

عرّف المشرع الجزائري الأمن السيبراني على أنه: "مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن إستخدامها في حماية الإتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسريّة البيانات المخزنة أو المعالجة أو المرسلة"⁵ (الجريدة الرسمية، العدد 27، ص 7).



2.1. خصائص الجريمة والجرم السيبراني :

تم تعريف الجرائم السيبرانية على أنها " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشرة أو غير مباشرة باستخدام شبكات الاتصالات مثل الإنترنت، غرف الدردشة، البريد الإلكتروني، والموبايل "6 (البيداني، 2014، ص 3) .

والبعض الآخر عرفها على أنها " نشاط إجرامي تستخدم تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود "7 (القرعان، 2017، ص 19).

وتتميز الجريمة السيبرانية عن غيرها من الجرائم التقليدية بـ :

1.2.1. جرائم عابرة للحدود : هي جرائم غير مقيدة بزمان ومكان لإرتباط العالم بشبكة واحدة، وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق والمحاكمة، وذلك تبعا لتعقيد الإجراءات التي تحكمها الإتفاقيات والعلاقات الدولية والتنازع فيما بينهما على أي القانون الواجب التطبيق .

2.2.1. جرائم صعبة الإثبات : وتكمن صعوبة إثباتها إلى أن متابعتها وإكتشافها عن طريق الصدفة، ومن الصعوبة حصرها في مكان معين، حيث أنها لا تترك أثرا واضحا للعيان، أو تشاهد بالعين المجردة، فما هي إلا أرقام تدور في السجلات والمواقع الالكترونية، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها لعدة أسباب :

- إنها كجريمة لا تترك أثرا بعد ارتكابها .
- صعوبة الإحتفاظ الفني بآثارها إن وجدت .
- سرعة التنفيذ حيث لا تتطلب الوقت الكثير وبضغطة واحدة يمكن ان تنتقل ملايين الدولارات من مكان لآخر وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ او استخدام معدات وبرامج معينة .
- تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها .
- تعتمد على الخداع في ارتكابها والتضبيب في التعريف على مرتكبيها .
- تعتمد على مستوى من الذكاء المرتفع في ارتكابها .

3.2.1. جرائم ناعمة : هي جرائم لا تمارس بالعنف، سهولة الإرتكاب وبعيدة عن أعين الرقابة الأمنية ولا تحتاج الى أدنى جهد عضلي عكس الجرائم التقليدية، فالجرم السيبراني يتميز بمهارات عالية، يعتمد على قدراته العقلية بالذكاء والدهاء ومعرفة الطرق السيبرانية لإتلاف البرامج وإختراق الحواجز الأمنية، ولعل الدافع لارتكاب الجرائم قد يكون بدافع المال أو غير المال مثل الدافع الشخصي للانتقام او التجسس وانتهاك الخصوصية و بدافع سياسي أو عقائدي⁸ (التميمي، 2016، ص 16).

أما بالنسبة للمجرم السيبراني فقد لا يكون هناك نموذج محدد له، وإنما هناك سمات مشتركة بين هؤلاء المجرمين ويمكن إجمالها فيما يلي :

- **مجرم متخصص :** له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته في إختراق الشبكات وكسر كلمات المرور أو الشفرات، ويسبح في عالم الشبكات ليحصل على كل غال وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسيب من خلال الشبكات .



- **مجرم محتزف :** له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الإختراق والسرقة والنصب والإعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال أو بدون مال.
 - **مجرم ذكي :** حيث يمتلك ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب .
 - **مجرم يعود للإجرام :** يتميز المجرم السيبراني بأنه يعود للجريمة دائما، فهو لا يحقق الجريمة بهدف الإيذاء فقط وإنما نتيجة شعوره بقدرته ومهاراته في الإختراق.
 - **مجرم ذو مكانة :** المجرمون السيبرانيون في الغالب يتميزون بأنهم أفراد ذوي مكانة في المجتمع من أصحاب الوظائف الحيوية سواء في القطاع العام أو القطاع الخاص، وقد أطلق عليهم مصطلح ذوي اليرقات البيضاء⁹.
- (قطب، دراسة قانونية عن الجرائم الالكترونية الممارسة ضد المرأة على صفحات الانترنت وكيفية محاربتها، <http://policemc.gov.bh/mcms-store/pdf/.com> تم الاطلاع يوم : 13-12-2022).
- 3.1. تطور الإجرام السيبراني في الجزائر وفق الإحصائيات والأرقام :



جدول رقم : 01 يوضح عدد القضايا الخاصة بالجرائم السيبرانية المسجلة في الجزائر 10 :

السنة	عدد القضايا المعالجة بالأمن الوطني	عدد القضايا المعالجة بالدرك الوطني	طبيعة القضايا
2009	29	18	صرائم المساس بأنظمة المعالجة الآلية
2014	211	102	للمعطيات كالاختراق، الحجب،
2015	409	240	التعطيل، التخريب، جرائم المساس بالنظام العام والاداب العامة، جرائم الاعتداء على البيانات والمؤسسات الاقتصادية، السرقات، الابتزاز، النصب والاحتيال، المساس بالحياة الخاصة، التهديد، اهانة هيئة نظامية، الارهاب المعلوماتي، الاستغلال الجنسي، القذف... الخ

المصدر: (عز الدين، 2015، ص30).

4.1. نسبة القضايا الخاصة بالإجرام السيبراني المسجلة بمصالح الأمن الوطني والدرك الوطني لسنة 2020 كانت كما يلي:

حذرت المصالح الأمنية من ارتفاع الجرائم الإلكترونية في الجزائر، بعد أن قفزت الجريمة من العالم الحقيقي إلى الافتراضي العابر للحدود نظرا لسرعة تنفيذها، حيث سجلت مصالح الدرك والشرطة ما يقارب 8 آلاف جريمة سيبرانية خلال 2020، مما جعلها تنافس الجريمة التقليدية.

حيث صرح وزير العدل عبد الرشيد طيبي على هامش اليوم الدراسي حول “دور التشريع والفقه والاجتهاد القضائي في تطوير القانون” المنعقد في قاعة المحاضرات بمجلس الدولة، “أن الإجهاد القضائي هو منبع للقانون فالقضاة عادة ما يستأنسون بالآراء الفقهية في المسائل الشائكة التي تعرض عليهم”.

كما صرح أيضا أنه : “حدث تعديل لقانون الإجراءات الجزائية، حيث تم إنشاء القطب الوطني المتخصص في محاربة الجريمة الإلكترونية وتشديد العقوبات على بعض الجرائم السيبرانية”، مؤكدا أنه لن يتم المساس بالمنشورات الفردية وكبح حريات المواطن، بل المنشورات التي تروج أخبارا مغلوطة وكاذبة من شأنها المساس بأمن الدولة والمجتمع، مبينا أن “الجرائم الإلكترونية أصبحت أكثر خطرا من الجرائم التقليدية، كونها إنتقلت من التهديد والتشهير والإبتزاز للأشخاص إلى المساس بأمن الدولة الجزائرية، وعليه، فإن التصدي لمثل هذه الهجمات من خلال التحضير الجيد لها من طرف جميع المصالح المعنية أصبح أمرا ضروريا، ولكن مع تحديد الآليات والمهام والصلاحيات لكل الأطراف”.



وكان رئيس الجمهورية عبد المجيد تبون، قد ثمن إنشاء القطب المتخصص في الجرائم السيبرانية، كمكسب لقطاع العدالة على غرار القطب الجزائري المتخصص في مكافحة الجرائم المالية والاقتصادية، مع التشديد على الإسراع في تنصيب القطب الجديد ومعالجة الجرائم السيبرانية المعروضة حاليا، أمام العدالة.

وفي ذات السياق، أكدت المصالح الأمنية من ارتفاع الجرائم الإلكترونية في الجزائر، فالمديرية العامة للأمن الوطني سجلت إرتفاعا قياسيا، أي من 500 جريمة سنة 2015، إلى 5200 قضية خاصة بالجرائم السيبرانية سنة 2020، في حين سجلت قيادة الدرك الوطني 1362 جريمة سيبرانية تورط فيها 1028 شخص خلال سنة 2020. وبينت عملية تحليل المعطيات للجرائم المسجلة أن القذف والسب عبر الفضاء الافتراضي إحتل الصدارة بنسبة تفوق 55 بالمائة، تليها الجرائم ضد الأمن العمومي، ثم الأفعال الماسة بالحياة الخاصة وإفشاء الأسرار، وأخيرا الإبتزاز والنصب والاحتيال والإستغلال الجنسي والأفعال المخالفة للآداب العامة وقضايا مشاهمة¹¹. (باشوش، 2021، الفقرة 5).

2. أهم التحديات التي تواجه الجزائر لمجابهة مختلف مخاطر الجرائم السيبرانية :

1.2 ضرورة إتخاذ تدابير وإجراءات الحماية :

إضافة الى التحديات التقليدية التي طرحها دخول تقنيات المعلومات والاتصالات منذ بداياته على الآليات التقليدية للعمل والتحرك داخل المجتمع، كفواعد إقراره وتوقيت إصداره وحدود تطبيقه، تبرز تحديات جديدة تستدعي حركة خاصة، يمكن أن تطل تحديت نماذج وآليات العمل.

فلتقنية المعلومات والاتصالات حركة سريعة ونبض دائم التغيير، وللفضاء السيبراني سمة عالمية وطبيعة عالية التقنية، الأمر الذي لا يتناسب مع حركة القانون البطيئة ولا مع الإطار السيادي الذي يبنى على أساسه. من هنا لا بد للقانونيين من الرد على تحديات ليس أقلها ربما إيجاد نماذج تشريعية جديدة وآليات عمل وهيئات قادرة على التعامل مع متطلبات السلامة والأمن. وفي القريب العاجل قواعد جديدة للتعامل مع مسائل الحوسبة السحابية والخدمات التي تقدمها شركات خارجية وأجنبية غريبة عن المؤسسات والإدارات صاحبة الأنظمة المعلوماتية في القطاعين العام والخاص.

في هذا السياق، تطرح مسائل عديدة منها :

- إعادة النظر في آليات إصدار التشريع وإقراره .
- الهيئات المخولة إقتراح وإصدار القوانين والأنظمة .
- برامج إعداد وتأهيل السلطات المعنية بالمكافحة والتحقيق .
- إستحداث إدارات خاصة تعالج المواضيع الإجرائية والإدارية الخاصة بقطاع المعلومات والاتصالات ومعالجة المعلومات، ويمكن إيراد بعض الأفكار في هذا المجال، مثل:

- التحول نحو إقرار القواعد التي تحكم تقنيات الإتصالات والمعلومات عبر مراسيم عوض عن القوانين، وذلك لكونها أكثر قربا من الواقع العملي ولا تتطلب وقتا طويلا لوضعها موضع التنفيذ.
- إيجاد هيئات تشريعية منتخبة ذات صلاحيات مماثلة لصلاحيات المجالس النيابية تلتزم التشريع في مجال الإتصالات والمعلومات، وعلى أن تراعى التداخلات التي يمكن أن تطرأ مع القوانين المرعية الإجراء. فالتقنية التي إقتحمت جميع مجالات النشاط الإنساني تحولت إلى قطاع تجاري وخدمي هي الأخرى، ولا بد لتنظيمها والقواعد القانونية الخاصة بها أن تتأثر بالقطاعات



التي دخلتها. ونورد على سبيل المثال: ما يفرض من إجراءات ومواصفات على البرامج المعلوماتية الخاصة بالأسواق المالية، بحيث تضمن الشفافية والاطلاع على المعلومات ومصادقيتها كما القوة الثبوتية للتقارير الصادرة عنها.

- تشكيل هيئات متخصصة من المجالس النيابية تتابع بشكل خاص عمليات التشريع والتنظيم في مجال الأمن السيبراني ولكن شرط أن تلتزم آلية عمل تؤمن سرعة إقرار القوانين وتحديثها في الوقت المناسب.
- خلق أصول إجرائية خاصة بالتبليغ والإنذار عن الاختراقات وتسرب المعلومات .

في الوقت عينه، سيكون القضاء مدعوا للإجابة عن مسائل تقليدية وتطبيق قواعد كلاسيكية معروفة على الأوضاع الجديدة، كتحديد صاحب المصلحة في الإدعاء في حالات تسرب البيانات يعطي الشخص حقا في اللجوء إلى القضاء. وما هي إمكانية الإدعاء على الجهة التي تسربت البيانات من أنظمتها في حال عدم وجود رابطة عقدية، وهل يمكن عندها أن تتم الملاحقة بسبب التخلف عن اعتماد معايير الحماية الضرورية. كذلك هل يمكن اعتبار عدم الالتزام بمعايير الحماية خرقا لقانون حماية المستهلك ومستخدم الشبكة، الى ما هنالك من مسائل خاصة بالضرر، الذي يمكن على أساسه المطالبة بتعويض، وكيفية تحديد هذا التعويض¹² (جبور، 2012، ص 22) .

2.1. حتمية تعزيز الوعي الاجتماعي بمخاطر الفضاء السيبراني :

إن توعية المستخدمين وتدريبهم على المبادئ الأساسية للأمن السيبراني يجب أن يكون جزءا أساسيا من أي إستراتيجية أو مبادرة وطنية أو إقليمية لمكافحة الجرائم السيبرانية¹³ (Gercke, 2012, P 18)

حيث قد تنبه معظم الدول الى ذلك، وهم حاليا يعملون على توعية المستخدمين بالمخاطر السيبرانية والجرائم السيبرانية وكيفية تفاديها، بالإضافة الى ذلك فالطبيعة التقنية والمعقدة للمعلوماتية وما تتطلبه من قواعد خاصة لحكمها سواء على الصعيد الإجرائي أو الصعيد الموضوعي واللغة التقنية الخاصة التي قد يُضطر القاضي لإستعمالها، تفرض إجراء دورات تدريبية خاصة للقضاة والمحققين ورجال الشرطة للتعامل مع الجرائم السيبرانية والأدلة المعلوماتية .

الحمالات المتعلقة بالثقافة والتوعية حول الأمن السيبراني في الجزائر تعاني من الضعف نسبيا لعدة أسباب من بينها ضعف التغطية أو التسويق وعدم إستهداف الفئات المعنية حقيقة إضافة إلى أن المناهج التعليمية في المدارس والجامعات لا تتضمن سياسة واضحة لتعليم الأمن السيبراني من حيث الإجراءات والتدابير المختلفة للحياة اليومية التي أضحت مملوءة بالمعاملات والخدمات الالكترونية سواء عبر الحاسوب أو الهواتف الذكية أو وسائل أخرى، كما يلاحظ ضعف تنظيم الحملات الإعلامية الخاصة بالتوعية عبر وسائل الإعلام .

لذا يجب إعتداد وسائل عدة لنشر الوعي الاجتماعي حول المخاطر في الفضاء السيبراني من خلال البرامج التلفزيونية والمقابلات الإعلامية وتوزيع الكتيبات والمحاضرات في المدارس والجامعات والأفلام القصيرة والمؤتمرات والخطابات الموجهة للجمهور، ويحذر لو تتفاعل المنظمات الحكومية مع المنظمات غير الحكومية ومنظمات المجتمع المدني لتثقيف كافة الشرائح داخل المجتمع حول الجريمة السيبرانية وآليات الحماية .

3.2 الإستجابة المشتركة بين الحكومة والمنظمات غير الحكومية والقطاع الخاص والأفراد :

تفتقر العديد من الحكومات من بينها الجزائر إلى موارد بشرية ومالية إضافة إلى إرادة واضحة وحازمة تساعد على متابعة ما يجري في الفضاء السيبراني من نشاطات غير شرعية تنطلق من أراضيها. وفي هذا المجال لا بد من التشديد على ضرورة التعاون بين القطاع



العام والخاص والمنظمات غير الحكومية والمجتمع المدني للتوصل إلى نشر ثقافة إحترام القانون في الفضاء السيبراني وحماية الحقوق والحريات الأساسية.

حيث تعد حماية البنية التحتية الحيوية للمعلومات والفضاء السيبراني مسؤولية مشتركة، ويمكن إنجازها على أفضل وجه عن طريق التعاون بين الوزارات والمؤسسات الحكومية على جميع المستويات ومع القطاع الخاص الذي يمتلك ويدير جانبا كبيرا من البنية التحتية، ويجب أن تكون للحكومة الكلمة الفصل في أي قرارات وطنية تتخذ من أجل التوصل إلى وجود نظام للأمن يستم بالفاعلية والإستمرارية .

ولكل من الحكومة والقطاع الخاص مصلحة دائمة في ضمان مرونة البنية التحتية وقدرتها على الوقاية من الصدمات، وبناءا على ذلك فإن الشراكة بين القطاعين العام والخاص أمر أساسي لتعزيز الأمن السيبراني لأنه لا يمكن لكيان واحد أن يوفر الحماية للبنية التحتية بكاملها، وبالنظر إلى معظم مرافق البنية التحتية السيبرانية في بلدان كثيرة يقوم بتشغيلها القطاع الخاص، فمن المحبذ أن تقوم الحكومة والقطاع الخاص كل في مجاله بالدور المنوط به، وبالعامل معا بطريقة هادفة، ويقتضي نجاح التعاون بين القطاعين توفر عدة عناصر من أهمها:

- توفير موردي البنية التحتية القدرات التي تقع عادة خارج نطاق الاختصاصات الأساسية للحكومة.
- تزويد المالكين والمشغلين بالمعلومات التحليلية والدقيقة والمفيدة في الوقت المناسب في شأن المخاطر التي تواجه البنية التحتية الحيوية .
- إشراك القطاع الخاص منذ البداية في وضع المبادرات والسياسات المتعلقة بحماية البنية التحتية الحيوية.
- التوضيح لقادة المؤسسات المنافع المحققة سواء على مستوى الأعمال أو على مستوى الأمن القومي عن طريق الإستثمار في تدابير أمنية تتجاوز مجرد إستراتيجيات الأعمال التجارية الخاصة بهم .
- تهيئة بيئة لتشجيع ودعم الحوافز للشركات لكي تقوم طواعية بإعتماد الممارسات الأمنية السليمة والمقبولة على نطاق واسع والقيام بحسب الإقتضاء بتحديث وتحسين عملياتها وممارساتها الأمنية .
- توفير الدعم للبحوث اللازمة لتعزيز مستقبل الجهود المبذولة في مجال الأمن السيبراني.
- تحديد الموارد اللازمة للمشاركة بدراسات شاملة مشتركة بين القطاعات عن طريق التدريبات والندوات والدورات مما يسفر عن دعم توجيه القرارات .
- زيادة الوعي بالسياسات والمنهجيات والتقنيات المتبعة لمكافحة الجرائم السيبرانية بما في ذلك كيفية حماية مستخدمي الانترنت¹⁴ (الباروك، 2017، ص ص 51-53) .

4.2. إقتراح حلول لردع الجرائم السيبرانية وإطار عمل للأمان السيبراني :

لردع ومكافحة الجرائم السيبرانية في الجزائر وجب وضع إستراتيجية وطنية وإطار عمل للأمن السيبراني بحيث هاته الإستراتيجية تتضمن عدة بنود من بينها :

- تحديث التشريعات بصفة دورية مع تشديد العقوبات الخاصة بالجرائم السيبرانية.
- دعم الصناعة المحلية للبرمجيات والتجهيزات وتطوير الحلول التقنية الخاصة بالحماية من المخاطر السيبرانية.
- تعزيز التوعية والتدريب والتأهيل لرجال الأمن ومستخدمي المؤسسات الرقمية في مجال الأمن السيبراني .
- وضع أسس التواصل والتعاون بين مختلف المؤسسات والهيئات و الدول ذات التجارب السابقة.



- إقتراح إنشاء مراكز للاستجابة السريعة لطوارئ الحاسوب والأمر التقنية.
- تعزيز الشراكة بين القطاع العام والخاص، والمجتمع المدني والجمعيات.
- إستخدام أفضل البرامج المضادة للفيروسات وبرامج جدران النار والتشفير وكذا إستخدام الخصائص الفيسيولوجية لحماية النظام مثل البصمة الالكترونية ، حدة العين، الإبهام، الصوت وغيرها .
- تشجيع اعتماد الهوية الإلكترونية للمستخدمين على الشبكة، وجميع الأنظمة الإلكترونية .

خاتمة :

إن مجال تأمين الفضاء السيبراني ومكافحة الجرائم المستحدثة فيه، على الصعيد التنفيذي يتطلب وضع سياسة شاملة وعامة من قبل الدولة ومؤسساتها وكذا توفير الوسائل المعلوماتية والمادية وتدابير الحماية التقنية والتنظيمية والتشغيلية وكيفية التصرف في مكافحة المخاطر السيبرانية والتبليغ عنها، وجب نشر هذه السياسة وتعميمها على مؤسسات الدولة والمنظمات ومختلف شرائح المجتمع المدني. فجهود الحكومة الجزائرية في حماية وتحصين الفضاء السيبراني هي غير كافية من ناحية الجهوية لمواجهة الأخطار والجرائم السيبرانية التي يمكن أن تكون لها آثار وخيمة في المستقبل على مختلف قطاعات الفضاء السيبراني والأفراد، لذلك وجب الإسراع في وضع خارطة طريق وتنظيم أولويات الدولة في هذا المجال .

نتائج الدراسة :

- يشهد المجتمع الجزائري وتيرة متصاعدة لنسبة الإجرام السيبراني بدليل الإحصائيات المسجلة والمعالجة على مستوى مصالح الأمن.
- إفتقار الجزائر إلى إستراتيجية واضحة ومتكاملة للأمن السيبراني .
- البيئة التنظيمية والتشريعية الخاصة بالأمن السيبراني في الجزائر، ما زالت في طور التشكل .
- عدم إكتمال التشريعات الخاصة بالجرائم السيبرانية في الجزائر وعدم كفايتها من حيث العقوبات الرادعة.
- ضعف الوعي الإجتماعي بمخاطر الفضاء السيبراني في الجزائر، ما يفسره النمو المتزايد للجرائم السيبرانية.
- عدم وجود مركز وطني خاص للاستجابة لطوارئ الحاسوب والجوانب التقنية مثل الذي أنشأ في عدة دول عربية من بينها تونس، عمان، قطر، مصر، الإمارات العربية المتحدة، السعودية، السودان.
- بناء الإستراتيجية السيبرانية الوطنية بالجزائر يتطلب تضافر جهود جميع الأطراف (القطاعين العام والخاص والمجتمع المدني، ومختلف الجمعيات) .

التوصيات :

- إتخاذ التدابير والإجراءات التي تعتمد على عنصر الأمن السيبراني هي جد ضرورية في الإنتاج، لاسيما ما يخص الشبكات والبرامج والأجهزة الإلكترونية المستخدمة .
- ضرورة تحيين التنظيمات والتشريعات الخاصة بردع الجرائم السيبرانية وهذا بصفة دورية، مع تشديد العقوبات.
- ضرورة وضع إستراتيجية وطنية لنشر الوعي وثقافة الأمن السيبراني لدى مختلف شرائح المجتمع للوقاية من الجرائم السيبرانية
- وضع إستراتيجية سيبرانية وطنية واضحة وملزمة، لكل المعنيين بصناعة المعلومات ووسائل الاتصالات، والبنى التحتية، كما لأولئك المعنيين بإستخدامها من موظفي المؤسسات ومختلف شرائح المجتمع المدني.
- حتمية إنشاء مراكز للسلامة المعلوماتية، ولطوارئ الاتصالات مثل عدة الدول الأخرى .



- تأهيل وتدريب وتكوين الأجهزة القضائية المختصة، و عناصر الأمن للقيام بواجبها على أحسن وجه في مجال ملاحقة ومحكمة المجرمين السيبرانيين.
- تحويل الأمن السيبراني إلى جزء من خطط التنمية بإستراتيجية وطنية شاملة يتدخل فيها جميع الأطراف .
- على الحكومة أن تمسك بزمام المبادرة في نشر ثقافة الأمن السيبراني ودعم جهود المشاركين .
- إقتراح إنشاء مجلس أعلى للأمن السيبراني حيث يتم التعاون مع جميع الجهات الحكومية والجهات الغير حكومية والمجتمع المدني .

قائمة المراجع :

- 1- مراد فيصل، "التحديات الإقليمية الراهنة للأمن القومي الجزائري"، رسالة ماجستير منشورة، المدرسة الوطنية العليا للعلوم السياسية : قسم الدراسات العسكرية والاستراتيجية، 2013-2014.
- 2- سليم قسوم، "الإتجاهات الجديدة في الدراسات الأمنية : دراسة في تطور مفهوم الأمن عبر منظارات العلاقات الدولية"، رسالة ماجستير منشورة، جامعة الجزائر : كلية الحقوق والعلوم السياسية 2010.
- 3- سورة قريش، الآية 4.
- 4- Martti Lehto, Pekka Neittaanmaki, "Cyber Security : Technology and Automation edition springer", 2015.
- 5- قانون رقم: 18-04، 13 ماي 2018، "المعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية بالجزائر"، المؤرخ في: 10 ماي 2018، المادة 10، الجريدة الرسمية، الباب الأول، القسم الثاني، العدد 27.
- 6- د. ذياب موسى البيداني، "الجرائم الالكترونية : المفهوم والأسباب، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، كلية العلوم الاستراتيجية، عمان / الأردن خلال الفترة : 2-4/09/2014.
- 7- محمود أحمد القرعان، "الجرائم الالكترونية"، دار وائل للنشر والتوزيع، عمان، الطبعة الأولى، 2017.
- 8- تميم عبد الله سيف التميمي، "الجرائم المعلوماتية في الإعتداء على الأشخاص"، مكتبة القانون والإقتصاد، الرياض، الطبعة الأولى، 2016.
- 9- محمد قطب، "دراسة قانونية عن الجرائم الالكترونية الممارسة ضد المرأة على صفحات الانترنت وكيفية محاربتها"، <http://policemc.gov.bh/mcms-store/pdf/.com> تم الاطلاع يوم : 13-12-2022.
- 10- عز الدين عز الدين، "الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، قيادة الدرك الوطني"، مداخلة بملتقى وطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة، 16-11-2015.
- 11- نؤارة باشوش، "أرقام مرعبة للجرائم السيبراني: تصريحات وزير العدل" [http:// Echoroukonline.com](http://Echoroukonline.com) ، أطلع عليه يوم : 16-02-2022.
- 12- د. منى الأشقر جبور، "الأمن السيبراني: التحديات ومستلزمات المواجهة"، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت 27 - 28 أغسطس 2012.
- 13-Marco Gercke, *Understanding Cybercrime : Phenomena, Challendes and Legal Response*, September 2012,P 18.
- 14-العميد الركن إبراهيم الباروك، وزارة الدفاع اللبنانية، التعاون مع الوزارات والقطاع الخاص في مجال الأمن السيبراني، "مؤتمر الأمن السيبراني والدفاع السيبراني : تحديات وآفاق"، الجامعة اللبنانية والوكالة الجامعية للفرنكوفونية AUF ، 2017 .



الجريمة الالكترونية ودوافع ارتكابها

إيمان بومدين

جامعة بجي فارس - المدينة -

حنان بن مزيان

جامعة بجي فارس - المدينة -

مقدمة

لازمت الظاهرة الإجرامية المجتمعات البشرية منذ أقدم العصور وتطورت بتطورها ، وبما ان الانسان دائما في تطور مستمر بفضل ثورة المعلومات والتكنولوجيا المتطورة فإننا نجد العلماء والمختصين وأفراد المجتمع يحاولون الاستفادة منها ، وبالمقابل نجد المجرمين يحاولون كذلك الاستفادة من هذا التقدم التقني ، بحيث أصبحت التكنولوجيا متاحة لكل الفئات المجتمعية ، بحيث استطاع المجرمين اكتساب خبرات ومهارات أكثر في تعاملهم مع الانترنت وارتكابهم للجرائم الالكترونية عبر الاقمار الصناعية ، فلم تعد جرائمهم تقتصر على اقليم دولة واحدة بل تجاوزت كل الحدود الإقليمية ، وهي جرائم مستحدثة تمثل ضربا من ضروب الذكاء الاجرامي ، ولهذا كان من الصعب ادراجها ضمن الاوصاف الاجرامية والجناائية التقليدية في القوانين الجنائية الوطنية والدولية لما لها من اساليب حديثة ومتعددة ، لذا وجب على المشرع القانوني تطوير الانظمة والقوانين الجنائية بذكاء مماثل للذكاء الاجرامي وبدقة وحكمة متناهية ومحاولة تكييفها حسب هذا النوع من الجرائم ، ومن خلال ما سبق يمكن الوصول الى سبل مواجهة هذه الجرائم الالكترونية من خلال تعاون الانظمة الدولية وفهمها للسبل الشرعية والعمل بها في مكافحة هذا النوع من الجرائم المستحدثة ، وبهذا يقل خطرها ويسعد افراد المجتمع ويعيشون في امن وسلام.

1. التحديد المفاهيمي للجريمة الالكترونية (السيبرانية)

لا يوجد اجماع على تعريف الجريمة الالكترونية من حيث كيف تعرف او ما هي الجرائم التي تتضمنها الجريمة الالكترونية ، وكما يقول فان هلمست وونيف هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة ، وفي اغلب الاحيان تستخدم مصطلحات الافتراضية والحاسوب والالكترونية والرقمية.

ويتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب الى الجرائم التي ترتكب بأي نوع من المعدات الرقمية ، وتعريف الجرائم الالكترونية باختصار على انها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال او الهاتف النقال (التنظيم القانوني والجرائم الالكترونية (ما بين امن المعلومات وتقييد الحريات) 2018، 07)

عرفت بأنها الممارسات التي توقع ضد فرد او مجموعة مع توفر باعث اجرامي ، بهدف التسبب بالأذى لسمعة الضحية عمدا ، او الحاق الضرر النفسي والبدني به سواء اكان ذلك بأسلوب مباشر او غير مباشر ، بالاستعانة بشبكات الاتصال الحديثة كالانترنت وما تتبعها من ادوات كالبريد الالكتروني وغرف المحادثة ، والهواتف المحمولة.

ادت الحادثة التي تتميز بها الجريمة الالكترونية واختلاف النظم القانونية والثقافية بين الدول الى اختلاف في مفهوم الجريمة الالكترونية من بينها :



حسب اللجنة الاوروبية فان مصطلح الجريمة الالكترونية يضم كل المظاهر التقليدية للجريمة مثل الغش وتزييف المعلومات ونشر مواد الكترونية ذات محتوى مخل بالأخلاق او دعوى لفتن طائفية.

حسب منظمة التعاون الاقتصادي للجريمة المرتكبة عبر الانترنت : هي كل سلوك غير مشروع او غير اخلاقي او غير مصرح به يتعلق بمعالجة الية للبيانات ونقلها (التنظيم القانوني والجرائم الالكترونية (مابين امن المعلومات وتقييد الحريات) (2018، 07) . وعليه يمكن القول ان الجريمة الالكترونية تتمثل في ممارسة كل الجرائم التقليدية ولكن بطريقة مستحدثة اي باستخدام القطاع المعلوماتي والتطور التكنولوجي.

2. خصائص الجريمة الالكترونية :

من المتبادر الى الذهن عند الحديث عن خصائص الجريمة الالكترونية ان الجاني له دور كبير في معظم حالاتها ، و نبي عليها تصور العمدية من الجاني ، لأنه في الغالب يعتمد التدخل في مجالات النظام المعلوماتي المختلفة مثل مجال المعالجة الالكترونية للبيانات ، ومجال المعالجة الالكترونية للنصوص ، والكلمات الالكترونية ، ففي مجال المعالجة الالكترونية للبيانات يعتمد الجاني ادخال البيانات التي يمكن ان تساعد في الحصول على المعلومات التي من خلالها تتم الجريمة الالكترونية بواسطة الحاسب الالي ، وفي مجال المعالجة الالكترونية للنصوص والكلمات يتمكن مستخدم الحاسب الالي كتابة الوثائق المطلوبة بدقة متناهية بفضل الادوات الموجودة تحت يده ، وإمكانات الحاسب الالي ايضا لها دور كبير في تيسير ارتكاب الجريمة ، فكلما ارتفعت امكانيات الحاسب تمكن المستخدم من التصحيح ، والتعديل ، والمحو ، والتخزين ، والاسترجاع ، والطباعة ، وغيرها (العريان، الجرائم المعلوماتية 2004، 37).

وبعد هذا العرض لبعض الصور من الجريمة الالكترونية يتضح ان خصائص الجريمة الالكترونية يمكن بيانها على النحو التالي:

- مرتكب الجريمة الالكترونية في الغالب شخص يتميز بالذكاء ، والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال انظمة الحاسب وكيفية تشغيله ، وكيفية تخزين المعلومات والحصول عليها ، في حين ان مرتكب الجريمة التقليدية في الغالب شخص امي بسيط متوسط التعليم .

- مرتكب الجريمة الالكترونية قد يكون منسجما اجتماعيا قادرا ماديا ، ا ان باعته على ارتكاب جريمته في كثير من الاحيان رغبته في قهر النظام ، وهذه الرغبة قد تزيد عنده على رغبته في الحصول على المال ، في حين ان مرتكب الجريمة التقليدية في الغالب يكون غير منسجم اجتماعيا ورغبته في الحصول على المال تفوق بكثير اي رغبة اخرى.

- تقع الجريمة الالكترونية في مجال المعالجة الالية للمعلومات ، وتستهدف المعنويات لا الماديات ، وهي بالتالي اقل عنفا وأكثر صعوبة في الاثبات ، لان الجاني مرتكب هذه الجريمة لا يترك وراءه اي اثر مادي خارجي ملموس يمكن فحصه ، وهذا يعرقل اجراءات اكتشاف الجريمة ومعرفة مرتكبها ، بخلاف الجريمة التقليدية التي عادة ما تترك وراءها دليلا ماديا او شهادة شهود او غيرها من ادلة الاثبات ، كما ان موضوع التفتيش والضبط قد يتطلب احيانا امتداده الى اشخاص اخرين غير المشتبه فيه او المتهم.

- الجريمة الالكترونية ذات بعد دولي ، اي انها عابرة الحدود ، فهي قد تتجاوز الحدود الجغرافية بسبب ان تنفيذها يتم عبر الشبكة المعلوماتية ، وهو ما يثير في كثير من الاحيان تحديات قانونية ادارية فنية ، بل سياسية بشأن مواجهتها لا سيما فيما يتعلق بإجراءات الملاحقة الجنائية (عطايا، الجريمة الالكترونية وسبل مواجهتها في الشريعة الاسلامية والانظمة الدولية)(دراسة تحليلية تطبيقية (2010، 374-373).



3. انواع الجرائم الالكترونية :

ان الجريمة الالكترونية عرفت اختف حول تقسيماتها ، وذلك بسبب الاختلاف في تسميتها ، حيث استند كل اتجاه على معيار معين ، فالبعض يصنفها حسب الاسلوب المتبع في الجريمة ، والبعض الاخر يستند الى دوافع ارتكابها ، وآخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحق المعتدى عليه ، اما بالنسبة للمشرع الجزائري فقد قسم الجريمة الالكترونية الى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها ، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الاعلام والاتصال ، اما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات ، وهذا ما سيتم بيانه في الفرعين المواليين.

1.3. الجريمة الالكترونية المرتكبة باستخدام النظام المعلوماتي

يشمل هذا التصنيف اهم الجرائم التي تتصل بالمعلوماتية ، ويعد الحاسب الالى وسيلة لتسهيل النتيجة الاجرامية ومضاعفا لجسامتها ، وهي انواع منها الجريمة الواقعة على الاشخاص ، الجريمة الواقعة على النظم المعلوماتية الاخرى ، الجريمة الواقعة على الاسرار ، وسنوضح كل نوع منها في البنود الآتية:

1.1.3. الجريمة الالكترونية الواقعة على الاشخاص الطبيعية

تنقسم هذه الجرائم بدورها الى جرائم واقعة على حقوق الملكية الفردية ، وجرائم واقعة على حرمة الحياة الخاصة.

1.1.1.3. الجريمة الالكترونية الواقعة على حقوق الملكية الفكرية

يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفردية ، ومثاله السطو على المعلومات وتخزين واستخدام هذه المعلومات دون اذن صاحبها ، لان استخدام معلومة معينة دون اذن صاحبها يعتبر اعتداء على حق معنوي ، اضافة الى كونه اعتداء على قيمتها المالية كون ان للمعلومة قيمة ادبية بجانب قيمتها المادية ، ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع ، اذ تمثل فكرة المخترع تحتوي على حق معنوي وآخر مالي للمخترع ، وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الامر رقم 03-05 الصادر في 2003 ، المتعلق بحقوق المؤلف والحقوق المجاورة ، والامر رقم 03-07 الصادر في 2003 المتعلق ببراءات الاختراع (سفيان 2011، 14-15-16).

2.1.1.3. الجريمة الالكترونية الواقعة على حرمة الحياة الخاصة :

لقد كرس المشرع الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الاعتداء على هذه الحرمة ، ولما كان الحاسب الالى بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين اكبر قدر ممكن من المعلومات ، وهذا ما جعل للحاسب الالى دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشاءها لتحقيق مصالح مختلفة ، ومثاله ان يقوم شخص يعمل بالنظام المعلوماتي يعلم الشخص المعني ولكن يقوم المكلف بحفظها بإطلاع الغير عليها دون اذن صاحبها ، او ان يقوم شخص باختراق معلومات هي بمثابة اسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص اخر.

2.1.3. الجريمة الالكترونية الواقعة على النظم المعلوماتية الاخرى :

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية ، او استخدام اداة الكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الاخرى ، بالإضافة الى اساءة استخدام البطاقة الائتمانية.

بالنسبة للحالة الاولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية ، حيث يستطيع الجاني هذا الاستيلاء شاشة النظام ، او الاطلاع على المعلومات بقراءة ما هو مكتوب عليها ، او باستخدام مكبر الصوت . اما الحالة الثانية في حالة اساءة استخدام العميل البطاقة الائتمانية ، وذلك عن طريق عدم احترام العميل المصدر اليه البطاقة الائتمانية شروط العقد الملزم بينه وبين البنك ، كاستعماله



بطاقة ائتمانية انتهت مدة صلاحيتها او ثم الغاؤها ، ام الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة ائتمانية للحصول على السلع والخدمات (سفيان 2011، 35-36-37).

3.1.3. الجريمة الالكترونية الواقعة على الاسرار :

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الاسرار ، سواء كانت اسرار عامة او اسرار خاصة تتعلق بالأفراد او المؤسسات المختلفة ، ويتخذ هذا النوع من الجرائم صورتين ، الاولى تتعلق بالجرائم الواقعة على اسرار الدولة ، حيث اتاح الانترنت للكثير من الدول ممارسة التجسس على دول اخرى ، وذلك بالإطلاع على الاسرار العسكرية والاقتصادية لهذه الاخيرة خاصة في الدول التي يكون فيها نزاعات ، والثانية تتعلق بالجرائم الواقعة على الاسرار المهنية ، و الهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص او بجماعة معينة او بيع هذه المعلومات لتحقيق مصالح مختلفة ، كالحصول على عائد مادي ممن يهمله الامر او يستخدمها للضغط على اصحابها من اجل القيام بعمل او الامتناع عن القيام بعمل (سفيان 2011، 38).

وقد حرص المشرع الجزائري على حماية هذه الاسرار من خلال الباب الاول المتعلق بالجنايات والجناح ضد الشيء العمومي من المادة 61 الى المادة 96 مكرر من قانون العقوبات ، بالإضافة الى المادة 394 مكرر 03 التي تنص على : " تضاعف العقوبات المنصوص عليها في هذا القسم اذا استهدفت الدفاع الوطني او الهيئات والمؤسسات الخاضعة للقانون العام ، دون اخلال بتطبيق عقوبات اشد (القانون رقم 04-15 ، الصادر في 10 نوفمبر 2004 ، يعدل ويتمم الامر رقم 66/156 ، الصادر في 08 جوان 1966 ، المتضمن قانون العقوبات ، جر ، العدد 71. بلا تاريخ).

2.3. الجريمة الالكترونية الواقعة على النظام المعلوماتي :

من اجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال ، جاء القانون رقم 04-15 الصادر في 10 نوفمبر 2004 ، المتضمن قانون العقوبات بتحريم كل انواع الاعتداءات التي تستهدف انظمة المعالجة الالية للمعطيات ، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات ، تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات ، وذلك في المواد 394 مكرر الى 394 مكرر 07 ، وتأخذ صور الاعتداء صورتين هما : الدخول والبقاء في منظومة معلوماتية ، المساس بمنظومة معلوماتية ، كما تضمن صور اخرى للغش .

1.2.3. جرمي الدخول والبقاء غير المشروعان في منظومة معلوماتية :

تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل او يبقى بواسطة استعمال الغش في كل او جزء من منظومة المعالجة الالية للمعطيات او يحاول ذلك ، وإذا نتج عن هذا الدخول او البقاء تخريب في النظام المعلوماتي فان العقوبة تضاعف ، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول او البقاء ، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول او البقاء غير المشروع اما محو او تغيير في المعطيات الموجودة في النظام (عقون، السلوك الاجرامي للمجرم المعلوماتي 2012، 182-183).

1.1.2.3. فعل الدخول غير المشروع : لا يعني هنا الدخول بالمعنى المادي ، اي الدخول الى مكان معين كمنزل او غيره ، وإنما

ينظر اليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول الى فكرة او الى ملكية التفكير لدى الانسان ، اي الدخول الى العمليات الذهنية التي يقوم بها نظام المعالجة الالية للمعطيات ، وتقع هذه الجريمة من كل انسان ايا كانت صفته سواء كان شخص يعمل في مجال المعلوماتية او لا يعمل ، وسواء كان يستطيع ان يستفيد من الدخول ام لا ، فيكفي ان يكون ممن ليس له الحق في الدخول الى النظام او من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها ، كما تقع الجريمة سواء تم الدخول الى النظام كله او الى جزء منه فقط ، اي ان الجريمة تقوم بفعل الدخول الى النظام مجردا عن اي نتيجة اخرى ، ولا يشترط لقيامها التقاط



او حصول الشخص على المعلومات الموجودة داخل النظام او البعض منها ، بل ان الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام ، ففعل الدخول يتسع ليشمل كل فنيات الدخول الاحتيالي في منظومة محمية كانت او غير محمية ، كما تشمل استعمال من لا حق له في ذلك المفتاح للدخول الى المنظومة.

2.1.2.3. فعل البقاء غير المشروع : يقصد بفعل البقاء التواجد داخل نظام المعالجة الالية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام ، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في النظام وقد يجتمعان ، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول الى النظام مشروعا ، ومن امثلة ذلك اذا تحقق الدخول الى النظام بالصدفة او عن طريق الخطأ ، وهنا يجب على المتدخل ان يقطع وجوده داخل النظام وينسحب ، فإذا بقي رغم ذلك فانه يعاقب على جريمة البقاء غير المشروع ، ويكون البقاء جريمة في الحالة التي يطبع الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الاطلاع فقط ، ويتحقق ذلك ايضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية ، والتي يستطيع الجاني فيها الحصول على الخدمة دون ان يدفع المقابل الواجب دفعه او يحصل على مدة اطول من المدة التي دفع مقابلها ، ففعل البقاء يشمل البقاء بعد الدخول الشرعي اكثر من الوقت المحدد ، وذلك بغية عدم الدفع ، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب او حصل عن بعد ، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية (عقون، السلوك الاجرامي للمجرم المعلوماتي 2012، 183-184).

2.2.3. جريمة المساس بالمنظومة المعلوماتية :

نصت المادة 394 مكرر 01 من قانون العقوبات رقم 15 /04 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الالية ، او ازال او عدل هذه المعطيات وذلك عن طريق استعمال الغش ، هذا السلوك الاجرامي يتجسد في ثلاث صور هي الادخال ، المحو ، التعديل ، كما ان المشرع لم يشترط اجتماع هذه الصور بل يكفي ان يصدر عن الجاني احدها فقط لكي يتوفر الركن المادي ، وأفعال الادخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الالية للمعطيات ، سواء بإضافة معطيات جديدة غير صحيحة او محو او تعديل معطيات موجودة من قبل ، كما ان هذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الالية ، مثال ذلك ادخال فيروس المعلوماتية في البرامج من اجل اتلافها.

وعليه ومن خلال ما تم التطرق اليه سابقا فان هذا النمط من الجرائم له ميزة خاصة ، بحيث يكون سهل حال ارتكابها ولكن شديدة الخطورة في نتائجها ، وقد ترتكب اخطر الجرائم في بضعة ثواني ، ودون النقاء بين الجاني والمجني عليه وهذا ما يؤدي الى صعوبة مكافحتها ، والشيء الذي يعاب على المشرع الجزائري انه اهمل المجرم الالكتروني وتسييل العقوبة عليه ولم يتعرض له في اي نص قانوني ، واهتم فقط بالجريمة الالكترونية بالنص على بعض الجرائم وليس كلها .

4.دوافع ارتكاب الجريمة الالكترونية :

هناك العديد من الدوافع التي تحرك الجناة لارتكاب افعال الاعتداء المختلفة في هذا النمط من الجرائم ، واهم هذه الدوافع سيتم بيانها كالآتي :

1.4.الدوافع الشخصية لارتكاب الجريمة الالكترونية :

تصنف هذه الدوافع الى دوافع مادية وأخرى ذهنية ، وسيتم تناوله لاحقا.

1.1.4.الدوافع المادية :

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الالكترونية ، وذلك لان الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الالكتروني الى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية ، ويستغل الفرص ويسعى الى الاحتراف



حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه ، فيتعهد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها ، أو اختراق نظم المعالجة الآلية من خلال اكتشافه لفجواتها الأمنية ، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه ، أو لحساب شركائه ، أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة ، كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج و المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب (المجالي 2005، 31).

2.1.4. الدوافع الذهبية لارتكاب الجريمة الالكترونية

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات ، وقد تكون هذه الدوافع مجرد شعف بالالكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية ، فاختراق الانظمة الالكترونية وكسر الحواجز الامنية المحيطة بهذه الانظمة قد يشكل متعة كبيرة لمرتكبيها وتسليية تغطي اوقات فراغه ، وعلى صعيد آخر قد يكون اقدام المجرم الالكتروني على ارتكاب جريمته بدافع الرغبة في قهر الانظمة الالكترونية والتغلب عليها ، اذ يميل هنا الى اظهار تفوقه على وسائل التكنولوجيا الحديثة ، وفي الغالب تكون لديهم دوافع حاقدة أو تخريبية ، وإنما ينطلق من دافع التحدي وإثبات المقدرة (نعيم بلا تاريخ، 61-62).

2.4. الدوافع الموضوعية لارتكاب الجريمة الالكترونية :

قد يتأثر المجرم الالكتروني ببعض المواقف قد تكون دافعة له على اقتواف الاجرام الالكتروني ولا يسعى في ذلك حينها لا للمتعة والتسليية ولا لكسب المال ، ويمكن ابراز اهم الدوافع كما الاتي :

1.2.4. دافع الانتقام وإلحاق الضرر برب العمل :

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله ، أو تخطيه في الحوافز أو الترفيه ، فهذه الامور تجعله يقدم على ارتكاب جريمته ، كما هذا الدافع من اخطر الدوافع التي يمكن ان تدفع الشخص الى ارتكاب الجريمة ، ذلك انه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها ، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية ، أو الطرد من الوظيفة ، فيتولد لدى المجرم الالكتروني الرغبة في الانتقام من رب العمل.

2.2.4. بدافع التعاون والتواطؤ :

هذا النوع يتكرر كثيرا في الجرائم الالكترونية ، وغالبا ما يحدث بالتعاون بين متخصص في الانظمة المعلوماتية ، اين يقوم بالجانب الفني من المشروع الاجرامي ، وآخر من المحيط أو خارج المؤسسة المجني عليه يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية ، وعادة ما يمارسون التلصص على الانظمة وتبادل المعلومات بصفة منظمة حول انشطتهم (نعيم بلا تاريخ، 62). وعليه فان هذا الدوافع الخاصة بارتكاب الجريمة الالكترونية فهي غير ثابتة ومعتمدة لدى الباحثين والمختصين لان السلوك الاجرامي والدوافع لارتكاب الجريمة الالكترونية قد تتغير وتتحوّل بسرعة من محاولة التحدي والتغلب على الانظمة الى تدميرها أو القيام بعمليات الابتزاز أو الحصول على الاموال ، وعليه فان كل جريمة جديدة دوافع جديدة .

5. مظاهر تحديات الجريمة الالكترونية :

يمكن ايجاز مظاهر تحديات الجريمة الالكترونية فيما يلي :

1- عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الالكترونية ، وبالتالي عدم وجود توافق بين قوانين الاجراءات الجنائية

للدول بشأن التحقيق في تلك الجرائم.



- 2- أيضا يمثل النقص الظاهر في مجال الخبرة لدى رجال الشرطة وجهات الادعاء والقضاء تحديا كبيرا في القضاء على هذه الجريمة.
- 3- الاعتداء على برامج ومعلومات الحاسب يجعلنا امام مشكلة قانونية ذات طبيعة خاصة سميت هذه الجريمة في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الالية للبيانات وهي جريمة مستحدثة.
- 4- ظهور وتنامي الأنشطة الاجرامية الالكترونية وتوسل مرتكبيها بتقنيات جديدة غير مسبقة في مجال تكنولوجيا المعلومات والاتصالات.
- 5- تستعصي بعض هذه الأنشطة الاجرامية الالكترونية على ادراجها ضمن الاوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.
- 6- ظاهرة الجرائم الالكترونية باتت تتخذ انماطا جديدة وضربا من ضروب الذكاء الاجرامي وهذا بلا شك يمثل تحديا جديدا في الوقت الحاضر.
- 7- هشاشة نظام الملاحقة الاجرامية التي تبدو قاصرة على استيعاب هذه الظاهرة الاجرامية الجديدة سواء على صعيد الملاحظة الجنائية في اطار القوانين الوطنية ام على صعيد الملاحقة الجنائية الدولية (عطايا، الجريمة الالكترونية وسبل مواجهتها في الشريعة الاسلامية والانظمة الدولية) (دراسة تحليلية تطبيقية (2010، 375).
- 8- يعد الجدل الحاصل في مسألة تخزين المعلومات او البيانات المعالجة الكترونيا خارج اقليم الدولة من اكبر تحديات الجريمة الالكترونية حيث نتج عنه اتجاهان لمكافحة هذا النوع من الجرائم : الاتجاه الاول يرى انه من غير المشروع ان تقوم سلطات الدولة ما بالتدخل وتفتيش النظم المعلوماتية الموجودة في اقليم دولة اخرى ، بهدف كشف وضبط ادلة اثبات جريمة كانت قد وقعت على اراضيها ، وذلك استنادا الى مبدأ اقليمية القانون.
- اما الاتجاه الثاني فيتمثل في ان القانون الدولي يمكن ان يتشكل من خلال توافق الاراء على الصعيد الدولي باتجاه السماح بتنفيذ هذه الإجراءات حال توافر ظروف معينة يتم تحديدها ، كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية.

6. آليات مواجهة الجريمة الالكترونية:

1.6. الأجهزة العملية المختصة في مكافحة الجرائم الالكترونية:

1.1.6. من الناحية القانونية:

❖ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261 وهي سلطة إدارية مستقلة لدى وزير العدل ، تعمل تحت إشراف ومراقبة لجنة مديريةية يرأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء. (عبان 2016، 91)

وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنسيق عمليات الوقاية منها ، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم ، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية ، وضمان المراقبة الوقائية للاتصالات الإلكترونية ، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.



وقد نص سابقا على إنشاء هذه الهيئة المادة 13 من القانون 09/04 المؤرخ في أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال : " تنشأ هيئة وطنية وتنظيمها وكيفية سيرها عن طريق التنظيم" أما مهامها فقد أوردتها المادة 14 من نفس القانون وتمثل في: (عطية بلا تاريخ، 04) (بارة دون سنة ، 445)

أ- الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال : إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيا الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات ، ومن أهم هذه الجرائم : التجسس على الاتصالات والرسائل الالكترونية ، التلاعب بحسابات العملاء ، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية...الخ.

ب- مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال : بحسب نص المادة 14 من القانون 09/04 هناك نوعان من المكافحة تقوم بهما هذه الهيئة:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة (ب) من القانون 09/04.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (CRAIYEN AND OTHERS,2014,P14) يقترح المشروع في هذا الفصل إنشاء هيئة وطنية مختصة تتولى مهام أهمها : تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية ومصالح الشرطة القضائية من التحريات التي تجريها بشأن هذه الجرائم، وما تقوم به أيضا من تجميع المعلومات من نظيرتها في الخارج قصد محاربة هذا النوع الخطير من الإجرام (بارة دون سنة ، 445).

2.1.6. من الناحية العلمية:

1.2.1.6. المصلحة المركزية لمكافحة الجريمة المعلوماتية -DGSN-(SCLC):

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم السيبرانية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة السيبرانية وعلى مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015 (عراية و النعيم 2016، 130)

2.2.1.6. مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني(CPLCIC):

وقد أنشئ في سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، وهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد راييس، وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية وللبنوك (رواجي 2010، 78).

ويهدف هذا المركز إلى مساعدة الأجهزة الأمنية الأخرى بالتعاون من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال استغلال المعلومة من خلال تنسيق مع وزارة العدل ومعهد خاص بعلم



- الإجرام لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، فالجزائر تعمل جاهدة على الاستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها (علوي 2008، 41)
- **الوقاية:** وتشمل حملة تحسيسية وتوعية بالتنسيق مع وزارة التضامن الوطني والأسرة والعمل على ملتقيات ومحاضرات وأياما دراسية ومنتديات دولية، ومشاركة في منتديات صحفية وحصاص تلفزيونية وإذاعية وغيرها من وسائل النشر والإشهار.
- **المكافحة:** توعية الجزائريين من خلال استعمالهم لشبكات التواصل واستخدام الانترنت وذلك من خلال تعليقاتهم المدافعة عن الجزائر ومعرفة الأخطار بسلوكيات مشبوهة أو اعتداءات عبر نشر فيديوهات توصل إلى الجناة، مما يسهل التحقيق لدى مصالح الدرك وإلقاء القبض على المشبوهين ومرتكبي الجرائم في الوقت المناسب.

3.2.1.6. المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني (INCC):

مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة (كريم 2008، 36)

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني "ببوشاوي"، حيث تم إنشائه بموجب مرسوم رئاسي 133/04 المؤرخ في 26 جوان 2004، ودخل حي المورد البشري واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من مهام الخدمة ابتداء من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و 2009 كرسست للتكوين التي من شأنها تلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة، قانونيا خاصة أثناء معالجة القضايا المعقدة (ربه 2006، 33-34-35).

والإسهام في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية، ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات؛ مصلحة البيئة؛ أما في ما يخص مجال الأمن السيبراني هناك مصلحة الإعلام الآلي؛ على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية (غزال 2014، 64).

خاتمة

في السنوات الاخيرة اصبح الكمبيوتر والانترنت محرك عجلة التنمية ووسيلة الرقي والتقدم في كافة العلوم، كما تعتبران هاتان الوسيلتان كاتمتان لأسرار عدة قطاعات ووسيلة تواصل رئيسية عبر العالم، الا انهما في نفس الوقت اصبحتا للأسف وسيلة ارتكاب اخطر الجرائم العابرة للدول والقارات الا وهي الجرائم الالكترونية، ولهذا يتطلب مكافحة الجرائم الالكترونية من خلال وضع سياسة وطنية ودولية محكمة تفرض عقوبات صارمة وراذعة على مرتكبي جرائم الانترنت، كما يستوجب الاعتماد على اساليب وتقنيات متطورة لحماية قطاع المعلوماتية والتمكن من الكشف عن مرتكبي هذه الافعال غير المشروعة.

ان من اهم التحديات التي تواجه المشرع هو موضوع التجريم والعقاب، اذ يتوجب على المشرع في كافة الدول التي لا تشمل قوانينها على نصوص تجرم الجرائم الالكترونية المبادرة الى ذلك في الحين، كما نجد بالمقابل ان معظم الجرائم الالكترونية مصنفة في كثير من الدول على انها جنح، بالرغم من خطورتها وشدة جسامتها، لكن هذه النظرة بدأت تتغير مؤخرا وذلك مع نمو ظاهرة الجريمة الالكترونية وتشعبها، وكذلك بسبب انشاء اقسام خاصة بملاحقة هذه الجرائم والتحقيق فيها والتي ساهمت بدورها ايجابيا في زيادة الوعي بخطورة هذا النوع من الجرائم.

التوصيات



يمكن وضع مجموعة من التوصيات وهي كالتالي :

- 1- تعديل قانون العقوبات ليشتمل على تجريم الجرائم الالكترونية ، او سن قانون مكافحة الجرائم الالكترونية.
- 2- تغليظ عقوبة الجرائم الالكترونية ، واعتبار خطورة الجريمة ، بتهديدها للأمن الداخلي والعالمي وحجم الضرر ، من الظروف المشددة للعقوبة التي ترفع مستوى الجريمة لتصبح جنائية.
- 3- عدم فتح اي رسالة الكترونية من مصدر مجهول ، لان مرتكبي الجرائم الالكترونية يستخدمون وسائل البريد الالكتروني ، لإرسال ملفات التجسس على الضحايا.
- 4- وضع ارقام سرية على الملفات المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط ، و محاولة تغيير كلمة السر باستمرار فهي قابلة للاختراق.
- 5- تطوير قدرات التقنية على شبكة الانترنت ، وإنشاء شرطة الانترنت للقبض على مرتكب الجرائم حال دخولهم على الشبكة من خلال التتبع الفني للجهاز او الخط الهاتفية الذي ارتكبت منه الجريمة.
- 6- العمل على انشاء محاكم للقضايا الافتراضية على شبكة الانترنت لتتمكن من التعامل مع هذه الانواع المستحدثة من الجرائم.
- 7- جعل القرصنة على البرامج بمثابة جريمة سرقة ، مثلها مثل سرقة اي سلعة اخرى.
- 8- الاحتفاظ بنسخ احتياطية لكل المعلومات الحساسة في اقراص اضافية ليست مرتبطة بالشبكة.
- 9- ضرورة استخدام بعض البرامج (مكافحة الفيروسات) التي صممت خصيصا للكشف والوقاية من الفيروس والبعد عن استعمال كلمة السر البسيطة.
- 10- العمل على تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم الالكترونية.

قائمة المراجع

- 1- ابراهيم رمضان ابراهيم عطايا. (2010). الجريمة الالكترونية وسبل مواجهتها في الشريعة الاسلامية والانظمة الدولية (دراسة تحليلية تطبيقية). القاهرة : دون دار نشر.
- 2- اسامة بن صادق عطية. (بلا تاريخ). الحكومة الالكترونية (نحو مجتمع المعرفة). معهد البحوث والاستشارات(العدد التاسع).
- 3- التنظيم القانوني والجرائم الالكترونية (مابين امن المعلومات وتقييد الحريات). (2018). القاهرة: مركز هردو لدعم التعبير الرقمي.
- 4- القانون رقم 04-15 ، الصادر في 10 نوفمبر 2004 ، يعدل ويتمم الامر رقم 66/156 ، الصادر في 08 جوان 1966، المتضمن قانون العقوبات. (بلا تاريخ).
- 5- القانون رقم 04-15 ، الصادر في 10 نوفمبر 2004 ، يعدل ويتمم الامر رقم 66/156 ، الصادر في 08 جوان 1966، المتضمن قانون العقوبات ، جر، العدد 71. (بلا تاريخ).
- 6- بن عبد ربه. (2006). النظام الاقتصادي الجديد المبني على المعرفة وتطور مجتمع المعلومات والتكنولوجيا الحديثة للاتصال (الحلول المقترحة لارساء مجتمع المعلومات ناجح ومنكامل في الجزائر) . رسالة ماجستير . الجزائر، كلية العلوم -السياسية والاعلام -جامعة الجزائر.-
- 7- حمزة بن عقون. (2012). السلوك الاجرامي للمجرم المعلوماتي . مذكرة ماجستير في العلوم القانونية تخصص علم الاجرام وعلم العقاب. باتنة ، جامعة الحاج لخضر.
- 8- خيرة وراحي. (2010). ثقافة الانترنت (دراسة ميدانية لاستعلامات الشبكة بمدينة تيهرت. رسالة ماجستير . وهران ، كلية العلوم الانسانية والحضارة الاسلامية (قسم علم المكتبات والعلوم الوثائقية).
- 9- سعيداني نعيم. (بلا تاريخ). اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مذكرة ماجستير في العلوم القانونية تخصص علوم جنائية . جامعة الحاج لخضر، باتنة : 2013.
- 10- سميرة بارة. (دون سنة). الدفاع الوطني والسياسات الوطنية للامن السيبراني في الجزائر : الدور والتحديات . ورقة : جامعة قاصدي مرباح.
- 11- سوير سفيان. (2011). جرائم المعلوماتية. مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الاجرام. جامعة ابو بكر بلقايد ، تلمسان.



- 12-شاهد الياس عرابية، و دفرو عبد النعيم. (2016). تقييم تجربة تطبيق الحكومة الالكترونية في الجزائر. المجلة الجزائرية للدراسات المحاسبية والمالية(العدد الثالث).
- 13-عادل غزال. (2014). مشاريع الحكومة الالكترونية من الاستراتيجية الى التطبيق، مشروع الجزائر ، الحكومة الالكترونية-انموذجا-. مجلة المكتبات والمعلومات(العدد 34).
- 14-عبد القادر عبان. (2016). تحديات الادارة الالكترونية في الجزائر (دراسة سوسيولوجية ببلدية الكاليتوس العاصمة). اطروحة دكتوراه ل م د . بسكرة ، جامعة محمد خيضر (كلية العلوم الانسانية والاجتماعية).
- 15-مجدي علي العريان. (2004). الجرائم المعلوماتية. الاسكندرية: دار الجامعة الجديدة.
- 16-محمود الحمود وضاح، و نشات نفضي المجالي. (2005). جرائم الانترنت (التعرض للاخلاق والاداب العامة ، الحظ على الفجور ، جرائم الاستغلال الجنسي للاطفال). عمان ، الاردن : دار المنار.
- 17-مراد كريم. (2008). مجتمع المعلومات واثرها في المكتبات الجامعية -مدينة قسنطينة انموذجا-. اطروحة دكتوراه . قسنطينة ، كلية العلوم الانسانية والاجتماعية -جامعة قسنطينة-.
- 18-هند علوي. (2008). المرصد الوطني لمجتمع المعلومات الجزائري (قياس النفاذ على تكنولوجيا المعلومات بقطاع التعليم بالشرق الجزائري). اطروحة دكتوراه. قسنطينة ، كلية العلوم الانسانية -جامعة منتوري قسنطينة-.
- 19-وضاح محمود الحمود ، نشات نفضي المجالي. (2005). جرائم الانترنت (التعرض للاخلاق والاداب العامة ، الحظ على الفجور ، جرائم الاستغلال الجنسي للاطفال). عمان ، الاردن: دار المنار.



الآليات المسخرة لمواجهة تحديات الأمن السيبراني في الجزائر

بوعرعار عادل

جامعة بجي فارس - المدية - (الجزائر)

bouarar.adel@univ-medea.dz

مقدمة:

لقد عرف العالم خلال العقد الأخير طفرة تكنولوجية في مجال الإعلام و الاتصال، هذه الأخيرة شملت ظهور فضاءات سيبرانية تتفاعل فيها مختلف الكيانات من أفراد و مؤسسات و شركات و إدارات و حكومات... الخ ، حيث وصل عدد مستخدمي الإنترنت في العالم سنة 2021 إلى 4.9 مليار شخص بنسبة 63% من سكان العالم ، و هو الأمر الذي ساعد في إرتفاعه حالات الحجر الصحي المرافقة لجائحة كورونا خلال السنتين الماضيتين، إن تفاعل هذا العدد الهائل من المستخدمين ينجر عنه ارتفاع عدد الجرائم السيبرانية التي تعددت أشكالها فمنها الجرائم التقليدية التي وجد مرتكبوها فضاءات افتراضية جديدة لارتكابها، و منها جرائم مستحدثة و آكبت التطور التقني و الرقمي .. و تماشيا مع هاته المستجدات كان على الدول و المؤسسات استحداث أنظمة أمن سيبراني لحماية بياناتها وقواعدها الرقمية.

والجزائر كذلك ككل دول العالم تحاول مجارات التطورات الرقمية عبر تحديث أنظمتها الأمنية، قصد حماية الأفراد و المؤسسات وكذا الإدارات وقواعد البيانات والنظم الرقمية الوطنية، وذلك عبر تحيين التشريعات القانونية لتتماشى مع الجرائم المستحدثة من جهة، وكذا إستحداث مؤسسات متخصصة ذات كفاءة في مجابهة تحديات الأمن السيبراني.

1. الجريمة السيبرانية :

1.1 ماهية الجريمة السيبرانية :

لقد تطورت أنماط الجريمة بشكل واضح خلال العشري الأخيرة، حيث تعدت أهدافها استهداف الضحايا في الأنفس و الأموال فقط بل طالت البيانات و المعلومات، حيث عرف هذا النوع من الجرائم في بعض الأوساط بإجرام ذوي "الباقات البيضاء" حيث يستطيع المجرم العصري ارتكاب جريمته ليس فقط دون عنف مباشر أو إراقة الدماء، و لكن دون أن يتحرك من مكانه أو ينهض من كرسيه، و هو ما جعل البعض يصفها بالجرائم الناعمة، فببضع ضغطات على لوحة المفاتيح من قبل المجرم السيبراني يمكن أن تتبعها آثار كارثية على الأفراد أو المؤسسات و حتى الاقتصادات، و ما زاد هذا النوع من الجرائم تأثيرا أنه غير مرتبط بإطار مكاني محدود فهي جريمة عابرة للدول و القارات، لذلك في تعتبر مشكلة عالمية تمس كل الدول على حد سواء. (سميرة 2010، 276)

2.1 تعريف الجريمة السيبرانية :

للجريمة السيبرانية عدة تسميات، فهناك من يسميها بجرائم الحاسوب أو جرائم الإنترنت، أو الجريمة التقنية، وبتعدد المسميات تتعدد التعاريف فمنهم من يربطها بالشق التقني، فيما يربطها آخرون بالشق القانوني، فتعرف على أنها فعل ضار يستخدم فيه الفاعل "الذي يفترض أن تكون لديه خلفية معرفية بتقنيات الحاسوب" نظاما حاسوبيا أو شبكة بيانات حاسوبية للوصول إلى البيانات أو البرامج بقصد (نسخها، تغييرها، حذفها، تزويرها، تخريبها، تجميدها، الاستيلاء عليها، توزيعها أو نشرها بشكل غير مشروع. (كامل 2000).



كما تعرف أيضا بأنها "الجرائم التي ترتكب ضد أفراد أو مجموعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب بالأذى الجسدي أو النفسي للضحية بشكل مباشر أو غير مباشر، باستخدام شبكات الاتصال الحديثة مثل الإنترنت (مواقع التواصل الاجتماعي، غرف الدردشة، البريد الإلكتروني...)، والهواتف النقالة (الرسائل النصية القصيرة ورسائل الوسائط المتعددة)، وتشمل الجرائم الإلكترونية أي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت، ولقد عرفها الدكتور عبد الفتاح مراد على أنها: "الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي و نظم المعلومات سواء لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الإلكتروني كما تسمى كذلك في هذا الإطار بالجرائم السيبرانية لتعلقها بالعالم الافتراضي"، وهناك من يسميها أيضا بجرائم التقنية العالية أو جرائم أصحاب الياقات. (إسرائيل جبريل 2016)

كما يشار إلى إساءة استخدام تكنولوجيا المعلومات والاتصالات من قبل المجرمين بالتبادل على أنها جرائم الإنترنت، أو إساءة استخدام الكمبيوتر، والجريمة المرتبطة بالحاسب الآلي، جريمة التكنولوجيا العالية، والجريمة الإلكترونية، والجريمة الإلكترونية كما عرفها رابطة كبار ضباط الشرطة (ACPO) تنطوي على "استخدام الكمبيوتر أو الإنترنت شبكات تكنولوجيا لارتكاب أو تسهيل ارتكاب الجريمة". بينما من جانب آخر فيعتبر المعهد الاسترالي لعلم الإجرام (AIC) بأنها "تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الاتصالات". (Brown 2015, 57)

أما في الجانب القانوني فقد اصطلح المشرع الجزائري على تسمية الجرائم الالكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرفها بموجب المادة 02 من القانون 04-09 المؤرخ في 05 أوت 2009، على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية. (القانون رقم 04-09 المؤرخ في 05 أوت 2009، 5)

وبشكل أوسع يمكن تعريف الجريمة الإلكترونية بأنها كل أشكال السلوك غير المشروع، والمتعمد الذي يرتكب باستخدام الحاسب الآلي المرتبط بالإنترنت، والتي تمس به أو بمحتوياته أو بالعمليات التي تتم بواسطته، بغرض إلحاق الضرر بالضحية أو الكسب المادي أو غير ذلك من الأغراض، من طرف أفراد على دراية كاملة بتقنيات التكنولوجيا المعلوماتية وأسرارها.

1.3 مجلات تصنيف الجريمة السيبرانية :

لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم الالكترونية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة، وعلى هذا الأساس يمكن تصنيفها إلى ما يلي: (صغير 2013، 43-58)

1.3.1 الجرائم الواقعة على الأموال: في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الالكترونية، وما انجر عنه من تطور في وسائل الدفع والاستلام، وفي خضم التداول المالي عبر الانترنت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم.

2.3.1 الجرائم الواقعة على الأشخاص: مع تطور شبكة الانترنت أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما جعلها عرضة للانتهاك من طرف هؤلاء المجرمين وجعلت سمعة الأفراد مستباحة.

3.3.1 الجرائم الواقعة على أمن الدولة: من أهم الجرائم الالكترونية التي تهدد أمن الدول وهي ما يلي:



- **الجماعات الإرهابية** : استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للإنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها.
- **الجريمة المنظمة** : استغلت عصابات الجريمة المنظمة الإمكانات المتاحة في وسائل الاتصال والإنترنت في تخطيط وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة.
- **الجرائم الماسة بالأمن الفكري** : يبقى الأمن الفكري من بين أخطر الجرائم المرتكبة عبر الإنترنت، حيث تعطي الإنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى.
- **جريمة التجسس الإلكتروني** : سهلت شبكة الإنترنت الأعمال التجسسية بشكل كبير حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي : التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي. وفي تصنيف آخر موسع يمكن تعداد مظاهر الجريمة السيبرانية فيما يلي:

 1. تخريب المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات تخريب الكتب تخريف المعلومات وتخريف السجلات الرسمية.
 2. سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني أو الصناعي أو العسكري أو تخريبها أو تدميرها. الخ.
 3. تزوير المعلومات ويشمل الدخول القواعد في النظام التعليمي وتغيير المعلومات وتخريفها، مثل تغيير علامات الطلاب.
 4. تزيف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.
 5. انتهاك الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم أو وضع معلومات تخص تاريخ الأفراد ونشرها.
 6. التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.
 7. التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
 8. التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل يقصد منه اغتيال شخصية الأفراد أو الإساءة.
 9. السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.
 10. سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.
 11. الدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.
 12. قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.
 13. قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.
 14. خلاعة الأطفال وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال وللإناث خاصة على الشبكات بشكل عام ونشر الجنس التخليبي.

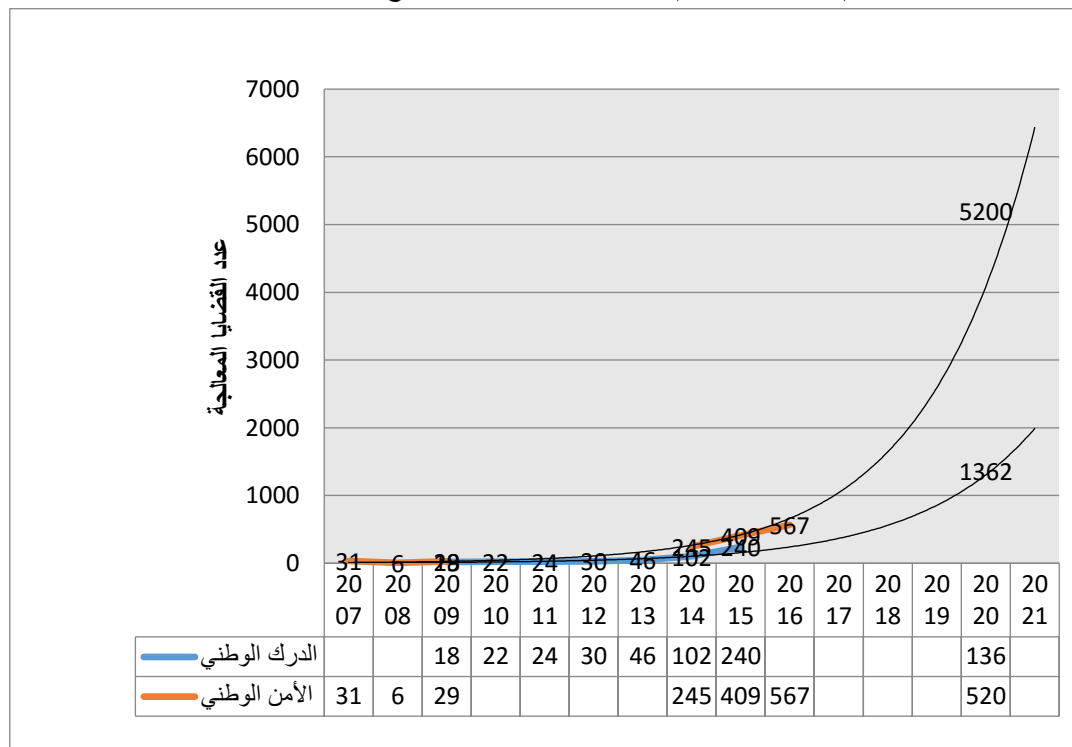


15. سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.
 16. التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو الهاتف، أو المحادثة.
 17. القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية.
 18. إفشاء الأسرار وتشمل الحصول على معلومات خاصة جدا ونشرها على الشبكة.
 19. الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو البطاقات المالية أو البطاقات الهاتفية.
 20. المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.
 21. الإرهاب الإلكتروني، يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادر هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.
- (إسرائيل جبريل 2016).

4.1 واقع الجريمة السيبرانية في الجزائر :

عرفت الجزائر بداية الجريمة السيبرانية قبل سنة 2008 بصورة محدودة نسبيا، حيث لم تتعد عمليات نسخ الأقراص بشكل غير قانوني وما إلى ذلك، فلم تكن تتطلب التدخل الأمني، لكن بعد اقتحام الجزائر عالم الأنترنت الفائق السرعة عبر خطوط ADSL والزيادة الطردية لعدد المشتركين سنة بعد سنة حتى وصل سنة 2021 إلى 26.35 مليون مشترك في مواقع التواصل حسب آخر تقرير لموقع "داتاريبورتال - DATAREPORTAL"، حيث أدى هذا التحول الرقمي الهائل إلى حتمية مواجهة السبلات المرافقة له، فمن خلال المخطط البياني التالي سنحاول استعراض تطور نسب الجرائم السيبرانية المسجلة بدلالة التسلسل الزمني:

شكل رقم 01: قضايا الجرائم السيبرانية المعالجة من قبل المصالح الأمنية خلال 15 سنة الماضية



المصادر: (حملاوي و المقدم عز الدين 2015) (باشوش 2021)



2. الأمن السيبراني :

1.2 تعريف الأمن السيبراني:

يعرف كل من Martti Lehto, Pekka Neittaanmäki الأمن السيبراني " على أنه مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قرصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة"، أما، وقد أيدته في الطرح واحد من أهم المختصين في الميدان: الأستاذ إدوارد أموروزو Edward Amoroso، الذي عرفه " بأنه تلك الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة، إلخ."

أما التعريف الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقريره حول " اتجاهات الإصلاح في الاتصالات للعام 2010-2011"، والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية " هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات امنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريب، وممارسات فضلي، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين". من هذا المنطلق، يمكننا إعطاء تعريف شامل بالقول " أن الأمن السيبراني أو الالكتروني هو مجمل القوانين، الأدوات، النصوص، المفاهيم والميكانيزمات الأمنية وطرق تسيير الأخطار والممارسات التقنية المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة لحماية مصالح الدول والأشخاص ليقى الهدف الاخير، هو قدرة هذه الادوات على مقاومة التهديدات المتعمدة من طرف قرصنة المعلومات أو غير المعتمدة من طرف المستخدمين (الخطأ البشري) للتعاي، وبالتالي التحرر من الأضرار الناجمة عن تعطيل أو سوء استخدام تكنولوجيا المعلومات والاتصالات. (جمال 2019، 1265)

2.2 الأمن السيبراني في الجزائر :

لقد قدمت الجزائر الأمن السيبراني كأحد أولوياتها على غرار باقي دول العالم التي سارعت تحديث سياساتها الأمنية، واعتمادها آليات وميكانيزمات جديدة تعني بهذه المسائل، بالموازاة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي، ويفرض مطالب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية. لقد أصبح الأمن السيبراني ركن أساسي ضمن العقيدة الأمنية الجزائرية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزتها المختلفة، ولا ننسى كذلك الجانب القانوني والمشرع الجزائري وكيف قام بمواجهة هذه الجرائم والاعتداءات الأمنية وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحاً تصاعدياً في الآونة الأخيرة، ولهذا فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم السيبرانية. (إدريس 2019، 112) .

3.2 تحديات الأمن السيبراني في الجزائر :

تواجه مصالح الدرك الوطني ومصالح الأمن الوطني العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن الإلكتروني، يمكن أن نذكر أهمها فيما يلي:

- زيادة عدد المشتركين في شبكة الإنترنت (أكثر من 10 ملايين مشترك بالجزائر): ومع زيادة عدد مستخدمي الشبكة تزداد المخاطر، لتتحول عملية اكتشاف هوية مرتكبي الجرائم الإلكترونية إلى تحدي بسبب صعوبة البحث والتحري ضمن هذا العدد الهائل والمتجه نحو الارتفاع باستمرار.



- **التطور التكنولوجي وظهور الإنترنت اللاسلكي WIFI/3G/4G:** عبر هذه التقنيات لم يعد المجرم يحتاج للجلوس وراء الحواسيب الموصولة سلكيا بشبكة الإنترنت، للقيام بجريمته، مما يستدعي من الجهات الأمنية رفع التحدي، والاستعداد بأحدث التقنيات لمواجهة والتصدي لهذه التطورات.
- **الاستعمال الواسع لشبكات التواصل الاجتماعي:** إذ وصل عدد مستعملي هذه المواقع في الجزائر إلى أكثر من 7 ملايين مستعمل، وهو ما ساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم الإلكترونية، مثل: القذف، التحرش الجنسي، استغلال القصر، وغيرها وهذا ما يستوجب وضع استراتيجيات جد محكمة لضمان الأمن السيبراني عند استخدام مواقع التواصل الاجتماعي.
- **انتشار تكنولوجيا الإنترنت فائقة السرعة والتدفق ADSL/ VSAT/SDSL:** تسهم التكنولوجيا المتطورة في سرعة إنجاز الجريمة، وهذا يضع الجهات الأمنية المختصة أمام تحدي سرعة مباشرة التحقيقات ومتابعة الجناة، والتسلح بالأجهزة المتطورة والبرامج الحديثة السريعة الخدمة.
- **عمليات التخفي أثناء استعمال خدمات شبكة الانترنت (Proxy):** وهي من أكبر الإشكاليات التي تواجهها الجهات المختصة بالتحقيق، ويتطلب تعاون جهات متعددة، والتسلح بالوسائل المتطورة التي يمكن لها رصد الجزئيات وفك الشفرات، وتطوير البنى التحتية الخاصة بالمعلومات وتحديثها باستمرار، وتصميم برامج عالية التطور.
- **غياب التنسيق بين الدول والحكومات:** إذ من المعلوم أن الجريمة الإلكترونية عابرة للحدود والقارات، وهو ما يعني أن مرتكبيها يمكنهم النفاذ إلى أنظمة الحاسوب في أحد الدول، ليمت التلاعب واختراق البيانات في بلد آخر، تسجل النتائج في بلد عن أنه من الممكن تخزين أدلة الجريمة الإلكترونية في حاسوب موجود في بلد آخر، غير الذي ارتكبت فيه الجريمة، وكل هذا يساعد المجرم الالكتروني في إخفاء هويته ونقل المواد من خلال قنوات موجودة في بلدان مختلفة ، وبالتالي ونتيجة القدرة على التنقل إلكترونيا من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، تصبح عدة دول ومحاكم وقوانين وقواعد معنية بذلك، ما يشكل تحديا حقيقيا، ولذلك فإن المحاربة الفعالة للجريمة الإلكترونية تستدعي تعاونا دوليا متزايدا ، سريعا، وفعالا ، وعلى أعلى درجات التنسيق.
- **التطور التكنولوجي في مجال الانترنت والاتصالات:** وهو ما يفرض على الأجهزة الأمنية المختصة بأن تسير هذا التطور، سواء من حيث اكتساب التكنولوجيا والتقنية أو من حيث التمكن من استخدامها واستثمارها بالشكل اللازم، وهذا قد يرهق ميزانيتها المحدودة، ولذلك يتوجب توفير جميع الامكانيات المادية، المالية والبشرية اللازمة للتحقيق الأمن السيبراني.
- **نشر التوعية بمفهوم الأمن السيبراني لمستخدمي شبكة الإنترنت:** وهو ما يستوجب القيام بحملات توعية بين مستخدمي شبكة الانترنت لاتخاذ التدابير اللازمة لضمان الحد الأدنى من الأمان، وتعليمهم آليات التشفير، والاحتياطات الواجب توفيرها عند استخدام مواقع التواصل الاجتماعي، كما يجب توعيتهم بضرورة التحلي بثقافة التبليغ في الوقت اللازم لتمكين الجهات المعنية من القيام بدورها في الوقت المناسب، والتوصل إلى مرتكبي الجرائم.
- **تفعيل القوانين على أرض الواقع وتطبيقها بصرامة:** إذ من بين أكبر الإشكالات التي تسهم في انتشار الجريمة الالكترونية، هو الإفلات من العقاب، والتأخر في تفعيل القوانين، وهو يمنح المجرم فرصا لتكرار جرائمه، ولذلك من الضروري تأكيد على تطبيق القوانين، كما يجب أن تتكيف النصوص القانونية مع التغيرات الحاصلة في هذا المجال، كما يتوجب إنشاء محاكم متخصصة بالجرائم الإلكترونية، نظرا للانتشار الواسع لهذه الجرائم. (سمير 2017، 275)



3. المؤسسات الأمنية المسخرة للتصدي للجرائم السيبرانية :

إن المحيط الكمي لإجرام المعلوماتي في الجزائر غير واضح لعدم وجود دراسات وبحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في بلادنا جراء هذا النمط الاجرامي. وإن كانت الجزائر ليست بمنادى عن خطورة الجرائم المعلوماتية طالما أنها تحتل جزءا من الفضاء الإلكتروني خاصة فيما يتعلق بالحاسوب المالية وبعض الهيئات الحكومية التي يعتبر اختراق مواقعها ضمن حجم الأضرار الناتجة عن الجريمة المعلوماتية.

1.3 مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني: CPLCIC

تم إنشاؤه سنة 2008 وبعد الجهاز الوحيد المختص بهذا الصدد في الجزائر، ويهدف إلى تأمين المنظومة المعلوماتية للأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رايس، وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادي أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك. (خيرة 2010، 78)

ويقوم هذا المركز بمساعدة الأجهزة الأمنية الأخرى بالتعاون من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال استغلال المعلومة من خلال تنسيق مع وزارة العدل وكذا من خلال معهد خاص بعلم الإجرام لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، فالجزائر تعمل جاهدة للاستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها: (هند 2008، 41)

الوقاية: وتشمل حملة تحسيسية وتوعية بالتنسيق مع وزارة التضامن الوطني والأسرة، والعمل على ملتقيات ومحاضرات وأياما دراسية ومنتديات دولية، ومشاركة في منتديات صحفية وحصص تلفزيونية وإذاعية وغيرها من وسائل النشر والإشهار.

المكافحة: توعية الجزائريين من خلال استعمالهم لشبكات التواصل واستخدام الأنترنت وذلك من خلال تعليقاتهم المدافعة عن الجزائر ومعرفة الأخطار بسلوكيات مشبوهة أو اعتداءات عبر نشر فيديوهات توصل إلى الجناة، مما يسهل التحقيق لدى مصالح الدرك وإلقاء القبض على المشبوهين ومرتكبي الجرائم في الوقت المناسب.

2.3 المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني: INCC

مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة.

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني «ببوشاوي»، حيث تم إنشاؤه بموجب مرسوم رئاسي 04/133 المؤرخ في 26 جوان 2004، ودخل حيز الخدمة ابتداء من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و2009 كرسست لتكوين المورد البشري واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة، قانونيا خاصة اثناء معالجة القضايا المعقدة ، وكذا تنظيم دورات الإلتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية، ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات؛ مصلحة البيئة؛ أما فيما يخص مجال الأمن السيبراني هناك مصلحة الإعلام الآلي؛ على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية. (عادل 2014، 64)



3.3 المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني: SCLC

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي انشئت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015. (إدريس 2019، 114).

4.3 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261 وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يرأسها وزير العدل وتضم أساسا أعضاء من الحكومة معينين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء. وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال

الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن جرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

وقد نص سابقا على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال النص: «تنشأ هيئة وطنية وتنظيمها وكيفية سيرها عن طريق التنظيم» أما مهامها فقد أوردت المادة 14 من نفس القانون وتتمثل في: (أسامة، ياسين و عصام 2013، 4).

1.4.3 الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية.. الخ

2.4.3 مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: بحسب نص المادة 14 من القانون 04/09 هناك نوعان من المكافحة تقوم بهما هذه الهيئة :

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجرّها بشأن الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة (ب) من القانون 04/09.

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يقترح المشروع في هذا الفصل إنشاء هيئة وطنية مختصة تتولى مهام أهمها : تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية ومصالح الشرطة القضائية من التحريات التي تجرّها بشأن هذه الجرائم، وما تقوم به أيضا من تجميع المعلومات من نظيرتها في الخارج قصد محاربة هذا النوع الخطير من الإجرام.



5.3 مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة :

بالنظر لحساسية قطاع الدفاع الوطني: أستحدث بتاريخ 06 نوفمبر 2015، على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة"، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية، ومن بين المحاور التي تناولتها الارضية العملياتية لهذه المصلحة، تذكر ما يلي: (جمال 2019، 1289).

- توجيه، تنفيذ وتأطير الاعمال في هذا المجال لا يجب أن يتعدى الإطار الوظيفي أو التنظيمي.

- تطوير وتعزيز المنظومة القانونية لتفادي التجاوزات أثناء استخدام التكنولوجيا وضمان حماية منظومات الاعلام.
- اعتماد التكوين التقني والعلمي لإنتاج الكفاءات والمهارات القادرة على خلق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية وبالتالي تفادي الاخطار الاجرامية.
- غرس ثقافة الاستعمال الكيفي لهذا العنصر الحيوي " تكنولوجيات الاعلام والاتصال "من خلال حملات تحسيسية لكافة مستخدمي المؤسسة بغض النظر عن الرتبة أو الوظيفة.

- الاعتماد وبطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع استجابة للتطورات الحاصلة في مجال التكنولوجيا.
- فتح مجال التعاون الدولي مع المؤسسات العسكرية الاجنبية، خاصة تلك التي لها رصيد في المجال لتبادل الخبرات والاستفادة من تجاربهم في هذا المجال.

كما أصدرت العديد من الوزارات على غرار وزارة البريد والاتصال، المالية، التعليم العالي، الداخلية، تعليمات وتوجيهات إلى مصالحها التنفيذية تتضمن الآليات والكيفيات الواجب تطبيقها من الناحية العملية لتفادي الوقوع في الاخطاء، نلخصها فيما يلي :

- عدم السماح لأي كان من الحصول على معلومات من الأنظمة المعلوماتية الموصولة بشبكة الأنترنت، ما لم يكن هناك إذن أو موافقة من المصلحة المؤهلة قانونا، كما لا يمكن استخدام الحسابات الخاصة للأفراد أو تداول أرقامهم السرية.
- احترام المقاييس المعمول بها في تداول المعلومات المشفرة "إرسالا واستقبالا"، سواء تعلق الامر بالأنظمة المعلوماتية الداخلية للشبكات الوطنية أو الدولية.

- احترام القواعد العلمية والمهنية المعمول بها عالميا في توظيف تكنولوجيا الاعلام سواء لأغراض شخصية أو مهنية حتى لا تعرض الأنظمة للقرصنة، لأن الاستخدام المفرط بقدر ما يخلق ثغرات، فإنه يساهم كذلك في حرمان الآخرين من الاستفادة من خدمات التكنولوجيا.

ما يلاحظ في هذا الباب، أن الجهود التي تبذلها الجزائر للإلمام بأهم العناصر الكفيلة بتحقيق الأمن السيبراني، ما زالت بعيدة، لأن الاجراءات الادارية المتخذة لحد الآن من طرف الهيئات المذكورة أعلاه للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تبقى غير كافية وتتطلب المزيد والاستمرارية في الموقف والنهج.

6.3 القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

المادة 211 مكرر 22 ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا.

يقصد بمفهوم هذا القانون، بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آليه ذات صلة بتكنولوجيات الإعلام والاتصال.



"المادة 211 مكرر 23 يمارس وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس القطب صلاحياتهم في كامل الإقليم الوطني."

"المادة 211 مكرر 24 مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و قاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتدقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها:

- الجرائم التي تمس بأس الدولة أو بالدفاع الوطني.

- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.

- جرائم نشر وترويج أنباء مغرضه تمس النظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية.

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.

- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.

- جرائم التمييز وخطاب الكراهية " (الجريدة الرسمية للجمهورية الجزائرية 2021، 8-9)

خاتمة:

تبذل الجزائر جهود هامة في إطار تعزيز منظومة الأمن السيبراني، وذلك من خلال مواكبة التطورات الرقمية المتسارعة، حيث تساهم عبر الاتفاقيات الدولية والإقليمية في ربط وتنسيق الإستراتيجيات الدولية وكذا الوطنية، بقصد إحتواء المد السيبراني في إطار دولي وكذا محلي، حيث تعمل الجزائر على تحديث واستحداث فروع ومؤسسات خاصة بالأمن السيبراني تحت سلطة مصالح الأمن ووزارة الدفاع وكذا المؤسسة القضائية.

رغم كل هاته الجهود إلا أن الجرائم السيبرانية تتميز بكونها عابرة للحدود وسرعة تطورها وتشعبها في مختلف المعاملات والفضاءات الرقمية، الأمر الذي يجعل من الدول في وضع دفاعي ويرفع من تحديات الأمن السيبراني.

قائمة المراجع:

1. معاشي سميرة. (أفريل، 2010). ماهية الجريمة الإلكترونية. مجلة المنتدى القانوني، 07، الصفحات 275-285.
2. السالك فريد كامل. (2000). الجريمة الالكترونية. ندوة التنمية و مجتمع المعلوماتية (الصفحات 1-9). سوريا: مؤتمر الجمعية السورية للمعلوماتية في حلب.
3. رشاد مرعي إسرائيل جبريل. (9 أوت، 2016). الجرائم الإلكترونية " الأهداف - الأسباب - طرق الجريمة ومعالجتها". تم الاسترداد من المركز الديمقراطي العربي <https://democraticac.de/?p=35426>
4. Brown, C. (2015, January-June 1). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology, 9(1), p 55-119. doi:10.5281
5. القانون رقم 04-09. (المؤرخ في 05 أوت 2009). والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجزائر: الجريدة الرسمية رقم 47.
6. يوسف صغير. (2013). الجريمة المرتكبة عبر الانترنت، رسالة ماجستير في القانون. تيزي وزو: كلية الحقوق و العلوم السياسية، جامعة مولود معمري.



7. عبد الرحمن (الأمن الوطني) حملاوي، و (الدرك الوطني) المقدم عز الدين. (2015). الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها / دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية. الملتقى الوطني "الجريمة المعلوماتية بين الوقاية والمكافحة". جامعة محمد خيضر بسكرة.
8. نؤارة باشوش. (23 11, 2021). الإجرام الإلكتروني.. أرقام مرعبة. تاريخ الاسترداد 02 19, 2022، من الشروق أونلاين : shorturl.at/hqrR8
9. بوزادية جمال. (أفريل, 2019). الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات و الآفاق المستقبلية". مجلة العلوم القانونية و السياسية، 10(01)، ص 1262-1293.
10. عطية إدريس. (2019). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. مصادقية، عدد 1، ص 100-121.
11. بارة سمير. (جويلية, 2017). الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني، 4، ص 255-280.
12. رواجي خيرة. (2010). ثقافة الأنترنت: دراسة ميدانية لاستعلامات الشبكة بمدينة تيهيرت. وهران: جامعة وهران، كلية العلوم الإنسانية و الحضارة الإسلامية.
13. علوي هند. (2008). قياس النفاذ إلى تكنولوجيا المعلومات والاتصالات بقطاع التعليم بالشرق الجزائري، أطروحة دكتوراه. الجزائر: جامعة منتوري- قسنطينة، كلية العلوم الانسانية.
14. غزال عادل. (مارس, 2014). مشاريع الحكومة الإلكترونية من الاستراتيجية إلى التطبيق، "مشروع الجزائر : الحكومة الإلكترونية 2013 أنموذجا". مجلة المكتبات والمعلومات، ص 34.
15. بن صادق طيب أسامة، فاطمي ياسين، و بن يحيى فيلاي عصام. (2013). الحكومة الالكترونية، نحو مجتمع المعرفة. معهد البحوث والاستشارات، ص 9.
16. الجريدة الرسمية للجمهورية الجزائرية . (26 أوت, 2021). امر رقم 21-11 المؤرا في 16 محرم عام 1443 الموافق 25 غشت 2021، يتم الأمر رقم 66- 155 المؤرخ في 18 صفر عام 1386 الموافق 8 ليونو سنة 1966 والمتضمن قانون الاجراءات الجزائية. 65، الصفحات 7-9.



الاجرام السيبراني

نبيل مكيد

مخبر البحوث النفسية و الاجتماعية جامعة المدية

mekid.nabil@univ-medea.dz

مقدمة :

مع التطور التكنولوجي الذي يشهده العالم في الآونة الأخيرة، وضرورة استخدام الوسائل التكنولوجية في الحياة اليومية ومع الانتشار الواسع لها وتعدد أصنافها وأشكالها، وأضحى الفرد منا لا يستطيع الاستغناء عنا ويواكب كل محدثاتها وتطوراتها اليومية. لكن سوء استخدام هذه التكنولوجيا فيما سخرت له أو في اطر غير شرعية من شأنه أن يحدث آثار وخيمة على الفرد والمجتمع ، خصوصا إذا ارتبط مصطلح الإجرام بالتكنولوجيا ، أو استخدام التكنولوجيا في أعمال إجرامية أو حتى الترويج لها ، هذا الأخير ينقلب سلبا وتتحول التكنولوجيا من نعمة نقمة .

ومع تنامي معدلات الجريمة خصوصا الالكترونية منها وتهديده المباشر عبر نظم وشبكات المعلومات والانترنت أصبح لزاما على الهيئات الوصية إعداد مخططات للحد من الانتشار الرهيب لها.

هذه الجرائم التي كان لها آثار وخيمة على أنظمة جهاز الحاسب الآلي وتقنية المعلومات والاتصالات وهذا بغرض إتلافها وتعطيلها ، هذا من جهة ومن جهة أخرى قد تكون هذه الوسائل أداة لارتكاب جرائم أخرى كالسرقة والاحتيال والنصب لبطاقات الائتمان والأرصدة والاختلاس والتزوير، والترويج لسلوكيات انحرافه .

1. واقع الجرائم الالكترونية في المجتمع الجزائري قياس الجريمة الالكترونية:

1.1 تعريف الجريمة الالكترونية: اصطلاح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، وعرفها بموجب أحكام المادة 02 من القانون رقم 09-04 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية ، العدد 47 على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات ، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية ، أو نظام للاتصالات الالكترونية.

قد تتحقق الجريمة الالكترونية بمجرد أن ترتكب الجريمة ، أو يسهل ارتكابها عن طريق منظومة معلوماتية ، أو نظام الاتصالات الالكترونية ، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم ، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الاتصالات الالكترونية يندرج ضمن مصطلح المنظومة المعلوماتية (سوير ، جرائم المعلوماتية ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام 2010/2011، 16).

2.1 تعريف الأمن السيبراني: هو النشاط أو العملية ، أو نظم المعلومات واتصالات الدولة حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف ، والاستخدام غير المصرح ب هاو التعديل ، أو الاستغلال .

الأمن السيبراني هو مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات، والتدريب ، وأفضل الممارسات ، وضمان التقنيات التي يمكن أن نستخدمها لحماية البيئة الالكترونية وتنظيم أصول المستخدم .

القدرة على الحماية أو الدفاع عن استخدام الفضاء الالكتروني من الهجمات السيبرانية .



فن ضمان وجود واستمرارية مجتمع المعلومات للأمة ، وضمان وحماية فضاء الانترنت والمعلومات الخاصة به والأصول والبنية التحتية الحيوية.

الأمن السيبراني هو عبارة برامج واليات تقنية ، وقدرات بشرية تفعل لمواجهة أي تعدي على المعلومات الالكترونية بشتى أنواع الجريمة الالكترونية (بارة، 2017).

تُعرف الجرائم الإلكترونية على أنّها أيّ نشاط إجراميّ تعرّض لها أجهزة الكمبيوتر أو أجهزة الشبكات ممّا يؤدّي إلى تعطيلها، أو إتلافها، أو استخدام البيانات والمعلومات التي تحتويها بصورة غير قانونية، أو خليط من جميع الأضرار السابقة معاً، وغالباً ما يكون ذلك عن طريق إصابة أحد الأجهزة بفيروس ينتشر في باقي أجهزة الشبكة.

3.1 الفئات التي تستهدفها الجرائم الإلكترونية: يُمكن تصنيف الجرائم الإلكترونية بناءً على الفئة المستهدفة من الهجوم كالآتي: الجرائم ضدّ الأفراد: تشمل هذه الجرائم عادةً الإزعاجات والمضايقات الإلكترونية، ونشر المحتوى غير الأخلاقي، وجرائم الاحتيال على بطاقات الائتمان، وسرقة الهوية الإلكترونية، والاستغلال، والتشهير أو الإساءة على مواقع الإنترنت.

1.3.1 الجرائم على الممتلكات: تهدف هذه الهجمات للوصول لأجهزة الكمبيوتر وخوادمها وسرقة محتوياتها، حيث تُخرب الأجهزة وتنتهك حقوق النشر والملكية.

2.3.1 الجرائم ضدّ الحكومات: تستهدف هذه الجرائم انتهاك سيادة الدول، والوصول إلى معلومات سرّية، ويُمكن أن تصل إلى شنّ الحروب وأعمال إرهابية.

3.3.1 أمثلة على الجرائم الإلكترونية: يوجد العديد من الأمثلة على الجرائم الإلكترونية التي حدثت في العالم وفي ما يأتي أشهرها السنة الجهة التي تعرّضت للاختراق الأضرار الناتجة عن الاختراق 2016-2013 شركة ياهو سرقة 3 مليار حساب مستخدم، والحصول على ملايين المعلومات الخاصة وكلمات المرور من هذه الحسابات وتمكّن المهاجمون من الوصول إلى حسابات المستخدمين في خدمات أخرى عبر الإنترنت.

في 2014 متاجر التجزئة الأمريكية اختُرقت أنظمة نقاط البيع، وسرق المهاجمون 50 مليون بطاقة ائتمانية شخصية وحصلوا على تفاصيلها. 2016م أكبر المواقع الإلكترونية استُخدم في هذا الهجوم أكثر من مليون جهاز كمبيوتر متصل على الإنترنت واختُرقت أغلبها باستغلال ثغرات أمنية على البرامج، وأدّى الهجوم لإيقاف مجموعة كبيرة من أكبر المواقع على الإنترنت. وفي 2017م مختلف مستخدمي الإنترنت أغلقت خلال هذا الهجوم محتوى 300000 جهاز كمبيوتر حول العالم، وطلب من المستخدمين دفع مبالغ مالية مقابل فكّ التشفير وإتاحة وصولهم لبياناتهم مرّة أخرى (الحيارى، 2012).

4.1 أسباب ارتكاب الجريمة الالكترونية : لا شك أن مرتكبي الجريمة الالكترونية يختلفون عن الجريمة التقليدية ويرجع ذلك لاختلاف الأشخاص من حيث السن والجنس والمستوى التعليمي وغير ذلك من المؤثرات الخارجية كما أن الأسباب والدوافع التي تدفعهم لارتكاب الجريمة هي أيضا تختلف ، حيث أنها العوامل المحركة للإرادة التي توجه السلوك الإجرامي كالحبة والشفقة والبغاء والانتقام وكسب المال ، فهي القوة النفسية التي تدفع الإرادة لارتكاب الجريمة ابتغاء تحقيق غاية معينة ولذلك فإن الجريمة الالكترونية تختلف عن الجريمة التقليدية ، وتبعاً لذلك فإن الأسباب والدوافع التي تدفع الجناة لارتكاب الفعل غير المشروع لها تختلف عن الأسباب والعوامل التي تدفع الجناة لارتكاب الفعل غير المشروع للجريمة التقليدية .

ثمة أسباب ودوافع تتمثل في الرغبة أو الولع بجمع المعلومات التي قد تكون محفوظة في أجهزة الحاسب الآلي أو منقولة عبر الشبكة العالمية للمعلومات كما قد تكون الأسباب والدوافع الرغبة في الأضرار بالغير من جهات معينة وأشخاص وكذلك الرغبة في الربح



والكسب الذي قد يدفع إلى التعدي على الحواسيب ونظم المعلومات إضافة إلى الدوافع الشخصية للجاني لإبراز الذات التي قد تكون سببا في ارتكاب الجريمة المعلوماتية ونذكر بعضا من الأسباب والدوافع فيما يلي :

1.4.1 الرغبة في جمع المعلومات وتعلمها: الذين يقدمون على ارتكاب هذه الجرائم بغية الحصول على الجديد من المعلومات وقد أشار الأستاذ ليفي في احد مؤلفاته الخاصة بقرصنة الأنظمة hackers إلى أن أخلاقيات هؤلاء القراصنة تركز على مبدئين أساسيين هما:

-الدخول إلى أنظمة الحاسب الآلي يمكن أن يعلمك كيف يسير العالم.

-إن جمع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود.

وكثيرا ما نجد أن قراصنة الأنظمة يعلنون أن هدفهم من الوصول للمعلومات ودخولهم للشبكات والحواسيب الالكترونية هو التعلم فقط (مجمع البحوث و الدراسات، 2016، صفحة 7).

2.4.1 الاستيلاء على المعلومات: الإقدام على ارتكاب هذا الجرم بواسطة تقنية المعلومات بهدف الحصول على المعلومة ذاتها والاستيلاء عليها والتصرف فيها يتمثل ذلك في الحصول على المعلومة المحفوظة في الحاسب الآلي أو المنقولة أو تغييرها أو حذفها أو إلغائها نهائيا من النظام، ويختلف الدافع لهذا التصرف فقد يكون دافع تنافسي أو سببه الابتزاز والحصول على مزايا ومكاسب اقتصادية ، كثيرا ما يكون هدف هذه الجرائم ذو طابع سياسي أو اقتصادي.

3.4.1 إلحاق الأذى بأشخاص أو جهات: بعض المجرمين الذين يقدمون على ارتكاب الجريمة عبر شبكة المعلومات العالمية وتقنية المعلومات بصورة عامة يتركز الدافع من ورائها على إلحاق الأذى بأشخاص محددين أو جهات معينة ، وغالبا ما تكون في صورة ابتزاز أو تهديد أو تشهير

4.4.1 تحقيق أرباح ومكاسب مادية: هناك بعض الجرائم الالكترونية التي ترتكب يكون الدافع منها تحقيق أرباح ومكاسب مادية كاستخدام شبكة الانترنت لإعلان عن صفقات تجارية غير مشروعة كصفقات المخدرات والاتجار بالبشر وقد ورد في بحث أعده هشام بشير المستشار الإعلامي للجمعية المصرية لمكافحة جرائم الانترنت أن عصابات الإجرام المنظم استعملت التكنولوجيا الحديثة في تسيير شئون الاتجار في البشر ويرى الباحث أن الاتجار بالبشر عبر الانترنت هو تجارة الالكترونية حيث أن تعريف التجارة الالكترونية تلك التعاملات التي تتم الكترونيا عبر شبكة المعلومات العالمية (الانترنت).

5.4.1 تهديد الأمن القومي والعسكري: بعض الجرائم الالكترونية المهدف منها أسباب ودوافع سياسية كتهديد الأمن القومي والعسكري ومن ذلك ظهر ما يعرف بالتجسس الالكتروني والإرهاب الالكتروني والحرب المعلوماتية كما هو حاصل بين الدول المتقدمة الكترونيا (مجمع البحوث و الدراسات، 2016، صفحة 28) .

5.1 أركان الجريمة الالكترونية: تتمثل أركان الجريمة الالكترونية في:

1.5.1 الركن الشرعي: وهو الصفة غير المشروعة للفعل ، وتتمثل قاعدة التجريم والعقاب فيها من خلال ما ورد في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

2.5.1 الركن المادي: يتمثل في ماديات الجريمة التي تبرز به إلى العالم الخارجي.

3.5.1 الركن المعنوي: وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ.

ويكون المجرم الالكتروني أي الجاني شخصا طبيعيا ذا أهلية وقدرة على تحمل العقوبة او شخص معنوي ، أما المجني عليه يكون في الغالب شخص معنوي ، كالبنوك والشركات وغيرها من المنظمات والهيئات التي تعتمد على الحاسب الآلي (دغش العجمي، 2014)



2. التهديدات السيبرانية وانعكاساتها على الأمن المجتمعي:

واقع الجريمة المعلوماتية في الجزائر ومكافحتها: تعد جرائم الانترنت احد مساوئ تطبيق تكنولوجيا المعلومات والاتصال ، وان الحديث عن موقع الجزائر من التطورات التشريعية لمواجهة الإجرام المعلوماتي يقودنا إلى ذكر أولى بدايات استعمال الانترنت في الجزائر التي تعود لسنة 1993 عن طريق مركز الأبحاث cerist ، وبعد أن تم تحرير القطاع سنة 1998 ازداد عدد مقدمي خدمة الانترنت ومستعمليها ليشهد تزايد غير مسبوق في الوقت الحالي.

وتجدر الإشارة إلى انه رغم تأخر الجزائر في استخدام تكنولوجيا المعلومات لم يقف حائلا دون أن تصدر تشريعات تكفل الحماية الجنائية للأنظمة المعلوماتية وتحفظ حقوق الأفراد من مخاطر الاستخدام السيئ لتكنولوجيا المعلومات ، وضرورة عدم الاكتفاء بالنصوص التقليدية ، بالإضافة الى ذلك فقد ضمن المشرع الجزائري الحماية الجزائية لنظم المعلوماتية من خلال القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 66-156 المتضمن الجرائم المساس بأنظمة المعالجة الآلية للمعطيات ، والذي تم تعزيزه بالقانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، وعليه فان ظاهرة الجريمة المعلوماتية بدأت تظهر في الجزائر إلى سنة 2005 أين سجلت سنة 2009 حوالي 88 حالة شخص متهمتا تتعلق بالجريمة المعلوماتية وتؤكد معطيات أمام ملتقى دولي حول الجريمة المعلوماتية أن هذا النوع من الجرائم لم ينتشر على نطاق واسع في الجزائر غير انه اخذ في التقدم وان المخالفات المسجلة تتعلق بالاطلاع غير الشرعي على البيانات قصد إتلافها والقرصنة ضد المواقع الرسمية والخاصة والدعاية المغرضة والإرهاب وسرقة المعلومات والتعدي على الحياة الشخصية وتستهدف الجريمة المعلوماتية 60% منها تستهدف الإدارات العامة والمؤسسات الصناعية ونسبة 20% الشركات الخاصة و 11% الشركات الأجنبية و 6% الأشخاص (مسكين ، 2020 ، صفحة 618).

1.2 الجريمة الالكترونية المرتكبة باستخدام النظام المعلوماتي: يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية ، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ، وهي أنواع منها الجريمة الواقعة على الأشخاص ، الجريمة الواقعة على النظم المعلوماتية الأخرى ، الجريمة الواقعة على الأسرار

2.2 الجريمة الالكترونية الواقعة على الشخص الطبيعي وتنقسم إلى:

1.2.2 الجريمة الالكترونية الواقعة على حقوق الملكية الفكرية: نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم 03-05 الصادر في 2003 ، والمتعلق بحقوق المؤلف والحقوق المجاورة ، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءة الاختراع.

2.2.2 الجريمة الالكترونية الواقعة على حرمة الحياة الخاصة: كأن يقوم شخص يعمل بالنظام المعلوماتي بأعداد ملف يحتوي على معلومات تخص شخص بدون علمه أو أن يجمع المعلومات بأعداد ملف يحتوي على معلومات تخص شخص بدون علمه أو أن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها باطلاع الغير عليها دون إذن صاحبها وأن يقوم المكلف بحفظها باطلاع الغير عليها دون إذن صاحبها ، أو أن يقوم شخص باختراق معلومات هي بمثابة أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص آخر (سوير ، جرائم المعلوماتية ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام 2010/2011، 34).

3.2.2 الجريمة الالكترونية الواقعة على الأسرار : تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار سواء كانت عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة ، ويتخذ هذا النوع من الجرائم صورتين الأولى تتعلق بالجرائم الواقعة على أسرار الدولة ، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية ، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة ، كالحصول على عائد مادي ممن يهيمه الأمر أو يستخدمها



للضغط على أصحابها من اجل القيام بعمل أو الامتناع عن القيام بعمل (سوير ، جرائم المعلوماتية ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام 2011/2010، 36-38).

4.2.2 الجريمة الالكترونية الواقعة على النظام المعلوماتي: جاء القانون رقم 04-15 الصادر في 2004/11/10 ، المتضمن قانون العقوبات بتجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات ، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ، وتأخذ صور الاعتداء صورتين وهما الدخول والبقاء في منظومة معلوماتية المساس بمنظومة معلوماتية .

3.2 الاستراتيجية الجزائرية: أدرجت الجزائر الأمن السيبراني كإحدى الأولويات في برنامج المواجهة ضد الجريمة الالكترونية والإرهاب الالكتروني ، بل أصبح يشكل جزءا لا يتجزأ من استراتيجيات الدفاع ، لان الدروس المستخلصة من التي لها تجربة في هذا المجال ، أثبتت أن النجاعة في التطبيق وفعالية المعايير والوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكن هناك تخطيط محكم وتنسيق بين الفاعلين في الميدان ، وعليه توجهت الجزائر إلى رسم استراتيجياتها مركزة على النقاط التالية:

- تحديد المخاطر واتخاذ التدابير اللازمة.
- تحديد الهيئات المكلفة بإدارة الأمن .
- تحديد الهيئات المكلفة بالتنسيق.
- تحديد الهيئة المكلفة بالجانب التقني للبحث عن الثغرات وتوجيه التحقيق ، أبقى الهدف في الأخير زيادة قدرات الأمن السيبراني لحماية الأنظمة المعلوماتية وتعزيز سبل المواجهة الوقائية ، التوعية والمواجهة الردعية ، وملاحقة الجريمة (بوازدي، 2019، الصفحات 1277-1278) .

حيث سجلت مصالح شرطة مكافحة الجرائم الالكترونية بالمديرية العامة للأمن الوطني المختصة في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خلال الـ 08 اشهر الأولى من السنة الجارية ، 567 قضية تتعلق بجرائم الانترنت ، تورط فيها 543 شخصا ، ومن خلال معالجة كافة المعطيات التقنية والأدلة المادية المرتبطة بالقضايا السالفة الذكر ، من معالجة 385 جريمة الكترونية من أصل 567 قضية مسجلة ومحل متابعة لفك خيوطها ، وهذا وفق ما توضحه المعطيات الواردة في الجدول التالي:



(1) جدول قضايا جرائم الانترنت

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	نسبة % القضايا المعالجة
جرائم المساس بالأشخاص عبر الانترنت	430	289	365	68%
جرائم الاعتداء على سلامة الأنظمة المعلوماتية	57	31	39	55%
جرائم الاحتيال عبر الانترنت	25	17	32	68%
جرائم التحريض والتطرف عبر الانترنت	14	14	31	100%
الجرائم المخلة بالحياة	12	08	22	67%
جرائم بيع السلع المحظورة عبر الانترنت	06	05	15	84%
جرائم مختلفة (نسخ البرامج دون حق القرصنة)	23	21	39	92%
المجموع	567	385	543	68%

المصدر المديرية العامة للأمن الوطني

التحليل الجنائي أفضى إلى أن عمليات الاحتيال عبر الانترنت استهدفت المواطنين من مختلف الفئات والأعمار عبر الوطن ، حيث يقوم المجرمون بعرض امتيازات أو خدمات و سلع وهمية والإيحاء بالحصول على أموال ما يجز ضحاياهم وفق خطوات احتيالية تدريجية لفتح روابط مشبوهة ومنه تحقيق النتيجة الإجرامية.

وبالموازاة تواصل المديرية العامة للأمن الوطني عبر صفحتها الرسمية على الفيسبوك والتويتر حملة توعوية حول جرائم النصب والاحتيال عبر الانترنت تدعو من خلالها مستعملي شبكات التواصل الاجتماعي والانترنت خاصة الأولياء إلى التحلي باليقظة من حيل المخترقين (الهاكر) والمحتالين الذين يلجئون للرسائل المزيفة التي تمكنهم من الحصول على البيانات الشخصية والكلمات السرية المتعلقة بحسابات ضحاياهم الشخصية أو حتى سرقة هويتهم الرقمية والدعوة إلى مراقبة الأطفال خلال استعمال الانترنت وتوعيتهم المستمرة من مساوئه (مجلة الشرطة).

3. تحديات الأمن السيبراني في مواجهة مخاطر الجرائم الالكترونية: وفي ملحق شهري يصدر عن دورية اتجاهات الأحداث رصدت دعاء الجهني انه كان للتطور السريع للتكنولوجيا ، خاصة الحرب السيبرانية تحديا لمفاهيم الأمن القومي ، حيث



أصبحت قضية الدفاع عن البنية القومية للمعلومات ذات أهمية قصوى وعليه سعت معظم الدول إلى تشكيل جيوش سيبرانية ورصدت ميزانيات ضخمة للتطوير في مجال الهجوم والدفاع والحماية (طالة، 2020، صفحة 65).

وبما أن التهديدات السيبرانية لا تفرق بين مدني وعسكري ، سعت الدول إلى تشكيل هيئات متخصصة في الأمن السيبراني تكون مهمتها :-إعداد الإستراتيجية الوطنية للأمن السيبراني ، والإشراف على تنفيذها.

-وضع السياسات وآليات الحكومة والإرشادات المتعلقة بالأمن السيبراني وتعميمه .

-وضع اطر إدارة المخاطر المتعلقة بالأمن السيبراني وضع اطر الاستجابة للحوادث والاختراقات .

-وضع السياسات والمعايير الوطنية للتشفير، ورفع مستوى الوعي بالأمن السيبراني.

كما يحدد الاتحاد الدولي للاتصالات ITU خمسة معايير لتصنيف مستوى الأمن السيبراني للدول وهي كالتالي : معايير تشريعية ، تقنية ، تنظيمية، بناء القدرات ، ومعيار التعاون، ونظرا لصعوبة الحد من سباق التسلح السيبراني من جهة ، وقصور القانون الدولي في هذا المجال ، نتيجة عدم وجود أي أساس قانوني ينظم اللجوء إلى الحروب السيبرانية من جهة أخرى ، تم إبرام صك قانوني عام 2013 يدعى دليل تالين الذي أعده مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسي الناتو قصد دراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية ، ويجيب دليل تالين على أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية التي تنظمها الدول ، أو تلك التي يقوم بها جهات فاعلة من دون الدول كمفهوم النزاع المسلح في إطار الحرب السيبرانية، وكذا مفهوم الجيوش السيبرانية وكيفية إدارة الحرب السيبرانية من خلال قواعد الاشتباك السيبراني ، وصفه المقاتل السيبراني إضافة إلى إمكانية مراعاة القانون الدولي الإنساني المعروفة كمبدأ التمييز ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكرية المادية كالمطائرات العسكرية بدون طيار.

أما على المستوى الدولي فقد لعبت هيئة الأمم المتحدة عبر القرارات الصادرة عنها التي تدعم الأمن والسلامة في الفضاء السيبراني وتوعية الوعي العالمي بالأمن السيبراني دورا في جذب انتباه الدول الأعضاء إلى أهمية التحديات السيبرانية، كم بذلت جهود عدة من قبل مجموعات عمل متخصصة بدعم من الاتحاد الدولي للاتصالات ، لإقرار مجموعة من المعايير والقواعد التي تضمن الاستخدام السلمي المجال السيبراني (طالة، 2020، صفحة 67).

خاتمة و اهم التوصيات:

وأمام هذا الخطر الذي يحدق بأمن الشعوب واستقرارها ، تسعى جل الدول وراء البحث عن السبل واهم الطرق الناجعة للوقاية و الحماية من أي هجمات سيبرانية محتملة الوقوع ، بتشكيل أنظمة وهيئات وأجهزة للتصدي لهذه الهجمات سواء على الصعيد الإقليمي والوطني وبالخصوص الدولي من جميع الجوانب وعلى رأسها الجانب القانوني باستحداث قرارات جديدة لمواكبة تطور هذه الجرائم المستحدثة .

لكي تتحقق فرضية القضاء على الجريمة السيبرانية والحد منها وانتشارها على مستوى ،أو على الأقل التقليل من تفاقمها ، لا بد من تضافر الجهود على المستوى الدولي والإقليمي لهذا الغرض .

وفر الأمن السيبراني مميزات عديدة و يشكل أفضل الحلول الأمنية لأمن تكنولوجيا المعلومات فهو يوفر الحماية الرقمية، ويعمل على ضمان وطمأننة المتصفح بأنه بعيد كل البعد عن التهديدات السيبرانية، بالإضافة إلى مد تغطية أمنية على جميع الأنظمة والبرامج والأجهزة من السرقة والاستغلال وإلحاق الضرر بها.



ويتعين فهم الجرائم الالكترونية لكي تتمكن من تحديد الخيار الأنسب لآلية الحماية التي نقوم باستخدامها، لأن استعراض لأبرز الهجمات الالكترونية بين المهاجمين لديهم خيارات عديدة أثناء الهجمات لاختراق أنظمة المعلومات وتعطيلها، وكذلك يتعين اتخاذ إجراءات استباقية في حماية الشبكة وتأمينها.

قائمة المراجع :

- الحياري، إ. (2012). فيفري <https://mawdoo3.com>. Consulté le 25 جانفي 2022, sur <https://mawdoo3.com>.
- بوازدية، ج. (2019). الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والآفاق المستقبلية. الجزائر: جامعة الجزائر 3.
- سفيان سوير. (2011/2010). جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام. جامعة أوبكر بلقايد، تلمسان.
- حنان مسكين. (2020). واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر. لة الاكاديمية للبحوث القانونية والسياسية، 4(1)، 618.
- سمير بارة. (جولية، 2017). الأمن السيبراني في الجزائر السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني، جامعة قاصدي مرباح(4)، 257-258.
- عبد الله دغش العجمي. (2014). المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، رسالة الماجستير في القانون العام. جامعة الشرق الأوسط.
- لامية طالة. (2020). التهديدات والجرائم السيبرانية، تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها. مجلة معالم للدراسات القانونية والسياسية، 4(2)، 65.
- مجلة الشرطة. (بلا تاريخ). مجلة الشرطة، المديرية العامة للأمن الوطني. تاريخ الاسترداد 2022، من www.algerie.police.dz.
- (2016). الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها. تأليف مجمع البحوث و الدراسات. عمان: أكاديمية السلطان قابوس لعلوم الشرطة نزوى.



عنوان المداخلة: آليات مواجهة المخاطر السيبرانية في المجتمع الجزائري مقارنة بالنظام الدولي.

لمعريوي ليلي

lamrioui.lila@cu-tipaza.dz

صيلع سعد

saila.saad@cu-tipaza.dz

مقدمة:

بعيدا عن الحديث عن الزوايا المضيق لقصة الإنسان مع الآلة التي تسجل عصرنا ذروة إبداعها متوجة بمختلف ابتكارات تكنولوجيا المعلومات والاتصال، وبعيدا عن انبهارنا بما وصلت إليه هذه التكنولوجيا التي أصبحت تشبه لدى البعض بالآليات الشيطانية القادرة على إحداث التغيير بمعدلات استثنائية، وعلى حل ما سبقها من تكنولوجيا، وما يستجد من مشكلات إلى حد أنها أضحت تضفي لمساحتها السحرية على معظم شؤون حياتنا.

ونظرا لأهمية موضوع الجريمة الإلكترونية التي غزت العالم وأثرت على العلاقات الترابطية في صورها البسيطة، أصبح العالم يواجه إشكالات جديدة فرضتها حراك جديد باتت فيه المعلومة و التكنولوجيا و التحكم فيهما مفاهيم مركزية تؤثر في مختلف التفاعلات الدولية و الوطنية، ولهذا ومن أجله نجد أن المشرع الجزائري تدخل لوضع آليات اللازمة عن طريق التشريع وهو شأن جميع التشريعات المقارنة في محاولة منه القضاء على مثل هذا النوع من الجرائم وهو ما سيتم التطرق إليه من خلال هذا الموضوع عبر طرح الإشكالية التالية: إلى أي مدى وفق المشرع في وضع آليات لمواجهة الجرائم السيبرانية؟ مقارنة بالجهود الدولية للتصدي لها.

حيث سيتم الإجابة على هذه الإشكالية من خلال ثلاث مستويات، يخصص المستوى الأول إلى تعريف الجرائم الإلكترونية والدوافع لارتكابها بينما يعالج المستوى الثاني للصور الجريمة الإلكترونية أما المستوى الثالث فيتمحور في الآليات القانونية لمجابهة الجرائم السيبرانية على المستوى الوطني والدولي.

1. تعريف الجريمة الإلكترونية:

قبل التطرق الى تحديد تعريف الجريمة الإلكترونية من الضروري الوقوف على أهم المصطلحات المرتبطة بحقل المعلوماتية و التي قد نراها تقنية و فنية أكثر مما هي قانونية وسنحاول شرح بعض المصطلحات المستعملة في الجريمة الإلكترونية كما يلي:

1.1. تعريف المصطلحات المستعملة في الجريمة الإلكترونية :

1.1.1. الأمن المعلوماتي: يقصد بالأمن المعلوماتي من الزاوية الأكاديمية ذلك العلم الذي يبحث في نظريات و استراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها (يعيش تمام، 2019، صفحة 14) أو هو مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيا التي يمكن استخدامها في حماية الاتصالات الالكترونية ضد أي حدث من شأنه المساس بتوفير وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة (الجريدة الرسمية 2018، العدد 27، 2018).

أما من الناحية القانونية فحسب ما جاء في المادة 02 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها فإن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال هي " جرائم المساس بأنظمة المعالجة الآلية



للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية" (الجريدة الرسمية 2009، العدد 47، 08-05-2009).

2.1.1. منظومة معلوماتية: يقصد بالمنظومة المعلوماتية كل نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين (الجريدة الرسمية 2009، العدد 47، 08-05-2009) أو هي مجموعة من المكونات ذات علاقة متداخلة مع بعضها تعمل على نحو متكامل داخل حدود معينة لتحقيق هدف أو أهداف مشتركة في بيئة ما وفي سبيل ذلك يقبل مدخلات وينتج مخرجات ويسمح باستقبال مدخلات مرتدة (شوقي يعيش و محمد، ماي 2018، صفحة 17)

3.1.1. الاتصالات الإلكترونية: يقصد بالاتصالات الإلكترونية كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية (الجريدة الرسمية 2009، العدد 47، 08-05-2009). وعلى العموم ومن خلال مقترحات الخبراء التابعين لمنظمة التعاون الاقتصادي والتنمية في الميدان الاقتصادي يمكن تعريف الجريمة السيبرانية بأنها "أي دخول غير قانوني أو غير مصرح به للمعالجة الآلية للبيانات وإرسال البيانات أو إرسال البيانات " ووفقا لوزارة الداخلية الفرنسية فقد عرفت الجرائم الحاسوبية بأنها: "كل الأعمال الإجرامية على شبكات الاتصالات السلكية واللاسلكية بشكل عام وخصوصا على الشبكات المرتبطة ببرنامج تعاون فني للملكية الفكرية والمعروفة باسم شبكة الانترنت " (فريجة محمد، 2011).

2. دوافع الجرم الإلكتروني :

سنستعرض فيما يلي أهم الدوافع التي تؤدي بالجرم الإلكتروني إلى ارتكاب فعله الإجرامي:

2. 2. 1 الدافع المادي: الكثير منا لجرائم الإلكترونية يكون الدافع من ورائها تحقيق الكسب المادي و تحقيق الربح دون عناء او جهد فقط بكبسة زر في لوحة المفاتيح يتم تحويل مبالغ طائلة الى حسابات أخرى.

2. 2. 2 دافع الانتقامي: وقد يكون ارتكاب الجريمة الالكترونية بدافع الانتقام من الضحية و تستهدف أشخاصا طبيعيين أو معنويين وذلك بإرسال رسائل تهديدية تزرع الخوف في نفس الضحية المراد الانتقام منها.

2. 2. 3 السعي إلى التفوق: إذ يعتبر التغلب على النظام المعلوماتي وقهر أساليب الحماية صورة من صور إثبات الذات والتفوق العلمي.

2. 2. 4 الابتزاز: إذ يعتمد الجرم الإلكتروني في هذه الحالة إلى ابتزاز الضحايا وذلك بعد تلاعبه بالنظام المعلوماتي؛ كحصوله على شفرات سرية لأحدى المؤسسات أو على ملفات تتعلق بالحياة الخاصة لبعض الأشخاص ليستغل ذلك لاحقا في ابتزازهم من أجل إجبارهم على القيام بأمور ما لصالحه.

2.2.5 الدافع السياسي: وذلك بغرض الإساءة لدولة ما أو تشويه سمعة حزب منافس أو فضح تصرفات مسؤول حكومي أو بغرض مناهضة نظام حكم ما. (بن يحيى، 2020-2021).

3. صور الجرائم الالكترونية:

تعد مسألة حصر الجرائم الإلكترونية في أنواع محددة مسألة في غاية الصعوبة وذلك نتيجة للتطور السريع والشديد الذي تشهده هذه الجرائم الأمر الذي يظهر معه أنواع جديدة مستحدثة وفيما يلي بعض صور الجريمة الإلكترونية:

3. 1. المساس بأنظمة المعالجة الآلية للمعطيات: و المتمثلة في الدخول أو البقاء عن طريق الغش في منظومة المعالجة الآلية للمعطيات وذلك ما جاءت به المادة **394 مكرر /01** من قانون العقوبات.

- تخريب نظام اشتغال منظومة المعالجة الآلية في المعطيات وذلك بنص المادة **394 مكرر 02** من قانون العقوبات.



- الإدخال أو الإزالة أو التعديل بطريق الغش للمعطيات في نظام المعالجة الآلية للمعطيات بنص المادة **394 مكرر 01** من قانون العقوبات.

- التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في المعطيات المخزنة أو المعالجة أو المراسلة عن طريق المنظومة المعلوماتية عمدا وعن طريق الغش طبقا للمادة **394 مكرر 03**.

- الحيازة أو الإفشاء أو النشر أو الاستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم المعالجة الآلية للمعطيات عمدا وعن طريق الغش المادة **394 مكرر 03**.

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المستهدفة للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام طبقا لنص المادة **394 مكرر 03**.

2.3. جرائم مرتكبة باستخدام مواقع التواصل الاجتماعي: يقصد بمواقع التواصل الاجتماعي أي مكان افتراضي تقدم العديد منها لخدمات لمستخدميها منها التواصل بين الأفراد من مختلف أنحاء العالم، تبادل الأخبار والمعلومات، التعليم وتبادل الثقافات والمعارف بالإضافة إلى الترفيه والتسلية، ولكن أصبحت هاته المواقع مرتعا للعديد من الجرائم من أهمها:

1.2.3. القذف والسب : تعد جرمي السب والقذف الأكثر شيوعا عبر شبكات الإنترنت عموما وشبكات التواصل الاجتماعي خصوصا فهي ترتكب لنيل من كرامة الأشخاص وشرفهم واعتبارهم، كما يمكن أن يكون السب والقذف وجاهيا عن طريق البث المباشر أو كتابيا عن طريق غرف الدردشة أو المجموعات عبر الصفحات الشخصية للفيسبوك، إنستغرام... الخ (هاجر، 2020، صفحة 35)، حيث عرّف المشرع الجزائري جريمة القذف من خلال قانون العقوبات الجزائري في نص المادة **296** منه والتي تنص على ما يلي : "يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف و اعتبار الأشخاص أو الهيئة المدعى عليها أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الإسناد المباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك وإذا قصد به شخص أو هيئة دون ذكر الاسم، ولكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة أما المادة **297** من نفس القانون فعرّفت لنا جريمة السب على ما يلي "يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة"

2. 2. 3. المساس بمجربة الحياة الخاصة: أصبح العديد من رواد مواقع التواصل الاجتماعي ينشرون الشائعات عن حالة أشخاص طبيعيين أو معنويين كنشر خبر سجن أو وفاة أو حصول حادث أو نشر صور مسيئة، فمثل هذه التجاوزات التي تقع عبر الشبكات الاجتماعية تتضمن انتهاك لخصوصيات الأفراد تطبيق نص المادتين **303 مكرر، 303 مكرر 1** في الحالات التي يقوم بها صاحب مواقع التواصل الاجتماعي بالاحتفاظ بصور الأشخاص ونشرها أو نشر مقاطع فيديو أو تسجيل صوتي سري دون علم أو إذن صاحبها.

3. 2.3. جرائم مرتكبة باستخدام شبكة الأنترنت: وهي عديدة و متشعبة يتم من خلالها نصب و الاحتيال على الضحية من خلال تضليله بوجود مشروع يحصل من وراءه على أموال مما يدفعه الى الانسياق وراء تغريير المجرم الالكتروني وقد يلجأ المجرم المعلوماتي الى انتحال شخصية الغير و الاستدراج بغرض الاستفادة من سمعته أو سلطته أو ماله او غيره من الأسباب و يكثر استخدام هذا النمط في الوسط التجاري (عمرو، 2006)، و قد يستعمل المجرم المعلوماتي التصيد في ارتكاب جرمته الالكترونية وهو نوع من الاحتيال الالكتروني يستعمله المجرم في تحقيق أهدافه غير المشروعة.

4.2.3. الإرهاب الالكتروني: يعتبر الإرهاب الإلكتروني من أخطر الظواهر الإجرامية التي تهدد أمن الدول، فهو الصورة المستحدثة للإرهاب التقليدي الذي استغل التكنولوجيا ووسائل الاتصال الحديثة ، وما وفرته من بث الرعب والخوف في نفوس الأفراد و



الاعتداء على أمن الدولة واستقرارها، وفي ظل التفوق الجوي وعصر المعلومات تزايدت النقاشات حول طبيعة الحروب وأصبحت مفاهيم كثيرة مثل "الثورة في الشؤون العسكرية" (Révolution in military affairs) هي الغالبة عند الحديث عن القوة الأمريكية وقدرتها على التحكم في الفضاء المعلوماتي، وارتباط هذا التحكم أساسًا بالقدرة التكنولوجية التي سهّلت من عمليات التحكم بالقوة الجوية، ومن أبرز الأمثلة على ذلك حرب الخليج الأولى التي استطاعت فيها القوات الأمريكية التغلب على القوات العراقية بخسائر قليلة، بفضل التطور في تكنولوجيا الاتصال لدى الأمريكيين (علاء الدين، 2021)، وبالرجوع إلى عام 1998 وهو تاريخ ظهور هذا المصطلح، صاغ كاتب الخيال العلمي ويليام جيبسون Gibdon William تصورا غريبا تحت عنوان: "هلوسة جماعية" يشترك فيها مليارات المشغلين يوميا في كل دولة، كتمثيل للبيانات المستخلصة من بنوك المعلومات في جميع أجهزة الكمبيوتر في العالم

ولتسمية هذه الفكرة، جمع جيبسون كلمة "السبرنطيقا Cybernetics" التي تعني علم التحكم الآلي مع كلمة "الفضاء"، Space وسك منهما مصطلح "الفضاء السيبراني" Cyberspace الذي أصبح حقيقة مع انتشار شبكة الإنترنت على نطاق العالم.

أما المشرع الجزائري فقد تناول تعريف الإرهاب الإلكتروني خلال نص المادة 87 مكرر 11 الفقرة الرابعة من قانون العقوبات الجزائري بأنه: "استخدام تكنولوجيا الإعلام والاتصال من أجل ارتكاب الأفعال الإرهابية....." (قانون العقوبات الجزائري، 2016)

4. الآليات القانونية لمجابهة الجرائم الالكترونية على المستوى الوطني والدول :

نظرا لما تتميز به الجرائم الإلكترونية من خطورة شديدة على المستوى الوطني و الدولي وذلك راجع لسهولة ارتكابها و صعوبة اثباتها، الأمر الذي يتعين معه ضرورة تضافر و تكاثف الجهود الدولية و الوطنية لمكافحة هذه الظاهرة الاجرامية ونظرا لأهمية ابراز آليات ووسائل مكافحة هذه الجرائم خصصنا هذا القسم للحديث عن تلك الآليات وفق النقاط التالية:

1.4. الآليات القانونية لمجابهة الجرائم الالكترونية على المستوى الوطني :

تعتمد الجزائر في مكافحتها لآفة الجريمة الإلكترونية الماسة بالأمن و الاستقرار القيم الاجتماعية و الثقافية إلى تفعيل الآليات القانونية وتكليف كل السلطات (المؤسسة العسكرية، القضائية و الأمنية) بالتنفيذ الصارم للحد من خطورة الجريمة، بحيث أدرجت الجزائر الأمن الإلكتروني كأحد الأولويات في برنامج المواجهة ضد الجريمة الإلكترونية والإرهاب الإلكتروني بل أصبح يشكل جزءا لا يتجزأ من إستراتيجية الدفاع بحيث اعتمدت الجزائر على مجابهة خطر الجريمة الإلكترونية من الناحية القانونية و من الناحية الإدارية كما سنبينه :

1.1.4. من الناحية القانونية:

- من خلال قانون حقوق المؤلف 03-05: حماية الحق الأدبي والمالي للموقع المسجل كمصنف، وحماية قانونية ألي حق آخر يتم الاعتداء عليه مثل الحياة الخاصة للأفراد كالحق في الاسم والصورة والمعلومات الخاصة... وفي كل الأحوال يمكن الفصل بين حماية المصنف المستعمل في الموقع وحماية الموقع في حد ذاته لأنهم يخضعون لقانون حق المؤلف والحقوق المجاورة في الوقت نفسه، ألن حماية الموقع تؤدي بالضرورة إلى عدم محتوياته بما في ذلك المصنف (بوضياف، 2018).
- من خلال تعديل قانون العقوبات 04-15: لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الألى وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون



العقوبات بموجب القانون رقم 04-15 الملوّخ في 10 نوفمبر 2004 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 المادة مكرر 8.

- من خلال القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: لقد جاء في القانون 04-09 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر، ومراقبة الاتصالات الإلكترونية فقد نصت المادة 04 من القانون 04-09 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الإلكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي:

- للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد أمن الدولة، و عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام .
- لضرورة التحقيقات والمعلومات القضائية حينما تصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية
- في اطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

2.1.4. من الناحية الإدارية والمؤسسية:

لتفادي الوقوع في تداخل الصلاحيات بين مختلف الأجهزة الفاعلة في مسائل الأمن و الدفاع الوطني حرص المشرع الجزائري على وضع ضوابط لاحترام الإطار الإداري المنظم لصلاحيات الهيئات المدنية، العسكرية و التقنية في إدارة الاستراتيجية للأمن المعلوماتي ويمكن قراءة ذلك من خلال انشاء الهيئات الوطنية التالية:

1.2.1.4. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: و التي أنشأت سنة 2009 وضعت تحت السلطة المباشرة لوزير العدل حافظ الاختصاص ولم تدخل حيز التنفيذ الا بعد صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08-10-2015 و التي تندرج مهامها في استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني من نشاطات غير مروعة بالإضافة الى تعزيز التنسيق بين مختلف الفاعلين في الميدان و التشديد على ضرورة التعاون بين القطاعين العام و الخاص و المجتمع المدني من أجل نشر ثقافة المواجهة لكل الممارسات التي تخالف القانون وحماية الحقوق و الحريات الأساسية، و العمل على التنسيق من اجل تحديد المسؤوليات لفرض الرقابة الصارمة بعد حصر المجالات المستهدفة من طرف محترفي الجريمة الإلكترونية، مع التوجه الى تحقيق الحوكمة الالكترونية التي تعتمد على المعاملات الالكترونية (شريف، 2016).

وهي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى رئيس الجمهورية (المرسوم الرئاسي، 7 نوفمبر 2021) هذا المرسوم رقم 21-439 أعاد تنظيم الهيئة حيث ألغى بموجب المادة 41 منه المرسوم 20-183، حيث تمارس الهيئة مهامها تحت رقابة السلطة القضائية طبقا لقانون الإجراءات الجزائية والقانون 04-09 هذه المهام مذكورة في المادة 04 من المرسوم 21-439 وتتمثل في تحديد الإستراتيجية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتنشيط وتنسيق عمليات الوقاية مع ضمان المراقبة الوقائية للاتصالات الالكترونية، بالإضافة الى تجميع وتسجيل وحفظ المعطيات الرقمية لأنظمة المعلوماتية وتكوين المحققين المتخصصين بتقديم مساعدة السلطات القضائية ومصالح الشرطة القضائية، ناهيك عن العمل على السهر عن تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي .

هذا وتشكل الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت سلطة رئيس الجمهورية ويقدمان له عرضا عن نشاطاتهما، كذلك تشكل الهيئة من مديرية المراقبة واليقظة الالكترونية.(انظر المادة 5 من المرسوم سالف الذكر).



2.2.1.4. السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: تم استحداث سلطة وطنية لحماية المعطيات الشخصية وذلك وفق ما جاءت به أحكام القانون 18-07 المؤرخ في 10 يونيو 2018 (جريدة رسمية رقم 34، 2018)، وذلك في الباب الثالث منه من المادة 22 إلى غاية المادة 31، حيث نصت المادة 22 منه تنشأ سلطة إدارية مستقلة لدى رئيس الجمهورية تتمتع بالاستقلال الإداري والمالي.

تتشكل الهيئة من ثلاث شخصيات يعينهم رئيس الجمهورية وثلاث قضاة وعضو عن كل من البرلمان بغرفتيه، بالإضافة إلى ممثل عن المجلس الوطني لحقوق الإنسان وممثل عن وزارة الدفاع والشؤون الخارجية وعن لداخلية والعدل والبريد والصحة والتشغيل يتم اختيارهم بالنظر إلى اختصاصهم في معالجة المعطيات ذات الطابع الشخصي طبقا للمادة 23 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المؤرخ في 10 يونيو سنة 2018.

حيث ذكرت المادة 25 منه مهام الهيئة الذي يتمحور أساسا في منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي و اعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، بالإضافة الى تقديم الاستشارات فيما يخص معالجة المعطيات ذات الطابع الشخصي و إصدار العقوبات الإدارية، والتصريح بنقل المعطيات ذات الطابع الشخصي إلى الخارج الأمر بإغلاق معطيات أو سحبها أو إتلافها، تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مرعاه المعاملة بالمثل.

3.2.1.4. المنظومة الوطنية لأمن الأنظمة المعلوماتية: من خلال المرسوم الرئاسي رقم 20-05 المتعلق بوضع المنظومة وطنية لأمن الأنظمة المعلوماتية (جريدة رسمية العدد 04، 20 جانفي 2020)، حيث تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني على مجلس وطني لأمن الأنظمة المعلوماتية حيث يتولى في إطار إعداد الإستراتيجية الوطنية لإعداد منظومات معلوماتية آمنة يعمل بالبت في عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة ودراسة مخطط عمل الوكالة و التقارير مع الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية وعلى تصنيف الأنظمة المعلوماتية و الموافقة على سياسة التصديق الالكتروني للسلطة الوطنية للتصديق الالكتروني طبقا لنص الماد 04 من القانون السالف الذكر.

4.2.1.4. وكالة لأمن الأنظمة المعلوماتية: مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية حيث ذكرت مهام الوكالة في المادة 18 من المرسوم 20-05 ومن أبرز مهامها تحضير الإستراتيجية الوطنية وتنسيق وتنفيذ الإستراتيجية وضمان اليقظة التكنولوجية مع مرافقة الإدارات العامة ، كذلك اعتماد منظومات إنشاء وفحص الإمضاء الالكتروني ، التكوين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية ، تقوم زيادة عن ذلك إبرام مشاريع شراكة في مجال أمن الأنظمة بعد موافقة المجلس وتقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية في مجال امن الأنظمة المعلوماتية

5.2.1.4. مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة: استحدثت بتاريخ 11 جوان 2015 على مستوى دائرة الاستعمال و التحضير لأركان الجيش الشعبي وأوكلت لها مهمة حماية المنظومات و المنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية وتطوير وتعزيز المنظومة القانونية لتفادي التجاوزات اثناء استخدام التكنولوجيا وضمان حماية منظومة الإعلام بالإضافة الى اعتماد التكوين التقني و العلمي لنتاج الكفاءات و المهارات القادرة على خرق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية دون ان ننسى الإعتماد المستمر على البحث العلمي لتطوير وسائل الدفاع استجابة للتطور في مجال التكنولوجيا، بالإضافة الى فتح مجال التعاون الدولي مع المؤسسات العسكرية الأجنبية خاصة تلك التي لها رصيد في المجال لتبادل الخبرات والاستفادة من هذا المجال (فضاء، أكتوبر 2017)



3.1.4. من الناحية العلمية: استنجدت الجزائر بالخبراء الدوليين لتمكين الإطارات الناشطة في المال من جميع الاسلاك لمعرفة أفضل الممارسات في تكنولوجيا الامن و السياسات العامة للأعمال الالكترونية المعمول بها في الخارج كما تم ارسال بعثات للحضور و المشاركة في المؤتمرات الدولية التي تهدف الى اصدار التوصيات المناسبة لآمن وسلامة المعلومات في الفضاء السيبراني كما ساهمت الجامعات ومؤسسات البحث العلمي من خلال تنظيم أيام دراسية وملتقيات اكااديمية نذكر الملتقى الدولي الذي نظمته كلية الحقوق جامعة برج بوعريش بتاريخ 12-04-2017 تحت عنوان " الاجرام السيبراني ، المفاهيم و التحديات " ، وكذا الملتقى الدولي المنظم من طرف قيادة الأركان للجيش الشعبي الوطني بعنوان " الدفاع السيبراني مكون أساسي للأمن و الدفاع الوطني " المنعقد بتاريخ 16-05-2017.

هذا ما يحتم على الدولة الجزائرية أن تحاول رفقة المجموعة الدولية أن تجد حلولاً للوقوف وصد هذا الإجماع العابر للحدود.

2.3. الآليات القانونية لمجابهة الجرائم الالكترونية على المستوى الدولي :

يلعب التعاون الدولي في مكافحة الجرائم دورا كبيرا في الحد منها والتصدي لها، حيث تزيد أهمية هذا التعاون لما يصعب اكتشاف الجناة واستعمالهم للتقنيات الجديدة العابرة للأوطان وبالتالي يؤثرون على أمن الدول واستقرارها، لاسيما أن جرائم الحاسوب والإنترنت هي جرائم عابرة للحدود وقد يساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة واحدة يقع ضحيتها عدد من الأفراد يقيمون في بلدان متعددة (بدرى، 2018، صفحة 60)، وبذلك يظهر الاختلاف بين تشريعات وطرق مكافحة هذا الجرم من دولة لأخرى، مما يؤدي بالزامية التعاون الدولي لمكافحة الإجماع الالكتروني وذلك من خلال التعاون القضائي الدولي والأمني والمساعدة القضائية من خلال تبادل المعلومات ونقل الإجراءات عن طريق الإنابة القضائية فبالرغم من فرض الإجماع المعلوماتي نفسه كظاهرة سلبية على المجتمعات ابتداء من لأفراد والجماعات وزرع كيان الدول في أمنها واستقرارها، فتكاثفت الجهود الدولية والإقليمية للحد من هذه الظاهرة الإجرامية وبذلك يقسم هذا الجزء إلى الجهود الإقليمية لمكافحة الجريمة المعلوماتية (السيبرانية) الجهود الدولية في الاتفاقيات الدولية.

1.2.4. الجهود الإقليمية :

عملت المجموعات الدولية الإقليمية على محاولة التصدي للجرائم الالكترونية بداية من الألفية الثالثة التي انتشرت فيها تكنولوجيا المعلومات والاتصالات وقامت الدول بإبرام عدة اتفاقيات تعاون تتناول أهمها بشيء من التفصيل على النحو التالي:

1.1.2.4. معاهدة بودابست لمقاومة جرائم المعلوماتية و الاتصالات 2001 :

تم اعتماد الاتفاقية وتقريرها التفسيري من لندن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة نوفمبر 2001، وفتح باب التوقيع عليها في 23 نوفمبر 2001 بمناسبة المؤتمر الدولي حول الجريمة الالكترونية.

ترمي الاتفاقية بشكل أساسي إلى مواءمة عناصر القانون الموضوعي الجنائي المحلي والإحكام المتصلة بالجرائم في مجال الجريمة الالكترونية، والتنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم ومتابعة مرتكبيها قضائي، علاوة على الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر أو التي تكون الأدلة المتصلة بها في شكل الكتروني وإلى إنشاء نظام سريع وفعال للتعاون الدولي (التقرير التفسيري ، 185)

هذه الاتفاقية ألزمت الدول المصادقة عليها تكييف تشريعاتها الوطنية وتجريم الافعال ضد سرية وسلامة وتوافر بيانات وأنظمة الكمبيوتر، هذه الجرائم مذكورة في المواد 2 و 3 و 4 و 5 و 6 من الاتفاقية و المتعلقة أساسا بالنفاذ و الاعتراض غير القانوني للأنظمة و التدخل في البيانات و النظام و جريمة إساءة استخدام الأجهزة و الجرائم المتصلة بالكمبيوتر (وهي الجرائم المذكورة من المادة 7 إلى



غاية المادة 10)، بالإضافة الى جريمة التزوير المتعلق بالكمبيوتر المادة 7، و الجرائم ذات الصلة بالمتنوع جاءت في المادة التاسعة 9 حيث ركزت على استغلال الأطفال في المواد الإباحية و أخيرا الجرائم المتعلقة بانتهاكات حق التأليف والنشر والحقوق المجاورة وهو ما جاءت به المادة 10.

2.1.2.4. الاتفاقية العربية لجرائم تقنية المعلومات 2010.

صادقت الجزائر على هذه الاتفاقية بموجب المرسوم الرئاسي 14-252 المؤرخ في 8 سبتمبر 2014.

حيث ألزمت المادة الخامسة من الاتفاقية كل دولة طرف بتجريم الأفعال المبينة في الفصل الثاني منها وذلك وفقا لتشريعاتها وأنظمتها الداخلية (أحمد، 2010)، و المتمثلة في الجرائم التي تستهدف تقنية المعلومات حيث نصت الاتفاقية محل البحث عن الجرائم التي تستهدف تقنية في المواد من 6 إلى 11 وهي جريمة الدخول غير المشروع، وجريمة الاعتراض غير المشروع، بالإضافة لجريمة الاعتداء على سلامة البيانات وجريمة استخدام وسائل تقنية المعلومات وجريمة التزوير وجميع الجرائم التي ترتكب بواسطة النظم المعلوماتية (وهي مجمل الجرائم التقليدية ترتكب بواسطة أنظمة المعلومات كالكذب والسب في وسائل التواصل الاجتماعي).

2.2.4. المؤسسات الإقليمية لمكافحة الجريمة الالكترونية:

تم إنشاء واستحداث مؤسسات إقليمية من أجل التصدي للجرائم الالكترونية، والحد منها والتعاون للتقليل منها، وذلك إنها عابرة للحدود وفي كثير من الأحيان السلوك المادي للجريمة يرتكب في أكثر من إقليم مما زاد من تغول المجرمون الإلكترونيون و المتمثلة فيمايلي:

- الأفريبول كمؤسسة اقليمية لمكافحة الجرائم الالكترونية.

- اليوروبول والأوروجيست آيتين إقليميتين لمكافحة الجريمة الالكترونية.

حيث يعتبر كل من اليوروبول والاوروجيست وكالتين للدفاع الأمني للصد واثبات والتحقيق في الجرائم الالكترونية.

3.2.4. التعاون الدولي ودوره في مكافحة الجريمة الالكترونية:

مع انتشار استخدام الانترنت و الشبكات المعلوماتية و تزايد استخدام الافراد لها، نتج عنها وارتفاع في نسبة الجريمة السيبرانية عن طريق منظمات إجرامية متخصصة في ارتكاب كافة الجرائم السيبرانية عن طريق نشرها في شبكات دولية تتعاون فيما بينها، الأمر الذي يدعو لتضافر الجهود الدولية و الإقليمية و المحلية بغرض التصدي لها و قد أولت الأمم المتحدة وكذا أغلب المنظمات الدولية اهتماما كبيرا بالجرائم السيبرانية لخطورتها الكبيرة عن طريق ابرام مجموعة من الاتفاقات الدولية التي تناولت هذه الجريمة وآليات مكافحتها و التصدي لها، وكانت أهم هذه الاتفاقيات مايلي :

1.3.2.4. اتفاقية برن: تعتبر اتفاقية برن التي تم التوقيع عليها في عام 1971 في سويسرا هي حجر الأساس في مجال الحماية الدولية لحق المؤلف وقد وقعت على هذه الاتفاقية 120 دولة من بينها جمهورية مصر العربية والمملكة العربية السعودية وتعد المادة التاسعة من تلك الاتفاقية هي الأساس لأنها تنص على منح أصحاب حقوق المؤلف حق استثنائي في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان وتم تعديل هذه الاتفاقية في سنة 1979 وازداد عدد الدول فيها إلى 140 دولة في 1999. (بدر، 2018)، وما نلاحظه أن اتفاقية برن تحمي المصنفات بأي شكل كانت أي سواء كانت مؤلفات رقمية أو مصورة كبرامج الحاسب الآلي وذلك ما نصت عليه في المادة 09.

2.3.2.4. معاهدة الويبو: باعتبار أن حقوق الملكية الفكرية من أكثر الحقوق التي يتم انتهاكها بصفة مستمرة بكافة شبكات الاتصال والمعلومات وخصوصا على شبكة الانترنت كان من الضروري إيجاد منظمات تسعى لتوفير الحماية للملكية الفكرية "ويبو" ، حيث تعتبر هذه المنظمة منظمة دولية غير حكومية وإحدى الوكالات المتخصصة التابعة لمنظمة الأمم المتحدة مقرها جنيف وقد



تأسست بموجب اتفاقية ستوكهولم التي أبرمت عام 1967 ودخلت حيز التنفيذ عام 1970. (بدري، 2018)، و عدلت سنة 1979 وبلغ مجموع أطرافها 192 دولة.

وتنقسم معاهدة الويبو بدورها الى معاهدتين اثنتين أولهما معاهدة الويبو بشأن حق المؤلف لسنة 1996 و معاهدة الويبو بشأن الأداء و التسجيل الصوتي لسنة 1996.

3.3.2.4. اتفاقية تريبس: تعد هذه الاتفاقية هي الأخرى من المعاهدات التي تم إنجازها في مجال حماية الملكية الفكرية من السطو عليها خصوصا مع انتشار عمليات السطو الإلكتروني على الأعمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية، والتي قام المجتمع الدولي بإنشائها لهذا الغرض .

4.2.4. المكافحة المؤسسية الدولية للجرائم الالكترونية:

1.4.2.4. التعاون الشرطي الدولي

البدايات الأولية للتعاون الدولي الشرطي ترجع إلى عام 1904 عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ 18 / 5 / 1904 والتي نصت في مادتها الأولى على " تعهد كل الحكومات المتعاقدة بإنشاء أو تعيين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة بعد ذلك أخذ التعاون الشرطي الدولي بأخذ صورة المؤتمرات الدولية".

2.4.2.4. صعوبة التعاون الدولي لمكافحة الجريمة السيبرانية:

في عالم مزدحم بشبكات اتصالية دقيقة ومتطورة تنقل وتشغل المعلومات والبيانات من مناطق متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا ويتاح في ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة مما يسبب لبعض الدول أو الأفراد أو الشركات أضرارا فادحة، مما اضطرت الدول إلى التعاون فيما بينها، ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية إلا ان هناك عوائق تحول دون ذلك وتجعل هذا التعاون صعبا ويمكن إيجاز ذلك في الأسباب التالية:

- هناك إشكالات مرتبطة بالقانون الواجب التطبيق على الجريمة الإلكترونية و المتمثلة في عدم كفاية مبدأ الشرعية الجزائية لاستيعاب كل صور النشاط الاجرامي المتعلق بالجريمة الالكترونية، إضافة الى ضعف التنسيق و التعاون الدولي لمكافحة الجريمة الالكترونية
- عدم وجود نموذج موحد للنشاط الإجرامي وتنوع واختلاف النظم القانونية الإجرائية في بلدان العالم كما انه لا يوجد تعريف محدد للنشاط المفروض الاتفاق على تجريمه وهذا راجع الى قصور التشريع ذاته في كافة بلدان العالم وعدم مساهمته لسرعة التقدم المعلوماتي بالإضافة الى الخلاف حول افضلية تعديل التشريعات العقابية لكي تستوعب نماذج الجريمة المعلوماتية.
- عدم وجود معاهدات ثنائية او جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذا الاجرام.
- قضية التجريم المزدوج وعدم وجود قنوات اتصال من خلال عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة بين الدول المختلفة خاصة ما تعلق منها بالتحقيق والحصول على الأدلة بالإضافة الى إشكالية الاختصاص في هذا النوع من الجرائم كزنها تعد من المشكلات التي تعوق الحصول على الدليل فيها بسبب التداخل و الترابط بين شبكات المعلومات وخاصة الجريمة العابرة للحدود الوطنية.

- الصعوبات المتعلقة بالمساعدات القضائية الدولية ناهيك عن صعوبات التعاون في مجال تدريب رجال القضاء.

- إضافة الى إشكالات المرتبطة بخصوصية الاثبات و التحقيق في الجريمة الالكترونية كونه من الدليل الرقمي غير الملموس المادي ، كذلك صعوبة وتعقيد إجراءات التحقيق في هذا النوع من الجرائم.



النتائج والتوصيات:

من خلال كل ما تم التطرق اليه نخلص إلى أن المشرع الجزائري خطى خطوة هامة في مجال مكافحة الجريمة السيبرانية و الحد من انتشارها، محاولة منه لتحقيق الأمن الإلكتروني وذلك من خلال استحداثه للعديد من النصوص القانونية بداية بتعديله لقانون العقوبات سنة 2004 ثم من خلال صدور القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، زيادة للاستحداث لبعض الهيئات الوطنية التي تقوم بالسهر على محاربة الجريمة السيبرانية بكل صورها، إلا أن هذه الجهود لازالت بعيدة لأن الإجراءات الإدارية المتخذة لحد الآن من طرف الهيئات المختصة للوقاية من هذه الجريمة تبقى غير كافية أمام الكمّ الهائل للإحصائيات المعلن عنها عبر وسائل الإعلام السمعية و البصرية و المقروءة، وتتطلب المزيد من الاستمرارية، وما تجدر به الإشارة اليه أن المشرع لم يستعمل مصطلح موحد في كلتا هاذان القانونان مما قد يخلق فجوة قانونية من حيث ضبط المصطلحات و كذلك ما أدرجته المادة 2 من القانون رقم 09-04 المذكور أعلاه بعبارة "أي جريمة أخرى" مما لا يمكن القياس عليها لمتابعة أي شخص جزائيا، وعلى هذا الأساس يستحسن بالمشرع الجزائري أن يكتف الجهود للعمل على تعديل النصوص القائمة لتستوعب الأمور فيما يخص هذه الجريمة المستحدثة وتوحيد المصطلحات ليحدد بمناسبتها معالم وحدود الجريمة الإلكترونية.

وفي الأخير لا يفوتنا ان ننوه الى بعض النقاط التي نعتبرها مهمة من اجل النهوض ومجابهة الجريمة السيبرانية و التي تتمثل في القاط التالية:

-على المشرع الجزائري استدراك الاختلاف في المصطلحات المستعملة للتنبؤ على الجريمة الالكترونية فتارة يشير لهذه الجريمة بجريمة المساس بأنظمة المعالجة الآلية للمعطيات في القانون العقوبات وهو مصطلح في وتقني أكثر مما هو قانوني وتارة يطلق على الجريمة الإلكترونية جريمة تكنولوجيا الاعلام والاتصال .

-تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة السيبرانية حيث أن التسليم بمبدأ العالمية اضحى ضرورة مجابهة النشاط الاجرامي المعلوماتي بصوره المختلفة بعد استفحال خطره و انتشار آثاره في أكثر من دولة مقابل عجز مبدأ الإقليمية النص الجنائي على التصدي لها .

- القضاء على مشكلة عدم وجود نموذج موحد للنشاط الإجرامي واختلاف النظم القانونية.

-الحد من ظاهرة عدم وجود قنوات اتصال وأسس التعاون الدولي لمواجهة خطر الاجرام المعلوماتي.

- حل مشكلة الاختصاص القضائي وذلك بتسهيل إجراءات الإنابة القضائية.

- محاولة تقريب وجهات النظر فيما يخص تدريب الأطقم (بدري، 2018)

-تنسيق الجهود والاعتماد على الكفاءات و اطلاق مشاريع بحثية باعتبارها جسر للتواصل بين الباحثين والأكاديميين والمهنيين لتعزيز الهياكل الوطنية وتقييم الإنجازات التي تم تجسيدها من طرف الهيئات المدنية او العسكرية المعنية بمكافحة الجريمة السيبرانية.

وجدير بالذكر أنه ظهرت فئة من المجتمع الدولي تنادي بإنشاء محكمة جنائية دولية تعنى بمعالجة الجرائم الإلكترونية (السيبرانية)، والأكد أن المجتمع الجزائري ليس بمنى عن تفشي ظاهرة الإجرام الإلكترونية التي تمس بالأشخاص وأموالهم بالإضافة إلى خطورتها في الجانب الأمني وظهور الإشاعات والأخبار الكاذبة، وخطاب التمييز والكراهية في الكثير من الأحيان تستعمل صفحات من خلال الوسائط الاجتماعية .

قائمة المراجع:

1. المرسوم الرئاسي 21-439 المؤرخ في (7 نوفمبر 2021). الجريدة الرسمية العدد 86.



2. إسماعيل بن يحي، التحقيق في الجرائم الالكترونية، أطروحة دكتوراه. جامعة تلمسان، كلية الحقوق والعلوم السياسية، الجزائر، 2020-2021.
3. أسنهان بوضياف، الجريمة الالكترونية و الاجرائية التشريعية لمواجهتها في الجزائر، 2018
4. قانون رقم 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، 2009-05-08، جريدة الرسمية العدد 47،
5. قانون رقم 04-18 مؤرخ في 10-05-2018 يحدد القواعد العامة بالبريد والاتصالات الالكترونية، الجريدة الرسمية عدد 27، 2018.
6. الحوار الذي أجرته مجلة الجيش مع المسؤول المباشر على مصلحة الامن السيبراني في المؤسسة العسكرية العمليات فضاء، أكتوبر 2017. العدد 651، 34-35.
7. بسام شريف، واقع الحوكمة الالكترونية في الدول العربية، مجلة العلوم الاجتماعية و الانسانية (العدد السادس)، 157، 2016.
8. تمام شوقي يعيش، و خليفة محمد، نظام المعالجة الآلية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري، مجلة جيل الابحاث القانونية المعمقة مركز البحث العلمي بيروت لبنان، بيروت، لبنان، ماي 2018.
9. القانون المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، جريدة رسمية عدد 04، 20 جانفي 2020
10. جريدة رسمية رقم 34. (2018). القانون رقم 07-18.
11. أحمد حمي، صور جرائم تقنية المعلومات وفقا لاتفاقية العربية، 2010، 177.
12. شوقي يعيش تمام، الجريمة المعلوماتية (دراسة تأصيلية)، سلسلة المطبوعات، جامعة محمد خيضر بسكرة، مخبر أثر الاجتهاد القضائي على حركة التشريع، 2019
13. فرحات علاء الدين، من الردع النووي إلى الردع السيبراني، دراسة لدى تحقيق مبدأ الردع في الفضاء السيبراني. مجلة الفكر، 2021
14. بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2018
15. كريم فريجة محمد، الجريمة الالكترونية، مجلة شؤون اجتماعية (العدد 110)، 2011، 138.
16. لاتفاقية الجريمة الالكترونية التقرير التفسيري لاتفاقية الجريمة الالكترونية، سلسلة المعاهدات الأوروبية 185، بدون نشر المؤلف.
17. موسى عمرو، الجرائم المعلوماتية (جرائم الحاسب الآلي في مصر وفي الدول العربية). الاسكندرية، مصر: المكتب الجامعي، 2006
18. واضح هاجر، الحماية الجنائية من إساءة استعمال مواقع التواصل الاجتماعي. خميس مليانة-الجزائر، كلية الحقوق والعلوم السياسية، جامعة الجليلي بونعامة خميس مليانة: جامعة الجليلي بونعامة خميس مليانة، 2020.

البعد الاجتماعي

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني



المخدرات الرقمية ومدى استيعاب المجتمع لأضرارها

Digital drugs and how conscious is the society to their side effects

بوزيان خير الدين

جامعة العربي التبسي - تبسة

نوار بورزق

جامعة العربي التبسي - تبسة

مقدمة

يختلف وعي الشعوب وفقا لاختلاف وعي مجتمعاتها ومدى إلمامهم بتطورات العصر المعاش، وبكمية المكتسبات الثقافية والمعرفية وميكانيزمات التأقلم مع شتى الأحداث والمشاكل الاجتماعية التي تعترض أفرادها وبنائها الاجتماعية، ولعل أسس مواجهة الانحرافات اليومية على اختلاف أنواعها وأشكالها ودرجات تعقيدها، الممارسة من أفراد الأسر بات في حاجة ماسة، وإلى درجة عالية من استيعاب ووعي الأولياء بسلوكيات وممارسات أبنائهم، لما أنتجت التطورات التكنولوجية والفضاءات الرقمية في الزمن الحاضر، وما تمخض عن هذا التقدم من تشابك وتنوع في الانحراف والمخدرات الاستهلاكية، والتي من بينها المخدرات الرقمية، الدخيلة على المجتمع كظاهرة إنحرافية لحداتها وصعوبة تتبع أثرها ومراقبتها.

من هذا المنطلق يمكن طرح التساؤل: ما التهديدات التي تشكلها المخدرات الرقمية على أفراد المجتمع، وما مدى وعي المجتمع بها واستيعابه لمخاطرها؟

1. مدخل مفاهيمي:

1.1. المخدرات:

في اللغة: المخدر بضم الميم وكسر الدال المشدد يعني كل ما يورث الفتور والاسترخاء الملحوظين في البدن، فيقال: خدر العضو أي ضعف فلا يطبق الحركة، ومنه خدر جسمه وخدرت يده وأرجله (إبن منظور، 1997، ص.312).

أما اصطلاحا: فقد عرفت بأنها كل مادة خام مصدرها طبيعي أو مصنعة كيميائيا، تحتوي على مواد مثبطة أو منشطة، إذا استخدمت في غير الأغراض الطبية فإنها تسبب خللا في عمل الدماغ، وتؤدي إلى حالة من التعود والإدمان عليها، مما يضر بصحة الشخص جسديا ونفسيا واجتماعيا (رضوان، 2018، ص.52).

2.1. المخدرات الرقمية: هي عبارة عن خليط من الترددات الصوتية مدتها تتراوح بين 15 إلى 30 دقيقة، ويعد هذا القرع على كلتا الأذنين بمثابة جرعات، وتبعث في كل أذن صوتين متشابهين بترددين مختلفين لكن قريبين جدا من بعضهما (Morlot, Web, 2012.p)، أو هي ملفات صوتية تحتوي على نغمات أحادية أو ثنائية يستمع إليها المستخدم تجعل الدماغ يصل إلى حالة من الخدر تشابه تأثير المخدرات الحقيقية (أبو سريع، 2010)، وتشمل عديد المصطلحات منها:



الملفات الصوتية الرقمية: هي التحويل الرقمي لأصوات نغمات مؤلفة ومعينة من طبيعتها التقليدية التي تخرج من صوت الآلات المستخدمة الأصلية، إلى قطع أو مواد إلكترونية مقروءة، بواسطة تقنيات الحاسبات الآلية، عبر النظام الثنائي -بيتات -، ليسهل نقلها عبر شبكة المعلومات الدولية (شعبان، 2019، ص.172).

الرنين الأذني SonBinaural: هي استجابة سمعية في الدماغ تحدث نتيجة سماع نغمة صوتية بترددتين مختلفتين بين الأذنين اليمنى و اليسرى، مما ينتج عنه الإحساس بصوت ثالث، إذ يقوم الدماغ حينها بإنشاء نغمة ثالثة تتمثل في الفرق في التردد بين الموجتين (رزان، 2021، موقع إلكتروني).

3.1. الوعي :

في اللغة: (بتشديد الياء) تعني: الفقيه، الحافظ، الكيس، أي يميز من هو واع، والوعي كلمة تفيد ضم الشيء، ووعي الشيء أي: حفظه وفهمه وقبله ومن ثمة فهو واع (المعجم الوسيط، 1966، ص.208).
وعى الشيء أي حفظه وفهمه وقبله، بمعنى استوعبه من جميع جوانبه لفظا وقصدا وغاية، والوعي " الحفظ والتقدير والفهم وسلامة الإدراك " (حامد والنجار، 2004، ص.1044).

أما في اللغات الأجنبية:

في اللغة اللاتينية: الوعي كلمة لاتينية الأصل conscieta وتعني معرفة الأشياء على نحو مستمر، فالوعي هو الأفكار إلى تمر في عقل الإنسان، كما أنه عملية أو حالة من الإدراك لخبرات ذاتية في لحظة معينة، أي أن الوعي هو إدراك للواقع بالرجوع للخبرات السابقة (شربال وبلعور، 2018، ص.98).

وفي اللغة الانجليزية: الوعي -Consciousness- تعود إلى الكلمة اللاتينية Conscientia والتي تعني (المعرفة المتشاركة SharedKnowledge) وإن تعددت التسميات كما Awar التي تعني (أن تكون على علم beinginformed)، أو (أن تعرف to know) وغالبا ما تستعمل كلمة awareness التي تفيد اكتساب الخبرة أو الخبرة ذاتها. في حين كلمة Consciousness فهي مشتقة من الكلمة اللاتينية Cumsciare التي تعني (أن تعرف عن to know about) (شربال وبلعور، 2018، ص.98).

في اللغة الفرنسية يذكر كل من شربال وبلعور أن الوعي في قاموس le petit Larousseillustré هو إدراك الفرد للشيء بوضوح سواء حول عالمه الخارجي أو ما بداخله، وهو إحساس داخلي يتبع الفرد للحكم على الأشياء والأفعال في حسننها وسيئها (شربال وبلعور، 2018، ص.99).

والوعي عند علماء النفس: هو الشعور، ويعني: مجموع عمليات إدراك الإنسان لنفسه وللعالم الخارجي المحيط به، والاستجابة لها ويقابل الوعي اللاوعي، بمعنى أن الوعي يسبقه مثيرا ليتم رد الفعل كإدراك وفهم لطبيعة الموقف (العرفي، 1416هـ، ص.24).
وفي علم الاجتماع: يعرفه قاموس علم الاجتماع أنه اتجاه عقلي مستمد من الواقع حيث يمكن الفرد من إدراك ذاته وبيئته ومجتمعه من حيث أنه عضو فيه، أي أن الوعي ينطلق من الواقع أو أنه انعكاس له، يعني إدراك العلاقات بين الأشياء والظواهر وفهمها للتصرف حسب الخبرة التي تأتي تباعا (شربال وبلعور، 2018، ص.101).

ومن الناحية الاصطلاحية: يشير الوعي إلى إدراك الإنسان لذاته ولما يحيط به إدراكا مباشرا وهو أساس كل معرفة، كما يشير الوعي إلى الفهم وسلامة الإدراك، ويقصد بهذا الإدراك إدراك الإنسان لنفسه وللبيئة المحيطة به (العرفي، 1416هـ، ص.131).

4.1. المجتمع:



في اللغة كما جاء في معجم المعاني الجامع، هو عبارة عن فئة من الناس تشكل مجموعة تعتمد على بعضها البعض، يعيشون مع بعضهم وترابطهم روابط ومصالح مشتركة وتحكمهم عادات وتقاليده وقوانين واحدة (معجم المعاني، 2021، موقع إلكتروني). أما اصطلاحاً يعرف على أنه عدد كبير من الأفراد المستقرين الذين تجمعهم روابط اجتماعية ومصالح مشتركة ترافقها أنظمة تهدف إلى ضبط سلوكهم ويكونون تحت رعاية السلطة (الجزولي، 2021، موقع إلكتروني). مما سبق من تعاريف يمكن اعتبار الوعي المجتمعي اتجاه عقلي يمكن الأولياء من إدراك مخاطر المخدرات الرقمية على الفرد والمجتمع، وذلك من خلال فهمهم لماهية المخدرات الرقمية وأنواعها وآليات تأثيرها وإدراكهم لخطورتها. أو هو تلك الدرجة من معرفة الأولياء لمخاطر المخدرات الرقمية، يفهمهم لمعنى هذه المخدرات ومعرفة أنواعها وآليات تأثيرها وإدراكهم لخطورتها، وكيفية حصول الأبناء عليها.

5.1. الضرر:

لغةً هو كل ما ضد النفع، والضرر بالضم الهزال وسوء الحال ومن هنا أتت المضرة، وهي خلاف المنفعة، ويرد الضرر أيضاً بمعنى الضيق والنقصان يدخل في الشيء (إبن منظور، 1997، ص. 153). وقد وردت لفظة الضرر في القرآن الكريم في مواضع كثيرة منها قوله تعالى "لا يستوي القاعدون من المؤمنين غير أولي الضرر" (سورة النساء، الآية 95) وكذلك قوله تعالى "والصابرين في البأساء والضراء" (سورة البقرة، الآية 177) وأيضاً قوله تعالى "وإذا مس الإنسان الضر دعانا لجنبه" (سورة يونس، الآية 12). كما وردت لفظة الضرر في السنة النبوية، ومن ذلك قول النبي صلى الله عليه وآله وسلم "لا ضرر ولا ضرار" (عبد الجبار، 1990، ص. 25).

أما الضرر اصطلاحاً هو الاعتداء أو الأذى الذي يصيب الإنسان بحق من حقوقه أو في مصلحة مشروعة له سواء كان ذلك الحق أو المصلحة متعلقة بسلامة جسمه أو عاطفته أو بماله أو بشرفه أو باعتباره، وسواء كان هذا الحق أو المصلحة مادياً أو معنوياً (سليمان، 1988، ص. 133).

وعليه فالضرر عكس النفع وهو كل ما تم رصده من سلبيات وانعكاسات غير ايجابية أو غير مرضية سواء كانت مادية أو معنوية، مخالفة للواقع (الاجتماعي، القانوني، الثقافي، الاقتصادي...) وغير مقبولة.

6.1. المخاطر: يرتبط مفهوم المخاطر بشكل عام بدرجة عدم التأكد، فكلما كان عدم التأكد أكبر ازدادت احتمالية حدوث تلك المخاطر، وتعرف المخاطر على أنها صورة من التهديد الوشيك الحدوث الذي قد يتعرض له الإنسان في نفسه أو ما يملك (علم الإجرام، 2021، موقع إلكتروني).

2. المخدرات الرقمية:

يطلق عليها في الولايات المتحدة الأمريكية اسم e-drugs، والمخدرات الرقمية ظاهرة اكتشفت منذ ما يقارب قرنين من الزمن، وترتكز على القرع على كلتا الأذنين **le battement binaural**، هذه الملفات الموسيقية القابلة للتحميل من الويب، هي عبارة عن خليط من الترددات الصوتية مدتها تتراوح بين 15 إلى 30 دقيقة، ويعد هذا القرع على كلتا الأذنين بمثابة جرعات **doses**، حيث تبعث في كل أذن صوتين متشابهين بترددين مختلفين لكن قريبين جداً من بعضهما، ويعتقد نتيجة لذلك أنها تحفز موجات الدماغ (Morlot. 2012.p Web).

تعتبر المخدرات الرقمية نوعاً جديداً من المخدرات، يتجسد في شكل ملفات صوتية، تستهدف موجات الدماغ مباشرة، ويعتقد أن بداية ظهورها في مدينة أوكلاهوما بالولايات المتحدة الأمريكية، حيث انتشر عبر وسائل الإعلام خبر أن هناك عدد من الطلاب



ظهرت عليهم أعراض النشوة و السكر، على الرغم من أنهم لم يتعاطوا المخدرات أو الكحوليات، وإنما استمعوا إلى نوع معين من الموسيقى بترددات صوتية خاصة (أبو دوح، 2016).

عرفت المخدرات الرقمية بأنها عبارة عن ملفات صوتية تحتوي على نغمات أحادية أو ثنائية يستمع إليها المستخدم تجعل الدماغ يصل إلى حالة من الخدر تشابه تأثير المخدرات الحقيقية أو على الأقل هذا ما يدعيه البعض، وقد صممت هذه الملفات الصوتية أو المخدرات الرقمية لمحاكاة الهلوس وحالات الانتشاء المصاحب لتعاطي المواد المخدرة عن طريق التأثير على العقل بشكل اللاوعي، هذا التأثير الذي يحدث عن طريق موجات صوتية عبر سمعية للأذن تسمى (الضوضاء البيضاء) مغطاة ببعض الإيقاعات البسيطة لتغطية إزعاج تلك الموجات (أبو دوح، 2016)، وقد عرفها الدكتور صلاح الناجم، المتخصص في اللغة الحاسوبية بجامعة الكويت بأنها عبارة عن ملفات صوتية mp3 مخزنة بصيغة تشغيل خاصة طورته أحد المواقع التجارية باستخدام تقنية مفتوحة المصدر GPL-Open source وتسوقها تحت اسم (المخدرات الرقمية) وكل ملف صوتي يتراوح بين 30 و 40 دقيقة، ويمكن تحميل هاته الملفات وتشغيلها من خلال تطبيق خاص لأنظمة التشغيل iso-android للاستماع لهذه الملفات عن طريق أجهزة الهواتف الذكية والأجهزة اللوحية، كما يتم استعمالها في الحواسيب العادية (الناجم، 2021، موقع إلكتروني).

فالمخدرات الرقمية هي عبارة عن سلسلة من الملفات الصوتية، يتم الاستماع إليها على نحو معين، من خلال الاعتماد على سماعات الأذن، وتؤدي إلى إحداث آثار الهلوسة، أو تعديل الحالات المزاجية والعاطفية والبيولوجية لدى من يستعملها، وتعديل قدرات الفرد على التركيز والتأمل والانتباه، وتعتمد هذه الملفات الصوتية على عمل تزامني بين الصوت وموجات دماغية معينة، وتكون النتائج النهائية بعد سماع هذه الملفات، دخول الفرد في حالة تشابه مع الحالات التي يحدثها تعاطي المخدرات الواقعية، مثال: المارخونا أو الأفيون أو الحشيش وغيرها (الصادق ومحمد، 2020، ص. 327).

لذلك فإن المخدرات الرقمية تقوم على استخدام الاستماع للموسيقى بطرق تتنافى مع استخداماتها الطبيعية بغرض المتعة وتهذئة النفس الراحة والاسترخاء إلى استخدام يعتمد الاستماع للموسيقى بترددات متباعدة بغرض الانتقال بالفرد إلى عالم اللاشعور واللاوعي، وبالتالي الانقطاع عن الواقع والدخول إلى عالم الهلوسة والنشوة (الزبيد، 2019، ص. 6).

1.2. آلية عمل المخدرات الرقمية:

تقوم آلية عمل المخدرات الرقمية على الاستماع إلى الموسيقى باستعمال تقنية القرع على كلتا الأذنين **l'ébatement binaural**، ولفهم آلية عمل المخدرات الرقمية وكيفية تأثيرها على عقل الإنسان وجب علينا توضيح الآلية الفيزيائية التي تعتمد عليها طريقة القرع على كلتا الأذنين **le battement binaural** التي يعود اكتشافها إلى العالم الألماني الفيزيائي هينريك فيلهيلم دوف **Heinrich Wilhelm Dove** عام 1839 .

وتنشأ عمليات الاستجابة الدماغية بفعل تغذية الدماغ بوجود المحفز - المثير، والذي بدوره يستثير عمليات الاستجابة الدماغية على القيام بالنشاط اللازم، إذ يمثل هذا المثير من خلال تقديم نغمتين (صوتين) على شكل موجات، ضمن نطاق موحد مع اختلاف في التردد لإحدى الموجات.

مثال: يتم تقديم نغمة صوتية للأذن اليسرى بمعدل تردد 200 هرتز في الثانية الواحدة، ونغمة صوتية للأذن اليمنى بمعدل تردد 210 هرتز في الثانية الواحدة، وفي ظل هذه الظروف المقصودة فإن عمليات الاستجابة السمعية في الدماغ لا تقوم بسماع صوت ذي نصف القيمة الإجمالية لمجموع الترددات مع ذبذباته أي 205 هرتز في الثانية الواحدة، ففعليا تقوم الاستجابة السمعية بالتأثر بالفارق الموجود في التردد ما بين الإشارتين وهو 10 هرتز، ويعود السبب في ذلك إلى أن هذا الفارق في التردد، والذي يسمى **بالرنين الأذني**، يحتوي في مضمونه على موجات تمتاز بأنها طويلة (الصادق ومحمد، 2020، ص. 327)، الأمر الذي يؤدي إلى حث الدماغ على



توليد موجات بطيئة كموجات (ألفا) المرتبطة بحالة الاسترخاء، أو سريعة كموجات (بيتا) المرتبطة بحالة اليقظة والتركيز، وأن المتلقي يشعر بحالة من اللاوعي مصحوبة بالهلوسات وفقدان التوازن الجسدي والنفسي والعقلي (أبو الدوح، 2016، ص.13). ومن خلال دراسة الدماغ وطبيعة الإشارات الكهربائية التي تصدر عنها بعد تعاطي نوع محدد من المخدرات يمكن تحديد حالة النشوة المرغوبة، حيث كل نوع من المخدرات الرقمية يمكنه أن يستهدف نمطا معيناً من النشاط الدماغي، فمثلاً عند سماع ترددات الكوكايين لدقائق محسوبة فإن ذلك سيدفع لتحفيز الدماغ بصورة تشابه الصورة التي يحفزها بعد تعاطي هذا المخدر بصورة واقعية (جمل الدين، 2018).

وتعد النغمات الصوتية السمعية ذات الترددات ما بين 90-1000 هرتز، هي الأنسب لحدوث الرنين الأذني، وأن لا يتجاوز الفارق في التردد من 35-40 هرتز، ويعد تردد النغمات الصوتية ذات 500 هرتز هو الأفضل للنغمات الصوتية المراد سماعها (Waebeh, H. Calabrese, C. and Zwickey, H. 2007. p13:25:32).

2.2. أنواع المخدرات الرقمية وطريقة استهلاكها:

1.2.2. أنواع المخدرات الرقمية: يقترح المروجون للمخدرات الرقمية عبر مواقعهم على الانترنت على غرار موقع I-doser.com أنواع عدة من المقطوعات الموسيقية بصيغة Mp3 بترددات مختلفة، بحيث أن كل نوع منهم له أثر خاص به، فمنها من له تأثير يحاكي تأثير المواد المخدرة على أنواعها: كالهروين، الكوكايين والحشيش، ومنها من يصل بتعاطيها إلى الاسترخاء وآخر للتركيز وحتى الهلوسة، إلا أن بعض أنواع المخدرات الرقمية تقدمت على سابقتها في الاستخدام، ونجد من بين استخدامات المخدرات الأخيرة إنقاص الوزن، ومسميات أخرى ك: -أبواب الجحيم، و-المتعة في السماء، وغيرها (ميسوم، 2016، ص.167). وهذه بعض أنواع المخدرات الرقمية المعروضة للبيع من قبل موقع I-doser.com، والذي يقوم بتقديم شرح لتأثير ومفعول كل نوع بطريقة تسويقية مدروسة حتى يغري الزبون ويسهل عليه عملية اختيار أين نوع يرغب فيه أو أي حالة يريد الوصول إليها : "الصليب الأبيض White Cross - عقار الاكستازي Extasy - مازوشي Masochist - سعادة سريعة Quick Happy - أول حب First Love - رحلة استراة Projection Astrala - اديرو كروم Adreno Chrome - ماريخوانا Marijuana - إثارة Excite - ييفو تواد Bufo Toad - نيتروس Nitrous - ديفينوروم Divinorum - النشوة الجنسية Orgasm - دلتا Delta - حلم واضح LucidDream - الشمس السوداء Black Sunshine - عقار المورفين Morphine - مضاد الصداع النصفي Anti-Migraine - أنسبير Inspire - عقارالاسيدي LSD - خارج الجسد Out Of Body - التخدير Anesthesia - الكحول Alcohol - الكوكايين Cocaine - يد الرب Hand Of God" (Morlot. 2012.p Web).

فمثلاً: يقدم المخدر الرقمي خارج الجسد Out Of Body عل أنه: تجربة فريدة من نوعها، سوف تخرج من جسدك وتستطيع أن ترى نفسك من الأعلى وأنت مستلقٍ على فراشك (Morlot. 2012.p Web). ويقدم المخدر الرقمي الهيروين Heroin: على أن مفعوله أقوى من الأفيون، يمنحك الإثارة الجنسية وكذلك الشعور بالنشوة ورأسك في السماء (Morlot. 2012.p Web).

2.2.2. طريقة استهلاك المخدرات الرقمية: طريقة تعاطي هذا النوع من المخدرات تتم وفق طقوس معينة، حيث تتطلب من المتعاطي أن يجلس في مكان خافت الإضاءة، ويغطي أي أجهزة تعتبر مصدر للتشويش أو الإزعاج، ويرتدي ملابس فضفاضة، ويضع السماعات على أذنيه ويغض عينيه، ويشغل الملف الصوتي، والجانب المخدر من هذه النغمات يكون عند تزويد طرفي السماعة بدرجتين مختلفتين من الترددات الصوتية، والفارق بينهم يكون ضئيل حيث يقدر بما يقارب 30 هرتز أو أقل، ولذلك يجب



أن تكون السماعة بجودة عالية جدا ومن نوع إستريو لتكون بدقة وتركيز عالي، والجدير بالذكر أن زيادة الفرق بين طرفي السماعة يعني زيادة الجرعة (ميسوم، 2016، ص.168).

3.2. مخاطر المخدرات الرقمية:

إن إدمان المخدرات الرقمية يعتبر من المشكلات التي تؤثر بداية على الشخص نفسه، ثم يمتد خطرها من بعدها إلى أسرته، ثم بعد ذلك على المجتمع برمته، سواء من الناحية القانونية والاقتصادية، أو حتى الاجتماعية، حيث تشير التجارب العلمية والدراسات المكثفة إلى أن المخدرات الرقمية تسبب انخفاض في كفاءة الذاكرة وتشنجات عصبية مع فقدان الوعي، حيث أصيب أكثر الذين خضعوا لتجربة المخدرات الرقمية بالاكتئاب وتدهور في القدرات العقلية وخلل شديد في الجهاز السمعي (لوحيدي، 2020، ص.165).

ومن أبرز مميزات المخدرات الرقمية أنها تؤثر مباشرة في دماغ الإنسان، حيث تعمل على تغيير الوعي لدى الإنسان وإيصاله إلى شعور يحاكي ما تؤدي إليه المخدرات التقليدية بمختلف أنواعها، بدءا بالكوكايين مروراً بالهيروين وصولاً إلى الحشيش وقد تصل بمتعاطيها للهلوسة أو إلى الاسترخاء، حيث أكد الدكتور راجي العمدة مستشار طب الأعصاب باللجنة الطبية للأمم المتحدة، أن هذه الجرعات من الموسيقى الصاخبة تحدث تأثيراً سيئاً على مستوى كهرباء المخ وهذا لا يشعر المتعاطين بالابتهاج والنشوة فقط، لأنه يحدث ما يسمى طبياً بلحظة شرود ذهني، وهي أخطر ما يكون، لأنهم يشعرون بشأنها بنشوة واستمتاع.

بينما هي لحظة يقل فيها التركيز بشدة، ويحدث فيها انفصال عن الواقع، وتكرر اختلاف موجة كهرباء الدماغ بهذا العنف وتأثيرها بالصخب لا يؤدي فقط للحظات شرود، ولكن لنوبات تشنج (أبو سريع، 2010، ص.7).

وتشرح الخبيرة الأمريكية في الفيزيولوجيا العصبية بريجيت فورجو Brigitte Forgeot هذه الآليات بقولها: "تعتمد المواد الرقمية على تقنية النقر في الأذنين... الأمر الذي يحث الدماغ على توليد موجات بطيئة كموجات "ألفا" المرتبطة بحالة الاسترخاء وسريعة كموجات "بيتا" المرتبطة بحالات اليقظة والتركيز، وهنا يشعر المتلقي بحالة من اللاوعي مصحوبة بالهلوسات وفقدان التوازن الجسدي والنفسي والعقلي".

وترى "فورجو" أن الاستخدام المفرط للأصوات المحفزة يمكن أن يؤدي على المدى الطويل إلى اضطرابات في النوم أو القلق تماماً كاستخدام المنشطات التي تستعمل في بعض الحالات المرضية كعلاج نفسي (Morlot. 2012.p Web).

ولقد ذكرت عديد الدراسات والبحوث، أن الأفراد الذين يتعرضون إلى عمليات القرع على الأذنين، هم عرضة للدخول في أعراض الاكتئاب والقلق، وتدهور حاد في الحالات المزاجية والانفعالية، بمعنى أنهم يعانون من تحولات كثيرة ومتباعدة وغير مبررة في حالاتهم الانفعالية على مدار اليوم الواحد، وهذا يلقي بتداعيات خطيرة وضارة، على مختلف جوانب حياتهم وتفاعلاتهم مع الآخرين (لوحيدي، 2020، ص.166).

إن انتشار المخدرات الرقمية من أخطر الآفات التي تهدد المجتمع وتعبث بكيانه واستقراره لما تتركه من آثار سلبية على صحة الأبدان والعقول، وتبديد للطاقات والثروات، وما تورثه من خمول واستهتار، تفسد معه العلاقات الاجتماعية، فأمثال هؤلاء يصيرون خطراً على المجتمع يهددون أمنه، بسبب انعزالهم في غرفهم المظلمة عن المجتمع، وبالتالي يتركون المجتمع و يتبعدون عن أسرهم (جبيري، 2015، ص.598)، وتعتبر خطورتها الاجتماعية أشد فتكا من المخدرات التقليدية للأسباب التالية (جبيري، 2015، ص.599):

أ- سهولة الحصول عليها من شبكة الانترنت.

ب- انخفاض تكلفتها المادية ما يصعب على الآباء ملاحظتها.

ج- عدم وجود أعراض جسمانية واضحة على متعاطي المخدرات الرقمية بخلاف الأعراض الواضحة في المخدرات التقليدية.

د- إمكانية الحصول عليها في أي سن حتى الأطفال، لأن الأمر يتطلب سوى جهاز كمبيوتر في غرفة النوم.



هـ- عدم وجود قوانين تمنع وتكافح هذا النوع من السموم السمعية الصوتية والفكرية.

ومما يفاقم خطورة هذا النوع الجديد من المخدرات، هو صعوبة ضبطها، كما أنها قد تقود المدمن إلى طرق أخرى من الانحراف لا يستطيع أحد التكهن بها، لأن كل شيء يجري في عالم افتراضي، كما احتلت أخبار هذا الوباء القادم أغلب المواقع الإخبارية في العالم، مع الإشارة إلى الخوف الأساسي يكمن في إمكانية تطوير هذه الأفكار لتصبح وباء يخرج عن السيطرة وفي الوطن العربي فقد أكدت بعض المواقع أن الكثير من المنتديات العربية بدأت تروج لهذا النوع من المخدرات، حتى بعضها قدم للمشاركين جرعات مجانية (ميسوم، 2016، ص.169).

3. الوعي المجتمعي :

للتطرق إلى عوامل تشكيل الوعي الاجتماعي لابد من التعرف على مكونات وأنواع وأشكال الوعي وذلك على النحو التالي:

1.3. مكونات الوعي الاجتماعي (ميسوم، 2016، ص.169):

1.1.3. القيم : وهي كل التفضيلات إزاء الأشياء والسلوك والوضعيات في الحياة الاجتماعية، والتي تنطلق من المبادئ المعتقد بها كأفكار ذات نجاعة ومردود، وكذا تلك الأحكام التي تطلق على الأحداث والأشخاص والمواقف والتي تؤسس لعلاقات اجتماعية، ومن ثمة فبلورة علاقة بين هذه القيم والسلوك المراد انتهاجه يفضي إلى وعي مستنبط من الواقع الذي هو المحك الأول، دون إغفال المحكّات الأخرى كما القانون ووسائل الضبط الأخرى كالعرف والتقاليد.

2.1.3. الاتجاهات: عادة الاتجاه هو الميل والاستعداد للاستجابة إلى منبه معين بطريقة أو أخرى في ظل ظروف ومتطلبات معينة أيضا، وما دام الأفراد لهم ميول لفعل اجتماعي ما، فهذا يعني وجود اختيار بين أحكام ترجحها الحاجة الاجتماعية والحنمية البيولوجية، وما يلقي إقرار التوجه الاجتماعي السائد لذلك فإنه بين المثير والهدف يوجد إشباع ويوجد تحقيق الدفاع عن الذات، والتعبير القيمي والمعرفة وتحقيق المنفعة، وهي الوظائف الأربعة للاتجاه.

3.1.3. المعتقدات: إن المعتقدات هي كل ما يدخل دائرة إيمان الفرد، ويفضله عن البدائل الأخرى سواء كانت هذه المعتقدات ذاتية تمتد إلى الفرد دون غيره بغض النظر عن أنها سوية أو وسواسية (مرضية)، أو كانت اجتماعية بحيث يكون هذا الإيمان تابع لمعتقد الجماعة دون تمحيص أو حتى اعتراض في حال كان الاعتقاد أيديولوجي. ويوجد المعتقد الديني، ويكون في الغالب خارج محاولات تحرر الأفراد سواء كان الدين وضعيا أو سماويا.

2.3. أنواع الوعي الاجتماعي:

1.2.3. الوعي الفردي: إن اتجاهات الفرد ومواقفه إزاء التجليات الاجتماعية والأحداث هو ما يشكل نمط التعاطي مع أنواع النشاط المادي والمعنوي (الفكري) للفرد وما يسعى إليه كطموح، بمعنى أن وعي الفرد " يرتبط بالوجود المحدد للفرد في جماعة وطبقة ومجتمع معين وبكل أساليب وفرص إشباع حاجاته الروحية والمادية" (مسعود، 2011، ص.103).

وعليه فالوعي الفردي تتحكم فيه الظروف الخاصة للأفراد وطبيعة الجماعة أو المطبقة الاجتماعية التي ينتمي إليها، والتي تشكل البيئة المحددة له وإذا تم الانتقال إلى حلقة أضيق لصيرورة الوعي كعملية ذاتية فهو " العملية التي يقوم بها العقل باستخدام المعرفة المختزنة لديه لتحديد دلالات المدركات الحسية ومعانيها، فالفرد لا يفسر الرسائل التي يستقبلها في معان مطابقة لها تماما، ولكن يكون التفسير في إطار التفاعل بين الرموز التي يتم استقبالها وبين المعرفة السابقة ذات العلاقة التي يستعين بها الفرد المتلقي" (شربال وبلعور، 2018، ص.106).

2.2.3. الوعي الجماعي: من الضروري استبعاد النظرة الضيقة للوعي الجماعي لأنه مختلف حسب البيانات وفي المراحل الزمنية والتاريخية المتعاقبة، ذلك أن الوعي الجماعي هو نتاج التفاعل الحاصل بين الأفراد ككيانات فردية أو جماعية، وكذلك الاحتكاك بين



وعى الطبقات والثقافات الخاصة في المجتمع الواحد. وعليه فالوعي الجماعي هو كل التجليات التي يفرزها المجتمع، ومن ثمة فير "منظومة عامة من الأفكار والنظريات للطبقات حول محمل العلاقات الاجتماعية القائمة، ويمثل فهما كلياً لها، وهذا الفهم الكلي بعد الشكل الأرقى والأعلى للوعي الاجتماعي (مسعود، 2011، ص.103).

3.3. أشكال الوعي الاجتماعي:

يتضمن الوعي الاجتماعي بمفهومه الشامل عدداً من الأبعاد الثقافية والدينية والاقتصادية والسياسية، فالوعي الاجتماعي وعي عام يتضمن إحاطة أفراد المجتمع بمختلف القضايا الاجتماعية والسياسية والاقتصادية وحتى العلمية التي ترتبط بحياتهم وهناك أنواع أخرى من الوعي الاجتماعي مثل الوعي الثقافي والوعي السياسي والوعي الأخلاقي والوعي الديني والوعي الصحي.

3.3.1. الوعي الثقافي: هو أحد أشكال الوعي الاجتماعي الذي يمكن الفرد من إدراك مجتمعه وقضاياها من منظور تاريخي شامل، وتحليل هذه القضايا على مستوى نظري متماسك والقيام بدوره الاجتماعي الملموس في الحفاظ على تراث المجتمع الفكري ومبادئه الأصيلة مستعينا بقدراته ومهارته وكفاءته العلمية والفكرية، لذا يعد الوعي الثقافي من أهم أشكال الوعي الاجتماعي إن لم يكن أهمها جميعاً نظراً لدوره الجوهرية في إعداد الشباب لمواجهة الغزو الثقافي الذي يحاول بسط سيطرته على فكر الأمة وثقافتها (كمال، 2006، ص.24).

3.3.2. الوعي الديني: هو شكل من أشكال الوعي الاجتماعي يمكن الفرد من فهم وإدراك المعارف الدينية وفقاً لرؤية كلية شاملة لا ينزل فيها الفرد عن سياق التاريخ والمجتمع الذي يعيش فيه، ولا تتعارض فيه المصلحة الفردية مع مصلحة المجتمع ولا مقتضيات العصر، وكلما ارتقى الوعي الديني لدى الأفراد كانت تعاملاتهم وفقاً لتصورات المجتمع وثوابته الدينية، ويبرز دور الوعي الديني للشباب في التصدي للأفكار المتطرفة والهدامة التي تعوق تقدم المجتمعات وازدهارها بل وتسعى في خرابها وتدميرها (السيد وآخرون، 2010، ص.113).

3.3.3. الوعي الأخلاقي: وهو جملة من الأفكار والتصورات للسلوك المطلوب والمستحسن، والمبادئ والنظم التي تحكم هذا السلوك في إطار ربط مصالح الفرد والجماعة، وضبط الصراع القائم بين الاتجاهات والأفكار المختلفة التي تهدد قيم المجتمع وظهور قيم جديدة لا تتفق مع ثقافة المجتمع، وتحسين الفرد بالأخلاق الحسنة مما يدفع سلوكه إلى الاتجاه نحو الصواب (كمال، 2006، ص.20).

3.3.4. الوعي الاقتصادي: ويتجه إلى نظام الحياة الاقتصادية لأفراد المجتمع وضبطها ويعكس الروابط بينهم في إطار عملية الإنتاج والتوزيع والتبادل والاستهلاك والدراسة عن طرق تطوير الاقتصاد والنهوض به، ويظهر الوعي الاقتصادي في شكل نظريات اقتصادية ذات ارتباط منطقي توضح مختلف المسائل والقضايا النظرية والعلمية للتطور الاقتصادي، ويرتبط تطور الوعي الاقتصادي باكتشاف القوانين الاقتصادية التي توجه توزيع السلع المادية واستهلاكها (السيد وآخرون، 2010، ص.111).

3.3.5. الوعي الصحي: هو معرفة أفراد المجتمع للمعلومات والحقائق الصحية وإحساسهم بالمسؤولية نحو صحتهم وصحة الآخرين، وإدراك المشكلات الصحية التي يماثل منها المجتمع وكيفية علاجها وتوفير العلاج والإرشادات والنصائح الطبية اللازمة لها (كمال، 2006، ص.22).

3.3.6. الوعي السياسي: وهو مجموعة من القيم والاتجاهات والأسس السياسية التي تتشكل عند الفرد وتمكنه من المشاركة الفعالة في قضايا مجتمعه ومشكلاته من خلال تحليلها والحكم عليها وتحديد موقفه منها والعمل على تغييرها أو تطويرها (السيد وآخرون، 2010، ص.109).

4.3. عوامل تشكيل الوعي الاجتماعي:



المقصود بالعوامل كل ما يهيئ لتشكيل الوعي الاجتماعي ويؤسس له واقعيا وإدراكيا. وهذه العوامل مختلفة ومتعددة حسب طبيعة المجتمع، وتباين فهم الأفراد وأعمارهم، وطبيعة الإيديولوجيا السائدة، وما يرجى تحقيقه في الواقع والمستقبل، كما أن هناك تفاوتات في تلك العوامل ما بين القوة والشدة (الحارثي، 1435هـ، ص.43).

وعلى العموم فإن هذه العوامل يمكن إيجازها في:

1.4.3. الدين وتشكيل الوعي الاجتماعي: يعتبر الدين أحسن وسيلة للضبط الاجتماعي ومصدرا للقيم والمعايير، التي ترتب للأولويات والسلوك بما يتضمنه من تعاليم وحدود وأوامر ونواهي، وسواء كان هذا الدين سماويا أو وضعيا فإن ضوابط الشرعية في الغالب تلقى القبول من طرف الأفراد من خلال الإيمان بها أو على الأقل مراعاتها، وبذلك فإن مضامين الدين تحدد اتجاهات الأفراد في تعاملهم مع الوضعيات والمواقف التي يصادفونها وحسب الديانة المتبعة يكون توقع استجابات الأفراد، والأکید أن عامل الدين لا يمكن عزله عن باقي العوامل الأخرى التي تدخل في تشكيل الوعي الاجتماعي (بدر، 1997، ص.174).

2.4.3. التعلم الاجتماعي وتشكيل الوعي الاجتماعي: إن التعلم كعملية تلقائية وعفوية غير مقصودة تساهم في تشكيل الوعي الاجتماعي من خلال التعرف على أنماط السلوك وتكوين نماذج كأمثلة وكمحركات للتعامل مع الآخرين ومع الأشياء والمواقف التي يصادفها الأفراد. والتعلم الاجتماعي له بيانات اجتماعية متعددة ومختلفة من حيث التأثير، ومن حيث القوة والتساهل، فالبيئة الأسرية وأساليب التربية المطبقة فيها تساعد على تكوين المثل من خلال اكتساب الأفراد فيها لمبادئ التعامل، والقيم الواجب مراعاتها، وكذا الاتجاهات المتوافقة مع ما يعتمد من عادات وتقاليد وأعراف، هذا باعتبار الأسرة السوية والمتجانسة. أما إذا كانت هذه الأسرة غير سوية، فالأكید أن أعضائها سيكونون جانحين ومنحرفين بوعي ما يحقق مصالحهم دون اعتبار للشرعية، ودون اعتبار لأي توافق مع النظام الاجتماعي القائم وبعد الأسرة تأتي جماعة الرفاق وهي تشكل بيئة اجتماعية، حيث يكون لأفرادها قيما مختلفة في بعض أجزائها وجماعة الرفاق هي من الجماعات المرجعية التي يعتبرها الفرد مرجعا واضحا لسلوكه، فهو يتحلى بطباع وقيم وأفكار أعضائها ويقلد سلوكهم ويتأثر بهم سواء كان ذلك بمنحى إيجابي يمثل للمعايير المعمول بها، أو بمنحى سلبي بالعزوف عن القيم والمعايير الاجتماعي المعمول به.

وعليه فجماعة الرفاق تمد الأفراد بقيم اجتماعية ونماذج سلوك تشكل وعيهم الاجتماعي إيجابا وسلبا ما دام الوعي هو انعكاس للواقع العيني المعاش، دون إغفال واقع الطبقة الاجتماعية التي ينتمي إليها الأفراد، والتي تفرض وعيا اجتماعيا ذا طبيعة خاصة لذلك فالتعلم الاجتماعي كتنشئة اجتماعية متعددة البيانات تتضمن إكساب الأفراد القيم الاجتماعية ومعايير السلوك، ووعي ذلك (البياي، 2001، ص.113).

3.4.3. التعليم وتشكيل الوعي الاجتماعي: إن عملية التعليم عملية مقصودة وهادفة لتزويد الأفراد بمجمل المعارف والطرق والأساليب التي تمكنهم من انتهاز الحياة، والتصرف الحسن في المواقف المختلفة، بما يعود بالصالح والمنفعة عليهم، وهذا التعليم يستهدف الفرد منذ صغره إلى أن يصير كبيرا، فيكسبه الشخصية المتزنة، ويزوده بالقيم المثلى ومعايير السلوك الاجتماعي، حتى يبنى لنفسه صورة اجتماعية مكتملة، ومن ثمة فهؤلاء الأفراد يتأثرون لهم إدراكا لا يشدّ عما هو سائد في المجتمع. والتعليم هنا تقوم به مؤسسات تنشئة اجتماعية، وخاصة المدرسة، وهي المحطة الثانية بعد الأسرة التي تنقل الأفراد (الأطفال) من بيئة الرعاية والتربية والتعلم العفوي إلى بيئة التربية والتعليم المقصود، ليتزودوا بالمعارف الممنهجة لأجل اكتساب أفكار وطرق تفكير والوعي بالحيط، والمتوقع حدوثه، فالمدرسة بذلك هي أهم مؤسسة لإكساب الأفراد الوعي بصفة عامة، والوعي الاجتماعي خاصة (شربال وبلعبور، 2018، ص.106).



4.4.3. وسائل الإعلام وتشكيل الوعي الاجتماعي: إن تعدد أشكال ومضامين وسائل الإعلام الحديثة المقروءة والمسموعة والمرئية جعلها من المدخلات المؤثرة في الأفراد سواء تعلق الأمر بالجانب الشخصي أو الاجتماعي أو العلمي، وهذا نظرا لكم المعلومات والمعارف التي تتدفق على الأفراد والتي تتحين تباعا، وخاصة ما يعرف الآن بالإعلام الإلكتروني الذي يعتمد الواقع والافتراض، ويتيح للأفراد خاصية التفاعل وإبداء الرأي، مما يجعلهم غير متلقين فقط، بل متفاعلين ومصادر في ذات الوقت، وهذا ما يسمح لهم بتشكيل مجالات معرفية للخوض في دواليب الحياة المختلفة، واكتساب المعارف وطرق وأساليب التعامل في المواقف المختلفة، وسبل التكيف مع المستجدات، ومن ثمّ اكتساب وعي اجتماعي غير متاح سابقا، لأن الرسائل تؤثر في طريقة إدراك الأفراد، وترسم الصورة الذهنية إزاء المواقف والقضايا المختلفة (شربال وبلعور، 2018، ص.106).

4. وظائف الوعي الاجتماعي وتحقيق أمن المجتمع:

الوعي آلية إدراك عالية المستوى، وهو نشاط متكامل وموحد، لذلك فالقول بوظائف الوعي "خاصة الاجتماعي" لا يعني تجزئته أو حصره في مجال دون آخر، بل ذلك من منظور تصنيفي منهجي يمكن من معرفة أهم وظائفه، وهو بذلك ليس مجرد معطى أو بناء فكري وفقط، بل هو موجود مركب ومعقد يشير إلى نشاط يمتد إلى جوانب مختلفة من حياة الأفراد في المجتمع، فهو يؤدي وظائف متعددة كصقل شخصية الأفراد، ومساعدتهم في تحقيق مصالحهم وفق أحسن الطرق والأساليب، كما أنه هو سبيل للتواصل الجيد بين الأفراد وفق الضوابط المعمول بها، وهو أيضا بمثابة صمام الأمان لضمان أمن واستقرار الفرد وضرورة النظم الاجتماعية بطريقة آمنة تضمن حياة الرخاء والرفاهية لكل مكونات المجتمع، ويمكن الإشارة إلى أهم الوظائف التي يُضمّن من خلال تحقيقها أمن المجتمع واستقراره:

1.4. الوظيفة المعرفية: باعتبار الوعي الاجتماعي فعل تفكير ناتج عن ذات عارفة في مقابل الطبيعة الاجتماعية كموضوع معرفة، ذلك أن الأفراد في سعيهم للمعرفة وإدراك العلاقات يبذلون جهدا كبيرا في التأمل والتقصي والاختيار، لذلك فالوعي الاجتماعي له وظيفة الاطلاع على أساليب الحياة عامة سواء المعرفة المتعلقة بالمصلحة الشخصية أو المتعلقة بالمصلحة الاجتماعية، وكذا مدى التوافق والانسجام مع العادات والتقاليد ومنظومة القيم في كل ما يتصل بالسعي إلى تحقيق أي منفعة، ومدى مشروعية ذلك، ومن ثمّ فالوعي الاجتماعي هو قبولية تفكير وسلوك الأفراد في مواقف معينة (شربال وبلعور، 2018، ص.113).

2.4. الوظيفة التربوية: للوعي الاجتماعي وظيفة تربوية تتجسد بتواصل أفراد المجتمع حسب الأعمار والأجيال لنقل التجارب والخبرات، وما يتصل بحسن الأداء الاجتماعي "وبعبارة أخرى فهي تنقل كل الإرث الثقافي والاجتماعي" (العريفي، 1416هـ، ص.37).

3.4. الوظيفة الإعلامية: يطّلع الوعي الاجتماعي أيضا بوظيفة الإعلام الذي يعني - فيما يعني إيراد الخبر بكل مضامينه الإخبارية منها والتثقيفية، وذلك باعتبار وسائل الإعلام التي تبادت أكثر من أي وقت مضى في صنع التفاعل الاجتماعي الذي يخضع للتحقق الاجتماعي، وكل شيء قد يعاد فيه النظر أو يثبت أو يعدل أو يرفض من خلال صياغة الطرح في نقاش مفتوح قد يؤدي إلى إعادة إنتاج وعي اجتماعي بديل (شربال وبلعور، 2018، ص.113).

4.4. الوظيفة الإيديولوجية: وهي أن الوعي الاجتماعي كعملية ممتدة لها مناحي قوة ومناحي قصور، يسعى لإيجاد نسق فكري يخدم التوجهات والمثل العليا للمجتمع، وكل نظام اجتماعي قائم، والوظيفة الإيديولوجية هذه لا تعني إجماعا قيميا سائدا بقدر ما تعني تخطيط فكري لتكريس توجه قائم يضبط النشاط والعلاقات الاجتماعية تحت إطار سياسي يهيمن على المجالات الأخرى (شربال وبلعور، 2018، ص.113).



5.4. الوظيفة العلمية والنفسية: وهي وظيفة تنطلق من الذات كإقبال على صياغة نموذج معرفي خاص لا يتعارض مع النموذج الاجتماعي السائد باعتبار مجموع المعارف والعلوم التي هي مقياس لكل إنجاز اجتماعي، هذا الإنجاز الذي يلقي القبول اجتماعيا، ويحظى بقناعة شخصية في مواقف مختلفة (شربال وبلعور، 2018، ص.113).

الخاتمة:

من خلال ما تم تقديمه في هذه الورقة البحثية، وحتى يتسنى للمجتمع تحقيق أمنه وسلامة أفراد من كل المخاطر المهددة لسلامته، ومن كل الاستخدامات غير العقلانية للشبكة العنكبوتية، بما تحتويه من انزلاقات وتهديدات لبنانياته الاجتماعية، كالمخدرات الرقمية المتوفرة عبرها، في شكل ملفات موسيقية ملغمة بمحتويات خطيرة تؤثر على دماغ الفرد، يترتب عليها مشكلات اجتماعية لا يمكن تداركها في الغالب، وهو ما سعت إلى إيضاحه هذه الورقة البحثية، مع إبراز ما يستوجب على المجتمع تحقيقه من وعي لأفراده ومكوناته، حتى يجنبهم الضرر الناجم عن الوقوع في مثل هذه الجرائم، ويضمن سلامتهم وأمنهم وصيرورة نشاطاتهم في شتى مناحي الحياة.

قائمة المصادر والمراجع:

القرآن الكريم، رواية ورش.

، لوحيدي فوزي وحامد، علي. (2020). مخاطر المخدرات الرقمية وكيفية مواجهتها. الوادي- الجزائر: الملتقى الوطني حول المخدرات و المجتمع، جامعة حمه لخضر.

البياتي، باسل. (2001). فضائيات الثقافات الرائدة وسلطة الصورة. بيروت: مركز دراسات الوحدة العربية.

الحارثي، محمد سليم مسعد. (1435هـ). الوعي الاجتماعي وعلاقته بالمسؤولية الاجتماعية لدى طلاب المرحلة الثانوية بمدينة الرياض. السعودية: جامعة نايف العربية للعلوم الأمنية.

بدر، أحمد. (1997). الرأي العام طبيعته و تكوينه وقياسه ودوره في السياسة العامة. القاهرة: مكتبة غريب.

كمال، شلدان فايز. (2006). نموذج مقترح لدور الجامعات الرسمية الأردنية في تنمية الوعي الاجتماعي لدى الطلبة من وجهة نظر أعضاء هيئة التدريس والطلبة. الأردن: كلية الدراسات العليا، الجامعة الأردنية.

المعجم الوسيط. (1966). القاهرة: مجمع اللغة العربية.

حامد، عبد القادر والنجار، محمد علي. (2004). الادارة العامة للمجمعات وإحياء التراث. مصر: مجمع اللغة العربية.

سليمان، مرقس. (1988). الوافي في شرح القانون المدني -الفعل الضار والمسؤولية المدنية. القاهرة: مطبعة السلام، المجلد 2، القسم 1، الطبعة 5.

شرارة، عبد الجبار حمد حسين شرارة. (1990). نظرية نفي الضرر في الفقه الإسلامي -دراسة مقارنة بالقانون. جامعة بغداد: رسالة دكتوراه، كلية الشريعة.

شربال، مصطفى وبلعور، الطاهر. (جوان 2018). الوعي الاجتماعي المفاهيم والاختلاف بين علم النفس وعلم الاجتماع. جيجل-الجزائر: مجلة أبحاث نفسية وتربوية، المجلد 9، عدد 3.

العرفي، محمد سعود. (1416هـ). الرياض: العلاقة بين الوعي الاجتماعي والحد من انتشار العقاقير المخدرة، المركز العربي للدراسات الامنية والتدريب. ابن منظور. (1997). لسان العرب. مصر: المطبعة الميرية.

رضوان، رضا اسماعيل. (2015). المخدرات الرقمية تتلاعب بأدمغة النشء. مصر: مجلة الوعي الاسلامي، العدد 604. وزارة الأوقاف والشؤون الاسلامية. أبو سريع أحمد عبد الرحمن. (2010) استخدام الانترنت في تعاطي المخدرات -المخدرات الرقمية. القاهرة: الإدارة العامة للمعلومات والتوثيق.

شعبان، خالد محمد. (2019). ظاهرة إدمان المخدرات الصوتية الرقمية بين الفقه الإسلامي وأهل الخبرة - دراسة مقارنة عند المعاصرين. مصر.

أبو دوح، خالد. (2016). المخدرات الرقمية وتأثيرها على الشباب العربي. السعودية: جامعة نايف العربية للعلوم الأمنية.

علاق، جميلة. (2017). الأمن المجتمعي - مقارنة في المفهوم والعناصر. الجلفة-الجزائر: مجلة البحوث السياسية والإدارية، جامعة الجلفة. المجلد 6، العدد 1.



- ستيبانوف، إيكاترينا. (2011). الاتجاهات المستقبلية للتهديدات الأمنية العنيفة في التطورات العالمية رؤية استشرافية. أبو ظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية.
- الصادق، عادل محمد ومحمد، شيرين حسن. (2020). مستوى الوعي بالذات فيما يتعلق بالمخدرات الرقمية لدى الشباب ودور الجامعة في مواجهتها. مصر: مجلة جامعة الفيوم للعلوم التربوية والنفسية، المجلد 14، العدد 3.
- الزبود، محمد صايل وعودة، طارق. (2019). مستوى وعي طلبة الجامعة الأردنية بظاهرة المخدرات الرقمية. الأردن: مجلة دراسات العلوم الانسانية والاجتماعية، المجلد 46، العدد 1.
- السيد وآخرون. (2010). الروافد الرئيسية في تشكيل الوعي الاجتماعي. مصر: مجلة كلية التربية، جامعة عين شمس. المجلد 02، العدد 12.
- جمل الدين، أمل. (2018). الوجه الآخر للموسيقى وتأثيره على الشباب. مصر: مجلة أمسياس. المجلد 4، العدد 14.
- السرطان، قطان. (2001). الاعلام الأمني والشباب. الرياض: مركز الدراسات والبحوث، أكاديمية نايف للعلوم الأمنية.
- معجم المعاني الجامع. (2021/04/11). 09,05. [http:// www.almaany.com](http://www.almaany.com)
- نجار، رزان. (2021/04/17). ماهي المخدرات الرقمية. 11,00. <http://WWW.NEWS.WEBTEB.COM>.
- الناجم، صالح. (2021.03.28). المخدرات الرقمية وغياب التشريع والبحث العلمي. 11.00. <http://www.alanba.com.kw/ar/kuwait-news/>.
- جبري، ياسين. (2021.04.05). المخدرات الرقمية. 22.20. <http://WWW.ASJP.CERIST.DZ/EN/ARTICLE>
- الجزولي، محمد بن علي البولوي. (2021/04/11). إصلاح المجتمع. 11,05. <http:// www.alquatan.org>
- علم الإحرام. (17.06.2021). 14:46. <https://specialistebayt.com/AR/specialities/q/266720>
- MORLOT Anthony. (2012). Les drogues numériques et ondes binaurales: I-Doser, phénomène de mode ou réel danger ?, Mémoire en vue de l'obtention du Diplôme d'Etat d'Audioprothésiste UNIVERSITE DE LORRAINE, FACULTE DE PHARMACIE.
- A .. Binaural Beat Technology in Humans)2007(Waebbeh, H. Calabrese, C. and Zwickey, H. Pilot Study to Assess. Psychologic and Physiologic Effects. The Journal of Alternative and Complementary Medicine.



المحتوى الرقمي ومدى مساهمته في تفاقم السلوك الإجرامي لدى الأطفال في المجتمع الجزائري

عرض تحليلي لمحتويات - youtube kids -

Digital content and its contribution to the exacerbation of children's criminal behavior in Algerian society- Analytical presentation of YouTube kids' content-

د. نبيح أمينة

Nebih.amina@univ-alger3.dz

د. غراز الطاهر

gherraz2015jijel@gmail.com

مقدمة

أضح المحتوى الرقمي، وبخاصة في العشر سنوات الأخيرة جزءاً لا يتجزأ من حياة الكثير من الأفراد والجماعات، ويظهر هذا جلياً من خلال انتشارها السريع في المجتمعات، ثم إن استخدامها والإقبال عليها لا يقتصر على فئة عمرية أو فكرية معينة أو جنس أو مجتمع بعينه، بل إن الأمر متاح للجميع بغض النظر عن المستويات الفكرية والمشارب العقائدية، كما أن هذه الوسائل وبحكم جاذبيتها لا تقف عند حد معين، فهي دائماً في تجدد مستمر وتأقلم مع المتغيرات الراهنة، الأمر الذي زاد من إقبال الأفراد عليها والتعلق بها.

وبالرغم من تأخر الجزائر نسبياً -حتى عن بعض الدول العربية- في استخدام المحتوى الرقمي بخدماته المتنوعة، التي بدأ الانتشار والاستخدام الفعلي لها في أوساط المجتمع الجزائري أواخر العشرية الأولى من الألفية الثالثة، لكنها في الخمس السنوات الأخيرة عرفت أرقاماً قياسية في عدد مستخدمي هذه المحتويات والمواقع، إذ وصل مثلاً عدد مستخدمي الفيسبوك 19 مليون مستخدم إلى غاية 31 ديسمبر 2019 (internet world stats, 2020).

ومع هذا التطور الكبير في عدد المستخدمين لهاته المحتويات الرقمية في الجزائر، خاصة لدى فئة الأطفال، فرضت عدة تساؤلات نفسها بقوة من قبيل هل يمكن لهذه الوسائل أن تكون مصدراً لاكتساب الثقافة والمعرفة وتطوير الذات وتحسين المستوى الدراسي؟ أم أن آثارها السلبية ستكون السمة الغالبة؟، وهل ستعزل هذه الوسائل الأطفال عن أسرهم ومجتمعهم وحتى عن دينهم، وبالتالي غياب الحضور الاجتماعي لديهم؟، أم أنها ستكون عاملاً مهماً في تعزيز نموهم السليم عقلياً وفيزيولوجياً؟ أو عامل هدم وبرز سلوكيات أقل ما يقال عنها سلوكيات جرمية في أغلب الأحيان.

بناء على التساؤلات السابقة فإن الدراسة تهدف لمعرفة مدى مساهمة المحتوى الرقمي في بروز وتفاقم ظاهرة الاجرام- السلوك الجرمي- لدى الطفل الجزائري، وهذا من خلال القيام بتحليل نماذج من مضمون موقع اليوتيوب الشهير لمعرفة طبيعة الأثر الذي تتركه هذه البرامج سواء كان هذا الأثر سلبياً أو إيجابياً، باختبار فرضيتين أساسيتين في إطار نظرية الحضور الاجتماعي، الفرضية الأولى ذات اتجاه إيجابي أما الثانية فهي ذات اتجاه سلبي.



1. الإطار المنهجي للدراسة:

1.1. الاشكالية:

ينتج عن استخدام المحتوى الرقمي بالنسبة للأطفال في المجتمعات العربية، عامة والجزائر على وجه الخصوص أثاراً إيجابية وأخرى سلبية، فالآثار الإيجابية تتمثل في اكتساب الأطفال لخبرات ومهارات معرفية وعلمية وتحقيق قدرات عقلية، من خلال الألعاب الالكترونية التمرن على مهارات اللعب والتعلم والاكتشاف، ولكن بالمقابل فإنّ لهذه المواقع والمضامين الالكترونية الكثير من السلبيات التي تؤثر على الطفل. وأكثر هذه السلبيات انتشاراً، ظاهرة التوحد، الادمان، الارتباط بالمجتمع الافتراضي والابتعاد عن الواقع الحقيقي، مما يفقده القدرة على تأدية دوره واقياً، سواء في الدراسة أو في الأسرة، مما يكسبه سلوكيات يكتسبها مع الوقت من خلال هذه المضامين سواء كانت ألعاب أو فيديوهات أو رسومات. وعليه جاءت هذه الدراسة لمعرفة مدى مساهمته في المحتوى الرقمي في تفاقم السلوك الإجرامي لدى الأطفال في المجتمع الجزائري.

وعلى هذا الأساس فالسؤال المحوري الذي تنبني عليه الإشكالية هو:

ما مدى مساهمة المحتوى الرقمي في تفاقم السلوك الإجرامي لدى الأطفال في المجتمع الجزائري؟

2.1. تساؤلات الدراسة:

1. ما هو المحتوى الرقمي؟ وما هي خصائصه؟
2. ما هو مضمون المحتوى الرقمي؟
3. ما نقصد بالسلوك الجرمي؟
4. مل هي أهم صور العنف التي تتضمنها المواقع الالكترونية- موقع يوتيوب كيدز- ؟ .

3.1. أهمية الدراسة:

بالرغم من وجود الكثير من الدراسات التي تناولت تأثير المحتوى الرقمي على سلوكيات مستخدميها، إلا أن دراستنا تركز خاصة على السلوك الجرمي عند أهم فئة من فئة المستخدمين وهي فئة الأطفال، وهي أهم فئة في المجتمع، خاصة وأنها تتعرض لهذه المحتويات بشكل عفوي وبدون إدراك لا إيجابياتها أو سلبياتها، وأيضاً دون رقابة من الأولياء أو دون وعي لما تحتويه بعض المواقع الالكترونية وهنا نتحدث بالتحديد عن موقع يوتيوب كيدز.

4.1. الخلفية النظرية للدراسة:

ترتكز هذه الدراسة على نظرية الحضور الاجتماعي (Social Presence Theory (short, williams, & christie, 1976, p. 47)، إذ تقوم هذه النظرية على فكرة التفاعل الاجتماعي بين الأفراد أثناء التواصل ودرجة الحضور الاجتماعي لهؤلاء الأفراد الذي يعتمد على التواصل المباشر مع الآخر، حيث تقاس درجة الحضور هنا بدرجة وعي الشخص بالتفاعل الافتراضي غير الثابت وغير الواقعي (الحلو و اخرون، 2018، ص239) خلف شاشة الهاتف الذكي أو الكمبيوتر أو الألواح الإلكترونية. والحضور الاجتماعي هو قدرة المشاركين في التواصل عبر الإنترنت على تقديم أنفسهم اجتماعياً وعاطفياً كأشخاص حقيقيين وصادقين في آرائهم وانفعالاتهم عبر الوسيلة الاتصالية المستخدمة على غرار مستخدمي وسائل التواصل الاجتماعي. تتأكد أهمية هذه النظرية في ظل انتشار مواقع التواصل الاجتماعي وتزايد عدد مستخدميها في العالم، حيث تدرس تأثير هذه المواقع على التفاعل الاجتماعي في ظل قلة الحضور الاجتماعي لدى المستخدمين في العالم الحقيقي، وتركز على ثلاث عناصر أساسية



هي: المدخلات التي تهم بالدوافع، والعمليات التفاعلية التي تركز على دخول الأفراد في عمليات تواصل اجتماعية تفاعلية، بينما تشمل المخرجات التفاعل والحوار (الحلو و اخرون، 2018، ص 239).

وعليه فإنَّ دراستنا تستفيد من نظرية الحضور الاجتماعي في تحديد مستوى التأثير ونوع هذا التأثير، ثم تفسير النتائج.

5.1. نوع الدراسة ومنهج البحث:

تنتمي هذه الدراسة إلى الدراسات الوصفية التحليلية التي هدفها الحصول على الحقائق المتعلقة بالجوانب النظرية والتطبيقية للموضوع المدروس، والتعرف على الظاهرة بطريقة مفصلة ودقيقة، إذ تقوم البحوث الوصفية عادة على تحليل الحقائق تحليلاً دقيقاً، كما تتميز بكونها تدرس الوقت الحاضر.

يعرف "هويتني Whitney" البحوث الوصفية بأنها تلك "البحوث التي تتضمن دراسة الحقائق الراهنة المتعلقة بطبيعة ظاهرة أو موقف، أو مجموعة من الأشخاص، أو مجموعة من الأحداث، أو مجموعة من الأوضاع" (المزاهرة، 2011، ص 106). وهو أسلوب من أساليب التحليل المركز على معلومات كافية ودقيقة عن ظاهرة أو موضوع محدد، أو فترة زمنية معينة من أجل الحصول على نتائج علمية وتفسيرها بطريقة موضوعية، وبما ينسجم مع المعطيات الفعلية للظاهرة.

ووفقاً لمتطلبات الموضوع اختارنا:

المنهج المسحي، إذ يعتبر المسح من المناهج العلمية الملائمة للدراسات الوصفية التي تعنى بجمع الحقائق واستخلاص دلالاتها طبقاً لأهداف الدراسة، فهو عبارة عن عملية تحليلية لجملة من القضايا الحيوية، إذ بفضلها يمكن الوقوف على الظروف المحيطة بالموضوع الذي نرغب في دراسته، والتعرف على الجوانب التي هي بحاجة إلى تفسير وتقييم شامل (بن مرسل، 2003، ص 172). يُعرف المنهج المسحي على أنه "جهد عملي منظم للحصول على البيانات والمعلومات وأوصاف الظاهرة، أو مجموعة الظواهر موضوع البحث خلال فترة زمنية كافية للدراسة، مستنداً على الطرق الكمية والإحصائية في عرض النتائج" (حسين، 1976، ص 127)، كما أنه التجميع المنظم للمعلومات من المستقصى منهم بهدف الفهم والتنبؤ بسلوك المجتمع محل الدراسة (Donald & Hawkins, 1993, p. 138).

يرى "محمد عبد الحميد": "أنَّ المسح أحد المناهج المستعملة في الدراسات الوصفية" (عبد الحميد، 2004، صفحة 15)، بل يعتبره أنسب المناهج العلمية ملائمة للدراسات الوصفية بصفة عامة، ذلك أنَّه يستهدف تسجيل وتحليل وتفسير الظاهرة في وضعها الراهن، بعد جمع البيانات اللازمة والكافية عنها، وعن عناصرها من خلال مجموعة من الإجراءات التي تحدّد نوع البيانات، وطرق الحصول عليها (عبد الحميد، 1993، ص 122).

6.1. مجتمع البحث وعينة الدراسة:

يتمثل مجتمع البحث في جميع المفردات التي يدرسها الباحث سواء كانت جمهوراً أو مواداً إعلامية، وعلى هذا الأساس لابد من التعرف على ما يحتويه مجتمع البحث من مفردات، إلى جانب التعرف على تكوينه الداخلي تعرفاً دقيقاً، لأنه أساس نجاح اختيار العينة فيما بعد (بوحوش، 1985، صفحة 147)، ويتمثل مجتمع البحث في هذه الدراسة في محتويات موقع يوتيوب كيدز. وبما أنَّه من الصعوبة القيام بمسح كامل لمجتمع البحث، نظراً لعدم توفر الوقت الذي يعد جوهرياً في الدراسات الإعلامية، نظراً للتغيرات السريعة والمتسارعة التي يعرفها هذا الحقل على مدار الساعة، فإنَّ الباحث استخدم أسلوب العينة لإجراء مسح على



بعض برامج الموقع الالكتروني، وهذا باختيار عدد أصغر من مفردات مجتمع البحث، شريطة تمثيلية مفردات العينة لمجتمع البحث، من أجل تحقيق أهداف الدراسة في حدود الوقت والإمكانات المتوفرة. - وسيتم شرح ذلك في الجانب التطبيقي -

7.1. أداة الدراسة:

1.7.1. تعريف أداة تحليل المحتوى:

التعريف الذي يعد من أشمل هذه التعريفات وأوضحها في تحديد مفهوم تحليل المحتوى هو كما ذكره الدكتور العساف وهو: تعريف بيرلسون (عبارة عن طريقة بحث يتم تطبيقها من أجل الوصول إلى وصف كمي هادف ومنظم لمحتوى أسلوب الاتصال) لأنه يؤكد على الخصائص التالية :

- تحليل المحتوى لا يجري بغرض الحصر الكمي لوحدة التحليل فقط وإنما يتعداه لمحاولة تحقيق هدف معين.
- أنه يقتصر على وصف الظاهر وما قاله الإنسان أو كتبه صراحة فقط دون اللجوء إلى تأويله .
- أنه لم يحدد أسلوب اتصال دون غيره ولكن يمكن للباحث أن يطبقه على أي مادة اتصال مكتوبة أو مصورة.

أنه يعتمد على الرصد التكراري المنظم لوحدة التحليل المختارة. (العساف, 1989, 235)

2.7.1. خطوات طريقة تحليل المحتوى

بدأ هذا المنهج في التربية عندما تم نقل المناهج الغربية إلى التخصصات العربية وهناك من يعتبره أسلوبا والآخر يراه أداة والبعض يقول بأنه منهج. بل تعدى ذلك إلى الاختلاف حول خطواته وطريقته، فبعضهم يصنفه على أنه تحليلاً للمضمون , وبعضهم عند الحديث عن خطوات تحليل المحتوى يذكر خطوات المنهج الوثائقي ومن هؤلاء: حسين عزوزي الذي يقول يمكن الحديث عن المنهج التحليلي من خلال استعراض الطرق العلمية التالية:

- **الطريقة التفكيكية :** وهي الطريقة التي تهدف إلى تفكيك وتحليل قضايا ومسائل جوهرية في العلوم الشرعية عامة والتراث الإسلامي على وجه الخصوص وتحتاج إلى تفسير وتعليل.

إن المنهج التحليلي يتخذ من تفكيك وعزل عناصر الشئ الواحد بعضها عن بعض وسيلة لتناول كل عنصر على حدة بالبحث لمعرفة مضمونه وتحليل خصائصه ثم تكون عملية التأليف بين الأفكار الجزئية التي تمخضت عنها عملية التحليل .

- **الطريقة الاستنباطية :** والمراد بها الاستنتاج والاستخراج المعتمد على الاجتهاد، ولعل أبرز ما يميز هذه الطريقة هو طرح مفاهيم وقضايا جديدة لم يسبق طرحها وهذا أمر طبيعي ما دام البحث قد اعتمد منهج الاستنباط والاستنتاج.

الطريقة النقدية: إن تحليل عمل ما لا يكون فقط تفكيكا أو تعليلا أو استنباطا، (عزوزي , 1986, 15) ، إذ يقول نعمة الله حويجي في كتابه تحليل محتوى أدب الأطفال أن السلوك اللغوي للإنسان شفويا كان أو تحريرا ، أدق تعبيرا عن هوية الشخص وميوله واتجاهاته، فإذا حصلنا على عينة كافية من أداء الفرد اللغوي أو التعبيري بوجه عام وأخضعنا هذه العينة لتحليل علمي منهجي فإننا نستطيع أن نتوصل بسهولة إلى معرفة اتجاهاته السياسية والعقائدية . (حويجي , 1995 , 150)

وترى نادية سالم عند حديثها على تحليل المضمون في اللغة العربية أن اللغة العربية تنفرد بسمات خاصة لا يفتن إليها باحثو تحليل المضمون مثل حذف الموصوف والاكتهاء بالصفة للدلالة الصفة عليه وهو في العربية كثير ومثله التوسع في الضمائر لغايات عملية وبلاغية وكذلك البديل وفهم علاقته بالمبدل منه والأفعال التي تتصل بها ضمائر الفاعل أو المفعول به أو هما معا مما يحتم إحصاء هذا الفعل وما اتصل به جملة كاملة. (سالم , 1983 , 49) .



فيما يرى عماد الخالدي استخدام طريقة تحليل المحتوى في التحليل النفسي حيث يكون تحليل محتوى الوثائق والخطب والإنتاج الأدبي إلى تحديد المعالم الشخصية والنفسية لكاتب الوثيقة , وليس للخروج باستنتاجات حول دلالات المحتوى فحسب , بل انه يمكن من خلال تحليل الإنتاج الفكري للشخص, التوصل إلى مؤشرات هامه تلقي الضوء على مشاعره ومعتقداته وطبيعته الشخصية . (الخالدي , 1986 , 100)

2. الإطار النظري للدراسة:

1.2. المحتوى الرقمي.

1.1.2 . تعريف المحتوى الرقمي:

يتمثل في المعلومات المتاحة على الموقع، سواء جاءت في شكل نصوص، أو مواد سمعية أو مصورة ثابتة أو متحركة، والخدمات المتاحة على الموقع، مثل الخدمة المرجعية الرقمية أو الفهارس أو مرصدا البيانات، إضافة الى الإمكانيات الأخرى مثل إمكانية البحث، ولكي تكون هناك قيمة للموقع ينبغي أن يكون محتواه حديث ومعلوماته جديدة، وذلك حسب طبيعة واختصاص الموقع، وعليه أن يكون تاريخ آخر تحديث ظاهر ، فكلما كانت المعلومات حديثة كانت تملك خاصية الجودة اذا ما استوفت باقي الشروط، ومسألة تحديث معلومات الموقع فرضتها ظاهرة النشر السريع خاصة على الانترنت. (الجبيري، 2000، ص 95) وبذلك نعرف المحتوى الرقمي أيضاً باسم الوسائط الرقمية، ويأتي في أشكال عديدة، من النصوص وملفات الصوت وملفات الفيديو إلى الرسومات والصور المتحركة والصور. عادةً ما يشير المحتوى الرقمي إلى المعلومات المتوفرة للتنزيل أو التوزيع على الوسائط الإلكترونية مثل eBook أو iTunes، لكن الكثير في صناعة المحتوى يجادلون بأن المحتوى الرقمي هو أي شيء يمكن نشره. بعد هذا التفكير، من الأسلم أن نقول أنه إذا كنت على الإنترنت، فعلى الأرجح أنك تنظر إلى محتوى رقمي أو تشاهده أو تستمع إليه.

2.1.2. نواع المحتوى الرقمي: نلخصها فيمايلي:

➤ النصوص المكتوبة: المدونات، المقالات، وصف المنتجات.

➤ الصور (المحتوى الصوري).

➤ محتوى الفيديو.

➤ لإنفوغرافيك.

- الكتب الإلكترونية.

- الملفات الصوتية.

2.2. موقع يوتيوب كيدز : youtube kids

1.2.2. تعريف يوتيوب كيدز :

يُعد يوتيوب كيدز إصداراً من تطبيق YouTube الشهير، يستهدف الأطفال ويتميز بالعروض التلفزيونية المنسقة والمدعومة بالإعلانات والموسيقى ومقاطع الفيديو التعليمية والمحتوى الذي أنشأه المستخدمون. وهو مصمم للأطفال من سن ما قبل المدرسة حتى سن 12 وهو متاح كتطبيق وموقع ويب ، ويتيح YouTube Kids إنشاء ملفات تعريف مستخدم فردية لكل طفل، حتى يتمكن كل منهم من تسجيل الدخول ومشاهدة مقاطع الفيديو الموجهة نحو أعمارهم. من أفضل ميزاته هو المؤقت، الذي يتيح لك تعيين حد (يصل إلى ساعة) لأطفالك للعب على التطبيق. (عبد المنعم، 2021)



2.2.2 المحتوى الرقمي الموجودة على YouTube Kids

غالبًا ما يكون YouTube Kids آمنًا، ولكن هناك احتمال ضئيل أن يرى الأطفال العنف أو مجرد أشياء غريبة، بالإضافة إلى إعلانات لأشياء مثل الوجبات السريعة. وجدت دراسة أن 27٪ من مقاطع الفيديو التي يشاهدها الأطفال بعمر 8 سنوات وأقل مخصصة للجمهور المستهدف الأكبر سنًا، مع كون العنف هو نوع المحتوى السلبي الأكثر احتمالًا. من الناحية الفنية، يعد التطبيق بوابة إلى خدمة YouTube الرئيسية ويستخدم خوارزمية لتصفية الأشياء الناضجة وتحويل أشياء الأطفال إلى التطبيق. لكن مقاطع الفيديو غير اللائقة يمكن أن تتجاوز الخوارزمية (عبد المنعم، 2021)

ومنذ إطلاق التطبيق في عام 2015، قامت Google بتحسين جهود التنظيم من خلال إشراك مراقبين بشريين لمراجعة مقاطع الفيديو التي تم الإبلاغ عنها على أنها غير ملائمة على التطبيق الرئيسي شخصيًا وتقديم مقاطع فيديو "تم التحقق منها" (تمت مشاهدتها وموافق عليها من قبل شخص). على الجانب الإيجابي للآباء، يقدم YouTube تحذيرًا عاديًا من أن الأطفال قد يرون شيئًا لا تريدهم أن يروه ويمكنك حظر مقاطع الفيديو غير اللائقة والإبلاغ عنها. (عبد المنعم، 2021)

3.2.2 ضبط أدوات الرقابة الأبوية على YouTube Kids

لإعداد أدوات الرقابة الأبوية، يجب القيام بتسجيل الدخول باستخدام حساب Google الخاص بالمستخدم. يمكن إنشاء رمز مرور شخصي، والذي يعمل كمفتاح رئيسي للوصول إلى إعدادات التطبيق. أو يمكن استخدام اختبار الضرب العشوائي في كل مرة للدخول. (يفترض أن يمنع الاختبار الأطفال من الوصول). ويسمح التطبيق للملفات الشخصية لما يصل إلى ثمانية أطفال، لكل منهم صورته الشخصية وإعداداته الفردية، بما في ذلك الحدود الزمنية ورمز المرور الشخصي لكل طفل حتى لا يتمكنوا من الوصول إلى الملف الشخصي لبعضهم البعض

. الشيء الرئيسي الذي سيحتاج المستخدم إلى تحديده هو ما إذا كان يريد السماح لطفله بالبحث في التطبيق بحرية، أو الاعتماد على إعدادات المحتوى القائمة على العمر للتطبيق (4 وما دون، و5-7، و8-12)، والتي تعمل مقاطع الفيديو المناسبة بشكل عام لكل فئة عمرية. يؤدي تحديد "الموافقة على المحتوى" إلى تعطيل البحث وتقديم مجموعات الفيديو بدلاً من ذلك، وهي مقاطع فيديو تم التحقق من أنها مناسبة للعمر. ويمكن الوصول إلى جميع إعدادات الملف الشخصي من خلال رمز القفل على كل شاشة، ويمكنك تحديثها كلما أراد المستخدم، ويتم تطبيقها فورًا على التطبيق والموقع الإلكتروني. (عبد المنعم، 2021)

3.2 السلوك الإجرامي

1.3.2 مفهوم السلوك الجرمي:

يعرف السلوك الإجرامي بأنه المظهر الخارجي للركن المادي للجريمة، وهو يأتي في صلب كل جريمة لأن المشرع لا يجرم على مجرد التفكير في الجريمة أو على مجرد الدوافع والنزاعات النفسية وإنما يستلزم أن تظهر تلك النزاعات والعوامل الدفينة في صورة واقعة مادية هي الواقعة الإجرامية، فالمشرع لا يستطيع الدخول إلى نفوس البشر ويفتش في تفكيرهم المجرد ليعاقبهم على ذلك. دون أن يتخذ هذا التفكير، وتلك العوامل النفسية مظهرًا ماديًا (خليل، 2008)

كما يُعرف بأنه سلوك منافي للقواعد الأخلاقية، وينتهك فيه صاحبه القوانين المعروفة، ويتصرف بطريقة سلبية مخالفة للقواعد والمبادئ السائدة في المجتمع، ويتضمن هذا السلوك أفعالاً تسبب الضرر للمجتمع. ما صاحب هذا السلوك فهو مجرم يفعل أفعالاً جنائية وعن سبق الإصرار والترصد. إن السلوك الإجرامي يصف نوعين من الأشخاص. النوع الأول هم الأشخاص المجرمين الذين يتحملون كامل المسؤولية عن أفعالهم الإجرامية. أمّا النوع الثاني هم الأشخاص الذين يفعلون الجرائم دون إدراكٍ منهم، لأنهم مصابين باضطرابات نفسية وعقلية.



2.3.2. أسباب السلوك الإجرامي:

بعد تبيان مفهوم السلوك الاجرامي لا بد لنا أن نذكر الاسباب والدوافع من وراء هذا السلوك. فالسلوك الإجرامي لا يأتي من فراغ، بل هنالك العديد من العوامل التي تؤدي إليه، وقد أشار الخبراء وعلماء الاجتماع إلى العوامل التي تكون محددة في السلوك الاجرامي، ومن هذه العوامل: (خلف، 1986)

- 1- أن يكون الولد منتمياً إلى عائلة يمارس أصحابها السلوكيات الاجرامية فيتعود عليها وبالتالي تصبح أمراً عادياً بالنسبة له وكأنه لا يخالف القانون ولا عادات المجتمع.
- 2- مُصادقة رفقاء السوء والاقتراء بأثرهم.
- 3- حب الانتقام والثأر من الآخرين.
- 4- التهرب من الواقع والتخلص منه، كالمشاكل المادية والعيوب والندم.
- 5- البطالة وقلة العمل يخلق فراغ كبير لدى الأشخاص مما يجعلهم مُهيئين لارتكاب الجرائم.
- 6- التأثير بالبيئة الاجتماعية الفاسدة
- 7- الرغبة في تحقيق كسب سريع بدون بذل أي مجهود.

3. الاطار التطبيقي للدراسة:

قراءات تحليلية لعينة من حلقات الرسوم المتحركة " المحقق كونان"

1.3. عينة الدراسة : هناك العديد من الرسوم المتحركة والفيديوهات المصورة من طرف أشخاص عاديين تحمل في طياتها العديد من الأساليب الاجرامية متاحة على موقع يوتيوب كيدز منها: عصابة الدلتون، المحقق كونان، فوزي موزي وكوزي، ميركيلوس، سوبر بن البطل الخارق،... وغيرها من المضامين التي تغلب عليها الكثير من المواضيع والتعابير والرسومات التي تعكس التصرفات التي يقوم بها الأطفال ممن يشاهدوها بكثرة ومن خلال اطلاعنا فمنا بإختيار رسوم متحركة واحد وهو رسوم " المحقق كونان " للاعتبارات التالية:

- يعد من الرسوم المتحركة العالمية.
 - لديه جمهور واسع وكبير من مختلف الفئات العمرية
 - لديه العديد من الأجزاء وهذا ما أعطى له صدى أكبر وأوسع فكل جزء أحسن مما سبقه وهذا نادراً ما يحدث إعلامياً.
 - يعتبر من أكثر الرسوم مشاهدة عبر منصات المحتوى الرقمي وحتى الوسائل الإعلامية الأخرى.
- وعليه قمنا باختيار وحدة العنوان في اختيار **08** حلقات من السلسلة الكرتونية وهي كالتالي: الانتقام الأعمى، جريمة في لعبة، جريمة الدعوة الغامضة، فخ العنكبوت السام، جريمة في الضباب، العصابة السوداء، الكتب القتالة. القناع المضلل.
- كما نشير للذكر أن من الحلقات من تحتوي على أكثر من جزء، ولقد اخترنا هذه العناوين لأنها توحى إلى مشكلات عندها علاقة بالجريمة أي بصلب موضوع دراستنا وهذا يسهل علينا عملية التحليل الضمني.

2.3. التعريف بسلسلة "كونان" :

كونان هي سلسلة مانغا ومسلسل أنمي وحلقات أوفاء وعدة أفلام يابانية مشهورة، من أعمال غوشو أوياما منذ عام 1994 وتحول لمسلسل أنمي في 8 يناير 1996 باليابان. تمت دبلجته إلى العربية بواسطة مركز الزهرة، وتأخر عرضه على قناة سبيس تون.(sondosbirat, 2011)



أخرج الحلقات "كينجي كوداما وتايتشيرو ياماموتو" وعرض في اليابان على قناة "نيبون تي في" وقناة "يوميوري" وقناة "أنيماكس". أذيعت الحلقة الأولى في 8 يناير 1996 وعرضت الحلقات بالتوالي إلى أن وصلت إلى الحلقة 574 التي أذيعت في 22 أيار/ مايو 2010. شهدت سلسلتي الأنمي والمanga مستويات عالية من الشعبية منذ تقديمها. كما تحولت السلسلة إلى 14 فيلم أصدر أولها في 19 أبريل 1997 وبعدها تم إصدار باقي الأفلام بمعدل فيلم لكل عام. عشرة من تلك الأفلام احتلت مركزا بين الأفلام العشرة الأكثر إيرادات في العام الذي عرضت فيه. كما تم إصدار 9 حلقات فيديو أصلية OVA تبلغ مدة عرض كل حلقة حوالي 25 دقيقة. (sondosbirat, 2011)

يعرض المحقق كونان على قنوات تلفزيونية خارج اليابان منها RTL 2 الألمانية، YTV الكندية، قناة FUNimation الأمريكية، سبيستون وسبيس بور العربيتين... الخ، ويعتبر هذا العمل الفني إعادة إحياء لشخصية المحقق "شارلوك هولمز" بصورة عصرية في إطار أحداث تتسم بالجريمة والغموض المثار حولها إلى جانب القليل من الرومانسية. كما أن العمل الفني ينقل وبشكل واضح للمشاهدين الثقافة والحياة العصرية لليابان، ويظهر ذلك بوضوح في الأفلام، فقد أبدع المؤلف "غوشو أوياما" في سرد أحداث المسلسل وربط حلقاته دون انقطاع لمدة 10 سنوات من خلال المانغا، كما نجح فريق العمل في دعم القصة من خلال أفضل موسيقى وأغاني لبدائيات ونهايات الحلقات والأفلام لجعل العمل مثال متكامل لنضوج في فن الأنمي (sondosbirat, 2011) المحقق كونان أنمي تلفزيوني ينتمي للأدب البوليسي (أكشن، دراما، كوميديا)، مخصص لفئة المراهقين تم إخراجها من قبل عدة أشخاص كينجي كوداما، ياسويشيرو ياماموتو، وقد ألف على يد "غوشو أوياما" وتم تصويره في استوديو طوكيو موفي شينشا، وعرض في 8 يناير 1996 عدد حلقاته قد وصلت الآن إلى أكثر من 574 حلقة تم دبلجتها إلى عدة لغات منها العربية والانجليزية. برنامج يتكلم عن رجل شديد الذكاء قد تقلص بسبب عقار ما أسقته إياه بعض العصابات، وهو يمر بمجموعة من القضايا والجرائم ويقوم بحلها.

أما شخصيات السلسلة فقد ظهرت أكثر من 20 شخصية رئيسية في المسلسل، بالإضافة إلى "سينشي كودو" "وران وتوغو موري يظهر العديد من الشخصيات الأخرى مثل أفراد المنظمة السوداء وأفراد الشرطة بالإضافة إلى متحري الغرب "هيجي هاتوري" و"كايتو كوروبا: و"جودي سانتيمليون" (كايتو كيد أو اللص الطائر) الذين يعلمون حقيقة ما جرى لسينشي. (sondosbirat, 2011).

3.3- المعالجة الفنية في "المحقق كونان" :

رسومات المحقق "كونان" تجسدية ومقاربة للواقع من حيث الألوان، الحركات، التحريك، خاصة وأن الشخصيات مرسومة بعناية فائقة تعبر عن شخصياتهم وكأنها شخصيات حقيقية، بالإضافة إلى الإحكام في بناء السيناريو، من حيث تطور الأحداث والشخصيات وغرابة الجرائم والايقاع الموسيقي المتدفق الممتاز، وتوفر عنصر الصراع بين الشخصيات، وتنوع الأحداث واختلافها.

1.3.3. اللغة:

يعرض "المحقق كونان" بالكثير من اللغات خاصة منها اليابانية والعربية على موقع "يوتيوب كيدز"، وتعرف لغته العربية بأنها لغة سليمة بأسلوب راق جذاب ومصطلحات تعبيرية تتخللها الإثارة في كثير من الأحيان مما يعمل على جذب الأطفال، وهذا ما يفسر مشاهدته من طرف حتى الأطفال حتى سن 14 وأكثر في العديد من الدراسات، فقد وفق القائمون على قسم الترجمة في هذه التجربة إلى حد كبير، وكان عامل في جذب ونجاح هذا الرسوم.

2.3.3. مضمون الحلقات عينة الدراسة:



كما سبق وأن ذكرنا قمنا باختيار وحدة العنوان لتسهيل عملية البحث عن الحلقات التي تحتوي على السلوك الاجرامي تحديدا والذي هو صلب موضوع دراستنا، وبالفعل من خلال قراءتنا ومشاهداتنا لهذه الحلقات رأينا أنها تشترك في نفس السلوك وهو السلوك المدروس - السلوك الجرمي - غير أنها تضمنت أكثر من مشكلة وقضية مثل ارتكاب جرائم القتل، محاولة قتل، اختطاف، كشف سر غامض، سرقة... الخ.

فيرى الطفل من جهة بشاعة وذكاء المجرمين وطرق ارتكابهم للجريمة لعدة دوافع ، ومن جهة أخرى ذكا وتفطن وشجاعة وطنية المحقق كونان في تعامله مع الآخرين، وبهذا يتجسد للطفل المشاهد الإحساس الخوف تارة والارتباك تارة والاثارة تارة أخرى في حلة واحدة.

3.3.3. القيم في سلسلة "المحقق كونان"

1.3.3.3. القيم الإيجابية في سلسلة "المحقق كونان"

أهم قيمة تطغى على سلسلة "المحقق كونان" هي قيمة الذكاء حيث تطغى هذه الصفة على المحقق محور السلسلة وعلى أصدقائه وعائلته التي تساعده في حل خيوط الجريمة، وهي قيمة يتمنى الكثير من الأطفال يتميزوا بها عن أقرانهم. كما نلاحظ أن هناك قيمة أخرى، وهي قيمة القوة حيث يعتبر "كونان" مصدرا للشجاعة والقوة عند الأطفال في بحثه عن المجرمين والالتقاء بهم ومواجهتهم بأعمالهم بمساعدة وبدون مساعدة من عائلته وأصدقائه، والأطفال بطبيعة الحال عليهم أن يمتلكوا هذه القيمة الإيجابية منذ الصغر. ويحذر للذكر أن هناك الكثير من القيم الإيجابية نلخصها فيمايلي: قيمة البحث، قيمة دقة الملاحظة، التضحية، الثقة بالنفس، التحدي، الصبر، الشجاعة، الجدية... الخ

2.3.3.3. القيم السلبية في سلسلة "المحقق كونان":

1.2.3.3.3. **تقصص الأبطال:** من الطبيعي أن يتقمص الطفل شخصيات بطل الرسوم، وهذا بالفعل ما يجري مع متتبعي "كونان"، وهذا يظهر من خلال التشبه به في حركاته وأسلوب كلامه وتكرار أشعر عباراته، فالبطل هو الذي سيوجه الطفل في مجرى القصة وهو معني أن يدفع المشاهد إلى الحماسة أو إلى خيبة الأمل وإلى الغضب والنقم، وبالتالي فإن تعلق الطفل بالبطل يعد الوسيلة التي يمكن من خلالها إيصال الرسالة الإعلامية فالطفل ليعيش دور البطل من الداخل وكأنه هو الذي يؤدي فعلا دور البطولة.

2.2.3.3.3. **الإدمان:** إن تعدد المغامرات الخيالية التي لا تستند على قاعد الحياة الحقيقية يمكن أن يؤدي إلى أخطار حقيقية ومنها أن الطفل الذي لم يكن سلبيا قد يصبح مدمن على مشاهدة التلفزيون، ذلك لأن الطفل يترك لنفسه العنان في تخزين صور تلفزيونية، خاصة وأن الكثير من حلقات الرسوم المتحركة "المحقق كونان" متتابعة في كثير من الأحيان وهذا ما يترك المشاهد يتشوق أكثر لما سيكون في الحلقة القادمة، هذا من جهة ، أما من جهة أخرى فالكثير من متتبعي هذا الرسوم يشاهدونه على التلفزيون ويعيدون مشاهدته على شبكة الأنترنت وهو الإدمان في أبسط صوره.

3.2.3.3.3. السلوك الجرمي في محتوى "المحقق كونان":

على سبيل المثال إن الانحرافات الاجتماعية يمكن أن تؤثر سلبا على المشاهد الصغير، وهنا يكمن خطر هذه المسلسلات المبنية على أساس التنافس وقهر الآخرين والاعتصاب واللاعذالة. وعندما يكون الشرير هو الذي يؤدي هذه الأعمال المشينة فإن ذلك لا يشكل خطر البتة ولكن الكارثة تكون عندما يقوم البطل المحبوب بأداء الأعمال الشريرة، لأن الأطفال سيندفعون عندها إلى الانحراف.

وما يعاب على "المحقق كونان"، هو التفصيل الممل أثناء التحقيق لكل الجرائم: من الأسباب والدوافع إلى التخطيط إلى الجريمة ونتائجها، وهذا ما يجعل الطفل يتعلم هذه الأشياء حتى يصبح عنده حمل السكين مثلا: شيء عادي في مثل سنه، فما بالك إن



تحدثنا عن الجريمة كاملا، وهناك الكثير من التحقيقات أثبتت أن الكثير من الجرائم تشابه ما وقع في الكثير من الأفلام السينمائية، وهنا نتحدث عن نقطة أخرى هي التقليد.

وبما يلاحظ أن الرسوم المتحركة "المحقق كونان" من خلال المشاهد التي يعرضها، وما يتخللها من مشاهد العنف والجريمة، وتقليد سلوكياتها تجد في كثير من الأحيان ردة فعل سلبية لدى الطفل على المجتمع، كالانعزال والميل إلى الاكتئاب نتيجة تلك المشاهد. وبالتالي فهي تلعب دورا مباشرا في التأثير على شخصية الطفل وسلوكه. إضافة إلى الانفعالات النفسية والعصبية، والتي تفضي إلى حالة من الغضب والكراهة، والتي قد تتحول إلى رد فعل غير مستحب، مثل العنف الجسدي على الآخرين أو تقليد ما رآه. في نفس السياق، يكون الطفل قادر على إدراك العنف المعروض في أفلام الرسوم المتحركة. فالأفلام التي تكثر فيها الحركة (أفلام الأكشن)، والتي يكثر فيها استخدام الأسلحة النارية والمسدسات والمعارك، لا تؤثر كثيرا على الطفل من النواحي النفسية والسلوكية والاجتماعية... غير أن مشاهد العنف التي تحتوي على استخدام الخناجر والسكاكين والسيوف، والتي يكون تأثيرها أكثر من أي استخدام آخر.

والمحقق كونان لا تخلو جرائمه من مختلف أشكال العنف وأدواته كالسكين والمسدس والتخطيط وطريقة القتل والدم... الخ. وهذه السلوكات بتقليدها من طرف الأطفال تصبح جرائم، يتمرن عليها الطفل منذ صغره عن طريق تقليدها بأبسط الأدوات وتقص الشخصيات، لكن مع مرور الوقت تصبح هذه التصرفات عادية بالنسبة للطفل على أساس أنها لعبة مع أقرانه لا أكثر ولا أقل، لكن ما يغيب عن الأولياء أن هذه السلوكيات تتطور إن لم يتم توجيه الطفل ومتابعته، لأنها تتطور وتعلق بالعمر والظروف الاجتماعية والتربية الأسرية.

ويجدر بالذكر أن هذا التأثير نسبي بين الأطفال يرتبط بالكثير من المتغيرات النفسية والاجتماعية. فالسلوك الجرمي عند الأطفال يظهر بمرور الوقت بتصرفات تتطور بتطور العمر وتأثير الظروف، ويجد سبله في هذا التطور في سن المراهقة على أكثر تقدير، زد على ذلك الوسط الدراسي والعلاقات الأسرية والظروف الاقتصادية والاجتماعية.

4.3- أشكال العنف في الحلقات عينة الدراسة:

عنوان الحلقة	أشكال العنف	الدوافع
جريمة في لعبة	ارتكاب جريمة قتل	الطموح في الثراء
جريمة الدعوة الغامضة	ارتكاب جريمة قتل	الانتقام
فخ العنكبوت السام	القتل	التضليل
جريمة في الضباب	القتل	الدفاع عن النفس
العصابة السوداء	الاحتيال والقتل	دوافع سياسية
الكتب القاتلة	القتل	مشاكل عائلية
القناع المضلل.	اختطاف	مرض نفسي

4- نتائج الدراسة:

- يعتمد رسوم "المحقق كونان" على سيناريو جذاب لاعتماده على الواقع.



- يتضمن رسوم المحقق "كونان العديد من القيم الإيجابية التي تساهم في بناء شخصية الطفل، كالقوة والنباهة والشجاعة..الخ.
- ينسلخ الكثير من الأطفال عن شخصياتهم الحقيقية بسبب نقص شخصيات رسومات " المحقق كونان"
- تؤدي كثرة مشاهدة وتكرار " المحقق كونان" في كثير من الأحيان الى الإدمان الى مشاهدته من خلال عمليات التكرار في مشاهدة الحلقات بدون ملل.
- يعتمد "المحقق كونان " على التفسير الممل لحل جرائمه، وبهذا يتعلم الطفل المشاهد العديد من السلوكيات الاجرامية بدون أن يدرك خلفياتها.
- يعمل الطفل المشاهد ل سلسلة " المحقق كونان" على تقليد المشاهد خاصة منها مشاهد العنف والجريمة، إضافة إلى الانفعالات النفسية والعصبية، والتي تفضي إلى حالة من الغضب والكراهة، والتي قد تتحول إلى رد فعل غير مستحب على الآخرين أو تقليد ما رآه.
- تتطور سلوكيات الطفل المشاهد من التقليد الى التكرار واللعب، ولكنها تأخذ أبعاد جد خطيرة مع التطور في العمر والظروف وبذلك يتنامى السلوك الجرمي عند الأطفال والذي بدأ بسلسلة كرتونية لينتهي بذلك الى اسنان مجرم.

خاتمة:

بناء على ما سبق، يمكن القول أن المحتوى الرقمي حتى وإن تشابهت مضامينه مع وسائل الاعلام والاتصال التقليدية، إلا أن خاصية الفاعلية وحرية الولوج والاختيار وتعدد المنافذ والمواقع شكلا ولغة ومحتوى، أثر على عادات الاستخدام والمشاهدة والاشباع لدى هذا المتلقي، الذي هو رغم اختلافه في الجنس والعمر واللغة والعادات والثقافات والدين... الخ، إلا أنه سلوكه واحد وهو السلوك الإنساني الذي يشترك في الكثير من المميزات أينما كان.

وهذا ما لاحظناه بالفعل لدى المتعرضين من فئة الأطفال لهذا المحتوى الذي أخذ أبعادا جديدة بتواجده في المحتوى الرقمي، هذا الأخير الذي شكل قيمة مضافة بالنسبة للكثير من البرامج ومنها رسوم "المحقق كونان" .

يدخل البرنامج ضمن الرسوم المتحركة العالمية نظرا لكثرة مشاهدته والمطالبة بتعدد أجزائه نظرا لأحداثه الشيقة حول تفكيك خيوط الجرائم، وهذا ما يستهوي الكبار فما بالك بالصغار، ولكن يجدر بالذكر ومن خلال دراستنا أن هاته المضامين تؤثر سلبا على متبعيها من الأطفال الذين يكتسبون بؤادر السلوك الجرمي في سنة مبكرة عن طريق التقليد والتقمص والتكرار والادمان.. الخ. لذا فالمرقبة والانتباه لتصرفات أطفالنا أصبح ضرورة قصوى على الأسر الانتباه لها.

توصيات :

- إنَّ أهم آليات مكافحة السلوك الإجرامي هي:
- مراقبة المحتوى الرقمي الذي يتابعه أطفالنا.
- العمل على دمج الأطفال في النشاطات التعليمية والتثقيفية
- تعريض المحتوى الرقمي السلبي بالإيجابي.
- وضع السلطات وهيئات المختصة، بالتعاون مع منظمات المجتمع المدني، الخطط والبرامج الشاملة، التي من شأنها القضاء على العوامل المؤدية إلى الإجرام أو الظروف المهيئة له.
- العمل على حل المشاكل الاجتماعية كالتفكك الأسري.
- تعزيز دور الأسرة في مكافحة السلوك الإجرامي من خلال التربية السليمة ووضع تشريعات التي توفر الحماية الاجتماعية و الاقتصادية للأسرة.



- القيام بندوات ومحاضرات في المدارس والجامعات بهدف التوعية من مخاطر السلوك الإجرامي.
- وضع عقوبات رادعه على الجرائم ذات خطورة الأكبر على المجتمع.
- العمل على تقليص نسبة الفقر والبطالة و الجهل.
- تقديم النصائح والإرشاد والنصح وذكر الأمور السلبية والمخاطر وهذا التوجيه يكون مباشر ليتعلم الطفل كيف يسلك طريق معين يتناغم مع عمره ومرحلة نموه ومتطلبات حياته اليومية دون انحراف عن القواعد والأعراف الاجتماعية.

قائمة المراجع:

- 01- العساف، صالح محمد، (1989) المدخل إلى البحث في العلوم السلوكية، مكتبة العبيكان، الرياض.
- 02- عزوزي، حسين، (1986)، منهجية البحث في العلوم الشرعية، فاس.
- 03- حويجي، نعمة الله إسماعيل، (1995) تحليل محتوى أدب الأطفال في ضوء معايير الأدب في التصور الإسلامي، مكتبة الملك عبد العزيز، الرياض.
- 04- سالم، نادية، (1983) إشكاليات استخدام تحليل المضمون، مجلة العلوم الاجتماعية، الكويت.
- 05- الخالدي، عماد وجيه، (1968) تحليل المحتوى طريقة بحث علمية لتحليل الوثائق، معهد الإدارة، الرياض، ع3، مجلد 13.
- 05- الحلو، كلير وآخرون (2018) مواقع التواصل الاجتماعي وأثرها على الحالة النفسية للطلاب الجامعي، المجلة الدولية التربوية والنفسية، عمان، المجلد 03، العدد 02.
- 06- مزاهرة، منال هلال (2011) بحوث الإعلام: الأسس والمبادئ، ط1، دار كنوز المعرفة العلمية للنشر والتوزيع، عمان.
- 07- بن مرسل، أحمد (2003)، مناهج البحث العلمي في علوم الإعلام والاتصال، ديوان المطبوعات الجامعية، الجزائر.
- 08- حسين، محمد سمير (1976) بحوث الإعلام: الأسس والمبادئ، عالم الكتب، القاهرة.
- 09- عبد الحميد، محمد (2004) البحث العلمي في الدراسات الإعلامية، ط2، عالم الكتب، القاهرة.
- 10- عبد الحميد، محمد (1993) دراسات الجمهور في بحوث الإعلام، عالم الكتب، القاهرة.
- 11- بيوحوش، عمار (1985) دليل الباحث في المنهجية وكتابة الرسائل الجامعية، المؤسسة الوطنية للكتاب، الجزائر.
- 12- الجبيري، خالد عبد الرحمن (2000)، تقييم مواقع المعلومات المتاحة على الأنترنت، مجلة مكتبة الملك غهد الوطنية، الرياض، مج: 05، ع 02.
- 13- محمد، خلف (1986)، مبادئ علم الاجرام، الجماهيرية الليبية، دار الجماهيرية للنشر والتوزيع والإعلام.

باللغة الفرنسية:

10-Social Presence Theory (short, williams, & christie, 1976, p. 47)

المواقع الالكترونية:

11- صبري محمد خليل، مقال بعنوان: الجريمة والسلوك الإجرامي: التعريف والأسباب والنظريات المفسرة واليات المكافحة، صحيفة سودانايل،

08/02/2018

https://sondosbirat.wordpress.com/wpincludes/js/tinymce/plugins/paste/pasteword.htm?ver=342-20110501-syntaxhighlighter2.3.9#_ftn34

12- اية عبد المنعم، يوتيوب كيدز،

[/https://faharas.net/youtube-kids19-10-2021](https://faharas.net/youtube-kids19-10-2021).



دو وسائل التواصل الاجتماعي في انتشار ظاهرة التنمر السيبراني لدى الطلبة الجامعيين -دراسة تحليلية نظرية -

The contribution of social media in the spread of cyberbullying among college students

د. عادل بضياف

أستاذ محاضر أ

adel1beddiaf@yahoo.fr

د. باشا ياسمين

أستاذ محاضر أ

bacha_vasmine@hotmail.fr

مقدمة :

يشهد العالم الكثير من التهديدات الأمنية على المجتمع، خاصة في ظل التطورات التكنولوجية الحديثة والتي أصبح العالم فيها عبارة عن قرية واحدة جمعت فضاءات ووسائل تكنولوجية متعددة قللت المسافات وزادت وسهلت في طرق وأنواع التواصل، ولكنها خلفت الكثير من السلبيات التي عرت وابانت عن الكثير من العيوب والتشوهات التي أصابت واخلت بمختلف العادات والنظم الاجتماعية ، لتفسح المجال لتهديدات طالت الافراد والمؤسسات وحتى الحكومات وأصبحت في بعض الأحيان تتحكم بمساراتها وتؤثر على اتخاذ قراراتها.

الاشكالية :

أصبح معظم افراد المجتمع عبر العالم بصفة عامة وبالجزائر بصفة خاصة عرضة لظاهرة التنمر السيبراني عبر جميع وسائل التواصل الاجتماعي وبالخصوص الفضاء الأزرق، او ما يطلق عليه الفاييس بوك، ونخص بالذكر هذا الفضاء لأنه يعتبر من اكثر الفضاءات استعمالا بالجزائر وانتشارا بالوسط الطلابي ، حيث يستعمل كوسيلة للتواصل بينهم وتبادل المعلومات وعرض مختلف الاخبار وبرامج الدراسة ، مما أدى الى سرعة انتشار المعلومات وكثرتها وهذا ما ساعد الكثير على استغلال هذا الفضاء لنشر شتى انواع العنف الرقمي والسلوك الإجرامي، فهو يستقطب العديد من فئات وشرائح المجتمع مما سهل تواصلها افتراضيا وجعلها فضاء مفتوحا لتفريغ النزوات العدوانية والانفعالات والتعبير عن مشاعر وسلوكيات لايسمح بها في الواقع، ونظرا لأسباب عديدة من بينها بعض الطابوهات التي تعتبر محضورة بالمجتمع الجزائري، والتي لايمكن التعبير عنها الا من وراء الستار ، فقد سمح هذا الفضاء للأفراد بتقمص شخصيات وهمية تسمح لهم بالتخفي ورائها والتعبير عن هذه المكبوتات في اشكال مختلفة، وتشكل ظاهرة التنمر السيبراني التي نسلط عليها الضوء تهديدا للعديد من الأشخاص الذين يعانون من عواقبها خاصة الوسط الطلابي، فمثل هذه الاعتداءات والتي تهدد في بعض الأحيان حياتهم الشخصية وامנם النفسي، ومسارهم الدراسي وتوجهاتهم وحتى نهجهم القيمي، أصبحت خطرا لا يمكن الاستهانة



به او السكوت عليه ، فالأمر يستوجب التجند لمواجهته من اجل عدم استفحال الظاهرة وتفشيها بالشكل الذي يصبح خطرا على الامن القومي والمجتمعي، وقد تم التركيز على هذه الفئة للتعرف اكثر على تأثيرات التنمر السيبراني بهذا

الوسط الذي نعتبره اكثر عرضة لهذه التهديدات ،خاصة وأنهم في مرحلة تعتبر جد حساسة فيما يتعلق بتكوين الشخصية وتحقيق الذات، والحاجة الى بناء العلاقات، فما هو دور هذا الفضاء في انتشار التنمر السيبراني لدى الطلبة الجامعيين ؟

وعليه نسعى للإجابة على التساؤلات التالية :ماهو الامن السيبراني ؟

- ماهو التنمر السيبراني ؟
- هل تساهم مواقع التواصل الاجتماعي في تعرض الطلبة الجامعيين للتنمر السيبراني؟
- هل توجد هناك علاقة بين التنمر السيبراني والتعليم لدى الطلبة الجامعيين ؟

-فرضيات الدراسة :

- لتشريعات الامن السيبراني دور في الحد من ظاهرة التنمر السيبراني .
- لمواقع التواصل الاجتماعي دور في تعرض الطلبة الجامعيين للتنمر السيبراني .
- يؤثر التنمر السيبراني على مستوى التعليم لدى الطلبة الجامعيين .

-اهداف البحث :

- معرفة انعكاسات التنمر السيبراني عبر وسائل التواصل الاجتماعي وبالتحديد فضاء فايس بوك وكذا الأسباب المؤدية إلى انتشارها بهذه البيئة الرقمية .
- الكشف عن ظاهرة التنمر في أوساط المتعلمين من اجل محاولة إيجاد حلول لها .

- منهج البحث :

هو المنهج الوصفي التحليلي، وهو المنهج الذي يعتمد في جوهره على وصف الظاهرة، والمتغيرات المتعلقة بها، والعوامل التي تؤثر فيها، ومن ثم استخلاص النتائج وتعميمها، ويشتمل المنهج الوصفي على أكثر من طريقة وسوف نستخدم طريقة التحليل : والتي تركز على وصف دقيق لمحتوى النصوص، من أجل استخلاص النتائج، بدون الحاجة للاستعانة بمصادر أخرى من المعلومات.

1. الامن السيبراني :

1.1 تعريف الامن :

يتشكل مفهوم الأمن الإنساني من مقومات أو دعائم تركز على تحقيق التنمية الاقتصادية المستدامة وصون حقوق الإنسان وحرياته، والحكم الراشد والمساواة الاجتماعية وسيادة القانون.

يضم مصطلح الأمن أربعة مستويات، هي

- أمن الفرد: ضداية أخطار حياته أو ممتلكاته أو أسرته.
- أمن الوطن: ضد اي أخطار داخلية أو خارجية للدولة وهو ما يعبر عنه الأمن الوطني.
- الأمن القطري أو الجماعي: وهي إتفاق عدة دول في إطار إقليم واحد على التخطيط لمواجهة التحديات التي تواجهها داخليا وخارجيا وهو ما يعرف بالأمن القومي .
- الأمن الدولي: وهو الذي تتولاه المنظمات الدولية سواء منها الجمعية العامة للأمم المتحدة أو مجلس الأمن الدولي، نظرا لدورها في الحفاظ على الأمن والسلم الدوليين.ⁱ



2.1 تعريف الامن السيبراني:

بناء على التعريف لحماية مصالح الدول والأشخاص ، ليبقى الهدف في الأخير، هو قدرة هذه الادوات على مقاومة التهديدات المتعمدة من طرف قرصنة المعلومات أو غير المعتمدة من طرف المستخدمين (الخطأ البشري) للتعافي، وبالتالي التحرر من الاضرار الناجمة الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقريره حول " اتجاهات الاصلاح في الاتصالات للعام 2010 - 2011"، والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية "هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات امنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين. " من هذا المنطلق، يمكننا إعطاء تعريف شامل بالقول " أن الامن السيبراني أو الالكترونى هو مجمل القوانين، الادوات، النصوص، المفاهيم والميكانيزمات الامنية وطرق تسيير الاخطار والممارسات التقنية المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة عن تعطيل أو سوء استخدام تكنولوجيا المعلومات والاتصالات. ⁱⁱ

2 مفهوم شبكات التواصل الاجتماعي :

شهد العالم خلال الآونة الأخيرة انتشارا رهيبا لما يسمى بمواقع التواصل الاجتماعي على شبكات الانترنت في محاولة من القائمين عليها لاستقطاب اكبر عدد من المشتركين وذلك من اجل تحقيق مكاسب مالية وكذا لتحقيق مختلف الإشباعات لمستخدميها ويأتي على راسها موقع فيسبوك، تويتر، تيك توك، يوتيوب، واتس اب وغيرها، وتم اطلاق الكثير من التعريفات على مواقع التواصل الاجتماعي، ، حيث يعرفها "بالاس" « 2006 » BALAS على " إنها مواقع تستخدم لبناء مجتمعات افتراضية على شبكة الانترنت تمكن للأفراد أن يتصلوا ببعضهم البعض للعديد من الأسباب المتنوعة".

1.2 مواقع شبكة التواصل الاجتماعي:

تعريف مواقع التواصل الاجتماعي بأنها مقهى اجتماعي يجتمع فيه بعض الأفراد للقيام بتبادل المعلومات فيما بينهم مع وجود فارق بين المقهى الحقيقي والمقهى التكنولوجي وهو أنك تستطيع حمل هذا المقهى التكنولوجي أينما كنت (علي محمد رحومة، 2007 ص 75) ⁱⁱⁱ

مفهوم "مواقع التواصل الاجتماعي" مثير للجدل، نظرا لتداخل الآراء والاتجاهات في دراسته. عكس هذا المفهوم، التطور التقني الذي طرأ على استخدام التكنولوجيا، وأطلق على كل ما يمكن استخدامه من قبل الأفراد والجماعات على الشبكة العنكبوتية العملاقة.

2.2 الأصول الاجتماعية و النفسية لاستخدامات وسائل الاتصال:

يعود الفضل في اكتشاف العلاقة بين الأصول الاجتماعية والنفسية ودوافع التعرض لوسائل الاتصال إلى الباحثة (ماتيلدا رايلي) حيث تناولت هذه الأصول من حيث:

1.2.2 الأصول الاجتماعية لاستخدامات وسائل الاتصال: لا يتعامل أفراد الجمهور مع وسائل الاتصال باعتبارهم أفرادا معزولين عن واقعهم الاجتماعي وإنما (باعتبارهم أعضاء في جماعات منظمة)، وعليه فإن العوامل الديموغرافية والاجتماعية مثل (النوع، السن، المستوى العلمي، المستوى الاجتماعي والاقتصادي،) لها تأثيرها في استخدام الجمهور لوسائل الاتصال.

2.2.2 الأصول النفسية لاستخدامات وسائل الاتصال: تؤدي الاستخدامات في بعض الأحيان إلى وجود حوافز أو دوافع معينة بحاجة إلى إشباع وبالتالي تحدد العديد من الاستخدامات لوسائل الإعلام، حيث يقوم مدخل الاستخدامات الإشباعية



على افتراض أن الأفراد المختلفين يختارون لأنفسهم مضامين إعلامية مختلفة وفقا للظروف النفسية بينهم، حيث تعد الظروف النفسية لأفراد الجمهور مشكلات، تواجههم (و يحقق التعرض لوسائل الاتصال العلاج الأمثل لمثل هذه المشكلات). (الشهري، حنان بنت شعشوع، 2012ص: 24) ^{iv}

3. أنواع شبكات التواصل الاجتماعي:

يقسم الخبراء شبكات التواصل الاجتماعي إلى نوعين كما أوردها (محمود 2011 م: 90) وهي كالتالي: أساسي يتكون من : ملفات شخصية للمستخدمين وخدمات عامة مثل المراسلات الشخصية ومشاركة الصور والملفات الصوتية والروابط والنصوص والمعلومات بناء على تصنيفات محددة مرتبطة بالدراسة أو العمل أو النطاق الجغرافي مثل مواقع فيس بوك وتويتر وكيك وواتس اب وبلاك بير وغيرها.

4. مميزات شبكات التواصل الاجتماعي:

يرى Kuss & Griffiths (2011) أن مميزات شبكات التواصل الاجتماعي هي:

- بناء لمح عامة أو شبه عامة عن المستخدمين في ضوابط يحددها النظام.
- التعبير عن الأفكار لقائمة من المستخدمين الآخرين.
- عرض قائمتهم والقيام بالاتصال بهم والتفاعل مع التعليقات التي أدلى بها آخرون داخل النظام.
- ولخص المنصور (2012) مميزات الشبكات الاجتماعية في الآتي:
- حرية الاختيار لمن يريدون في المشاركة معهم في اهتماماتهم.
- إتاحة المجال للأفراد للدخول إلى المواقع الاجتماعية والتعرف بأنفسهم، ومن ثم التواصل مع الآخرين الذين تربطهم بهم اهتمامات مشتركة.

-تتيح إرفاق الملفات والكتابة حول مواضيع محددة ومعينة.

-التعليق على المواضيع المطروحة فيها.

5. التفسيرات النفسية لإدمان الانترنت:

استعرض "جينفر وفيريز (1999)، بعض التفسيرات النفسية لإدمان شبكة الانترنت وتتمثل في ما يلي:

1.5 التفسير السيكودينامي:

وذلك من خلال خبرات التي يمر بها الأطفال في مرحلة الطفولة، أو ما يسمى بصدمة الطفولة المبكرة وارتباط ذلك ببعض سمات الشخصية الاضطرابات والميول والنزعات الموروثة لدى الفرد، فقد يكون لدى الفرد استعداد نظري لإدمان الانترنت، ولكنه لا يقع في الإدمان إلا إذا توافرت ظروف وأحداث ضاغطة في حياته وساعدت أو دفعته إلى إدمان الانترنت، ليصبح الفرد مدمن انترنت. و في ضوء صدمات الطفولة المبكرة، وارتباطها بسمات الشخصية، وأحداث ضاغطة الحياة الضاغطة، والاستعدادات النفسية والموروثة، قد تؤدي لوقوع الفرد في إدمان الكحوليات أو المروين أو المقامرة أو الجنس أو التسوق أو الكمبيوتر والانترنت وما تقدمانه من خدمات مع وجود بعض العوامل المهيأة كالاستعدادات المرضية.

2.5 التفسير السلوكي:

يعتمد التفسير السلوكي على وجهة نظر "سكنر" في النظرية السلوكية على أساس أن الفرد يقوم بمجموعة من السلوكيات والأنشطة، بهدف الحصول على المكافأة أو التعزيز، وهذا ينطبق على الإدمان على المخدرات والكحول وإدمان الانترنت وما تقدمه تلك الشبكة



للفرد من الراحة والمتعة النفسية، بجانب أنها طريقة سهلة وبسيطة وسهلة ، للهروب من الواقع بهدف الحصول على معززات للسلوك. (محمد نوبى محمد علي، 2010 -3 -33).

وقدم "دافيز" (2001) نظرية سلوكية معرفية، كمحاولة لبناء نموذج يجمع بين النواتج السلوكية المرتبطة بالاستخدام المفرط للإنترنت، ويقوم نموذج "دافيز" على افتراض أن الأفراد الذين يعانون من ضغوط أو مشكلات نفسية (مثل الوحدة، والاكتئاب) يحملون إدراكات سلبية عن كفاءاتهم الاجتماعية، هؤلاء الأفراد يفضلون التفاعل الاجتماعي عبر الإنترنت لأنه أقل تهديداً وأقل مخاطرة، وينتج عن ذلك استخدام قهري للكمبيوتر والإنترنت، وهذا بدوره يفرز كثيراً من المشكلات الشخصية والاجتماعية والمهنية.

3.5 التفسير الطبي:

يعتمد التفسير الطبي للإدمان على الإنترنت قائم على أساس على سلوكيات الأفراد تحكمها مجموعة من العوامل الوراثية الجينية وتغيرات كأن يتوهم الشخص باعتدال المزاج لممارسة نشاط معين، مثل تناول العقاقير الكيميائية في المخ وناقلات العصبية، وما يتعلق بها من تغيرات الكروموزومات والهرمونات والمواد الكيميائية

الضرورية لتنظيم نشاط المخ والجهاز العصبي. فقد أظهرت البحوث في هذا المجال أنه توجد عقاقير قد تحدث خلل في التواصل العصبي، مما يترتب عليه إرسال المخ للمعلومات غير صحيحة أو المخاطرة، أو المقامرة، وبتطبيق مثل هذا التفسير على حالة الاعتماد على الإنترنت، حيث تتيح الإنترنت للفرد شعوراً بالمتعة والإثارة. ^v (محمد النوبى محمد علي، 34، 2010).

6. أعراض إدمان شبكات التواصل الاجتماعي:

ذكر Das & Sahoo (2011) أنه إذا كان العالم يواجه أي نوع جديد من أنواع الإدمان، بعد إدمان المخدرات والكحول فإنه سيواجه إدمان شبكات التواصل الاجتماعي، وسيذهب الناس بجنون وراء ذلك، الأمر الذي سيشكل حياة افتراضية، وسيقوم الناس بنسيان العالم المادي من حولهم.

وقدم Hanyum (2011) أربعة أعراض تدل على إدمان شبكات التواصل الاجتماعي وهي:

- سيطرة شبكات التواصل الاجتماعي على الفرد والانشغال المفرط بها.
- النتائج السلبية لاستخدام الفرد المفرط لشبكات التواصل الاجتماعي؟؟.
- تصاعد المشاعر السلبية حين استخدام شبكات التواصل الاجتماعي.
- فقدان الاهتمام بالنشاطات الاجتماعية حيث يفضل الفرد استخدام شبكات التواصل الاجتماعي على
- نشاطات الحياة الواقعية مع أصدقائه وعائلته. ^{vi}

7. وسائل الاتصال الحديثة:

تتعدد وسائل الاتصال الحديثة التي تُتيح إمكانية التواصل بين الأفراد بسرعة وسهولة، ومن هذه الوسائل ما يأتي:

1.7 وسائل التواصل الاجتماعي: (بالإنجليزية: **Social Media**)؛ ظهرت وسائل التواصل الاجتماعي مع ظهور الإنترنت، وزاد تطورها وانتشارها مع مرور الوقت، حيث يستخدمها الملايين من المستخدمين يومياً مما جعلها أكثر وسائل الاتصال شيوعاً، ومن أهم ميزات القدرة على نشر رسائل عامة لا تقتصر على فئة معينة ويستطيع الجميع رؤيتها والتفاعل معها وإبداء آرائهم وتعليقاتهم.

2.7 الرسائل الخاصة على وسائل التواصل الاجتماعي: (بالإنجليزية: **Social Media – Direct Message**)

(DM)؛ تُقدّم وسائل التواصل الاجتماعي خدمة الرسائل الخاصة بين الأشخاص التي تمتاز بأنها أقل رسميةً من البريد الإلكتروني، كما يُمكن استخدامها كوسيلة اتصال بين العملاء ومُقدّمي الخدمة؛ للإجابة على استفسارات العملاء وتسؤالاتهم.



1.2.7 الرسائل الفورية: (بالإنجليزية: **Instant Message (IM)**)؛ تنتشر العديد من تطبيقات الرسائل الفورية التي تُسهّل التواصل بين شخصين أو أكثر بشكل خاص، وترتبط بعض هذه التطبيقات بوسائل التواصل الاجتماعية، ومنها ما يُتيح التواصل عبر منصة خاصة فقط للرسائل الفورية.

2.2.7 الرسائل النصية القصيرة: (بالإنجليزية: **SMS Text Messaging**)؛ تُستخدم الرسائل النصية القصيرة لإيصال معلومات أو ملاحظات قصيرة، وتُعتبر وسيلة سهلة للتواصل بسبب إمكانية استخدامها عن طريق الهاتف الذكي الذي يستخدمه معظم الأشخاص حول العالم للتواصل.

3.2.7 المدونات: (بالإنجليزية: **Blogging**)؛ تُعتبر المدونات منصات شخصية مُتاحة للجميع يستطيع الفرد من خلالها نشر المعرفة والمعلومات والأخبار والكثير من المعلومات الأخرى؛ ومن أهم ميزاتها أنّ أغلبها يحتوي على قسم خاص بتعليقات الزوّار ممّا يُمكن صاحب المدونة من التفاعل مع الأشخاص الذين يُشاركونه اهتماماته.

4.2.7 المكالمات الصوتية: (بالإنجليزية: **Voice Calling**)؛ وهي من أكثر وسائل الاتصال شيوعاً، وتُتيح قدراً من الخصوصية أكثر من باقي وسائل الاتصال، كما أنّها توصل نبرة الصوت وحّدته وبالتالي تصل من خلالها المشاعر والعواطف بشكل أفضل.

5.2.7 المكالمات المرئية: (بالإنجليزية: **Video Chat**)؛ تُتيح المكالمات المرئية قراءة تعابير الوجه ولغة الجسد أثناء المحادثة، وهناك العديد من التطبيقات التي تُقدّم هذه الخدمة مجاناً.

6.2.7 الدردشة المباشرة على مواقع الويب: (بالإنجليزية: **Live Web Chat**)؛ تُتيح الدردشة المباشرة للأشخاص الذين يستخدمون موقعاً إلكترونياً ما أن يطرحوا أسئلتهم واستفساراتهم بشكل مباشر وسريع، وتكون هذه الخاصية فعّالة ومفيدة في حال وجود شخص متفرّغ للرد على الرسائل والاستفسارات خلال ثوانٍ معدودة.

7.2.7 الواقع الافتراضي: (بالإنجليزية: **Virtual Reality**)؛ يُعدّ الواقع الافتراضي من وسائل الاتصال قليلة الاستخدام في الوقت الحالي، إلّا أنّه يُتوقع أن يزداد عدد الأشخاص الذين يستخدمونه بسبب استمرارية تطوّره وانخفاض أسعار الأدوات الخاصة به مثل سماعات الرأس.

8.2.7 البريد الإلكتروني: (بالإنجليزية: **Electronic Mail**)؛ وهو من وسائل الاتصال الحديثة بين الأشخاص التي بدأ استخدامها منذ اختراع شبكات الحاسوب، ويشيع استخدامه بين الأشخاص الذين يستخدمون الحاسوب بشكل أساسي في عملهم، ومن المتوقع أن يزداد استخدامه حتّى من قبل باقي الأشخاص.¹

وتُعرف اجرائياً في هذا البحث بأنّها المواقع الموجودة على شبكة الانترنت كما تم ذكرها و التي تسمح لمستخدميها بالتواصل البصري والصوتي و تبادل الصور و غيرها من الإمكانيات التي تساهم في تحقيق تواصل إيجابي وفعال ، فيما بينهم كما يمكن استعمالها كالية من اليات تحسين العمل والتواصل داخل المؤسسات .

8. مميزات وسائط التواصل الاجتماعي :

تختص الوسائط الاتصالية والإعلامية بمجموعة من الخصائص تميزها عن وسائل الاتصال الجماهيري، و نلخصها في:

1.8 التفاعلية :

تُعتبر التفاعلية أهم خاصية للوسائط الاتصالية والإعلامية وهي التي تميزها عن وسائل الاتصال والإعلام الأخرى وبفضل نموذج الإعلام الرقمي على شبكة الانترنت أضحت التفاعلية نظاماً أكثر قدرة على تنمية مشاركة المستخدم وتحقيق درجة عالية من التحكم

¹ <https://mawdoo3.com/> مفهوم وسائل الاتصال الحديثة ، تم كتابة المقال بتاريخ 2020/08/17



في الاتصال، والمشاركة والنشر الفوري في الشبكة سواء في منتديات النقاش أو تحرير مقال و إرساله مباشرة عبر البريد الالكتروني، وتتخذ التفاعلية على شبكة الانترنت عدة أشكال وهي:

- التفاعل مع الوسيلة.
- التفاعل مع المحتوى .
- التفاعل مع الفاعلين و المستخدمين.

2.8 التنوعية: تعمل شبكات التواصل الاجتماعي على توفير مجموعة من العناصر التي تساعد على توضيح الموقف الاتصالي .

3.8 الكونية: أي أنها ليست حكرًا على بلد معين أو شعبًا ما، بل هي متاحة على مستوى عالمي

4.8 الفردية: ميزة الاستخدام الفردي.

5.8 التزامنية: وهو تناسب توقيتات تداخل العناصر المختلفة والموجودة في البرنامج زمنيا، تتناسب مع سرعة العرض بحيث يحدث توافق بين جميع عناصر الوسائط المتعددة كعنصر الصوت مع عنصر النص المكتوب و الكلام المنطوق .

6.8 الالكترونية: تعتمد الوسائط الاتصالية والإعلامية الجديدة في إنتاجها و تنفيذها على العديد من الأجهزة الالكترونية وكذلك أنظمة شبكات المعلومات بهدف توفير الجهد و الوقت.

7.8 الإتاحة و السهولة والتوافق: ما يجعل التحكم في أسلوب المشاهدة والعرض وعملية التعلم بأكملها في يد المستخدم نفسه حسب قدرته. 1

9. التمر بوسائل التواصل الاجتماعي:

التمر هو سلوك عدواني متنوع الأساليب قد يتعرض له أو يتعرض أبناؤك ومعارفك له، ويمكن أن يكون جسديًا كالضرب أو السرقة أو التحرش، ويمكن أن يكون لفظيًا كالسخرية والإهانة اللفظية والتهديد، كما يمكن أن يكون التمر عبر الإنترنت وعبر الهواتف الذكية ورسائل البريد الإلكتروني ووسائل الاتصال الاجتماعي، والهدف منها المضايقة أو التهديد أو الإذلال وهذا النوع من التمر لا يتطلب المواجهة ولا يتطلب قوة جسدية كالأشكال الأخرى، ولذلك قد يستمر على مدار اليوم وطيلة أيام الأسبوع، ولا يقل ضررًا وتأثيرًا عن الأنواع الأخرى من التمر، بل ربما يزيد عليها؛ لأنه قد يصعب في بعض الأحيان تجنبك له، ويستخدم المتنمرون أساليب عديدة تختلف بين إرسال الرسائل أو اختراق البريد الإلكتروني وسرقة هوية من يتنمر عليهم عبر الإنترنت أو إنشاء صفحات أو مواقع خاصة لإهانة شخص معين. عادةً ما تختلف أساليب التمر بين الجنسين فكما أن التمر بالضرب أو

الأفعال الجسدية شائع عند الذكور في التمر على أرض الواقع فالشائع عندهم في التمر عبر وسائل التواصل الاجتماعي هو التمر المرتبط بالجنس، بينما ينتشر التمر اللفظي بين الفتيات عادةً، فيكون التمر عندهم عبر وسائل التواصل الاجتماعي عن طريق نشر الأكاذيب والأسرار والفضائح أو الاستبعاد من قوائم الأصدقاء، وللتنمر أسباب متعددة منها رغبة المتنمر بلفت الانتباه أو كسب شهرة أو شعوره بالغيرة أو تعرضه للتنمر وقد يستخدم المتنمر كوسيلة للهروب من المشكلات الشخصية. ^{vii}

كما يمكن أن يتم التمر الالكتروني عبر الانترنت أو عبر تطبيقات الهواتف الذكية والأجهزة اللوحية ومواقع التواصل الاجتماعي وتطبيقات الرسائل ومواقع الألعاب وغرف الدردشة. ويبدو للباحث من خلال التعريف السابق أن مدلول التمر الالكتروني أوسع من المدلول التقليدي من حيث الضحية، فإذا كان التمر التقليدي محله الطالب فإن التمر الإلكتروني قد يكون على أي مستخدم مهما كان عمره أو وضعه الاجتماعي مع التأكيد على خطورة التمر الذي يقع على الطفل، بالإضافة إلى الأثر من حيث سعة

- سميرة الشبحاني، (2010) "الإعلام الجديد في عصر المعلومات"، مجلة جامعة دمشق، العدد الأول، (دون مكان نشر)، ص(447)¹



الانتشار وظهور العلانية في تصرفات المتنمر المتسلط، وطرق التنمر الإلكتروني متعددة ومتنوعة، وفيما يأتي أهم أنواعها وأشكالها عبر الإنترنت.

1.1.9 المضايقة: هو إرسال الرسائل المسيئة والوقحة أو تعليقات سيئة أو مهينة على المشاركات والصور وغرف الدردشة أو أن تكون هجوما صريحا على مواقع اللعب.

2.1.9 تشوية السمعة: هذا عندما يقوم شخص ما بإرسال معلومات عن شخص آخر مزيفة أو ضارة أو غير صحيحة ومشاركة صور لشخص ما بغرض السخرية ونشر الشائعات المزيفة والقبل والقال ويمكن أن يكون ذلك على أي موقع عبر الإنترنت أو على التطبيقات. حتى أننا نسمع عن أشخاص يغيرون صور الآخرين وينشرون على الإنترنت لغرض التنمر.

3.1.9 الإهانة: هو عندما يستخدم شخص ما عن قصد لغة متطرفة وعنيفة للغاية ويدخل في الحجج والمعارك عبر الإنترنت للتسبب في ردود الفعل والتمتع بحقيقة أنه يسبب شعور بالضيق لشخص ما.

4.1.9 انتحال الهوية: عندما يخترق شخص ما حساب البريد الإلكتروني أو حساب الشبكات الاجتماعية لحد الشخص ويستخدم هوية الشخص عبر الإنترنت لإرسال مواد فاحشة أو محرجة إلى الآخرين أو نشرها، كذلك إنشاء ملفات تعريف مزيفة على مواقع الشبكات الاجتماعية والتطبيقات ويكون من الصعب جدا إيقافها.

5.1.9 الخداع: عندما يقوم شخص ما بمشاركة معلومات شخصية عن شخص آخر أو خداع شخص ما لكشف الاسرار وإرسالها إلى الآخرين، وقد يكون ذلك أيضا مع الصور ومقاطع الفيديو الخاصة.

6.1.9 التكرار في الهجوم : هو تكرار إرسال الرسائل التي تتضمن تهديدات الذي أو المضايقة أو رسائل التخويف أو الانحراف في أنشطة أخرى عبر الإنترنت تجعل الشخص خائفا على سلامته .

7.1.9 الاستبعاد: هذا عندما يقوم الآخرون بترك شخص ما خارج مجموعة ما عمدا على تطبيقات الإنترنت ومواقع الألعاب، وهذا هو أيضا شكل من أشكال التنمر الاجتماعي وشائع جدا. ^{viii}

2.9 سلوك التنمر الإلكتروني:

يعرف التنمر الإلكتروني علي أنه واحد من طرق إساءة استخدام التكنولوجيا، فيقوم المعتدي بإلحاق الأذى والضرر بالآخرين وذلك من خلال العديد من الطرق والوسائل التي من خلالها يتم مهاجمة الضحية مثل الرسائل المؤذية والقاسية ونشر الصور المزعجة ونشر أكثر اللحظات إخراجا للآخرين من خلال الإنترنت والهاتف الخليوي وغيرها من التقنيات التكنولوجية التي توجد في يد المعتدين للحصول علي ضحاياهم)

والتنمر الإلكتروني هو إرسال أو نشر المواد الضارة أو الانحراف في أشكال أخرى من العدوان الاجتماعي باستخدام الإنترنت أو غيرها من الوسائل التكنولوجية الحديثة، ويحدث طوال الأسبوع بدون توقف في أيام الدراسة و الإجازة، وقد يكون نص أو صورة ضارة ومن المستحيل إزالتها وتعرفه الباحثة بأنه أحد أشكال العدوان باستخدام أجهزة الكمبيوتر والهواتف المحمولة والأجهزة التكنولوجية الأخرى عن طريق إرسال أو نشر نصوص أو صور أو فيديوهات بغرض الأذى والإهانة والسخرية والتهديد والضرر لشخص آخر بشكل متعمد ومكرر.

3.9 أسباب التنمر الإلكتروني:

يذكر براون Brown:2014 (وبيترسون Peterson:2013) (أن أسباب التنمر تشمل

- يستخدم الألف ا رد التنمر الإلكتروني من أجل الإغاطة والسخرية والتهكم من الآخرين.
- ضغط بعض الأقران للمشاركة في التنمر الإلكتروني علي الآخرين.



- بعض المراهقين يقلدون السلوك القاسي ضد الآخرين من الأفلام وبرامج التلفزيون والفيديوهات التي توجد علي مواقع اليوتيوب. **You Tube**
- بعض المراهقين يستخدمون الإنترنت والهاتف المحمول لإيذاء الآخرين عن عمد بكلماتهم وأفعالهم.
- المعتدي يقوم بالتنمر إلكترونياً لأن الناس يخافون من المعتدين، كما أنه لا أحد يحب أن يكون هدف للمعتدي الإلكتروني ولا أحد يريد أن يُعتدي عليه إلكترونياً.

4.9 من هم المتنمرون الكترونياً :

- هم أشخاص يتظاهرون بأنهم لطيفون ولكنهم يستخدمون تكتيكات وأساليب خفية للتنمر الإلكتروني علي الآخرين بنشر الشائعات.
- الأشخاص المتنمرين إلكترونياً يشعرون بالقوة عندما يمارسون التنمر علي الآخرين.
- المتنمر إلكترونياً شخص مكر وحريص جداً ويتميز بالقسوة ، ويعرف أيضاً ماذا يفعل.
- من الممكن أن يكون المتنمر إلكترونياً لطيفاً ولكنه غير صادق، كما أنه يخطط جيداً وبحرص ويفضل أن يظل في الخفاء.
- يحتاج المتنمر الكثير من القوة حتي يسيطر علي الضحية وعلي طرقهم الخاصة بهم.
- يظهرون القليل من التعاطف مع ضحاياهم..
- يتعاملون بشكل فظ وعدواني تجاه الراشدين.
- لا يتبعون القواعد بشكل جيد.
- يعملون علي الدفاع علي أنفسهم ويفقدون مـ ا زجيتهم وانفعالاتهم بسهولة.
- المتنمرين إلكترونياً يقومون بالسخرية والتهكم علي أنفسهم أيضاً.
- لا يقومون بالتنمر الإلكتروني بمفردهم ولكن بوجود غيرهم من المعتدين معهم.
- يعلمون أن هذا السلوك خطأ ولكنهم يفعلوه من أجل إعجاب أصدقائهم.
- يقومون المتنمرين بالتنمر الإلكتروني تحت ضغط الأقران.
- عصابات المتنمرين أكثر تنظيماً ويقومون بإيذاء ضحاياهم عن عمد. ^{ix}

5.9 التنمر الالكتروني لدى الطالب الجامعي :

ويعرف جرادات 2008 التنمر بأنه قيام الطالب بسلوكات سلبية بشكل متعمد ومتكرر خلال فترة من الوقت ضد طالب آخر أك أكثر من أقران ، كما يعرفه أبو غزال بأنه سلوك متعمد متكرر ضد طالب او أكثر يتضمن الإيذاء الجسدي أو اللفظي أو الإذلال أو إتلاف الممتلكات ينتج عن عدم تكافؤ القوى ويشير أبو الديار (2012) إلى أف التنمر يتضمن عناصر متعددة، منها: طبيعة سلوك التنمر، والشخص المتنمر، وحدوث سلوك التنمر وتكراره عن قصد بشكل منتظم وخفي، عدم توازن القوة بين المتنمر كالضحية، وإلحاق الأذى والألم النفسي والجسدي بالضحية.

وبتطور وسائل الاتصالات الإلكترونية الحديثة ممثلة بالإنترنت فقد تصاعدت كثيره التهديدات الإلكترونية بين الطلبة بما يعرف بالتنمر الإلكتروني. إذ أشارت دراسة روبن وسوزان Robin & Susan, إلى أن ما نسبته 42 % من الطلبة كبيرري السن قد تم التنمر



عليهم خلال تواجدهم على الانترنت. كآف هذه النسبة قد تزايدت بشدة في عام 2008 لتقفز من 42 % الى 42 % في دراسة Juvonen & Gross, 2008

6.9 أسباب اكتساب الطلبة سلوكيات التنمر :

قد يكتسب الطلبة سلوك التنمر نتيجة لبعض العوامل الشخصية، فالاضطرابات السلوكية والانفعالية ، تؤثر على سلوك الطلبة، لاسيما أن الطلبة المضطربين سلوكيا وانفعاليا هم أناس أسوياء في الأساس من حيث قدراتهم العقلية والجسمية، ولكن الفرق بينهم وبين الطلبة العاديين في درجة أداء السلوك وليس نوعه، فينتابهم الخوف والاحراج، ويظهرون الانسحاب والعزلة، ويظهرون سلوكيات عدوانية وعدم ثقة بالآخرين .

ومن المهم فهم مدى ارتباط التنمر الالكتروني ببعض المشكلات والاضطرابات السلوكية او الانفعالية لدى الطلاب لاسيما التنمر الالكتروني يرتبط بمؤشرات شخصية لدى الطلبة، من اضطراب انفعالي وتدن في التحصيل، وعدم الرضا عن الجامعة ، ونقص في العلاقات مع المجتمع المحلي واولياء الأمور Williams, Guerra 2007 ولعل اهم تلك المؤشرات الاضطرابات السلوكية والانفعالية التي أصبحت من اكثر المشكلات شيوعا ، كما انها مشكلة أصبحت تفرق الاولياء والمعلمين والتربويين والمهتمين بهذا المجال ، ومثل هذه الاضطرابات تعكس خللا معينا في السلوك بشقيه الموجه من الفرد الى الخارج، والذي يعبر عن الاضطرابات السلوكية، والموجهة الى الداخل والذي يعبر عن الاضطرابات الانفعالية .^x

7.9 أسباب انتشار سلوك التنمر الإلكتروني :

لم يكن استخدام القوة بين الأقران سلوكا جديدا في المجتمعات التعليمية، بل يمكن القول إنه سلوك بشري طبيعي وغريزي بين الناس في كل المجتمعات الإنسانية، ويمكن مواجهته وتقويمه لكن المشكلة القائمة تكمن في أمرين، أولهما انتشاره وتحوله إلى سلوك مرضي ينذر بخطورة شديدة، وثانيهما عدم مواجهته المواجهة التربوية الحاسمة التي تسيطر عليه وتحد من انتشاره وتقلل من آثاره، لهذا كان لا بد من البحث عن الأسباب التي أدت إلى انتشاره ذلك الانتشار السريع والتي تشمل الآتي:

- الألعاب الإلكترونية العنيفة التي اعتاد الكثير من الأبناء على قضاء ساعات طويلة في ممارستها والتي تقوي

لديهم النزعة العدائية تجاه الآخرين.

- شيوع الأفلام العنيفة؛ حيث وجد أن مشاهد العنف في الأفلام التي يشاهدها الأطفال والبالغون قد زادت بصورة مخيفة.

- الخلل التربوي في بعض الأسر، ويعتبران أن مقياس أدائهما إذ ينشغل الوالدان عن متابعة أبنائهما سلوكيا لوظيفتهما تجاه أبنائهما هو تلبية احتياجاتهم المادية فقط، ويتناسيان الدور الأهم الواجب عليهم وهو المتابعة التربوية وتقويم السلوك وتربيتهم التربية الحسنة.

- العنف في المنزل وفي المجتمع المحيط: يتأثر كل إنسان منذ صغره بالتصرفات والسلوكيات التي يلاحظها داخل في المجتمع الخارجي المحيط به بيئته الصغيرة كالأُسرة وكذلك ما يشاهده يوميا، فالذي يلاحظ السلوكيات والعنف بين الوالدين، والذي عانى بنفسه وتعرض للعنف من قبل والديه أو إخوته، والذي شاهد عنفا وخصوصا في البلاد التي ضعفت فيها القبضة الأمنية نتيجة الثورات وغيرها مجتمعا ، فمن المؤكد أنه يتأثر بما شاهده، وقد يكتسب تلك السلوكيات العنيفة ويمارسها مع غيره وهكذا يجني المجتمع على أبنائه ويساهم الوالدان في التأثير السلبي على سلوك أبنائهم .^{xi}

8.9 الآثار السلبية للتنمر وسائل التواصل الاجتماعي:



ان التعرض للتنمر عبر وسائل التواصل الاجتماعي له آثار سلبية عديدة طويلة المدى على ضحايا هذا التنمر من مختلف الأعمار بما فيهم الأطفال أو المراهقين وحتى البالغين، ومن هذه الآثار السلبية التي يمكن أن تظهر على الفرد .:

- الشعور بالضيق الشديد والخوف والعجز والإهانة والخجل وحتى الشعور بالذنب وانخفاض الثقة بالنفس خصوصاً عند الفتيات المراهقات اللواتي يتعرضن للتنمر بسبب مظهرهن.
- ارتفاع احتمالية الإصابة بالأمراض النفسية، كالإكتئاب والقلق ونوبات الهلع وقد يتبادر لذهن البعض أفكار انتحارية والبدء بتعاطي المخدرات والكحول، وقد وُجد أنّ كثيراً من الحالات التي تعرّضت للتنمر أقدمت على فعل خطير كهذا.
- الانسحاب من الجو الأسري وزيادة أوقات العزلة وتقليل محيط الأصدقاء، وتدني المستوى التحصيلي في المدرسة أو التهرب من الذهاب للمدرسة أو العمل وصعوبة في التركيز والتشتت بسبب الانشغال بالتفكير
- وزيادة مفاجئة أو انخفاض في الوقت الذي يقضونه عليه، وقد يلجأ بعضهم إلى تعطيل حسابات في كيفية تجنب هذا التنمر
- تغيير في الشخصية كزيادة الغضب وكثرة البكاء وعدم الاستمتاع بالأعمال والأنشطة التي كانت سبباً في الحماس والتحفيز، وفقدان الدافع وزيادة الجدل مع الآباء أو المعلمين واستخدام العنف
- رفض الأطفال المعرضين للتنمر عبر وسائل التواصل الاجتماعي مشاركة ذويهم ما يفعلونه على الإنترنت، التواصل الاجتماعي الخاصة بهم.
- اضطرابات في الأكل واضطرابات النوم كقلة النوم أو الكوابيس المستمرة.^{xii}

10. النتائج والتوصيات :

بالنظر الى أهمية وحداثة الدراسة فإننا قد توصلنا الى مجموعة من النتائج عبر تحليل ماهو موجود من دراسات نظرية وكان أبرزها:

- يفضي التنمر السيبراني الى اعمال عدوانية تضر بالغير دون الشعور بذلك في بعض الأحيان بسبب الإدمان على وسائل التواصل الاجتماعي، خاصة في ظل التخفي في صور شخصيات وهمية .
- ظاهرة التنمر ظاهرة تقليدية لكن وسائل التواصل الاجتماعي إعادة تقديمه بشكل جديد، في قالب عصري جعلته التقنيات الحديثة أكثر انتشار.
- الظاهر متفشية بين الطلبة الجامعيين بصفة تتجلى للعيان حيث نلاحظ كباحثين وكممارسين في الميدان تقدم عدة طلبة بشكاوى ضد زملائهم مفادها تعرضهم للتنمر لعدة أسباب .
- تعرض الكثير من الطلبة الى الاحباطات النفسية، والمضايقات تودي في بعض الأحيان الى التخلي عن الدراسة بسبب التنمر .
- التنمر اصبح كظاهرة متفشية اثر على السلوك العام للأسرة الجامعية فاصبح الكثير يمارس السلوك كتقليد وقد لاحظنا ذلك في ردود أفعال الطالبة على مواقع التواصل الاجتماعي خاصة فايس بوك حيث يتم التهجم على مختلف الاطراف بالصفحات الرسمية وغير الرسمية مما اثر سلبا على مستعملها حيث سبب لهم ذلك اضرار نفسية وهو ما يتطلب التدخل سريعا لردع مثل هذه السلوكات في ظل غياب قوانين تشريعية.
- التنمر الالكتروني يعتبر ارسال او نشر نصوص او تعليقات ضارة بالغير عبر شبكات التواصل الاجتماعي الغرض منه التشهير او تشويه صورة الاخرين او نشر الشائعات، او الإطاحة بمعنويات الاخرين.

التوصيات :

- انشاء قوانين وتشريعات تخص التنمر السيبراني قصد الحد من الظاهرة.



- دراسة الظاهرة عبر مختلف وسائل البحث للاطلاع أكثر على أسبابها وأسباب تفشيها.
- تحسيس الاولياء برعاية الأبناء الرعاية المثلى من اجل تنمية الصلابة النفسية لديهم وحثهم على عدم إيذاء الآخرين مع تنمية شخصياتهم وصقلها بالطريقة الصحيحة.
- ادانة المتنمرين وتسليط عقوبات ردعية بحقهم.

قائمة المراجع

- i - عائشة عبد الحميد، ملوك نوال، (2020): " الاجرام السيبراني واثره على تهديد الامن الثقافي في الجزائر "مجلة المفكر للدراسات القانونية والسياسية، المجلد 3، العدد، الجزائر ص(213)
- ii - جمال بوازدي، (2019): " الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية، التحديات والافاق المستقبلية " مجلة العلوم القانونية والسياسية، المجلد 10 العدد 1 الجزائر، ص(1262).
- iii - علي محمد رحومة، (2007): "الانترنت والمنظومة التكنو-اجتماعية «مركز دراسات الجودة -العربية، بيروت، ص 75
- iv - الشهري، حنان بنت شعشوع، (2012): " أثر استخدام شبكات التواصل الإلكترونية على العلاقات الاجتماعية "الفيس بوك وتويتر نموذجاً" دراسة ميدانية كلية الآداب والعلوم الإنسانية، جامعة الملك عبد العزيز، المملكة العربية السعودية، ص(24).
- v - هبة يحيى الدين ربيع (2003): إدماج شبكة المعلومات والاتصالات الدولية (الانترنت) في ضوء بعض المتغيرات، مجلة الدراسات النفسية، العدد (04)، المجلد رقم (12) مصر-ص(34-32)
- vi - علي بن حمد با احمد دغيري (2018): " ادمان شبكات التواصل الاجتماعي وعلاقته بالشعور بالوحدة النفسية لدى المراهقين " المجلة العربية للعلوم ونشر الأبحاث، العدد الأول -المجلد الثاني، المملكة العربية السعودية ص-ص(94-95)
- vii - زين عميرة 7/ماي/2020 " ما هو تنمر وسائل التواصل الاجتماعي " <https://hyatoky.com> ما هو تنمر وسائل التواصل الاجتماعي <https://hyatoky.com>
- viii - صخر أحمد الخصاونة (2020)" مدى كفاية التشريعات الإلكترونية للحد من التنمر الإلكتروني- دراسة في التشريع الأردني " المجلة الدولية للدراسات القانونية والفقهية المقارنة، تشريعات إعلامية- معهد الاعلام الاردني- عمان- الاردن ص(54)
- ix -مروة عبید عبد الحليم عبید (2020): "الأفكار اللاعقلانية وعلاقتها بسلوك التنمر الإلكتروني لدى طلبة الجامعة، رسالة ماجستير، كلية التربية، مجلة كلية التربية، جامعة دمياط، العدد 86 ص-ص(313-312)
- x -هشام عبد الفتاح وآخرون: (2018) " التنمر الإلكتروني لدل عينة من الطلبة المضطربين سلوكيا كانهاليا في مدينة الزرقاء " مجلة الدراسات التربوية والنفسية مجلد 12 عدد 1، جامعة السلطان قابس، المملكة الهاشمية، ص-ص(171-170)
- xi - سوزان بنت صدقة بسيوني وآخرون(2020): " التنمر الإلكتروني وعلاقته بالوحدة النفسية لدى طالبات كلية التربية بجامعة أم القرى " مجلة العلوم التربوية والنفسية، المجلد 4 العدد 12 المملكة العربية السعودية، ص(131).
- xii - زين عميرة 7/ماي/2020 " ما هو تنمر وسائل التواصل الاجتماعي " <https://hyatoky.com> ما هو تنمر وسائل التواصل الاجتماعي <https://hyatoky.com>



تحليل أبعاد السلوك الإجرامي الرقمي وانعكاساته على المستوى الفردي والمجتمعي Analyzing the proportions of the digital criminal behavior and its repercussions on individuals and society

واكلي بدبعة

aitmedjber63dz@yahoo.fr

بوعمامة منال

Bouamama.manel.psy@gmail.com

مقدمة:

شهد العالم خلال العقود الأخيرة تطورا علميا متسارعا كان من أبرز ملامحه ما أطلق عليه "الثورة التكنولوجية" والتي أدت إلى الغزو التقني لكافة مجالات الحياة حيث أصبحت الأدوات والوسائل الإلكترونية أمرا لا غنى عنه في مختلف الهيئات والمؤسسات وكذلك لدى الأفراد بحيث أنّ الغالبية العظمى من الأشخاص أصبحت لديهم المهارة والقدرة على استخدامها والتعامل معها بكفاءة عالية.

ظهر في عالم الإجرام نوع حديث ومتميز من السلوكات الإجرامية سميت "بالجرائم الإلكترونية"، تنفرد بخصوصيات لا مثيل لها في الجرائم الأخرى ومنها: ظهور وولادة طائفة جديدة من المجرمين تتمتع بسمات وشخصية مغايرة للمجرم الذي اعتدنا على دراسته وهذا ما زعزع وقبّل الدراسات التقليدية لعلم الإجرام.

وتعددت أبعاد الجريمة الإلكترونية واكتسبت بُعدا جديدا بتطور أدواتها فيقوم المجرمون بتطبيق أوجه التقدم العلمي والتكنولوجي في دعم أهدافهم غير المشروعة، ونتيجة للاستخدام المستمر لوسائل التكنولوجيا بأشكالها المتعددة كالهاتف والبريد الإلكتروني والمواقع الإلكترونية فضلا عن مواقع التواصل الاجتماعي وغيرها من المواقع والمنشآت التي يقصدها فئة الشباب بوجه عام وبحكم أهم الأكثر استخداما لها، انتشرت آفة الاستخدام الخاطيء لهذه التكنولوجيا وهي ظاهرة التحرش الإلكتروني باختلاف أشكاله؛ والذي يتم عن طريق استخدام المواقع الإلكترونية، كما تواجد في الآونة الأخيرة العديد من المنتديات الخاصة بنشر الثقافة الإلكترونية والمواقع التي تُساعد على الانحراف.

وتأتي أهمية دراسة هذا الموضوع من حيث خطورة الفعل الإجرامي بأنماطه وتنطلق من حقيقة مفادها أنّ هذه الظاهرة الخطيرة قد استفحلت وأنّ هذا النوع من الجرائم لم يعد يقتصر على دولة دون أخرى مهما كانت درجة تطورها أو مؤسسة دون أخرى مهما اختلف طبيعة نشاطها أو أهدافها، وبالتالي كانت هناك حاجة ملحة للتعامل مع هذه الظاهرة الإجرامية المستحدثة والحد من الأضرار الكبيرة التي تلحقها سواء بالدول والمؤسسات أو الأفراد على المستوى الاجتماعي، الأمني و خاصة النفسي.

ومن هذا المنطلق فان إشكالية هذه الدراسة تتمحور في الأسئلة الآتية: ما هي الجريمة الرقمية ومن هو المجرم الرقمي؟ ما هي خصائص المجرم الرقمي وخصائص الجريمة الإلكترونية؟ وما هي أهم الدوافع التي أدت به إلى ارتكاب السلوك الإجرامي؟

وللإجابة على هذه الإشكالات قسمنا مداخلتنا إلى:

المبحث الأول: مفهوم الجريمة الرقمية و المجرم الرقمي.

المبحث الثاني: خصائص المجرم الرقمي وخصائص الجريمة الرقمية .



المبحث الثالث: قراءة تحليلية لأبعاد السلوك الإجرامي الرقمي .

1. المبحث الأول: مفهوم الجريمة الرقمية والجرم الرقمي

1.1. تعريف الجريمة الرقمية:

إنّ الجريمة الرقمية حديثة نسبيا، وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، ونتيجة لحداثة هذه الجريمة فقد كانت هناك عدّة اتجاهات مختلفة في تعريفها، كما أنّها اتّسمت بمجموعة من الخصائص التي ميّزتها عن سائر الجرائم الأخرى، هي نوع من الجرائم التي يكون الحاسوب وسيلة هامة للقيام بها، بحيث يتمّ استخدامه من أجل تحقيق أهداف معينة تتنافى على ما هو متعارف عليه في العالم الرقمي وتتضارب مع مبادئ المجتمع بحيث أنّها تسبب الأذى للأفراد وتمسّ استقرارهم في جوانب مختلفة. (الصغير، 2002) وقد أوردت الدراسات المتعلقة بها عدّة تعريفات مختلفة بها وانقسمت إلى أربعة اتجاهات تتمثّل في:

1.1.1 على أساس وسيلة ارتكاب الجريمة:

يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: " الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا" ، وتعتبر الجرائم الإلكترونية من هذا المنطلق أيّ فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية .

2.1.1 على أساس توافر المعرفة بتقنية المعلومات:

يستند أنصار هذا الاتجاه إلى معيار شخصي الذي يستوجب أن يكون فاعل هذه الجرائم ملماً بتقنية المعلومات، ومن بين هذه التعريفات تعريف David Thompson للجريمة الإلكترونية بأنها : " أية جريمة يكون متطلّبا لاقتوافرها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب". (رستم، 2000)

3.1.1 على أساس موضوع الجريمة:

يرى واضعو هذا التعريف أنّ الجريمة الرقمية ليست هي التي يكون الحاسب أداة ارتكابها بل التي تقع على الحاسب أو داخل نظامه، ومن نماذج مساهمة هذا المنطلق تعريف Rosenblatt بأنها: " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه". (محمد، 2004)

- وحدينا تبني مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين تعريفا جامعاً حيث عرّف الجريمة الإلكترونية بأنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة رقمية". (المناعسة، 2001)

2.1. المجرم الرقمي:

لقد تعدّدت التسميات التي أطلقت على هذه الفئة من المجرمين بين "قراصنة المعلوماتية" و "الهكرة" والمجرم الإلكتروني والمجرم الرقمي و"مجرم الأنترنت" و " مجرم التقنية"... وغيرها

ويقصد بالمجرم الرقمي هو المجرم الذي له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني بملاحظات مع الوسائل التواصلية الرقمية، وذلك بأداء فعل الامتناع عنه، مما يحدث اضطرابات في المجتمع الدولي والمحلي نتيجة لمخالفة. وهو كلّ شخص طبيعي أو معنوي يتوافر لديه كشرط أساسي معرفة كافية بآلية عمل وتشغيل الحاسب الآلي، بحيث تمكنه هذه الأهلية إلى اختراق وارتكاب أفعال تقنية عبر العالم الافتراضي لإحداث نموذج إجرامي بالاعتداء على حقّ أو مصلحة. (الفتاح، 2017).

1.2.1 تصنيف المجرم الرقمي:

يمكن تصنيف المجرم الإلكتروني إلى الفئات التالية:



الفئة الأولى: صغار مجرمي المعلوماتية

كما يسميهم البعض صغار نوابغ المعلوماتية وهم غالبا ما يكونون في مرحلة المراهقة وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع النظم البنكية والشركات والمؤسسات المالية، ويتميز هؤلاء المراهقون عن غيرهم من مرتكبي الجرائم التقليدية في أنهم لا يعتبرون ما يقومون به جريمة لأنهم يعتقدون أنّ النظام غير القادر على حماية نفسه ليس من الخطأ اقتحامه، ولذلك يعتبرون أنفسهم أبطالا لمساعدة المجتمع في تحديد نقاط الضعف الخاصة بالبرنامج الذي تمّ اقتحامه، ويمكن لجماعات صغار نوابغ المعلوماتية أن تتحوّل إلى فئة القراصنة لأنه عندما يصبحون على درجة عالية وكبيرة من الخبرة والمهارة يتمّ استئجارهم واستغلالهم في أعمال ذات أهداف إجرامية.

الفئة الثانية: القراصنة

تغيّر لفظ القراصنة مع ظهور شبكة الأنترنت عما كان عليه في الماضي لأنه لم يعد معنى القرصنة سفك الدماء والقتل وعمليات التفجير باستخدام الأسلحة ولكن أصبح للفظ القرصنة مدلول آخر ارتبط بالتطوّر التكنولوجي. (إبراهيم، 2009) ويمكن تصنيف القراصنة إلى صنفين هما:

أ. **القراصنة الهواة العابثون أو الهاكرز:** هذا القسم من القراصنة أو ما اصطلح على تسميتهم "الهاكرز" يطلق هذا اللفظ على المقتحم التقليدي الذي يقوم بالتلصص على الغير ويتاجر في قطاع المعلومات، وإذا ما واجهته حماية لا يستطيع تخطيها فهو ليس له علاقة بتكنولوجيا المعلومات.

ب. **القراصنة المحترفون أو الكراكرز:** هذه الفئة تعكس اعتداءاتهم ميولات إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب ويتميز هؤلاء بقدرتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدّثون أضرارا بالغة، وقد يؤلّف المجرمون في إطار هذا النوع أندية لتبادل المعلومات فيما بينهم ويفضلون العمل في جماعات، وغالبا ما يكون دافعهم لارتكاب الجريمة إمّا الحصول على المال أو بغرض الشهرة، أو إثبات تفوقهم العلمي ومدى ما يتمتعون به من ذكاء.

الفئة الثالثة: الموظفون العاملون في مجال الأنظمة المعلوماتية

بحكم طبيعة عمل هؤلاء الموظفين ونظرا لأنّ النظام المعلوماتي هو مجال عملهم الأساسي ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها فإنهم يقترفون بعض الجرائم الرقمية التي من الممكن أن تحقق أهدافهم الشخصية وأهمها الكسب المادي، فالعلاقة الوظيفية التي تربط بين الموظف والمجني عليه تجعل عملية ارتكابه للجريمة الرقمية أسهل نظرا للثقة التي يتمتع بها.

الفئة الرابعة: المجرمون أصحاب الآراء المتطرفة

تتألف هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكوّن من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي ويتركّز نشاطهم بصفة عامة في استخدام العنف ضدّ الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه. وأصبحت شبكة الأنترنت والبيئة الرقمية مناخا خصبا لنشر آرائهم ومعتقداتهم وأخبار أخرى تحمل في ثناياها مساسا بنظام وأمن الدول والإساءة والتشهير.

الفئة الخامسة: المجرم الرقمي في إطار الجريمة المنظمة

تقوم جماعات الجريمة المنظمة بتبني أصحاب الكفاءات وأصحاب الخبرة والموهوبين في مجال تقنية المعلومات، وذلك بإغرائهم بالمال لينظموا إلى صفوفها وتقوم بتدريبهم وزيادة مهارتهم في هذا المجال لخلق مجرمين متخصصين في الجرائم الإلكترونية في إطار هذه المنظمات، ويمارس المجرم الرقمي في نطاق هذه المنظمات نشاطات تدرّ على المنظمة أرباحا هائلة فيقومون بتزوير البرامج وتقليدها



واختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى العالمية، كما يمارسون أعمال التجسس الصناعي والتجاري. (الفتاح، 2017)

المبحث الثاني: خصائص المجرم الالكتروني والجريمة الإلكترونية

1.2 خصائص المجرم الرقمي:

ليس هناك اتفاق على صفات مرتكبي الجرائم الإلكترونية ومنفذيها، ولا يوجد قالب يتضمن الفئات والسمات التي يتسم بها مرتكب الجريمة الرقمية إلا أن هناك صفات ذات دلالة مشتركة يجمع المختصون بأنها توجد في كل الأشخاص الذين تم التحقيق والقبض عليهم في جرائم من هذا النوع، حيث أوردت العديد من الدراسات العربية والأجنبية في هذا المجال بأن متوسط عمر مرتكبي هذه الجرائم بين 14-38 سنة، وهذا يدل بأن أغلب مرتكبي الجرائم الإلكترونية من فئة الشباب، ويتميز المجرم الرقمي بعدد من السمات والخصائص هي:

- ✓ المجرم الرقمي يتمتع بالمهارة والمعرفة والذكاء، حيث يمكنه التغلب على الكثير من العقبات التي تواجهه أثناء ارتكاب الجريمة.
- ✓ المجرم الرقمي يتمتع بالسلطة اتجاه النظام المعلوماتي، حيث أن المزايا التي يتمتع بها تمكنه من ارتكاب جرمته، وقد تتمثل هذه السلطة مثلا في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي المجرم إمكانية فتح الملفات وقراءتها أو كتابتها ومحو المعلومات.
- ✓ المجرم الرقمي شخص ذو مهارات فنية عالية متخصص في الإجرام المعلوماتي (الرقمي)، قادر على استخدام خبراته في الاختراقات وتغيير المعلومات.
- ✓ المجرم الرقمي قادر على تقليد البرامج وتحويل الأموال، محترف في التعامل مع شبكات الحاسوب، وهو شخص غير عنيف لأن هذه الجريمة لا تلجأ إلى العنف لارتكابها.
- ✓ هو إنسان اجتماعي بطبعه يمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى. (صليحة، 2017)

2.2 خصائص الجريمة الرقمية:

تتميز الجريمة الإلكترونية بجملة من الخصائص التي تجعل عملية محاربتها صعبة نوعا ما، وتجعل الدول والمنظمات تجتهد لإيجاد آليات مناسبة لمكافحتها، وترتبط هذه الخصائص بمميزات الأجهزة الإلكترونية التي تستخدمها والبرامج وشبكة الانترنت ومختلف التطبيقات التي توظفها، ومن أهم هذه الخصائص نذكر:

1.2.2 العالمية: بمعنى أنها تتعدى الحدود الجغرافية للدول، إنها جرائم عابرة للقارات، ألنه مع انتشار شبكة الاتصالات العالمية والانترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد والجني عليه في بلد آخر. (الفتاح م.، 2007)

2.2.2 صعوبة الإثبات: صعوبة متابعتها واكتشافها بحيث لا تترك أثرا فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الإلكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها، على أساس أنها تفتقر إلى الدليل المادي التقليدي كال بصمات، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، تحتاج خبرة فنية خاصة يتعذر على المحقق التقليدي منالها أو التعامل معها، لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع والتضليل بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل وقد يلجأ مرتكبها لتشفير التعليمات لمنع إيجاد أي دليل يدينه. (مراد ، 2007)



3.2.2. عدم التبليغ: عند وقوع الجريمة بواسطة الانترنت نجد أن بعض المجني عليهم يمتنعون عن إبلاغ السلطات المختصة خشية على السمعة والمكانة، وعدم اهتزاز الثقة في كفاءته خاصة إذا كان كيان أو هيئة معينة. هذا بالإضافة إلى اتسامها بمجموعة من الخصائص الأخرى، أهمها:

- أنها جريمة غير مقيّدة بزمان ومكان إذ تتمّاز بالبعد الجغرافي وعدم تقيدها بالتوقيت الزمني.
- سهولة إخفاء آثار الجريمة والأدلة التي تدلّ على الجاني نظرا للترميز والتشفير الذي يحدث على الرموز المخزّنة على وسائط التخزين الممغنطة.

المبحث الثالث: قراءة تحليلية لأبعاد السلوك الإجرامي الرقمي

1.3 أبعاد السلوك الإجرامي الرقمي:

تختلف الأسباب الكامنة وراء أي جريمة مهما كان نوعها وطبيعتها وعلى الرغم من التطورات الحاصلة في مجال البحوث والدراسات في مجال علم الإجرام والجريمة إلا أنّ من بين أهمّ الصعوبات التي تواجه الباحثين في هذا المجال هو صعوبة تحديد العوامل أو الدوافع الأساسية للجريمة بأشكالها المختلفة إذ يمكن القول أن كلّ جريمة هي جريمة في حدّ ذاتها لها أسبابها الخاصة التي قد تشترك مع بعض الجرائم في بعض الجزئيات أو العموميات لكن لا يمكن أن تكون لها نفس الدوافع خاصة من حيث درجة حدّتها، لذا يصعب فهم الدوافع الكامنة وراء الجرائم بأنواعها المختلفة.

إنّ فهم الجريمة الرقمية في أبعادها مهمّ للغاية للحدّ منها ومحاولة محاربتها خاصة وأنّ الجريمة الرقمية وبالنظر إلى خصوصيتها تعدّ أخطر أنواع الجريمة خاصة في حالة صعوبة معرفتها واكتشافها، وعلى الرغم من أن هناك عدّة دوافع كامنة وراءها .



جدول رقم 01: أسباب الجريمة الرقمية وفق مستوى التحليل

أسباب الجريمة على المستوى الفردي	أسباب الجريمة على المستوى المجتمعي	أسباب الجريمة على المستوى الكوني
البحث عن التقدير: هي جرائم يرتكبها شباب طائش وصغار السن وذلك من باب التحدي وحب الظهور	التحضر: أحد أسباب الجريمة الرقمية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة	التحول للمجتمع الرقمي: تكونت التفاعلات والسلوكيات الافتراضية، والشخصيات الافتراضية والمجتمع الرقمي.
الفرصة: لقد وفّرت التقنيات الحديثة فرصا غير مسبوقة لانتشار الجريمة الرقمية.	البطالة: الظروف الاقتصادية الصعبة والبطالة وسوء الوضع الاقتصادي.	العولمة: إنّ ظهور الفضاء الرقمي يكون ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر والفرص المباشرة للجريمة التي وفّرتها هذه الأجهزة.
ضبط الذات المنخفض: عدم الضبط الذاتي مع وجود الفرصة لارتكاب السلوك الطائش يعدان عاملين مؤثرين في ارتكاب الجريمة.	الضغوط العامة: تعدّ الضغوط التي يتعرض لها المجتمع من فقر وبطالة وظروف أمنية واقتصادية صعبة عوامل مؤدية لهذه الجرائم.	الترايط الكوني: هناك عامل يمكن أن يساهم في دفع مستويات الجريمة هو ظهور الترايط العالمي في سياق تحولات العالم الاقتصادية والديمقراطية.
الضغوط العامة: تلعب العوامل الاجتماعية ولاقتصادية دورا هاما في زيادة الجريمة الرقمية.	البحث عن الثراء: يلجأ بعض الأشخاص إلى الجريمة الرقمية لسهولة التنفيذ وسرعة المردود وقلة الخطورة.	انكشاف البنية التحتية الرقمية الكونية: تعود إلى الإهمال البشري وسوء التصرف وبالتالي يصعب ربط التهديد الرقمي بمكان أو زمان، أفراد أو جماعات، شخص عادي أو محترف.
النشاط الروتيني: إنّ التغيرات في أنشطة الأفراد الروتينية، من استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك والمواقع والايمل وغيرها، قد كونت فرصا للجنة مع وجود أهداف سهلة في الحيز الرقمي.	ضعف تطبيق القانون في الجرائم الرقمية: هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لتتمكن من مجاراة التقدم في مكافحة هذه الجرائم الرقمية وأساليبها.	

2.3 الدوافع النفسية للسلوك الإجرامي الرقمي :

الدوافع النفسية للسلوك الإجرامي الرقمي هي مختلف العوامل والأسباب النفسية التي ترتبط بذاتية المجرم والتي تدفعه للقيام بالجريمة الإلكترونية أين يكون إتيانه للسلوك الإجرامي الإلكتروني بسببها وهي ترتبط بشخصية المجرم وطبيعة تكوينه النفسي وبنائه الذاتي. (خرموش، 2021)

حيث يصف بول تايلور وأساتذة آخرون في علم النفس، حسب مقال لنورا جبران نشر بجريدة الحياة السعودية حول سيكولوجيا الجرائم الالكترونية: الانترنت تعري استعدادنا للجريمة، دوافع المجرمين الإلكترونيين بالفضول الشديد والانتقام، وأنهم يعانون من فراغ يسمح لهم بتمضية أوقات طويلة على شبكة الإنترنت، كما أنهم يتصفون وفقاً لما جاء في كتاب The psychology of cybercrime أو سيكولوجية الجرائم الإلكترونية، بأنهم يعانون من الوسواس القهرية، فلا يمكنهم السيطرة على رغبتهم في ملاحقة الآخرين وإيذائهم.



كما أنهم مصابون باضطراب الشخصية النرجسية، ويعانون من تقدير ذات متدنٍ، ولا يملكون القدرة على المواجهة أو التعامل مع المشكلات وإدارة العلاقات جيداً، ويفشلون في بناء علاقات صحيّة، ويقلل اضطراب الشخصية النرجسية من قدرتهم على تقدير نتائج أفعالهم، ويرتكبون أفعالاً تخدم شهوتهم إلى الانتقام، أو فضول التجسس لديهم، بغض النظر عن عواقب هذه الأفعال. - كما أنّ استخدام الوسائل الإلكترونية في إيذاء الآخرين وملاحقتهم، مستترين خلف هوية غير حقيقية، يشعرون بمزيد من القوة والسيطرة اللتين تتطلبهما نرجسيّتهم، وهوسهم المرضي بملاحقة ضحاياهم، وهو ما يوفره بسهولة الاتصال الدائم لهم ولضحاياهم على الشبكة العنكبوتية، من خلال أجهزة الهواتف والأجهزة المحمولة الأخرى، المرتبطة دائماً بالإنترنت، حيث تتركز إستراتيجيتهم في إيذاء الآخرين على الإصرار والمطاردة، وتتبع أصدقائهم ومن يتفاعلون معهم على شبكات التواصل الاجتماعي، ليروّجوا إشاعتهم عن ضحاياهم وتشويههم أمامهم.

وتفيد دراسات أخرى بأن مجرمي الإنترنت هم أشخاص لديهم ميل مرتفع إلى القلق الخارج عن السيطرة، الذي يؤدّي إلى التهور في استخدام الوسائل الإلكترونية في شكل غير مدروس، في تصفية الحسابات والإساءة إلى الخصوم. كما أنّ لديهم اعتقاداً بأن الوسائل الإلكترونية أسرع في نشر الفضائح أو التشهير بالآخرين. وهم كذلك عرضة للاكتئاب أكثر وأسرع من غيرهم، ويشعرون بأن الإساءة الإلكترونية أكثر أماناً لهم، واهمين أن من الصعب الوصول إليهم أو تحديد هويتهم الحقيقية.

ورغم أنه حتى الآن لم تظهر ملامح الصورة واضحة في تحديد صفات مجرمي الإنترنت والمعلومات وشرح سماتهم النفسية وتحديد دوافعهم، حسب ما تؤكده رجاء كامل في مقال حول الجريمة الالكترونية: الخطر داخل البيوت، خاصة مع قلة الدراسات الخاصة بهذه الظاهرة من جهة، ولصعوبة الفهم الجيد لمداها الحقيقي من جهة ثانية، والتطورات السريعة الحاصلة في ميدان الكمبيوتر والإنترنت من جهة ثالثة، فالمزيد من الوسائل والتكنولوجيات يعني المزيد من التغير في أنماط الجريمة وطرق الاعتداء، مما يساهم في إحداث تغير في سمات مجرمي الإنترنت.

3.3 الدوافع الاجتماعية للسلوك الإجرامي الرقمي:

الدوافع الاجتماعية للسلوك الإجرامي الرقمي هي العوامل البيئية التي تحيط بالفرد ومنها الاقتصادية والجغرافية، السياسية والثقافية والحضارية التي تؤثر في تكوين الشخصية فتبني سلوكاً يتوافق أحياناً مع متطلباتها وشاذاً في أحيان أخرى . (فتيحة، 2020) ومن خلال المنظور الاجتماعي وفي ظل التطورات الهائلة لتكنولوجيا المعلومات، ونظراً للعدد الهائل من الأفراد والمؤسسات الذين يرتادون هذه الشبكة، فقد أصبح من السهل ارتكاب أبشع الجرائم بحق مرتادها سواء كانوا أفراداً أم مؤسسات أم مجتمعات محافظة بأكملها، وهو ما دفع العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التي تهدد كل مستخدمي الإنترنت حيث أصبحت أسهل الوسائل أمام مرتكبي الجريمة، فراح المجرمون ينتهكون الأعراض ويغرون بالأطفال، إضافةً إلى اقترافهم لجرائم التشهير وتشويه السمعة عبر مواقع إلكترونية مخصصة لهذا الهدف. (طبي، 2017)

خاتمة:

لقد أدّى تطور انتشار تكنولوجيا الإعلام والاتصال إلى استحداث الكثير من المفاهيم المتعلقة بالبيئة الرقمية، من بين هذه المفاهيم نذكر المواطنة الرقمية، المواطن الرقمي، الإعلام الإلكتروني أو البديل، شبكات التواصل الاجتماعي، والجريمة الالكترونية. تتشابه الجريمة الرقمية مع الجريمة التقليدية في أطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة وضحية والذي قد يكون شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة، وهنا يكمن الاختلاف الحقيقي بين نوعي الجريمة ففي الجريمة الالكترونية الأداة ذات تقنية عالية وأيضاً مكان الجريمة الذي لا يتطلب انتقال الجاني إليه انتقالاً فيزيقياً ولكن في الكثير من تلك الجرائم فإن الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة.



ومن أجل ذلك لابدّ من فهم ماهية هذه الظاهرة الإجرامية المستحدثة في الفضاء الرقمي، وفهم أدواتها وطبيعتها مرتكبيها، ولأجل ذلك لابد من تضافر جهود كل الأطراف من أكاديميين، مختصين نفسانيين وقانونيين وسياسيين للحد من تفشي هذه الجرائم التي تنتشر بسرعة فائقة وتستخدم تقنيات فائقة تصعب من إمكانية مكافحتها.

قائمة المراجع:

1. أحمد المناعسة. (2001). جرائم الحاسب الآلي والإنترنت. عمان-الأردن: دار وائل للنشر والتوزيع.
2. بن غدفة شريفة، القص صليحة. (2017). الجريمة الإلكترونية ضد المرأة على صفحات الانترنت و طرق محاربتها . الجزائر.
3. بيومي عبد الفتاح. (2017). خصوصية المجرم الإلكتروني. الاسكندرية: منشأ المعارف.
4. جميل عبد الباقي الصغير. (2002). الجوانب الإجرامية للجرائم المتعلقة بالإنترنت . القاهرة: دار النهضة العربية .
5. خالد ممدوح إبراهيم. (2009). الجرائم المعلوماتية . الاسكندرية: دار الفكر الجامعي
6. مراد عبد الفتاح. (2007) . شرح جرائم الكمبيوتر والإنترنت. الاسكندرية: دار الكتب والوثائق
7. منير طي . (2017) . الجريمة الإلكترونية : المنظور النفسي، الاجتماعي والأمني . شبكة النبا المعلوماتية.
8. شيخ فتيحة. (2020). السلوك الإجرامي: مقارنة سيكولوجية للعوامل المؤدية لحدوثه، والوقاية منه. مجلة أبعاد ، 293-304.
9. صابر بحري، منى خرموش. (2021). أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية. مجلة دراسات في سيكولوجية الانحراف ، 36-59.
10. نائلة عادل محمد. (2004). جرائم الحاسب الاقتصادية (دراسة نظرية تطبيقية) . القاهرة: دار النهضة العربية.
11. هشام محمد رستم. (1 ماي، 2000). الجرائم المعلوماتية أصول التحقيق الجنائي الفني. بحوث مؤتمر القانون والكمبيوتر ، صفحة 407.



السلوك الإجرامي الرقمي وانعكاساته على المجتمع الجزائري

Digital Criminal Behavior and Its Repercussions on Algerian Society.

. خليدة ولد قويل

kh.ouldgouail@univ-bouira.dz

مصباح أمال

a.mesbah@univ-bouira.dz

مقدمة

مع التطور التكنولوجي و المعلوماتي الهائل الذي شهدته العديد من المجتمعات ظهر نوع جديد من الجرائم و المتمثلة في الإجرام الرقمي أو ما يعرف بالجرائم الالكترونية , والتي هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي أو الهواتف الذكية الموصولة بشبكة الانترنت لتنفيذ الفعل الإجرامي هذا الأخير الذي يتخذ بدوره العديد من الصور كجرائم الواقعة على الأشخاص من سطو وسرقة وانتهاك للخصوصية وتشهير... الخ. حيث أضحت هذه السلوكيات الإجرامية الرقمية في الآونة الأخيرة تشكل تهديد على أمن وسلامة الأفراد والمجتمعات والدول لما أفرزته بين هذه المجتمعات التي عرفت تناميا في هذا النوع من السلوكيات الإجرامية الرقمية على مستوى أفرادها ومؤسساته حيث من انعكاسات على العديد من المستويات سواء الشخصية أو الاجتماعية أو الاقتصادية أو الأمنية و المجتمع الجزائري من كان له الأثر البالغ في كثير من الجوانب ما دفعنا لتسليط الضوء على هذه الظاهرة الإجرامية المستحدثة محاولين بذلك تحليل الوضع السائد لهذه الظاهرة من خلال تبيان ماهيتها وأهم خصائصه وتداعياته السلبية على المجتمع الجزائري بهدف معالجة وتبعية عواقبها .

مشكلة البحث: تبعا لما تقدم تتحدد مشكلة دراستنا بطرح التساؤل التالي: ما هي أهم انعكاسات السلوك الإجرامي الرقمي على المجتمع الجزائري؟

والذي يتفرع منه الأسئلة الفرعية التالية :

- ماذا نقصد بالسلوك الإجرامي والجريمة الإلكترونية والمجرم الرقمي؟
 - ما هي أنواع وأهم خصائص الجريمة الالكترونية ؟
 - ما هو واقع الجرائم الرقمية على المستوى الدولي والعربي والوطني؟
 - ما هي انعكاسات السلوك الرقمي الإجرامي على المجتمع الجزائري؟
- أهمية الدراسة:** تكمن أهمية هذا البحث في تناولنا لأحد الظواهر الإجرامية المستجدة والخطيرة والتي كان لها تداعيات وأبعاد خطيرة على العديد من المجتمعات ومنها المجتمع الجزائري ولهذا ارتأينا إلى البحث في هذا الموضوع من خلال تبيان أهم إفرازات الإجرام الرقمي في المجتمع الجزائري .

أهداف الدراسة: تتلخص أهداف البحث في ما يلي :

- التعرف على ماهية السلوك الإجرامي الرقمي.
- التعرف على أهم أنواع وخصائص الجرائم الرقمية .
- تسليط الضوء على واقع السلوك الإجرامي الرقمي على المستوى الدولي والعربي والوطني.



- تسليط الضوء على انعكاسات السلوك الإجرامي الرقمي على المجتمع الجزائري.

المنهج المعتمد في الدراسة : من أجل الإجابة عن الإشكال والتساؤلات البحثية المطروحة تم الاعتماد في هذه الدراسة على وصف و تحليل المعطيات من خلال الإحصائيات و الدراسات المتوفرة في موضوع الجرائم الالكترونية خاصة في المجتمع الجزائري مع محاولة تفسيرها في ضوء المقاربات السوسيولوجية و العلمية التي يراها الباحث أنها مناسبة.

الدراسات السابقة:

دراسة قيسي،(2010) بعنوان الجرائم الموجهة ضد مستخدمي الانترنت دراسة مسحية لبعض مستخدمي الانترنت بالمملكة العربية السعودية تهدف إلى الكشف عن حجم الجرائم الجنسية وجرائم الاختراق والجرائم المالية الموجهة ضد مستخدمي الانترنت , ومن أبرز نتائجها أن 53 % من مستخدمي الانترنت وجهت لهم دعوات من المواقع الجنسية عبر الانترنت، و 2 % تعرضوا للتشهير من قبل أشخاص على الانترنت وأن 7.7 % تعرضت مواقعهم الإلكترونية للاختراق، وتعرض 24.6 % تم تعرض أجهزتهم الشخصية للقرصنة، و 3.5 % تم العبث برصيد البطاقة الائتمانية و 29.5 % تعرضوا لدعوات للعب القمار و 2.9 % تعرضوا لدعوات من مواقع خاصة بتجارة المخدرات. (قيسي، 2010)

دراسة إيمان(2014) : بعنوان "الجريمة الإلكترونية عبر الانترنت في أوساط الطلبة الجامعيين "هدفت الدراسة الكشف عن مدى انتشار الجرائم الالكترونية عبر الانترنت في أوساط الطلبة الجامعيين وأنماط استخدام الطالب الجامعي للانترنت في الجزائر، وقد توصلت الدراسة إلى أن "الفيسبوك" من أهم مواقع الشبكات الاجتماعية التي تستأثر بقبول وتجارب الطلبة، وأن أكثر المواقع التي يرتادها الطلبة هي المواقع الترفيهية، كما أظهرت النتائج أن 60 % قد تعرضوا للشتم، وأن 10.77 % قد تعرضوا للابتزاز، و 4.62 % قد تعرضوا للتحرش الجنسي، كما تعرض 23.33 % للتشهير. (ميرة، 2014)

دراسة حسن (2015):هدفت هذه الدراسة إلى بيان سياسة المشرع الإماراتي تجاه الخطر الدائم للجرائم الالكترونية , والتعرف على التشريعات الموجودة بدولة الإمارات للتعامل مع هذه النوعية من الجرائم مع تبيان موقف المشرع الإماراتي منها , وسعت هذه الدراسة التي تناولناها إلى التعرف إلى واقع الجريمة الالكترونية في الإمارات مع الوقوف على التشريعات الصادرة بشأنها والتعرف على التوجهات الفكرية لدى المشرع الإماراتي في ظل التغيرات المتسارعة في عصر الثورة التقنية , كما اعتمدت هذه الدراسة على المنهج الوصفي التحليلي وذلك بتعرض لماهية الجرائم الالكترونية ومفهومها وأنماطها وخصائصها وسماتها ومخاطرها ومن أبرز نتائج هذه الدراسة: وجود مخاطر عديدة و أضرار تشكلها الجرائم الالكترونية بأنواعها المختلفة , عدم اقتصار المخاطر والأضرار التي تشكلها الجرائم الالكترونية على جانب واحد إذا اتسمت تلك الأخطار والأضرار بالتعدد والتنوع , هناك جوانب قانونية جديدة يجب على المشرع القانوني مراعاتها عند إعداد وصياغة القوانين المنظمة للتعامل مع الجرائم الالكترونية بأنواعها. (الكحلوت، 2019، الصفحات 22,21)

دراسة حفصي (2015) تناول دراسة بعنوان جرائم التزوير الإلكترونية (دراسة مقارنة), اعتمد الباحث من خلالها على كل من المنهج التحليلي والاستقرائي والمقارن, فيما هدفت إلى تبيان مدى معالجة كل من الشريعة الإسلامية وقانون العقوبات الجزائري لهذا النوع من الجرائم , كما بحثت في شكل العقوبة وأثارها بين كل من الشريعة والقانون , إضافة للبحث في ما إذا سن المشرع الجزائري قانون يعنى بهذا النوع من الجرائم , كما هدفت لتبيان القصد من جريمة التوقيع الالكتروني وتزوير البريد الالكتروني , و الأضرار الناجمة عن هذا النوع من الجرائم دنيا وقانونيا واقتصاديا .ومن النتائج التي خلصت إليها :وجود قصور في ضبط مصطلح التزوير حيث أنه لم ينل سبكا علميا أو قانونيا دقيقا الأمر الذي أدى ببعض القوانين ومنها القانون الجزائري إلى عدم تعريفه والاكتفاء بتحديد الأطر العامة التي تفهم من خلاله ,وجود اختلاف بين جريمة التزوير الالكتروني والتقليدي لاشتراط الأول استخدام الحاسب الآلي ,تنوعت



العقوبات المفروضة من قبل مرتكبي جريمة التزوير الالكتروني من الناحية القانونية بين عقوبات سالبة للحرية وغرامات وعقوبات تبعية كالحرمان من الحقوق في حين تمثلت في العقوبات التعزيرية كالنفي الجلد أو الحبس، كما خلصت إلى تعدد فئة الجناة في هذا النوع من الجرائم من أشخاص عاديين ومحترفين وقرصنة، بينت أن تزوير التوقيع الالكتروني هو صورة من صور التزوير المعلوماتي، قصور المقنن الجزائري في معالجة تزوير التوقيع الالكتروني بصفة خاصة والتزوير الالكتروني بصفة عامة. (حفصي، 2015)

دراسة شالح، وقرشي (2017) دراسة بعنوان "انتشار الجريمة الإلكترونية الماسة بالأشخاص في البيئة الجزائرية" هدفت الدراسة التعرف إلى أنماط وعادات استخدام الأشخاص للإنترنت في البيئة الجزائرية والتعرف إلى أهم صور وأشكال الجريمة الإلكترونية الواقعة على الأشخاص، وتكونت عينة الدراسة من "2. من مستخدمي الإنترنت من شتى المقاهي بولاية المسيلة، وتوصلت الدراسة إلى نتائج مفادها أن الأشخاص يتعرضون لجريمة وصناعة الإباحية بدرجة متوسطة، وأن جرائم انتحال الشخصية والتغريب والاستدراج يستهدف هذا النوع من الجرائم صغار السن بصفة كبيرة و الأشخاص بصفة عامة للتغريب بهم والضغط عليهما بالالكتروني بصفة عامة . (شالح و القرشي، 2017)

دراسة نمر محمد حسن البدوي (2020): تناول دراسة بعنوان "الجرائم الواقعة على العرض بالوسائل الالكترونية" التشريع الأردني" , اعتمد من خلالها الباحث على المنهج الوصفي التحليلي , ومن خلال تحليل القواعد العامة ومدى تطبيقاتها على الجرائم الواقعة على العرض بالوسائل الالكترونية مع المقارنة بين التطبيقات القانونية المقارنة وتحليل بعض النصوص القانونية النافذة , ومن النتائج المتوصل إليها : بينت الدراسة مدى خطورة الوسائل الالكترونية إذا ما استخدمت للمساس بالأداب والأخلاق العامة وموقف المشرع الأردني تجاه تلك الأفعال التي تتم بالوسائل الالكترونية. كما بينت الدراسة مجموعة الجرائم الواقعة على العرض ومدى مساهمة الوسائل الالكترونية في قيامها حسب النموذج القانوني لتلك الجرائم . وإشارات الدراسة إلى الجرائم الالكترونية التي عالجها المشرع الأردني في قانون الجرائم الالكترونية . كما بينت صور الاعتداءات التي مست القاصرين بالوسائل الالكترونية . (البدوي، 2020)

التعقيب على الدراسات السابقة: نلاحظ من خلال ما تم عرضه من دراسات سابقة اهتمامها بموضوع الجرائم الالكترونية إلا أنها اختلفت في الأهداف المسطرة لكل دراسة منها. فنجد أن دراسة كل من قيسي (2010) و إيمان (2014) و شالح وقرشي (2017) قد سلطا الضوء على أهم أشكال وصور الجرائم الواقعة في الوسط الرقمي حيث خلصت دراسة كل منهم إلى تفشي مجموعة من صور الإجرام الرقمي والتي شملت حسب نتائج دراسة إيمان (2014) الجرائم الماسة بالأفراد و تمثلت حسب نتائج الدراسة في الشتم والتحرش الجنسي والتشهير، والابتزاز في حين تمثلت حسب دراسة قيسي (2010) في كل من جرائم القرصنة والاختراق و تلقي دعوات من مواقع خاصة بتجارة المخدرات) وفي ذات الصدد بينت دراسة شالح وقرشي (2017) التي سلطت الضوء بدورها على أشكال الجرائم الالكترونية الواقعة على الأشخاص في المجتمع الجزائري والتي تمثلت صورها من خلال نتائج الدراسة في (صناعة الإباحة، وجرائم التغريب والاستدراج التي استهدفت حسب النتائج فئة الصغار أكثر من الفئات الأخرى)، وبينما تناولت دراسة كل من حسن (2015) ودراسة نمر محمد البدوي (2020) موضوع الإجرام الالكتروني (الرقمي) من خلال تسليط الضوء على الجانب القانوني أي المواد القانونية ومدى نجاعتها وإلمامها بهذا النوع من الجرائم في كل من التشريع الأردني والتشريع الإماراتي إضافة إلى تبيان واقع هذا النوع من الجرائم والذي تحدد حسب نتائج الدراستين بمدى مساهمة الوسائل الالكترونية في تفشي العديد من الجرائم و تبيان الأضرار المترتبة عليها والحث على ضرورة سن قوانين رادعة وشاملة كما أشارت إلى خطورة الوسائل الالكترونية إذا ما استخدمت للمساس بالأداب والأخلاق العامة. في حين تناولت دراسة حفصي (2015) جرائم التزوير الإلكتروني وذلك بتسليط الضوء على الناحية الشرعية والقانونية (دراسة مقارنة) مع البحث في الأضرار الناجمة عنها و البحث أيضا في سن المشرع الجزائري لقانون خاص بهذا النوع من الجرائم و خلصت هذه الدراسة لوجود قصور في ضبط مصطلح التزوير والاقتصار على



عرضه من خلال الأطر العامة ما أسهم بدوره في قصور المقتن الجزائري في معالجته كما بينت النتائج أن هذا النوع من الإجرام لا يقتصر على القراصنة والمحترفين إنما يشمل الأشخاص العاديين أيضا. وتتوافق دراستنا الحالية مع مجموعة الدراسات المقدمة كونها تناولت ظاهرة الإجرام الإلكتروني (الرقمي) حيث تتداخل معها في عدة جوانب ما ساهم في الاستفادة منها سواء في ما تقدم ضمن إطارها النظري وما تضمنه من عرض لماهية هذه الظاهرة وخصائصها وأنواعها أو من خلال النتائج البحثية والإحصائيات الميدانية المتحصل عليها خاصة تلك التي عنت بالمجتمع الجزائري والتي ساعدتنا في استخلاص أبعاد الظاهرة المتناولة لدراسة، في حين تختلف الدراسة الحالية عن ما تقدم كونها تركز على البحث في انعكاسات السلوك الإجرامي الرقمي في المجتمع الجزائري سواء على مستوى الأفراد أو الاقتصاد أو الأمن. الخ.

1. الجانب النظري ولفاهيمي:

1.1. تعريف السلوك الإجرامي: لقد برز في التراث الاجتماعي حول تعريف الجريمة ثلاث اتجاهات أساسية:

2.1.1. الاتجاه الأول: ويعتبر هذا الاتجاه الجريمة هي جميع أنماط السلوك المضاد للمجتمع، والذي يترتب عليه ضرر بالمصلحة الاجتماعية و هذا التعريف يستند في أساسه على رد الفعل الاجتماعي والاستنكار للأفعال ومن ناحية أخرى يشير إلى الأفعال إلى يكون لها رد فعل استنكاري ومع ذلك يتم تدارك خطرها من قبل السلطة.

3.1.1. الاتجاه الثاني: فيركز على معايير السلوك حيث يرى أنصار هذا الاتجاه أهمية التركيز على المعايير للسلوك وهذا الجانب يرتبط مباشرة بقضية الضبط الاجتماعي وما يتضمنه من معايير تحكم سلوك الأفراد سواء في جانبه الرسمي أو غير الرسمي. (عزيز و عيساوي، الجريمة من منظور سوسيولوجي - الأسباب والآثار، 2021، صفحة 13)

4.1.1. الاتجاه الثالث: والذي يستند إلى إعادة تعريف الجريمة وذلك من خلال ما قام به سيدرلاند بدراسته للجرائم الخاصة أو الجريمة ذات الياقات البيضاء، وقد عضد كل من "هارتينج" و "كلينا رد" هذا الاتجاه لتوسيع من مفهوم الجريمة ليشمل كل الأفعال الإجرامية أو الأفعال المخالفة للمعايير الاجتماعية التي تخضع للعقاب لما يترتب عليها من أضرار على المصلحة الاجتماعية. (عزيز و عيساوي، الجريمة من منظور سوسيولوجي - الأسباب والآثار، 2021، صفحة 136)

5.1.1. التعريف الإجرائي للجريمة: هي مجموعة من السلوكيات الإجرامية ذات الطابع الرقمي (الالكتروني) التي ترتكب ضد الأفراد أو المؤسسات أو الدولة مع وجود دافع إجرامي لإلحاق الضرر النفسي أو الجسدي أو المادي أو الأمني للضحايا سواء بصورة مباشرة أو غير مباشرة باستعمال وسائل التكنولوجيا الحديثة من حواسيب وهواتف ذكية وتختلف وتنوع هذه السلوكيات الإجرامية بحسب طبيعة الجرم المرتكب فيها، والتي يكون لها تداعيات خطيرة على الفرد والمجتمع والوطن.

2.1. تعريف الجريمة الإلكترونية (الرقمية): إن مسألة وضع تعريف للجريمة الإلكترونية كانت ولا تزال موضع أخذ ورد بين مختلف الأوساط الفقهية، لهذا لا نجد تعريف محدد للجريمة الإلكترونية نتيجة ظهور عدة اجتهادات فقهية متشعبة في هذا المجال، وعلى إثر ذلك فقد رصد الفقهاء والدارسون لمفهوم الجريمة الإلكترونية عدد من التعريفات التي تباينت ما بين ضيقة وأخرى موسعة والتي سنحاول عرض البعض منها: (سعيد، 2019، صفحة 225)

1.2.1. التعريف الضيق للجريمة الإلكترونية: من التعريفات التي وضعها أنصار هذا الاتجاه نجد أن هناك من عرفها على أنها " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى " كما عرفت على أنها " الجرائم التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط "، كما عرفت على أنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه " (خالد، صفحة 2)



كما عرفت على أنها " الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا هاما , أو هي كل فعل إجرامي يستخدم الجانب الآلي في ارتكابه كأداة رئيسية". (زيوش، 2019، صفحة 130)

ما يؤخذ على هذه التعريفات أنها أتت مختصرة وقاصرة عن الإلمام بكل أوجه ظاهرة الإجرام الالكتروني , حيث ذهب البعض من أنصار هذا الاتجاه إلى التركيز على معيار موضوع الجريمة في حين ركز البعض الآخر على وسيلة ارتكابها بينما ركز البعض الآخر على معيار النتيجة .

2.2.1. التعريف الموسع للجريمة الالكترونية : عرفها أنصار هذا الاتجاه على أنها " كل سلوك إجرامي يتم بمساعدة الكمبيوتر " (خالد، صفحة 2) كما عرفت على أنه " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها " كما عرفت في إطار المنظمات الأوروبية للتعاون والتنمية الاقتصادية بأنها " كل فعل أو امتناع من شأنه أن يؤدي إلى الاعتداء على الأموال المادية يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية " كما عرفت من قبل الأمم المتحدة في مؤتمر فيينا 2000 على أنها " أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي , والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئته الإلكترونية".

وما يؤخذ على هذه التعريفات التي اتسمت بالتوسع في مفهوم الجرائم الالكترونية على أن هذا التوسع من الممكن أن يدفع بها إلى وصف بعض الممارسات على أنها جرائم إلكترونية في حين قد لا تكون كذلك لمجرد مشاركة الحاسوب الآلي في النشاط الإجرامي, فبعض جرائم سرقة الحواسيب أو الأقراص مثلا لا يمكن تصنيفها كجرائم الكترونية لمجرد أن الحاسوب أو أحد مكوناته المادية كان محل لفعل الاختلاس. (زيوش، 2019، صفحة 130)

3.2.1. التعريف التشريعي للجريمة الالكترونية: تأثر المشرع الجزائري بغيره من التشريعات الأجنبية الأوروبية منها والعربية , فيما يخص القواعد التي استند إليها أو أتى بها لمكافحة الجرائم المعلوماتية , حيث اتجه إلى خلق نصوص جديدة وخاصة تتعلق بهذا النوع من الإجرام رغبة منه تأمين أنظمة المعلومات من اعتداءات المجرمين , حيث اصطلح المشرع الجزائري على تسمية الجريمة الإلكترونية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال , حيث تبنى بذلك التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي بموجب المادة الثانية من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وعرفها على أنها : " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية " ومما يستخلص من هذا ما يلي:

- أن المشرع الجزائري قد اعتمد معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية
- معيار وسيلة الجريمة وهو نظام الاتصالات الالكترونية .
- معيار موضوع المساس بأنظمة المعالجة الآلية للمعطيات.
- معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.
- الإقرار بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه, الأمر الذي يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري. (غيدلي، 2017، صفحة 6)

4.2.1. التعريف الإجرائي للجريمة الالكترونية: هي الجرائم ذات طابع الكتروني والتي ترتكب بواسطة أداة الكترونية أو داخل بيئة رقمية و التي تمس بالأشخاص والمجتمع و شكل من أشكال مخالفة المعايير الأخلاقية التي يرتضيها المجتمع ويعاقب عليها القانون .

3.1. تعريف الجرم الرقمي (الالكتروني): لقد تعددت التسميات التي أطلقت على هذا النوع من المجرمين منها "قراصنة المعلوماتية" "الهكرة" "المجرم الالكتروني" "المجرم المعلوماتي" "مجرم الانترنت" الخ



ويقصد بالجرم الرقمي " هو مجرم سلك سبيل التقنية لارتكاب جرائمه والمتمثل في استخدامه لتقنية المعلومات " (يونس و عمر، 2004، صفحة 233)

يعرف أيضا " انه الشخص الذي يمتلك مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الالكتروني والقادر على استخدام هذا الاختراق "الكود" السري لتغير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب فيه . (قشقوش، 1992، صفحة 32) يعرف أيضا " هو المجرم الذي له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الالكتروني في ملحقاته ووسائل الاتصال الرقمية ، وذلك بأداء فعل الامتناع عنه ، مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفته". (بكوش و هروال، 2021، صفحة 76)

التعريف الإجرائي للمجرم الرقمي: هو الشخص الذي يمارس الجريمة داخل البيئة الرقمية ويكون له دراية واسعة بتقنيات التكنولوجيا المتطورة والتي يستهدف من خلالها إما الأشخاص أو المؤسسات أو الدولة بهدف إلحاق الضرر المادي أو المعنوي أو بهدف البحث عن الانتفاع المادي الخاص .

4.1. النظريات: اخترنا لدراستنا كل من نظرية النشاط الروتيني ونظرية الضغوط العامة لما تركز عليه من أفكار نرى أنها تتناسب وتساعد في تحليلنا لموضوع الدراسة.

1.4.1. نظرية النشاط الروتيني: ظهرت هذه النظرية أواخر السبعينات. و تركز على فكرة جوهرية مفادها أن الجريمة تحدث في حالة ما التقت العناصر الثالث المتمثلة في المجرم الذي لديه الدافع والهدف المناسب، إضافة إلى غياب الحراس ، وهذا يعني أن احتمالية وقوع الجريمة (الرقمية) تزداد إذا تواجد شخص أو أكثر لديهم الدافع لارتكاب الجريمة (المجرم الرقمي)، وإذا تواجد الهدف المناسب أو الضحية المحتملة (أفراد، مؤسسات، دول)، وكذلك إذا غاب الحراس الرسميون أو غير الرسميين والذين يمكن أن يردعوا أو يوقفوا المجرم المحتمل (الضبط الرسمي) (الخرابشة و الزير، 2012)، كما ويمكن تفسير زيادة ضحايا الجريمة الرقمية في المجتمع الجزائري من خلال التغيرات في أنشطة الناس الروتينية في الحياة اليومية للأفراد، فمع ظهور شبكة الإنترنت تغيرت طريقة الناس التي يتواصلون بها أو يتفاعلون من خلالها مع الآخرين من حيث تكوينهم للعلاقات الشخصية، وفي طرق الترفيه التي يعتمدونها، و النشاطات التجارية والاستهلاكية الخاصة بهم... الخ (البدانية، 2014، صفحة 13.12). والتي ارتبطت بشكل أساسي برقمنة ، كما تغيرت أنشطة الناس الروتينية إلى استخدام شبكات التواصل الاجتماعي كال فيسبوك وغيرها من الوسائط الرقمية كل هذه الممارسات الروتينية المستجدة، قد ساهمت في فتح المجال للمجرمين الرقميين لترصد لضحاياهم في البيئة الرقمية سواء من خلال الولوج إلى حساباتهم والترصد لكل شؤون حياتهم وعلاقاتهم وخصوصياتهم مما يجعل منهم أهداف سهلة للابتزاز الرقمي أو الاحتيال وكثير ما تسهم هذه الممارسات الإجرامية إلى خلق جرائم أشهد خطورة داخل المجتمع الجزائري حيث أنها قد تكون الدافع لتحكم في الآخرين والدفع بهم للممارسة سلوكيات إجرامية أخرى كالديارة و التجسس لصالح بلدان أخرى والسرقة أو بالاشتراك ببعض الممارسات الإجرامية الأخرى .

2.4.1. نظرية الضغوط العامة : ترجع هذه النظرية الانحراف وخرق القانون إلى الدوافع الناجمة عن قوى البناء الاجتماعي واستجابات النفس البشرية للحوادث والظروف والتي تعمل كضغوطات أو مقلقات ، خاصة عندما لا تتاح الفرصة للأفراد لتحقيق أهدافهم المقبولة اجتماعيا ، وأن مصادر الضغوط لا تقف على الإحباط الذي يختبره الفرد عندما يفشل في تحقيق هدفا معين بل تشمل تلك المشاعر السلبية التي تحدث في المواقف الاجتماعية المختلفة . (البدانية، 2014، صفحة 13) كما وقد تلعب العوامل الاقتصادية والاجتماعية التي يعاني منها الأفراد داخل المجتمع الجزائري دورا هاما في زيادة تفشي السلوكيات الإجرامية الرقمية ، حيث تعمل الضغوط العامة التي يتعرض لها الفرد من فقر وبطالة وظروف اقتصادية صعبة وعوامل نفسية ضاغطة على المجتمع عامة وعلى الشباب



خاصة إلى توليد المشاعر السلبية ضد هذه الظروف الصعبة الأمر الذي قد يدفع بهم إلى امتحان الإجرام الرقمي الذي تتعدد صوره وأنماطه بكونه يستهدف كل الفئات ويمس كل الجوانب الحياتية , كما و يكون الهدف من هذه الممارسات الإجرامية في أكثر الأحيان الانتفاع المادي وذلك من خلال الكسب عن طريق السرقة أو الاحتيال الالكتروني أو عن أو الانتفاع المعنوي من خلال إلحاق الضرر بالآخرين سواء من خلال المساس بسمعتهم وشرفهم أو إفشاء أسرارهم , الأمر الذي من شأنه أن يسهم في تفشي عديد الممارسات الغير قانونية و الإخرافية والإجرامية التي تضرب بقيم المجتمع الجزائري وتعتبر خرقا لمعاييرها الاجتماعية .

2. خصائص الجرائم الالكترونية (الرقمية):

تتميز الجرائم الالكترونية بمجموعة من الخصائص منها:

1.2. جرائم ذات بعد دولي: أي أنها تتعدى الحدود الجغرافية للدول , لكونها عابرة للقارات , وذلك نتيجة الانتشار الواسع لشبكة الاتصالات والانترنت مما ساهم في ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر

2.2. عدم التبليغ: عند وقوع الجريمة بواسطة الانترنت نجد أن بعض الضحايا يمتنعون عن الإبلاغ لدى السلطات المعنية وذلك خشية على السمعة والمكانة, وخوفا من اهتزاز الثقة في كفاءته خاصة إذا مثل كيانا أو هيئة معينة (بن زعومة و بلفكيرات، 2019، صفحة 514)

3.2. سرعة محو الأدلة : وذلك أن هذا النوع من الجرائم يكون سهل محو أدلته من على الكمبيوترات المستعملة وفي زمن قياسي من خلال استخدام برامج مخصصة لذلك بمجرد إحساس المجرم الرقمي بأي خطر يستطيع التخلص من كل الأدلة التي تدينه الأمر الذي يوحى بصعوبة هذا النوع من السلوكيات الإجرامية الرقمية المنتشرة في مجتمعاتنا.

4.2. الجاذبية : نظرا لما تمثله سوق الكمبيوتر والانترنت من ثروة كبيرة للمجرم الرقمي وخاصة في الإجرام المنظم , فلقد غدت أكثر جديبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويها مسارها أو استخدام أرقام البطاقات. (بن خليفة و حفوطة، 2017، صفحة 157)

5.2. التمتع بالسلطة : من مميزات المجرم الرقمي تمتعه بالسلطة سواء المباشرة أو الغير مباشرة تجاه النظام الالكتروني أو المعلوماتي والتي تتمثل في المزايا التي يتمتع بها وتكون مساعدة له على ارتكاب سلوكاته الإجرامية , والتي قد تتمثل في امتلاكه للأرقام السرية الخاصة للولوج إلى النظام الذي يحتوي على المعلومات التي تمده بمزايا متعددة كفتح الملفات وقراءتها وكتابتها والتعديل فيها أو محوها. (حبيباني، 2020، صفحة 610)

3. أنواع الجرائم الالكترونية (الرقمية):

شهد المجتمع الجزائري بروز العديد من الجرائم المتعلقة بشبكة الانترنت والتي تستخدم فيها الوسائل التكنولوجية كأداة للقيام بالفعل الإجرامي والتي اختلفت ما بين من تستهدف الأشخاص ومنها من تقع على المال وأخرى ضد الدولة والصالح العام:

1.3. الجرائم الرقمية ضد الأشخاص : والتي تشمل العديد من السلوكيات الإجرامية الرقمية كجرائم السطو على بنوك المعلومات في برامج النظام المعلوماتي الخاص بالأفراد, وأيضا الجرائم التي تمس بأخلاق وسمعة الآخرين, إضافة إلى الجرائم التي تستهدف الحياة الخاصة للأفراد وذلك من خلال التجسس على الأفراد داخل البيئة الرقمية من حيث ممارساتهم داخل هذه البيئة وحياتهم وأسرارهم وصورهم الأمر الذي قد يفرض بعدها إلى العمل على استعمال كل هذه البيانات المتحصل عليها من قبل المجرم الرقمي أما لابتزاز الضحية أو التشهير به الأمر الذي يسهم بدوره إلى تعرض الأفراد إلى الدخول في صراعات نفسية أو خلق التفرقة



2.3. الجرائم الواقعة على الأموال: والتي تشمل بدورها عدد من الجرائم كجرائم السطو على المعاملات التجارية من خلال الجو سسه وجرائم القرصنة وما تدره من أموال على الجناة، جرائم السرقة والسطو على أموال البنوك، القمار وغسيل الأموال عبر الانترنت

3.3. الجرائم الواقعة ضد الدولة: والتي تعتبر جرائم ضد المصلحة العامة، والتي تنال بالاعتداء أو التهديد بالخطر لصالح العام، ومن أبرز هذه الجرائم نجد نشر الأخبار الخاطئة على الحاسب، خلق الإشاعة الموجهة بغرض ضرب مصالح دولة ما أو بغرض خلق توترات داخلها من خلال توجيه الرأي العام تجاه أفكار هدامة، جرائم تعطيل الأعمال الحكومية، الإرهاب الإلكتروني.. الخ (حمشاشي، ص13)

4. واقع السلوك الإجرامي الرقمي:

1.4. على المستوى الدولي: مع شيوع استخدام الكمبيوتر أواخر سبعينيات القرن الماضي برزت ظاهرة الجريمة الالكترونية وسرعان ما تحول السلوك الرقمي من انحراف للمراهقين الشغوفين بالتكنولوجيا إلى سلوكيات إجرامية رقمية تستهدف الأشخاص و مصالح الدول وتهدد المنشآت الحيوية، كما شملت تدمير المخزون النقدي للبنوك والدول كما تستهدف المعطيات السرية للأفراد والهيئات والدول، وهذا ما ذهب لتأكيد العديد من الإحصائيات.

أكدت أن بريطانيا قد شهدت سنة 2007 أن هناك جريمة الكترونية تقع كل 10 ثواني بمعدل 3 مليون جريمة بالسنة أو 8 الآلاف جريمة باليوم، حيث مثلت فيها جرائم التحرش الجنسي أعلى نسبة بما يعادل 850، في حين مثلت جرائم سرقة الهوية أي الحصول على معلومات شخصية حول مستخدم الانترنت، و145 ألف حالة لاختراق الحواسيب بهدف سرقة المعلومات أو تخريبها، كما بلغت نسبة جرائم الاحتيال على الأموال 207 ألف حالة والتي تمثلت في جرائم السطو والاحتيال على أرقام البطاقات الائتمانية، كما أكدت إحصائيات شركات التأمين على أن 70% من هذه الجرائم تستهدف الأفراد. (دياب و بوترة، 2020، صفحة 16)

كما بينت دراسة لموقع (أرقام ديجيتال) أن عدد ضحايا الإجرام الرقمي قد بلغ ما يقارب 1,5 مليون ضحية، كما بين أن من أكثر أنواع الجرائم الرقمية المنتشرة جريمة سرقة الهويات والتي بلغت نسبتها 224 مليون سرقة، كما بينت هذه الدراسة أن مواقع التواصل الاجتماعي هي الأكثر اختراقا حيث أن أكثر من 600 ألف حساب فيسبوك يتم اختراقها يوميا، فيما أكدت ذات الدراسة أن الكلفة السنوية المخصصة للأمن المعلوماتي قد قدرت ب 100 مليار دولار، بعدما كانت في حدود 63,1 مليار دولار سنة 2011. وحسب التقرير الذي نشرته شركة مشاريع الأمن السيبراني فإن العالم سينفق على منتجات وخدمات الأمن السيبراني لمكافحة الإجرام الرقمي أو ما اصطلح عليه بالجرائم الالكترونية في الفترة ما بين 2017 إلى 2021 ما قيمته 1 تريليون دولار. (زبيدي و حفوفة، واقع جرائم تكنولوجيا الإعلام والاتصال في العالم وآليات مكافحتها، 2017، صفحة 79)

2.4. على المستوى العربي:

شهد الوطن العربي بفعل التطور التكنولوجي والاستعمال الموسع لوسائل التقنية مع ما رافقه من التوسع في درجة الإمداد بالانترنت في البلدان العربية والتي انتقلت من الاستعمال الضيق إلى الاستعمال الموسع على كل المستويات إلى ظهور تهديد كبير على اقتصاديات هذه الدول ومجتمعاتها خاصة مع تزايد في نسبة الإجرام الرقمي. إذ كشف موقع جوبال ريسك إنسايتس أن المملكة العربية السعودية تعد البلد الأكثر استهدافا بالهجمات الإلكترونية في الشرق الأوسط، كما نوه التقرير إلى أن الإمكانات الرقمية الالكترونية الكبيرة للسعودية تجعلها هدفا مميذا للعديد من الهجمات الالكترونية حيث تمتلك المملكة السعودية أكبر عدد من المشتركين في خدمة الانترنت في الوطن العربي.



في حين بلغت عمليات القرصنة الالكترونية التي تعرضت لها المصارف اللبنانية حصرا منذ 2011 حتي الفصل الثاني من سنة 2016 ووفق أرقام هيئة التحقيق الخاصة لدى مصرف لبنان 233 عملية , وصلت فيها قيمة الأموال التي تعرضت للقرصنة إلى نحو 26 مليون ونصف المليون دولار , من ضمنها 15 مليون دولار بين عامي 2015-2016 . (زيبيدي و حفوطة، جرائم تكنولوجيا الاعلام والاتصال في العالم وآليات مكافحتها، 2017، صفحة 82)

3.4. على المستوى الوطني: عرفت الجزائر هي الأخرى على غرار باقي الدول تزايد مستمر من سنة لأخرى في عدد الإجرام الرقمي بعدما تم تسجيل 2130 جريمة الكترونية سنة 2017 ارتفع عددها سنة 2018 إلى 1392 جريمة الكترونية. - كما أثبتت الإحصائيات الوطنية للأمن الوطني أنه خلال الفترة ما بين 2017-2018 تصدرت جرائم المساس بالأشخاص عبر الانترنت قائمة الجرائم المرتكبة بنسبة تقدر ب 71% و 68% على التوالي من مجموع الجرائم المسجلة, بينما مثلت باقي الأنواع الأخرى من الإجرام الرقمي نسبة ضعيفة مقارنة بها. - في حين تصدرت جرائم المساس بالأنظمة المعالجة الآلية للمعطيات في السداسي الأول لسنة 2019 قائمة الجرائم المرتكبة بنسبة قدرت بحوالي 65% و هي النسبة الأكبر مقارنة مع باقي الجرائم الرقمية الأخرى.. (نافع و شعباني، الجريمة الالكترونية، 2020، صفحة 788.787).

5. انعكاسات السلوكيات الإجرامية الرقمية:

مهما اختلف نوع الجرائم الالكترونية (الرقمية) ومهما زاد حجمها تظل تمس النظام , أي قد تقع على النظام ألمعلوماتي أو تقع بواسطته ومن خلال مراحل مختلفة سواء تعلقت بمرحلة إدخال البيانات أو مرحلة إخراجها أو مرحلة جمع البيانات , إلا أن الآثار المترتبة عنها تختلف باختلاف نوع الجريمة ونوع الأنظمة المعلوماتية أو بحسب أهمية البيانات المستهدفة لذلك . ولهذا تتنوع وتتفاوت الخسائر الأضرار المترتبة عن الجرائم الالكترونية .

1.5. تأثير السلوك الإجرامي الرقمي على الأفراد : شهد المجتمع الجزائري انتشار لعدة سلوكيات إجرامية رقمية خطيرة استهدفت العديد من الأفراد , كجريمة الولوج للأنظمة المعلوماتية الخاصة والتي تعد من أهم مظاهر الجريمة الالكترونية التي تمس بحقوق الإنسان, والتي يلجأ فيها المجرم الرقمي إلى الدخول الغير قانوني لبعض الحسابات وبطرق احترافية , ويدخل هذا النوع من الجرائم بالتصيد الاحتيالي الذي أصبح يعرف انتشارا كبيرا بين الدول.

ومن التأثيرات التي باتت تشكل انعكاسات جد خطيرة لما تحمل في طياتها من انزلاقات وتهديدات للفرد والمجتمع على حد سواء , حيث دفعت وسائل التكنولوجيا الحديثة بعض الأشخاص ذوي الميول الإجرامية إلى استغلال التقدم العلمي والرقمي في إنتاج نوع جديد من الممارسات الإجرامية ذات الطابع الرقمي من مثل :نشر صور الإباحية الفاضحة والأفعال الفاحشة المخلة بالآداب العامة على الشبكة والتي تتجسد من خلال المضامين الإباحية التي تقدمها بعض المواقع , كعرض صور وفيديوهات لمناظر غير أخلاقية لإفساد الأخلاق والقيم الاجتماعية للأفراد داخل المجتمع الجزائري مما ساعد على تزايد الانحلال الخلقي في أوساط أبناءنا وأسرنا خاصة مع غياب الرقابة الوالدية والتوعية الدينية , و الموجه بالدرجة الأولى للمراهقين والأطفال الذي يكون من السهولة بمكان الاحتيال عليهم سواء عن طريق استدراجهم وتصويرهم في أوضاع مخلة بغية ابتزازهم , أو من خلال استخدام تقنية "الديجيتال" لتكوين صور الضحايا الأبرياء على أجساد آخرين في أوضاع جنسية مخلة. وكل هذا من شأنه أن يتسبب في عدة أضرار للضحايا سواء من الجانب النفسي الذي يتأزم بفعل التهديدات التي يتعرض لها الضحايا والتي تطرحهم في الكثير من الأحيان إلى تقديم تنازلات أكثر للمجرمين الرقميين خوفا من التشهير بهم ومن ردة فعل الأسرة والمجتمع اتجاههم . (بوفاتح، صفحة 63), وهذا ما أكدته دراسة مباركي بعنوان "أشكال الجريمة الإلكترونية المرتكبة عبر الفيس بوك" والتي هدفت لتعرف إلى الجرائم الإلكترونية المرتكبة عبر الفيس



بوك التي تطل الشباب مستخدمو المواقع في الجزائر والتي خلصت إلى أن 37.1 % منهم تعرض حسابهم الشخصي للاختراق وأن 77.1 % قد تعرض للتشهير والقذف، و 19.3 % تعرض للابتزاز والتهديد، و أن 22.6 % أنشأ أحدهم حسابا وهميا بأسمائهم، و 61.4 % تلقوا مواد إباحية جنسية . (مباركي، 2014)

كما أن الاطلاع على المواقع الإباحية يعد من بين أهم الأسباب التي أدت إلى زيادة الجرائم الرقمية ، الأمر الذي ساعد بدوره على خلق سلوكيات إنحرافية كالتهرش الجنسي وذلك من خلال المواقع الإباحية التي ولدت التهرش الجنسي الالكتروني الذي يتم من خلال وسائط التواصل الاجتماعي . (قواجلية، 2020، صفحة 698)

حيث ارتفعت حالات استغلال الأطفال جنسيا عبر شبكة الانترنت حول العالم بشكل كبير. بحيث تزايد عدد المواقع الإباحية لاستغلال الأطفال بنسبة 400 بين سنة 2004 وسنة 2005. فوصل إلى 3433 موقعا سنة 2004 كما بلغ دخل تجارة الجنس عبر الانترنت سنة 2006، 97.06 مليار دولار منها 3 مليارات خاصة بالاستغلال الجنسي للأطفال، أما عدد القوائم العربية الإباحية في موقع ياهو فقد بلغ 171 قائمة، كما بلغ عدد أعضاء أقل تلك القوائم 3 في حين وصل عدد أكثرها إلى 8683. أما موقع قلوب لست فقد احتوى على 6 قوائم إباحية عربية، في حين وجد عدد 5 قوائم عربية إباحية على موقع توبيك. (رحماني،

2014، صفحة 76)

من المظاهر الإجرامية التي تطل الأشخاص داخل البيئة الرقمية نجد أيضا جرائم السب والشتم والتنمر إذا كثيرا ما يتعرض الكثير منا لهذه الممارسات بسبب أو من دونه ، بل أن المضامين الالكترونية أصبحت ثرية جدا بهذا النوع من السلوكيات الهدامة ، ناهيك عن محتوى بعض القنوات الذي يوجه خصيصا لتشهير وضرب مصداقية شخصيات معينة الأهداف تنافسية أو انتقامية ، ناهيك عن ما تتسبب به السلوكيات الإجرامية الرقمية من خلق العزلة الاجتماعية وضربا للقيم المجتمعية واستبدالها بقيم وأفكار سلبية مريضة ومشوهة . وهذا ما أكدته دراسة الدكتور إبراهيم بن سعد الجماد في مدينة الرياض بعنوان استخدام الانترنت يؤثر على العلاقات الاجتماعية تحدث خلاله عن أهمية الانترنت كونه خدمة حيوية وضرورية ففي عصر التقدم العلمي وخلص إلى أن الاتصال بالشبكة العالمية إلى شيوع أنماط جديدة من السلوكيات والقيم والأفكار التي تساهم بشكل كبير في التأثير سلبيا على المجتمع . (بوفاتح)

2.5. تأثير السلوك الإجرامي الرقمي على الاقتصاد: يتغير الأثر الاقتصادي المترتب عن السلوكيات الإجرامية الرقمية باختلاف نوع الجريمة ونوع الأنظمة المعلوماتية أو بحسب أهمية البيانات المستهدفة ، ولهذا تتفاوت الخسائر الاقتصادية الناجمة عن الإجمام الرقمي ، حيث يمكن أن يكون ضررها مرتبط بقيمة التجهيزات والبرمجيات موضوع الجريمة ، كما قد ترتبط بالأثر الناجم عن توقف هذه المنظومات عن العمل مثل اختراق منظومات عمل معينة أو شركات أو مؤسسات التي تؤدي إلى إلحاق خسائر تقدر بالآلاف الدولارات ، وهذا ما أكدته دراسة عنيت بالجرائم الالكترونية في المملكة البريطانية . والتي أكدت نتائجها أن هذا النوع من الإجمام يستهدف أكثر القطاع المالي، حيث أن أغلبها تمس البنوك وشركات التأمين في قطاعها وينسب أقل في القطاع العام والتعليمي.

كما أن الأثر الاقتصادي للسلوك الإجرامي الرقمي لا يستهدف في حقيقة الأمر التجهيزات والمؤسسات فقط إنما هو يمس بدرجة الأولى الأفراد ، فالجريمة الاقتصادية المستحدثة مست كل فئات المجتمع فأثرت بذلك على الأفراد والجماعات كما أثرت على الشركات والمؤسسات ، وذلك نتاج الاستعمال المفرط للإنترنت التي يسرت ودعمت ونوعت من السلوكيات الإجرامية وأصبحت تمارس بطرق أسرع وأسهل ، ومن بين الجرائم التي تؤثر على الجانب المادي والاقتصادي نجد جرائم نقل ملكية الأسهم ، نقل أو تحويل الحسابات المصرفية ، سرقة بطاقة الائتمان الخاصة ، عمليات الاحتيال على الشركات ، عمليات الابتزاز والتهديد وسرقة الهوية .

كما أن المؤسسات المالية و المؤسسات التجارية الرقمية والمؤسسات الحكومية والاتصالات تأتي في طليعة المؤسسات المستهدفة من قبل القرصنة الرقمية على مستوى العالم. ومن الجرائم التي تتعرض لها المؤسسات ذات الطابع المالي والاقتصادي ، الاطلاع على



معلومات أو بيانات سرية خاصة بصفقات هامة , العبث بمخازن البيانات الخاصة بمؤسسة معينة قصد تخريبها أو التعديل فيها أو حذفها وكل هذه الممارسات من شأنه أن تعود بضرر على أصحاب هذه المؤسسات ومن ثمة على اقتصاد الوطن (قويقح، 2020، صفحة 6.5)

الغش و الخداع والاحتيال التي تكون أما من خلال الترويج لبضائع زائفة موجه للاستهلاك الفردي كالسلع التي يتم التسويق لها عبر الوسائط الالكترونية كال فيسبوك إذا كثيرا ما نتوقف على مثل هذه السلوكيات التي تعود بضرر المادي والنفسي على الضحايا إذ تستنزف جيوب المواطن البسيط الذي كثيرا ما يتم استدراجه من خلال الأسماء والعلامات التجارية الزائفة أو بيع السلع المحظورة . (عبد الرحيم و عبد الرحيم، 2017، صفحة 131) ولقد إشارات الإحصائيات الوطنية للجرائم الالكترونية المسجلة من طرف الأمن الوطني خلال الفترة ما بين 2017-2019 بأن جرائم بيع السلع المحظورة على شبكة الانترنت قدر ب 203 قضية. (نافع و شعباني، تحديات الحكومة الالكترونية في الجزائر (الجريمة الالكترونية نموذجاً)، 2020)

3.5. تأثير السلوك الإجرامي الرقمي على المجال الثقافي: ساعدت العولمة الثقافية من خلال تسريباتها عبر الأقمار الصناعية في شكل منتجات سينمائية ومعلوماتية وفنية وفكرية على نشر ثقافة الرذيلة والعنف والإدمان في المجتمع , كما ساهمت على تسريب الثقافة الإجرامية وتعليم السلوك الإجرامي فانتشرت بذلك أنواعا جديدة من الجرائم نابعة من الوسط الرقمي , كما تكمن خطورة أثره الثقافي على المجتمع الجزائري في الترويج للأفكار المتطرفة ومحاولة استقطاب الشباب بواسطة إنشاء مواقع الكترونية تعمل على نشر ثقافة الغلو والتطرف كما كان له دور في تفكيك الروابط الاجتماعية والعلاقية داخل المجتمع من خلال نشر الانحلال والتدني الأخلاقي ونشر الثقافة المضادة للمجتمع كبديل لنمط الثقافي السائد في المجتمع الجزائري, خاصة وأن الاستخدام الفردي للوسائل الإلكترونية يعزز الميل للعزلة مما يقلل من فرص التفاعل والنمو الاجتماعي والانفعالي الصحي (فتاش، 2021، صفحة 818), كما بينت بعض الدراسات أن الاستخدام الغير مدروس لبعض المواقع يسهم في تنمية بعض الأفكار غير العقلانية خصوصا ما يتصل منها بنمط العلاقات الشخصية و أنماط الحياة والعادات والتقاليد السائدة في المجتمع مما يؤدي إلى تدمير نسيج الموروث الاجتماعي الوطني , إضافة إلى تمجيد وتشجيع الثقافات الفرعية المعارضة لثقافة المجتمع الأصلية والتي تسعى لنشر قيمها ومعاييرها الجديد على حساب الثقافة الأصلية, كما كثيرا ما يسهم السلوك الإجرامي في خلق اختلال معياري داخل المجتمع مما يضعف بدوره القيم المجتمعية ويفقد المعايير سلطتها على المجتمع فيختل بذلك السير وتنتشر الجريمة . (التائب، 2008، صفحة 169)

4.5. تأثير السلوك الإجرامي الرقمي على المجال الأمني: من بين الجرائم التي تشكل تهديدا صارخا للأمن الوطني ما اصطلح عليه بالإرهاب الالكتروني والذي يعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية لإلحاق الضرر ببلد محدد وفي الحقيقة أن هذا النوع من الجرائم لا يقل خطورة عن جرائم الإرهاب التقليدية لما له من آثار سواء على الأفراد من حيث استقطابهم والعمل على التغيرير بهم للعمل ضد أوطانهم وذلك بغسل أدمغتهم بالأفكار متطرفة تستهدف بالدرجة الأولى أمن الفرد والمجتمع أو من خلال تداعيات الممارسات الإرهابية وما تنتجه من انفلات أمني, حيث أنشأت في هذا الصدد العديد من المواقع المشبوهة لتعليم صناعة المتفجرات وكيفية اختراق وتدمير المواقع والتي من بينها قيام بعض التنظيمات الإرهابية بتصميم لموقع مثل موقع النداء المخصص لتنظيم القاعدة الإرهابي مثلا , و التي تنصيد من خلاله الأفراد للانخراط في صفوفها أو لتكوين مجموعات الدعم التي تعمل على توفير الدعم المادي والمالي للجماعات الإجرامية الإرهابية , وكل هذه السلوكيات من شأنها أن تؤثر على أمن الوطن والأفراد كما تسهم في خلق الفوضى العامة و اللانظامية في صفوف المواطنين وما يتبعه من أضرار نفسية واقتصادية على المجتمع



كما يعمل الإجرام الرقمي على زيادة الاضطرابات الأمنية وتفاقم المشكلات الاجتماعية والسياسية شأن الفساد والتظاهرات وتهديد الملكيات المادية و الفكرية, كما تمثل عوامل مساهمة في إنتاج بيئة خطرة تهدد السيادة الوطنية للدولة , كما قد تمس بعضويتها في المنظمات الدولية مما يؤدي إلى خسارة العديد من الاستثمارات الأجنبية . (قديري و حسن، 2013، صفحة 160)

و تعد الجوسسة أيضا من الجرائم الجد خطيرة و المنتشرة في الوسط الرقمي والتي تتجسد من خلال اختراق أو قرصنة بعض المواقع الحساسة للدولة مما يتسبب في العديد من الآثار والأضرار سواء الاقتصادية أو التي تمس الجانب الأمني, كما و تتجسد في عمليات التجنيد ضد أمن الوطن من خلال استقطاب البعض عن طريق الابتزاز أو الاحتيال للخدمة ضد أوطانهم خاصة ونحن نعيش اليوم في نوع آخر من الحروب والذي يعتمد على الحروب التقنية خاصة مع ظهور حروب الجيل الرابع والخامس التي تستهدف اقتصاد وأمن البلدان من خلال التردد لثغرات وخلق الفوضى وللأمن والعمل على محاربة مصالح البلد المستهدف من خلال الشائعات المغرضة ونشر البلبلة والدسائس.

خاتمة:

لقد قمنا من خلال ما تقدم في هذه الدراسة بتسليط الضوء على ظاهرة الإجرام الرقمي التي شهدت تفشيا واضح في المجتمع الجزائري خاصة مع اقترانها بالتطور التكنولوجي والتقني الذي عرف هو الآخر توسعا ملحوظا في مجتمعنا مما ساهم في إحداث العديد من التغيرات سواء على مستوى التفاعلات الاجتماعية بين الأفراد التي اتخذت من البيئة الرقمية أرضية جديدة لها أو من خلال المعاملات التجارية و الاستهلاكية والمادية التي اكتست طابع الرقمنة الأمر الذي أسهم في إنتاج العديد من السلوكيات الإجرامية الرقمية والتي تجلت بدورها في العديد من الصور و الممارسات, التي ساهمت في زيادة حجم الآثار والانعكاسات التي شملت عديد الجوانب الأمر الذي يتطلب تسليط الضوء على السبل الكفيلة بردع هذا النوع من الجرائم وذلك بأخذ التدابير الأمنية الذي يكفل حماية المعلومات والبيانات الموجودة على شبكة الانترنت .

التوصيات:- على المؤسسات اتخاذ كافة تدابير الحماية الأمنية وفق المعايير العالمية لحماية بياناتها وأنظمتها من الاختراق.

- ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية والاقتصادية المترتبة عن الاستخدام السليبي للتكنولوجيا.

- ضرورة غرس ثقافة التبليغ لدى المواطنين لأي ممارسة إجرامية قد تعترضهم في البيئة الرقمية .

- العمل على تحديث التقنيات باستمرار للتمكن من التصدي لهذا النوع من الجرائم.

- ضرورة خلق فرق أمنية مختصة في مراقبة المضامين الرقمية الموجهة للأفراد.

- تعزيز التعاون الدولي في مجال مواجهة الإجرام الرقمي وذلك برسم سياسات تهدف لتشديد العقوبات .

- ضرورة حجب الدولة لأي موقع ترى أنه يسهم في زيادة الانحلال الأخلاقي ويشكل تهديدا لقيمنا الاجتماعية .

قائمة المراجع

- 1- نوال بنت علي قيسي, «الجرائم الالكترونية الموجهة ضد مستخدمي الانترنت», رسالة ماجستير, جامعة الإمام محمد بن سعود الإسلامية. المملكة العربية الإسلامية. 2010.
- 2- إيمان ميرة, "الجريمة الالكترونية عبر الانترنت في أوساط الطلبة الجامعيين", رسالة ماجستير, جامعة محمد بوضياف. المسيلة, 2014.
- 3- محمد عزو الكحلوت, "اتجاهات الصحفيين الفلسطينيين نحو تطبيق قانون الجرائم الالكترونية وانعكاساته على حرية الرأي والتعبير(دراسة ميدانية على المحافظات الشمالية) , رسالة ماجستير في الصحافة, كلية الآداب, الجامعة الإسلامية بغزة, 2019.
- 4- نمر محمد حسن البدوي, "الجرائم الواقعة على العرض بالوسائل الالكترونية -التشريع الأردني", رسالة ماجستير في القانون العام, 2020.



- 5- سامية عزيو و ماريا عيساوي , " الجريمة من منظور سوسيولوجي - الأسباب والآثار", مقال نشر بمجلة الدراسات في سيكولوجية الانحراف , مجلد 06, العدد 1, سنة 2021.
- 6- عزوز سعدي, "التجارة الالكترونية وتحديات الجريمة المعلوماتية", مقال نشر بمجلة الدراسات والبحوث القانونية, المجلد الرابع, العدد 01, جوان 2019.
- 7- خالد محمود ابراهيم , الجرائم المعلوماتية .
- 8- عبد الرؤوف زيوش, "الجريمة المعلوماتية في التشريع الجزائري, مقال نشر بمجلة العلوم القانونية والاجتماعية , جامعة زيان عاشور بالجلفة, الجزائر, المجلد 4, العدد 03, 2019.
- 9- رحيمة ميد لي , " خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة", مقال نشر في أعمال المؤتمر الدولي الرابع عشر للجرائم الالكترونية جامعة محمد لمين بولوغين سطيف , طرابلس 24-25 مارس 2017.
- 10- عمر محمد أبو بكر يونس, "الجرائم الناشئة عن استخدام الانترنت الأحكام الموضوعية و الجوانب الإجرائية", دار النهضة العربية , القاهرة , 2004, ص 233.
- 11- هدى حامد قشوش, " جرائم الحاسب الالكتروني في التشريع المقارن , القاهرة, 1992 .
- 12- محمد أمين بكوش ونبيلة هبة هروال, "خصوصية المحرم الالكتروني (مجرم الانترنت نموذجاً)", مقال نشر بمجلة البحوث في الحقوق والعلوم السياسية, مجلد 7, العدد 1, 2021.
- 13- عبد الكريم عودة الخرابشة وغدير بنس الزير, "الجرائم الالكترونية ومستوى الوعي بخطورتها-دراسة ميدانية على عينة الشباب الأردني, مقال نشر بمجلة الجامعة الإسلامية للدراسات الإسلامية كلية الأميرة رحمة , جامعة البلقاء التطبيقية, الأردن , مجلد 29, عدد 2, سنة 2012.
- 14- موسى دياب البدانية , "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية, الملتقى العلمي , كلية العلوم الإستراتيجية , ورقة علمية بعنوان الجرائم الإلكترونية -المفهوم والأسباب-بتاريخ 8-9/11/2014..
- 15-عبد القادر بن زعمة و بلفكيرات , " الجريمة الالكترونية كتهديد للأمن الوطني الجزائري ", مقال نشر بمجلة العلوم القانونية والاجتماعية , جامعة زيان عاشور الجلفة, المجلد 4, العدد 01, 2019.
- 16- أحمد بن خليفة حفوظة الأمير عبد القادر , " الجريمة الالكترونية وآليات التصدي لها ", مقال نشر بمجلة الامتياز لبحوث الاقتصاد والإدارة , مجلد 1, العدد 1, جوان 2017.
- 16-بثينة حبيباني , "الطبيعة الخاصة للجريمة المعلوماتية, مقال نشر بمجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية, مجلد 12, عدد 3, 2020.
- 17- أمينة حمشا شي, كلية العلوم القانونية , جامعة مصطفى إسماعيل , معسكر .
- 19- سليمة دياب , بلال بوترة , الجريمة الالكترونية الأسس والمفاهيم , مقال نشر بمجلة تطوير العلوم الاجتماعية , مجلد 13 , العدد 01, 2020.
- 20-البشير زيدي , "واقع جرائم تكنولوجيا الإعلام والاتصال في العالم وآليات مكافحتها", مقال نشر بمجلة الدراسات الاقتصادية المعاصرة , العدد 03, 2017.
- 21 -زينب نافع , شعباني مجيد, " تحديات الحكومة الالكترونية في الجزائر (الجريمة الالكترونية نموذجاً) , مقال نشر بمجلة العلوم الاقتصادية والتسيير , المجلد 13, العدد 1, 2020.
- 22-محمد بلقا سم بوفاتح , " الجريمة الالكترونية -دراسة سويسو قانونية , كلية الحقوق والعلوم السياسية , الجلفة.
- 23- مباركي, منال. إشكال الجريمة الإلكترونية المرتكبة عبر الفيسبوك", رسالة ماجستير . جامعة العربي بن مهيدي - أم البواقي, الجزائر, 2014.
- 24-أمال قوا جليلة (الجرائم الالكترونية بين دور النظام القانوني والمعايير الاجتماعية المكتسبة لمستخدمي المواقع الاجتماعية -دراسات حالة للجرائم الكترونية من القضاء الجزائري لولاية عنابة , مقال نشر بمجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية, مجلد 12, العدد 3, جويلية 2020.
- 25-نعيمة رحمانى جامعة تلمسان "إدمان الأطفال على الانترنت جريمة رقمية, مقال نشر بمجلة التراث, العدد 12, فبراير 2014.
- 26-حورية قويقح, "الأبعاد الاقتصادية للجريمة الالكترونية ", مقال نشر بمجلة مجلد 14, العدد 1, 2020.



- 27- صباح عبد الرحيم ووهيبة عبد الرحيم , "واقع تسوق المستهلك عبر شبكة الانترنت بين الحماية والجريمة , مقال نشر بمجلة الاجتهاد القضائي , العدد 14 , افريل 2017.
- 28- نورة فتاش , "الجريمة المنظمة عبر الوطنية نموذجا , مجلة الدراسات القانونية , جامعة المديّة , المجلد 7 , العدد 2, جوان 2021.
- 29- عائشة التائب , "مقاربة سوسيولوجية لجرائم الفضاء الالكتروني " . مقال نشر بمجلة إضافات , العدد 1 , 2008.
- 30- محمد قدرى وعبد الرحمان حسن, مقال نشر بمجلة الفكر الشرطي, المجلد 22, العدد 86, 2003.



الجريمة المعلوماتية عبر المنصات الإلكترونية

موسى معطوي

Moussa.mouadh10@gmail.com

نعيمة تواتي

Naima.touati@univ-bouira.dz

1. الاطار المفاهيمي والدراسات السابقة :

1.1. المقدمة:

لا يوجد خلاف في ان الثورة الصناعية حقيقة قد أوجدت عوالم جديدة تميزها العصرنة والحداثة ، والتي يعتبر التقدم التكنولوجي قاسمها المشترك والرابط بين المجتمعات والشعوب بمظاهره العلمية وفضاءاته الرقمية الهائلة ، الذي منحى للجانب التواصل صبغة مختلفة تماما عن ما كانت عليه سابقا، ووفر كل الطرق والوسائل المتنوعة لذلك ، في شكل اكثر إتاحة للأفراد وأكثرها اتساعا، فالتغيرات التي حملتها الثورة الصناعية لم تكن تغيرات سطحية او مؤقتة بل كانت بمثابة إعادة تصنيع الأمم من جديد، لتغير مع ذلك مراكز القوة وتتمركز في القدرة على استخدام التكنولوجيا الحديثة وقوة التحكم فيها ، فنجد ان ما عرفه العالم من تطور يرجع الى ما تتضمنه هذه التكنولوجيات الحديثة وما تتميز به من خصائص، فبالإضافة الى أنها تمكنت من إلغاء حواجز الوقت والمسافة فهي قد تمكنت من الجمع بين أقطاب العالم ككل ضمن عالم افتراضي من خلال شبكة الأنترنت العالمية، حيث ان هذه الأخيرة استطاعت بعوالمها الافتراضية ووسائلها وشبكاتها الضخمة الخاصة بما ان تتماشى مع كل فرد على اختلاف احتياجاته، بكل سهولة ومن اهم ما أنتجته الأنترنت هي "ما يعرف بالمنصات الإلكترونية"، التي تعتبر اليوم المحرك الأول لكل النشاطات التي يمارسها الأفراد بمختلف جوانبها، ومن جهة أخرى وبالتزامن مع كل هذه التغيرات التي طرأت على شكل المجتمعات، نجد ان هذه الأخيرة تعرف تغيرات أخرى على مستوى الأمني والإجرامي إذ باتت تعرف أنواع مستحدثة من الجرائم، وتنتشر بسرعة كبيرة والتي اطلق عليها بالجرائم المستحدثة التي ما يميزها اعتمادها الأساسي على التقنيات الحديثة، ومن اهم هذه الجرائم تلك التي تمارس عبر الفضاءات الإلكترونية ومنصات التواصل الاجتماعي، وسنخص حديثنا هنا عن الجرائم المعلوماتية التي مست بدورها الجانب الشخصي الفردي والجانب العام، وكان لهذا مظاهر متنوعة مستغلة بذلك وفرة هذه المنصات الإلكترونية وتعدد أنواعها ووسائلها في ممارسة مثل هذه الجرائم، كموقع فيسبوك ومنصة يوتيوب كنماذج لهذه المنصات ، وكثير من الدراسات تؤكد على الاستخدام غير الأخلاقي لهذه المواقع الإلكترونية في عملية الاعتداء على الأفراد والمجتمعات ، كما ان هناك الكثير من النظريات المفسرة لتأثير هذه التقنيات الحديثة في انتشار الجريمة وبرزها تلك التي تفسر طرق التعلم والاكتساب المعرفي من خلال نماذج تعليمية والتي لها القدرة على تفسير كيفية ممارسة الجرائم عبر الفضاء الإلكتروني، ومثال عن الجرائم المعلوماتية السب والشتم والتشهير الابتزاز وانتهاك الخصوصية وغيرها على المستوى الفردي ونجد أيضا سرقة المعلومات والنصب والاحتيال ..الخ على المستوى العام، لتتمثل مشكلة دراستنا حول ماهية الجرائم المعلوماتية عبر المنصات الإلكترونية؟ وماهي اهم المواقع المعتمد عليها في هذه الجرائم ؟ .

2.1. أهداف الدراسة : يتجه الباحثين اليوم لدراسة مختلف تحليلات العولمة والتقدم التكنولوجي على الأفراد والمجتمعات، من خلال التركيز على اهم المتغيرات التي ظهر تأثيرها بشكل واضح على التفاعل الاجتماعي واتجاهاته وأشكاله، ومن هذه المتغيرات تلك التي ترتبط بشبكة الأنترنت او العالم الرقمي وهي المنصات الإلكترونية بمختلف ما تحتويه من مواقع وفضاءات مختلفة، لذا سنحاول التركيز عليها من ناحية علاقتها بانتشار بعض أنواع الجرائم وهي الجريمة المعلوماتية التي تشكل خطر حقيقي على امن الشخصي او



الأمن العام ، وذلك بهدف الكشف عن اهم هذه المنصات التي تساهم في ذلك وماهي المميزات التي توفرها هذه المنصات لمركبي هذه الجريمة ،واهم الإحصائيات المتعلقة بها وأيضاً السعي الى معرفة اهم التدابير القانونية التي تعتمدها الدول في تعاملها مع هذا النوع من الممارسات الإجرامية المستحدثة.

3.1. تحديد مصطلحات الدراسة :

1.3.1. الأنترنت : هي شبكة معلومات عالمية ترتبط من خلال مجموعة ضخمة من الحواسيب حول العالم والتي يتم الدخول في مجالها الرقمي من خلال المواقع المتخصصة لذلك وهي كثيرة ومتنوعة (أمل 2011، 112)، كما تعرف الأنترنت على أنها نظام عالمي للمعلومات يرتبط به أنظمة متفرعة عنه او نقول أنها شبكة عالمية تتكون من حاسبات تعتمد على بروتوكول TCP/IP والبروتوكولات الأخرى للاتصالات الفائقة السرعة التي تربط بين الملايين من المستخدمين حول العالم (فتيحة 2012-2011، 8،9).

2.3.1. المنصات الإلكترونية : او ما نقصد به في بحثنا بمنصات التواصل الاجتماعي والتي يمكن تعريفها بأنها هي الطرق الجديدة للاتصال في البيئة الرقمية مما يسمح للمجموعات الأصغر من الناس بإمكانية الالتقاء والتجمع على الأنترنت وتبادل المنافع والمعلومات (بشرى 2012، 91)، كما عرفت على أنها منصات على الأنترنت أو الهاتف المحمول توفر إمكانية التفاعل الثنائي الاتجاه عبر محتويات المستخدمين إضافة إلى التواصل الاجتماعي بينهم، وهي ليست كوسائل الإعلام مصدرها واحد أو موقع شبكي ثابت وإنما هي وسائل للتواصل عبر منصات صممت خصيصاً لتمكين المستخدمين من إيجاد وإنتاج المحتويات بأنفسهم، والتفاعل مع المعلومات ومصدرها (شينا 2015، 11).

التعريف الإجرائي : هي عبارة عن مجموعة المواقع الإلكترونية والمثلة للبيئة الافتراضية التي يتمكن من خلالها الأفراد من التواصل وتبادل المعارف والثقافات عبر العالم ككل، إضافة الى أنها توفر الكثير من الخدمات بفضل ما يميزها من دقة وسهولة في الاستعمال وأنواعها الكثيرة أيضاً.

3.3.1. السلوك الإجرامي : السلوك لغة "من سلك أي سلك الطريق" أما الجريمة فهي من "الجرم وهي التعدي والقطع او الذنب"، أما عند علماء الاجتماع السلوك الإجرامي يشير الى كل سلوك غير مقبول اجتماعياً، او هو الخروج عن مظاهر السلوك الذي يضبطه المجتمع والانحراف عن القواعد والمعايير الخاصة بسلوكه العام، وهذه الانحرافات تكون بمثابة تهديد للأفراد وكيان المجتمع، أما من الناحية القانونية السلوك الإجرامي يدل على عمل او الامتناع عن عمل ما ويترتب معاقبة الفرد بعقوبة جزائية (عماد الدين 2012-2011، 17-18).

4.3.1. الجريمة المعلوماتية: يرتبط تعريف الجريمة المعلوماتية بعدة مفاهيم والتي يمكن تصنيفها من أنواع الجرائم الإلكترونية التي يشهدها العالم اليوم، والتي يتم ارتكابها باستخدام تكنولوجيا المعلومات والاتصال الحديثة ويمكن تعريفها على أنها : جريمة غاية في الدقة والتي تختلف على الجريمة التقليدية من حيث أركانها ووسائلها وحتى ضحاياها، ترتبط بصفة أساسية بالتقنيات الحديثة لشبكة الأنترنت الضخمة، فنقول أنها جرائم مرتبطة بالبيانات والمعلومات على مستوى أنظمة الأجهزة الإلكترونية "الحواسيب"، وتشمل هذه الجرائم كل الأفعال التي يتجاوز بها الأفراد الشرعية القانونية او المجتمعية في الفضاء الإلكتروني وفي اطار نظامه الرقمي الذي يسير ضمن مجال الأنترنت العالمي، ومن أمثلة هذه الأفعال عملية نقل او نسخ او حذف المعلومات المخزنة دون إذن او تصريح بذلك، او استعمالها لأغراض ومصالح شخصية كالابتزاز والتهديد وسرقة الأموال والاحتيال، من خلال مختلف عمليات الاختراق للحسابات الشخصية او الأنظمة المعلوماتية، لتكون هذه الجرائم هي عملية الاعتداء على معلومات النظام العام



او المعلومات الشخصية باستغلال الكفاءة العالية في استخدام وسائل التكنولوجيا والاتصال الحديثة (خالد ابراهيم 2008، 1، 3)، وتعرف أيضا بأنها كل فعل ينشأ باستخدام الغير المشروع لتقنية المعلوماتية بهدف الاعتداء المادي او المعنوي والتي يعاقب عليها قانونيا او يأخذ في حقه تدبيرا احترازيا ، لتشمل بذلك كل أشكال السلوك غير المشروع المرتب باستخدام الحاسوب الألي (ادهم 2018، 7-8) .

التعريف الإجرائي : تشير الجريمة المعلوماتية الى كل السلوكات الإجرامية التي يتم ارتكابها بواسطة وسائل التكنولوجيا الحديثة، والتي تشمل كل من الحواسيب وأنظمة المعلومات وشبكة الأنترنت ومختلف المواقع الافتراضية على مستواها، وهي من الجرائم المستحدثة الخطيرة والتي تدل على الدقة وذكاء مرتكبيها .

يمكن تعريف السلوك الإجرامي الرقمي بصفة إجرائية: على انه كل سلوك يرتكبه الأفراد في البيئة الرقمية والذي يخالف به معايير وقيم مجتمعه ويعاقب عليه قانونيا وهذا من خلال التكنولوجيا الحديثة والنظم المعلوماتية بمختلف مجالاتها وفضاءاتها الإلكترونية المتاحة .

4.1. دراسات سابقة:

1.4.1. دراسة حمزة بن عقون 2011-2012 حول السلوك الإجرامي للمجرم المعلوماتي : الذي اتجه نحو دراسة طبيعة السلوك الإجرامي المعلوماتي الذي يختلف عن السلوك الإجرامي التقليدي، ومن اجل هذا اشتملت دراسته على ماهية الجريمة المعلوماتية وكل المفاهيم المصاحبة لها، والتطرق الى اهم السلوكيات التي تميز المجرم المعلوماتي عن غيره وخصائصه ومن ثم موقف المشرع الجزائري اتجاه التعامل مع هذه الجرائم المستحدثة، وهدفت الدراسة الى الإحاطة بكل ما يرتبط بالجريمة المعلوماتية وبيان الحماية الجنائية للمعلومات من السلوك الإجرامي التي تتعرض له اليوم نتيجة التطور التكنولوجي، كما هدفت أيضا الى التركيز على ما يتميز مرتكبي هذه الجرائم واطلقت عليه اسم المجرم المعلوماتي نظرا لنوع سلوكات التي يقوم بها والتي تتمثل في الاعتداء على المعلومات الشخصية والعامة باستخدام التقنية الحديثة، إضافة الى هذا سعت لمعرفة الدافع وراء ارتكاب هذه الجريمة من خلال دراسة شخصية المجرم كخطوة مهمة تساعد التشريعات على نص قوانين مناسبة للحد منها وإصلاح المجرم أيضا، وفي الأخير توصلت مجموعة من النتائج أهمها :

1- ان مفهوم الجريمة المعلوماتية يدل الى الاعتداء على أنظمة الحاسب الألي كما تعرف على أنها جرائم الكترونية في بعض الدراسات التي سيتم التطرق اليها لاحق، وهذا ماجعل إمكانية إعطاء تعريف شامل وموحد للجريمة المعلوماتية امر ليس بالسهل لارتباطها بالكثير من الممارسات المرتكبة عبر فضاء النظام الرقمي، لكن المتفق عليه هو أنها جرائم مستحدثة وجدت من الحاسب الألي او الفضاء الرقمي المكان المناسب لها .

2- الجريمة المعلوماتية لها أركان خاصة بها وتتمثل في: الركن الشرعي الذي يدل على تجريم كل أشكال الاعتداء على المعلوماتية بهدف حماية نظامه، والركن المادي الذي يملك صورتين (الاعتداء على نظام معالجة الألية للمعطيات و الاعتداء على منتوجات النظام او التزوير)، أما بالنسبة للركن المعنوي فهو يشير الى صعوبة إثبات الجريمة المعلوماتية وهذا لأنها تختلف من شكل الى اخر ولكل شكل جانب قانوني خاص بها .



3- يمكن للجريمة المعلوماتية ان تستخدم الحاسب الألي كأداة للجريمة للاعتداء على البيانات المتعلقة بالفرد كسرقة أموالهم او التجسس على حياتهم الخاصة ..، كما يمكن ان يكون الحاسب الألي هدف للجريمة المعلوماتية من خلال استهداف المعلومات المخزنة به او المنقولة منه او تخريب برامجه .. الخ .

4- ان مبدا الشرعية الجنائية هو لا يوجد جريمة بدون عقوبة ولا عقوبة إلا بنص، وهذا يعني ان غياب النصوص القانونية وقتها في مجال الإجرام المعلوماتي هو التقصير في مكافحتها خاصة مع وجود أنواع منها غير واضحة الأركان، وهذا ما يصعب الحماية الجنائية منها .

5- من اهم القوانين التي يعمل بها المشرع الجزائري ما يعرف بقانون المساس بنظام المعالجة الآلية للمعطيات رقم 4-15 الذي صدر في 10 نوفمبر 2004، وقانون 9-4 في 5 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (حمزة 2010-2011، 5-198-198-215).

1.4.2. دراسة صغير يوسف 2013 بعنوان الجريمة المرتكبة عبر الأنترنت : اتجهت الباحثة للحديث عن الجريمة المرتكبة عبر الأنترنت والتي عرفها بالجريمة المعلوماتية وأسس ارتكابها وخصائصها واهم ما تستهدفه هذه الجرائم وأنواع مرتكبيها وأركانها ومن ثم انتقل الى طرق التحقيق وبرز الجهود التشريعية الدولية والوطنية لمواجهة هذه الجرائم وفي هذا الاطار استخدمت مصطلح الجرائم السيبرانية الدال على الجرائم المرتكبة على الأنترنت وذكر اهم الاتفاقيات والقوانين المعمول بها واهم الصعوبات التي واجهتها في اطار مواجهة الجريمة المرتكبة عبر الأنترنت نظرا لطبيعة هذه الأخيرة واهم ما توصلت اليه هذه الدراسة ما يلي :

1- تعتبر الجريمة المرتكبة عبر الأنترنت هو شكل اخر ومستحدث للجريمة والذي رافقها الكثير من المشكلات من ناحية إثباتها واطرق اكتشافها وهذا لإمكانية إخفاءها من جهة ولذكاء ومهارة المجرم الإلكتروني في مجال أنظمة المعلومات وبرامج الكمبيوتر .

2- هناك سعي على الصعيد الدولي والوطني من اجل التعامل مع هذه الجرائم من خلال إيجاد تشريعات ونصوص قانونية واهم هذه القوانين نذكر 9-4 المؤرخ في 5 أوت 2009 الخاص بالتشريعات الجزائرية الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، أما عربيا فكان هناك نموذج موحد يتمثل في المواد 461 و 464 التي تتعلق بالفصل الخاص بالاعتداء على حقوق الأشخاص من خلال المعالجات المعلوماتية ، أما على المستوى الدولي فنذكر اتفاقية مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والو م ا التي دخلت حيز التنفيذ 2004 وهي متاحة لك الدول للانضمام اليها . وغيرها من المنظمات والاتفاقيات تسعى لحماية كل ما يتعلق بالجرائم المرتكبة عبر الأنترنت كالمنظمة العالمية للملكية الفكرية والاتحاد الأوروبي " اتفاقية بوابست لمكافحة الجرائم المعلوماتية "

3- كما توصلت الدراسة الى اهم أنواع الجرائم المرتكبة عبر الأنترنت والتي اطلق عليها بالجرائم المعلوماتية ومن أمثلتها (قرصنة البرامج، الدخول غير المصرح به ، جرائم نشر الإباحية وصنعها ، جرائم القذف وتشويه السمعة ، .. الخ كما عملت على تحديد أركان الجريمة المرتكبة عبر الأنترنت، وهو الشيء الذي تتفق فيه مع الدراسة السابقة (يوسف 2013، 52 الى 113).

1.4.3. دراسة عبد الله دغش العجمي 2014 التي اهتمت بالمشكلات العلمية والقانونية للجرائم الإلكترونية: والتي كانت بمثابة دراسة مقارنة بين التشريع الأردني والتشريع الكويتي في اطار التعامل مع الجرائم الإلكترونية واهم ما اشتملت عليه هذه الدراسة هو إمكانية تقديم دليل رقمي الكتروني مقبول وله شرعية أما القضاء الجزائري و مدى قدرة القوانين التقليدية في التصدي للجرائم الإلكترونية وهل هي كافية حقا كما تناولت أيضا المشكلات الموضوعية والإجرائية وكيفية معالجة المشرع للمشكلات التي تواجهها



في تعاملها مع الجرائم الإلكترونية، واهتمت أيضا بالقوانين الأردنية والكويتية من خلال المقارنة بينها التي تعتبر الحدود الخاصة بالدراسة الى جانب بعض القوانين العربية في حدود زمنية 2013-2014 والمواد التي طبقت عليها الدراسة هي رقم 16 لسنة 1960 و رقم 17 و 31 لسنة 1970 بالنسبة للتشريع الكويتي، والقانون رقم 16 لسنة 1960 ورقم 9 لسنة 1961 ورقم 30 لسنة 2010 للتشريع الأردني وتوصلت الى نتائج هي :

- 1- طبيعة الجرائم الإلكترونية تمس كل من النظام الاقتصادي والوطني والدولي وكذا المنظومة الأخلاقية للمجتمعات.
- 2- هي جرائم تأخذ أشكال وأبعاد مختلفة ما ترتب عنها مشكلات موضوعية وإجرائية.
- 3- بالمقارنة بين التشريعين الأردني والكويتي نجد ان هذا الأخير لم يطور او يضع قانون خاص بالجرائم الإلكترونية واكتفى بالقوانين التقليدية على عكس القانون الأردني الذي اصدر قانون خاص بالجريمة الإلكترونية المتمثل في قانون المعاملات الإلكترونية 2001 .
- 4- كما توصلت الى انه يمكن ان توجد حلول علمية وقانونية في شان الجريمة الإلكترونية الى جانب التأكيد على قصور القوانين التقليدية في ذلك وهذا لأنها قوانين خاصة بالجرائم المادية الملموسة على عكس الجرائم الواقعة عبر الأنترنت الغير المادية كالجريمة المعلوماتية التي لها الكثير من الأشكال (عبد الله 2014، 6، 120).

4.4.1. دراسة جرائم الدم والقدح والتحقيق الإلكتروني في القانون الاردني 2016 : التي اعتبرها احدى المواضيع التي ازداد ظهورها مع التطور التكنولوجي وتعدد الوسائل المساعدة على ذلك واهمها الوسائل الإلكترونية المعتمدة على النظم المعلوماتية المتطورة حيث حاولت الدراسة الى التطرق شكا من أشكال الجرائم المستحدثة المعروفة بالجريمة الإلكترونية او المعلوماتية والتي ترتكب من خلال الوسائل التكنولوجية التقنية والحديثة وتطرت على التعريف الى جرائم القدح والدم وأركان تجريمها والتعريف أيضا بالجريمة الإلكترونية وذكر أنماطها وخصائصها وطرحت اهم الوسائل المستخدمة في ذلك كمنصات التواصل الاجتماعي باختلافها وأخذت فيسبوك ، واتساب وتويتر نماذج لهذه المنصات كما أدرجت الجانب القانوني الخاص بتا ودور الوسائل القانونية في إثباتها وكانت حدود الدراسة في اطار إجراء مقارنة بين التشريعات الخاصة بمواجهة هذا النوع من الجرائم وانتهت بمجموعة من النتائج أهمها :

- 1- ان جرائم الدم والقدح الإلكتروني من اكثر الجرائم الإلكترونية انتشارا خاصة وانها تعتمد في ذلك على مختلف الوسائل الحديثة ابرزها منصات التواصل الاجتماعي .
- 2- ان القانون الأردني يختلف عن بعض القوانين الأخرى كالقانون المصري والإماراتي حيث اطلقت عليها اسم قوانين الجرائم الإلكترونية أما المشرع الإماراتي فاطلق عليها قوانين تقنية المعلومات لتكون الجرائم او الجرائم المعلوماتية هي جرائم مستحدثة يجب ان يكون لها قواني خاصة بها.
- 3- هناك أنماط كثيرة ومتنوعة من الجرائم الإلكترونية التي تناولتها مختلف التشريعات في مجال هذه الجرائم ويعتبر التشريع الإماراتي اكثر من توفيق في شمل كل الجرائم الإلكترونية .

4- يمكن ان تقع الجرائم المستحدثة ونخص بالذكر جرائم القدح والتحقيق الإلكتروني من خلال فيسبوك وتويتر ... الخ والتي يمكن ان تعاقب طبقا للنصوص التقليدية مع ضرورة إيجاد قوانين خاصة بها لان هناك أنواع أخرى للجريمة الإلكترونية غير واضحة الأركان كما تم التطرق اليها في الدراسة التي سبقت كالجرائم الخاصة بالنظم المعلوماتية او الاحتيال الإلكتروني وغيرها ... الخ (حسين 2016 ، 7، 112، 113).

5.4.1. دراسة وسائل التحري في الجرائم الإلكترونية 2018 ادهم باسم نمر بغداددي :



تناولت هذه الدراسة مختلف وسائل المعتمدة في التحري والبحث عن الجرائم الإلكترونية من منظور القانون الفلسطيني وهذا بعد صدور قانون خاص بها في 2017 تحت رقم 16 ومن خلال هذه الدراسة سعى الباحث للتعريف بطبيعة هذه الجريمة وكذا التعريف بعملية البحث والتحري فيها وذكر اهم صفات المكلفين بهذه العملية باعتبارها جريمة مستحدثة تتميز عن الجرائم التقليدية الأخرى ، كما سعت الى التأكيد على البحث الذي يراعي عدم المساس بحرية الأشخاص والحقوق الإنسانية ، من خلال ذكر الإجراءات المعتمد عليها في ذلك في حال الوقوع في الجريمة الهيا مهما كان نوعها ومن اجل هذا انطلقت من تساؤل ما مدى صلاحية الوسائل التقليدية في البحث والتحري في الجريمة الإلكترونية ؟ والذي تبع بالتساؤل عن الوسائل المستخدمة في ذلك ؟ واعتمدت على تحليل النصوص القانونية المتعلقة بالموضوع وجمع الحقائق والبيانات ووصفها من خلال المنهج التحليلي الوصفي وتوصلت الى نتائج تمثلت في ما يلي :

- 1- إصدار القانون رقم 16 سنة 2017 نظرا لخطورة الجرائم الإلكترونية والذي اصبح حيز التنفيذ في المحاكم الفلسطينية.
- 2- التوصل الى ان هناك نوعين من الضبط في اطار مواجهة الجرائم الإلكترونية وهوما الضبط الإداري الذي يعمل على حماية المجتمع من المخاطر من خلال الإجراءات الوقائية أما الضبط القضائي فيختص ما بعد وقوع الجريمة الإلكترونية من خلال عملية البحث والتحري وتفتيش الأدلة المادية باعتماد برامج خاصة .
- 3- وجوب احترام القوانين والالتزام بالإجراءات المرسومة وعدم تجاوزها واحترام الخصوصية على منصات التواصل الاجتماعي او الحاسب الألي وعدم الاعتداء عليها .
- 4- ما يميز هذه الجرائم أنها تستهدف الاعتداء على النظم المعالجة للمعطيات كما أنها تختلف عن الجرائم التقليدية فهي جرائم تمس بالمعلومات الإلكترونية المتواجدة على مستوى البيئة الرقمية وهذا ما يعني الاختلاف بين الأدلة الخاصة بكل جريمة (ادهم 2018، 5 - 99)

1.4.6. دراسة سارة محمد حنش بعنوان المسؤولية الجنائية عن التهديد عبر الوسائل الإلكترونية 2020 : حيث توجهت الباحثة نحو إجراء دراسة مقارنة بين التشريع الأردني والتشريع العراقي من خلال تناول المسؤولية الجزائية المترتبة عن ممارسة جرائم التهديد عبر الوسائل الإلكترونية حيث تطرقت الى التعريف بمهامية المسؤولية الجزائية ومهامية جرائم التهديد وأيضا الى الجوانب الموضوعية بجريمة التهديد عبر الوسائل الإلكترونية وكيفية ملاحقة مرتكبيها من الجهات القانونية حيث تمحورت مشكلة الدراسة في البحث عن الأحكام الإجرائية والموضوعية للمسؤولية الجزائية لجريمة التهديد عبر الوسائل الإلكترونية بين القانون الأردني والقانون العراقي وفيما تتمثل سياسة البادين في حماية الأفراد منها حيث اعتمدت على المنهجين الوصفي التحليلي والمنهج المقارن في حدود زمانية شملت الفترة ما بعد انقضاء قانون الجرائم الإلكترونية رقم 27 لسنة 2015 لتصل في الأخير الى مجموعة من النتائج تمثلت في :

- 1- ان خطورة جرائم التهديد عبر الوسائل الإلكترونية تتمثل أساسا في سرعة انتشارها والذي أدى الى إصدار قانون الخاص بالجرائم الإلكترونية رقم 27 لسنة 2015 والقانون الخاص بمكافحة جرائم تقنية المعلومات وفق المشرع المصري تحت رقم 175 لسنة 2018 على عكس المشرع العراقي الذي يعد متأخر في اطار مكافحة الجرائم الإلكترونية .
- 2- التأكيد على ضرورة استعمال الوسائل الحديثة التي يعتمد عليها مرتكبي هذه الجرائم من اجل البحث والكشف عنها.
- 3- الاعتماد على الدليل الرقمي كدليل لإثبات الجرائم المعلوماتية (سارة 2020، 3، 4، 77) .

1.5. تقييم الدراسات السابقة : في نهاية عرض الدراسات السابقة المعتمد عليها يمكن ان نقوم بتقييمها وهذا بذكر اهم النقاط التي تتقارب فيها مع موضوع دراستنا واهم ما يجمع بين هذه الدراسات أيضا ويمكن ان نعرض هذا في ما يلي : معظم الدراسات



التي تناولت الجرائم الإلكترونية أو المعلوماتية اعتمدت على نفس مبدأ الدراسة وهي التعريف بماهية هذه الجرائم وذكر خصائصها أركانها، وعرض القوانين التي تم النص عليها في إطار مكافحتها، وعرض أهم أنواعها لكن اقتصر هذا على شرح الأنواع فقط فلم تقدم إحصائيات حول نسبة انتشار هذه الجرائم بمختلف صورها، وما لوحظ أن مفهوم هذه الجرائم المستحدثة كله انحصر بين مصطلح الجرائم الإلكترونية، الجرائم المعلوماتية، وجرائم الأنترنت أو التقنية الحديثة، كما أن أغلب الدراسات هي دراسات مقارنة بين تشريعات مختلفة في إطار مكافحة الجرائم المعلوماتية هدفها الوصول إلى معرفة مدى كفاءة القوانين في الحد من مثل هذه الجرائم وحماية الأفراد والمجتمعات منها والتي كلها اتفقت أن للجريمة المعلوماتية والجرائم المعلوماتية خصائص تميزها عن ما هو تقليدي أما من خلال الوسائل والطرق المعتمدة أو حتى من ناحية الكفاءة والخبرة والدكاء الذي يمتلكه مرتكب الجريمة كما أنها اتفقت حول عنصر الركن المادي الذي يصعب إثباته في الجرائم المعلوماتية لأنها جرائم تقع ضمن فضاء الكتروني رقمي كما أن الدراسات أشارت إلى وجود الجرائم المعلوماتية يمكن أن تكون موضوع للجريمة من خلال استعمال تقنية المعلومات كأداة في ذلك ويتم أن تكون هدف للجريمة من خلال سرقة مختلف أشكال المعلومات والبيانات الخاصة أو العامة وإساءة استخدامها، إما بالنسبة للاقترب بين الدراسات السابقة وموضوع بحثنا يمكن أن نراه من جانب الموضوع المراد بحثه الذي يمثل المحور الأساسي أو من أجزاء الدراسات المعروضة سابقا فبعض الدراسات كانت عن الجرائم المعلوماتية والبعض الآخر تناولها كشكل من أشكال الجرائم الإلكترونية ومن ناحية أخرى بعض الدراسات تناولت المنصات الاجتماعية كأداة للجريمة المعلوماتية وهذا ما تهدف دراستنا البحث عن من خلال تقديم إحصائيات عن مدى استخدامها وعلاقتها بالجرائم المعلوماتية وهذا ما سنتطرق إليه لاحقا .

6.1. المقاربة النظرية المفسرة للجريمة المعلوماتية عبر منصات التواصل الاجتماعي : هناك الكثير من النظريات الاجتماعية التي سعت إلى تفسير مختلف أنواع السلوكيات الإجرامية في ظل مختلف الظروف المجتمعية التي يعيش فيها الأفراد ومن بين هذه النظريات المهمة هي نظرية التعلم الاجتماعي "لألبرت باندورا" التي كان لها منظورها الخاص في تفسير الجريمة وسوف نعتمد على أهم ما جاء فيها لتفسير الجريمة المعلوماتية ومنصات التواصل الاجتماعي وهذا على النحو التالي :

1.6.1. أهم ما جاء في نظرية التعلم :

ظهرت نظرية التعلم أو نظرية التعلم بالملاحظة سنة 1977 م، حيث اهتم ألبرت باندورا بالتعلم الاجتماعي كعامل أو مدخل لدراسة شخصية الفرد، وذهب إلى أن الفرد يتعلم أنماط السلوك المختلف من خلال الملاحظة للآخرين وتقليدهم داخل البيئة الخارجية المحيطة به، والتي توفر له نماذج سلوكية كثيرة تعتبر نماذج تعليمية بالنسبة له يتعلم من خلالها مختلف أنواع السلوك الإيجابية كانت أو السلبية فيتفاعل مع محيطه ويتأثر به ويضيفها إلى خبراته المتواجدة لديه من قبل إما من خلال عملية التقليد أو الملاحظة فنجد أن نظرية التعلم والتي تعرف أيضا بنظرية الاكتساب المعرفي قد قسمت عملية التأثير التي تمر بها الأفراد إلى مرحلتين وهما :

"مرحلة ما قبل اكتساب السلوك والقيام به والتي ترتبط بالتأثير على الفرد نحو اكتساب سلوك معين وفقا لعوامله الفيزيولوجية والعاطفية الخاصة به والتي تختلف من فرد إلى آخر إضافة إلى كل الخبرات والأحداث

المعرفية الموجودة لديه مسبقا، إما المرحلة الثانية وهي ما بعد إصدار السلوك" والتي ترتبط في مدى اكتساب الفرد لسلوك ما في إطار عوامل التعزيز والدعم أو ما يقابلها من عوامل الردع والعقاب الداخلي والخارجي وحسب نظرية التعلم فكل سلوك إنساني هو سلوك مكتسب من خلال اتباع نموذج أو مثال حي وواقعي وتتطور هذه العملية بمساعدة المعلومات السابقة التي توجهه نحو سلوك معين لينتج عن التعلم بالملاحظة أفكار إيجابية جديدة وإبداعية ويمكن أن ينتج عنها عكس ذلك وهذا راجع لشكل التفاعل



مع المتغيرات البيئية ومدى ملائمة الظروف الوقفية التي تحدث أثناء عملية التعلم إضافة إلى حجك التفاعل بين فرد الملاحظة ونموذج الملاحظة ليشمل مع هذا كل العلاقات الترابطية والنفسية الموجودة بين الظواهر (مراد و يوسف 2016، 16-14).

2.6.1. الاقتراب النظري بين الجريمة المعلوماتية عبر منصات الاجتماعية وبين نظرية التعلم:

ان مختلف الوسائل التقنية الحديثة والتي وفرت العديد من إمكانيات التواصل الضخمة والتي تعد المنصات الاجتماعية من بينها كانت المكان المناسب الذي يكتسب منه الأفراد مختلف السلوكيات والأفكار والممارسات فأتاح مصات التواصل الاجتماعي لكل الأفراد والمجتمعات حرية عرض نشاطاتهم التي يمارسونها والتي تختلف حسب ثقافة وأخرى وقيم وأخرى كما أتاح لهم نشر كل يمكنهم من اكتساب المعرفة على اختلاف نوعها والتي في أحيان كثيرة تكون مفيدة لهم ولحياتهم لكن من جهة أخرى اكتسبهم لهذا الكم الهائل من المعرفة يمكن ان يساء استخدامه ويوجه نحو أفعال إجرامية ومن ناحية أخرى هذه المنصات توفر نماذج إجرامية بالفعل والتي يتم نشرها بشكل كبير جدا ويتم الدعوة إليها والتي تؤثر على الأفراد وتدفعهم نحو اكتساب هذه الممارسات رغم خطورتها كتعلم جرائم الاختراق والاحتيال وسرقة المعلومات والابتزاز مقابل أرباح مادية أو اكتسابهم لأفكار متطرفة ومتعصبة نحو قضايا معينة والتي تدفع بهم إلى ممارسة العنف ونشر صور الكراهية والتخويف والتهديد لتكون هذه المنصات عبارة عن مكان يحمل مختلف النماذج الإجرامية التي يلاحظها و يكتسبها الفرد ويتأثر بها ويمارسها ومن أمثلة هذه الممارسات الجرائم المعلوماتية باختلاف نوعها وحجمها وحدتها.

2. الاطار النظري للدراسة : الجريمة المعلوماتية عبر منصات التواصل الاجتماعي

1.2. كيف ظهرت منصات التواصل الاجتماعي :

ان ظهور ما يسمى بمنصات التواصل الاجتماعي مر بمراحل وأول شكل لها كان في فترة التسعينات كموقع Classmates.Com عام 1990م، وموقع six Degrees.Com عام 1997م التي تعتبر مواقع للربط بين الأشخاص (محمد و داعة 2016، 19)، وبعدها ظهرت مواقع أخرى مثل لايف جوناك وكأي ولد سنة 1999 واهم ما ميزتها في هذه الفترة هي خدمة الرسائل القصيرة والتواصل بين الأصدقاء.

وبعد هذا نجد ان مجموعة من التطبيقات على الويب بدأت بالظهور مثل المدونات وموقع مشاركة الوسائط المتعددة وغيرها لتتجه هذه المرحلة إلى تطوير التجمعات الافتراضية التي تتيح درجة كبيرة من التفاعل والاندماج وإمكانية التعاون بين الأفراد وارتبط هذا أيضا بتطوير في خدمة الأنترنت حيث تعتبر هذه الفترة مرحلة اكتمال المنصات الاجتماعية وأرخ هذا من خلال اطلاق موقع ماي سبيس و منصة فيسبوك الأمريكية في 2004 الذي عرف انتشارا كبيرا والذي تناسب مع تزايد في نسبة مستخدمي الأنترنت في العالم وبدأت هذه المنصات بالانتشار أكثر فاكتر كما ظهرت منصات أخرى مثل موقع سكاى روك كمنصة للتدوين فقط في أول الأمر ومن ثم أصبح شبكة اجتماعية بشكل كلي في 2007 والذي حقق نجاحا كبيرا وقد أتاح هذه المنصات وغيرها لخبرة مطوري البرامج والذي نتج عنه زيادة كبيرة جدا في مستخدمي فيسبوك الذي ظهر إلى جانبه أشكال أخرى كتويتر وانستغرام ويوتيوب وغيرها من المنصات الاجتماعية المعتمد عليه اليوم بشكل واسع جد على مختلف الاتجاهات لذا سوف نتطرق في ما يلي إلى بعض النماذج عن المنصات الاجتماعية ومحاوله تقديم إحصائيا عن مدى استخدامها (احمد و سليم 2019، 19).



2.2. بعض نماذج منصات التواصل الإلكتروني:

1.2.2. منصة فيسبوك : هو موقع أنشئ سنة 2004 من طرف مارك زكربيرج Mark Zuckerberg طالب بجامعة هارفارد في وقتها ، ويقصد بمصطلح فيسبوك ب "كتب الوجوه" التي وجهت في البداية إلى الطلاب ليتمكنوا من التعارف على بعضهم البعض والتواصل ، ومن ثم بدا في الانتشار والتوسع ليشمل الجامعات الأخرى والمؤسسات كما عرف العديد من التطورات التقنية بهدف جعله أكثر فعالية وسهولة، ومن هذه التطورات إلغاء شرط انتماء مستخدمي الفايسبوك لجامعة ما أو مؤسسة ، ليصبح متاحا أمام كل فرد فوق سن ال13 (علي خليل 2014، 64، 65)، كما يمكن التعريف به على انه موقع إلكتروني تملكه شركة فيسبوك المساهمة العامة في إحدى وسائل الاتصال الاجتماعية الحديثة، ويعد من أشهر المواقع الاجتماعية على الأنترنت ويقدر عدد مستخدميه بمئات الملايين (بطرس 2016، 3)،

واستمر بالتطور وتحقيق الانتشار حول العالم ليتم الإعلان بحلول سنة 2017 بواسطة مؤسسه "مارك"، بأن عدد المستخدمين يقدر بحوالي 2 مليار مستخدم ما يمثل 4/1 من سكان العالم، وتزامنا مع هذا أعلنت عن توفيرها لتطبيقات أخرى أيضا (ميمي 2018، 23، 24)، وحسب إحصائيات قدمت من طرف "داتا ريبورتال data reportal، و ستيتس برو status brew، وبرودباند سيرش، broadband search في 18 يوليو 2021"، والذي صرح ان مستخدمي موقع فليسبوك قد بلغ 2.85 مليار مستخدم نشط شهريا واحتل المركز الثالث بين المواقع الأكثر زيارة بعد قوقل و منصة يوتيوب (رماح 2021).

2.2.2. منصة يوتيوب : اختلفت الآراء حول موقع يوتيوب ما اذا كان موقع تواصل اجتماعي فمنهم من يذهب إلى اعتباره موقع لمشاركة الفيديو. وهناك من يذهب إلى اعتباره وتصنيفه كنوع من أنواع مواقع التواصل الاجتماعي وهذا يعود إلى اشتراكه معها في عدة خصائص ، والتي جعلت التحدث عنه كاهم مواقع التواصل الاجتماعي وهذا لأهميته الكبيرة التي يقوم بها في مجال نشر الفيديوهات واستقبال التعليقات عليها ونشرها بشكل كبير ، وتقوم فكرة يوتيوب على مبدا بث لنفسك أو ذع لنفسك Broadcast. Yourself، ويوضع هذا الشعار في الصفحة الأولى ، ويعد اهم وسيلة لبث مقاطع الفيديو على شبكة الأنترنت إذ تحمل عليه يوميا أفلام من صنع الهواة من حول العالم ، وكثيرا منها تم إنتاجه لدوافع فنية أو سياسية أو اجتماعية (مريم نزيهان 2011-2012، 65) ، وقد اطلقت نسخته التجريبية في ماي 2005 وبعد ستة اشهر تم اطلاق النسخة الرسمية ، وفي عام 2006 قامت شركة قوقل بالاستحواذ عليه ليصبح من اشهر المواقع والتي تطورا بشكل سريع على شبكة الأنترنت والذي كان يحظى ب100 مليون مشاهدة يوميا ، ومن ثم بدا الاتفاق مع الكثير من القنوات لبث مقاطع من برامجها على غرار قناة CBS (ياسين 2014، 339، 340)، إذ يعد يوتيوب الموقع الأول لبث مقاطع الفيديو والذي بلغ عدد مستخدميه في 2021 حوالي 2 مليار ب100 إصدار محلي حول العالم كما يتيح إمكانية التنقل في نظامه الأساسي بأكثر من 80 لغة مختلفة (Sarah 2021).

3.2. الجريمة المعلوماتية عبر فيسبوك ويوتيوب :

ان التطور في البنية التحتية للأنترنت كان مرفوق بتزايد كبير في نسب استخدامها حول العالم، فلو رجعنا مثلا لسنة 2011 فان مستخدمي الأنترنت قدر ب2.3 مليار نسمة ما يشكل 3/1 من إجمالي السكان ، موزعة بنسب مختلفة على كل دول العالم لتتمتع الدول المتقدمة ب70 بالمئة من حجم الأنترنت مقابل 24 بالمئة للدول النامية ، وما يميز هذا الاستخدام الهائل لشبكة الأنترنت هو توفرها على نظم رقمية ومواقع ومنصات تواصل مختلفة، تلبى كل احتياجات الأفراد في كل المجالات، ومن بين أكثر المواقع استخداما على شبكة الأنترنت "المنصات الالكترونية"، التي قدر عدد مستخدميها لسنة 2020 بحوالي 4 مليار شخص وهذا حسب ما نص عليه تقرير هوتسويت و وي ارسوشل الذي أكد على انه ينضم حوالي 2 مليون شخص يوميا لهذه المنصات الاجتماعية



بنسب مختلفة بين أنواعها الكثيرة، (واشنطن 2020)، ومن جهة أخرى ولأن مصطلح الجريمة السيبرانية مرتبط بالتطور التكنولوجي والتفني، فهي الأخرى شهدت ارتفاعا في نسب جرائمها المرتكبة على مستوى الفضاءات الرقمية أو النظم المعلوماتية المختلفة، ومن أجل هذا كان لابد من مواجهة هذه الجريمة المستحدثة على المستويين الدولي والوطني، والعمل على إيجاد قوانين تتماشى مع طبيعة هذه الجرائم من جهة وان تكون قادرة على حماية الأفراد وحقوقهم من جهة أخرى، ونظرا لتعدد الأساليب المتعمدة من طرف مرتكبي هذه الجرائم سنحاول التطرق لبعض النماذج المعتمدة في ممارسة الجريمة السيبرانية، وهنا سوف نتحدث عن الجرائم المعلوماتية المرتكبة على مستوى منصات التواصل الاجتماعي فيسبوك ويوتيوب، والذي سيرتبط في هذا الإطار بالجرائم الإلكترونية التي سنذكر بعض الأمثلة عنها ونسب انتشارها (موسى 2014، 8-1)، حيث نجد أن من أكثر الجرائم التي يتم ممارستها من خلال موقع فيسبوك هو الابتزاز والتهديد والتنمر وسرقة المعلومات الشخصية وعمليات اختراق الحسابات الشخصية التشهير ونشر الإشاعات، والاحتيال الإلكتروني إذ يعتبر هذا الأخير من أكثر الجرائم المنتشرة عبر منصة الفيسبوك من خلال عملية الجذب والإغراء الممارسة على الأفراد ودفعهم للدخول في مواقع ورابطات إلكترونية، ولفت انتباههم وميولهم ليقعوا ضحية للجريمة المعلوماتية من خلال سرقة كل بياناتهم الخاصة، وتتمتع هذه الجرائم بدقة وكفاءة عالية من طرف مرتكبيها الذي لا يترك أثر أو دليل على جرمته، ونجد أيضا التحرش الإلكتروني الذي يشمل التحرش الجنسي واللفظي والاستدراج والاعتداء بالألفاظ المسيئة باستغلال غرف الدردشة التي يفورها فيسبوك لمستخدمين، وقد أثبتت مختلف الإحصائيات على ممارسة وانتشار التحرش بين مستخدمي فيسبوك وقدرت في سنوات مضت ب 40 بالمئة سنة 2017 بنسب متفاوتة بين الفئات العمرية، كما أكدت إحصائيات أخرى على انتشار ظاهرة التنمر بين أوساط المراهقين على منصة فيسبوك من خلال استعمال ألفاظ وكلمات الإهانة، والتي قد تؤدي إلى جرائم أكثر خطورة على أرض الواقع كالانتحار.

ولا يمكن تجاهل جرائم التجسس على الحسابات الشخصية والمطاردة والاطلاع على المعلومات وانتهاك الحياة الخصوصية خاصة، بإتاحة موقع فيسبوك إمكانية ذلك من خلال إشعارات الموقع الخاص بحسابات الأفراد، كما أن امتلاك شركة فيسبوك معلومات ضخمة أدى إلى انتهاك خصوصية 88000 مستخدم، إضافة إلى جرائم سرقة وانتحال الشخصية والتشهير بالسمعة وتناقل الأخبار والإشاعات عبر صفحات الفيسبوك (حفيدة 2019، 4)، حيث يقوم المجرم بنشر معلومات قد تكون سرية أو خاطئة عن الضحية والذي يمكن أن يكون فرد أو مؤسسة (مركز هردو 2018، 9)، ووفق استطلاع لموقع (بيو أنترنت اند أمريكان لايف) سابقا فإن 55 بالمئة من الفئة العمرية 12 إلى 17 سنة عرضة للتحرش الإلكتروني عبر فيسبوك (محمود سيد 2021، 7).

كما هناك صور أخرى للجريمة المعلوماتية عبر منصة التواصل فيسبوك وهو الإرهاب الإلكتروني من خلال الدعوة إلى التطرف واستدراج الأفراد نحو المنظمات الخاصة بها، وكشف عنه إحصائيات سجلت سابقا حول الجرائم المرتكبة فيسبوك والتي تتعلق معظمها بالدعوة إلى العنف وجرائم التنمر وألفاظ ماسة بالأفراد، والمحتوى التي يستهدف الهجوم على الأفراد حسب الجنس أو العرق أو الإعاقة أو غيرها عبر مختلف صفحات فيسبوك، التي تنشر بسرعة كبيرة جدا وتشكل خطر وتهديد حقيقي على المجتمع ونظرا لخطورة هذه الجرائم نجد فيسبوك قد وافق على مدونة خاصة بضبط السلوك، حسب اتفاقية خاصة بالاتحاد الأوروبي منذ 31 ماي 2016، على غرار المنصات الأخرى كتيوتر وقوقل... الخ (محمود عبد العزيز 2021، 9).

ومن بين المنصات التي تستخدم اليوم أيضا في الجرائم المعلوماتية نجد منصة يوتيوب، التي يتم استعمالها طرف المنظمات الإرهابية حيث تعمل هذه الأخيرة على إنشاء صفحات القنوات خاصة بها، تحت مسميات تمويهية من أجل بث أفكارها وهذه القنوات تقوم من طرق القيادات العليا التابعة لها، فتقوم بنشر مقاطع لتعليم كيفية تصنيع الأسلحة والدعوة إلى المشاركة بهذه الحسابات التي



تكون في اصلها تسعى الى الدعوة الى المبادئ الإرهابية والتدريب عليها، باستغلال الوسائل التكنولوجية والتقنية الحديثة على غرار المنصات الاجتماعية الأخرى، وتعتبر هذه الجرائم خطيرة جدا لما لها من تداعيات على الفرد والمجتمع والتي يطلق عليها "جرائم الخطر"، والتي تستهدف الأفراد او المؤسسات او الجماعات المختلفة ما يؤثر على الاستقرار الأمني ونشر الخوف، كما ان هذه الجرائم الممارسة عبر منصة يوتيوب والمنصات الأخرى تكون مسبقة بأهداف معينة تعمل على الوصول إليها، والتي تجد في هذه المنصات الوسيلة الأسهل والأكثر انتشارا واستخداما من قبل الأفراد، وهذا ما يسهل عليها مهمتها إذ اثبتت الإحصائيات أنها تزداد مع تطور هذه المنصات، وتصبح أكثر اتساعا لتشمل الحكومات التي أصبحت اليوم تمارس مختلف أنشطتها على منصات الاجتماعية مثل يوتيوب التي تحتوي على ملايين القنوات الرسمية لمختلف المؤسسات او الحكومات والأفراد (صدام حسين 2019، 222، 233، 234)، ليكون يوتيوب من أكثر المنصات استخداما وهذا ما منحه قوة التأثير، التي يستغلها جهات معينة لأغراض إجرامية كالابتزاز والتشهير والتحريض والدعوة الى بث الكره والتفرقة بين المجتمعات من خلال نشر مختلف الأفكار الداعية لذلك، من خلال جهات إعلامية معروفة والتي تمتلك عدد كبير من المتابعين وهذا طبعا مقابل الحصول على الدعم المالي والتمويل لهم من طرف الجماعات المستفيدة من ذلك، والكثير من الجرائم الأخرى كنشر الإشاعات والمحتوى الغير أخلاقي والمساهمة في صنع ونشر المواد الإباحية ونشر الأفكار المغلوطة عن الحرية والدعوة الى التمرد على القوانين واستعمال القوة... الخ، إذ نجد ان جرائم الابتزاز الأكثر انتشارا على منصة يوتيوب من خلال نشر الصور والألفاظ المسيئة للأشخاص والتعدي على حياتهم الخاصة ونشر الإشاعات عنهم، والتحقير والقذف التي تعتبر من جرائم المساس بالشرف والمكانة الاجتماعية، ومن اخطر الجرائم المنتشرة على يوتيوب هي نشر المواد الإباحية واستدراج الأطفال نحو الأمور الجنسية وهذا لنقص خبرتهم وقدرتهم على التحكم في سلوكياتهم ليمتد استغلالهم في الأعمال غير المشروعة، كل هذه الجرائم الممارسة باستغلال التقنية المعلوماتية والمنصات الاجتماعية هي معاقب عليها في مختلف التشريعات التي تسعى لمحاربة الجرائم المستحدثة بمختلف أشكالها وطرقها (عمر و وآخرون 2020).

خاتمة :

وفي نهاية الدراسة ما يمكننا ان نقول عن الجريمة المعلوماتية هي من الجرائم المستحدثة التي بدأت المجتمعات تعرفها لتنتشر بشكل سريع وكبير جدا، مستغلة في ذلك التطور التقني والمعلوماتي ومختلف المواقع والمنصات التي نتجت عن هذا التقدم، هذا ما جعل الجريمة المعلوماتية تختلف عن التقليدية منها من حيث طبيعتها وأركانها أيضا وسمات مرتكبيها، فهي جريمة غاية في الدقة وهذا ما يدل على الذكاء الكبير الذي يتمتع به المجرم المعلوماتي، الذي يستغل ثغرات التقنيات الحديثة لارتكاب جرائمه دون ان يترك ما يدل عليه، إضافة إلى أنها جرائم يصعب إثباتها بالدلة المادية هذا ما دفع إلى ضرورة الاعتماد على الدليل الرقمي الإلكتروني كدليل لإثباتها، ونتج عن الطبيعة الخاصة للجرائم المعلوماتية وجوب التعامل معها بنفس أسلوبها واعتماد الوسائل الحديثة والمتطورة في الكشف عنها، والعمل على جعل القوانين موازية للتطور التي تعرفه باستمرار، كي لا يكون هناك نقص في جانب الحماية منها أو مكافحتها وهذا ما تعمل عليه الدول جاهدة من اجل تحقيقه، من خلال كل القوانين والمواثيق الخاصة بها

قائمة المراجع:

1. أمل كاظم، إدمان الأطفال والمراهقين على الأنترنت وعلاقته بالانحراف: مجلة العلوم النفسية 2011 .
2. رصاع فيحة، الحماية الجنائية على شبكة الأنترنت: رسالة ماجستير كلية الحقوق والعلوم السياسية، تلمسان جامعة أبي بكر بلقايد 2011-2012.



3. بشرى جميل الراوي، دور مواقع التواصل الاجتماعي في التغير مدخل نظري: مجلة الباحث الاعلامي، العدد 18، كلية الاعلام، جامعة بغداد، 2012.
4. شينا كايسر، وسائل التواصل الاجتماعي: دليل علمي للهيئات المعنية بالإدارة الانتخابية، ترجمة شركة بانغلوس، 2015.
5. وادي عماد الدين، السلوك الإجرامي لدى المرأة: رسالة ماجستير كلية الحقوق والعلوم السياسية جامعة الحاج لخضر باتنة، 2011-2012،
6. خالد ممدوح ابراهيم، الجرائم المعلوماتية والإلكترونية: <https://kenanonline.com> موقع الكتروني، 2008.
7. ادهم باسم نمر، وسائل التحري في الجرائم الالكترونية: رسالة ماجستير كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، 2018.
8. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2011.
9. صغير يوسف، الجرائم المرتكبة عبر الانترنت: رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.
10. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية: رسالة ماجستير، جامعة الشرق الاوسط، 2014.
11. حسين زلوم، جرائم القذف والذم والتحقيق الإلكتروني في القانون الأردني دراسة مقارنة: رسالة ماجستير، كلية الحقوق، كلية الدراسات العلمية، جامعة الاسراء، عمان، 2016.
12. سارة حنش، المسؤولية الجنائية عن التهديد عبر الوسائل الإلكترونية دراسة مقارنة، رسالة ماجستير: كلية الحقوق، جامعة الشرق الاوسط، 2020.
13. مراد شعشوعة يوسف داودي، مواقع التواصل الاجتماعي وتنامي السلوك الانحرافي للتلميذ: مجلة تطوير العلوم الاجتماعية، 2016.
14. محمد العوضي داعة الله، مواقع التواصل الاجتماعي وقضايا الشباب الجامعي: دار الخليج للنشر والتوزيع، 2016.
15. احمد قاسمي سليم جدادي، تأثير مواقع التواصل الاجتماعي على الأمن المجتمعي للدول الخليجية: دار النشر المركز الديمقراطي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، 2019.
16. علي خليل شنفرة، الاعلام الجديد (شبكات التواصل الاجتماعي): دار أسامة للنشر والتوزيع، عمان، 2014.
17. بطرس الحلاق، اثر مواقع التواصل الاجتماعي على تنمية السلوكيات والقيم لدى طلاب الجامعة: مجلة تشرين للبحوث والدراسات العلمية، 2016.
18. ميمي محمد عبد المنعم توفيق، شبكات التواصل الاجتماعي النشأة، التأثير: مجلة كلية التربية، 2018.
19. رماح الدلقموني، وسائل التواصل الاجتماعي حقائق وارقام: مكة المكرمة، موقع الكتروني، <https://www.aljazeera.net>، 2021.
20. مريم نوبمان نومان، استخدام شبكات التواصل الاجتماعي وتأثيره في العلاقات الاجتماعية: رسالة ماجستير، كلية الاتصال والاعلام، جامعة الحاج لخضر، باتنة، 2012-2011.
21. ياسين خضير البياني، الإعلام الجديد الدولة الافتراضية الجديدة: دار البداية للنشر والتوزيع، بغداد، 2014.
22. سارة مختاري، اهم إحصائيات اليوتيوب التي يجب على كل متسوق معرفتها (2022): موقع الكتروني، <https://expaandcart.com>، 25 سبتمبر 2021.
23. واشطن العربي الجديد، نصف البشر يستخدمون مواقع التواصل الاجتماعي: موقع الكتروني، <https://www.alaraby.co.uk>، 2020.
24. موسى ذياب البدانية، الجرائم الإلكترونية: الملتقى العلمي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الاردن، عمان، 2014.
25. حفيضة سليمان احمد الراشدية، الفايس بوك والجرائم الإلكترونية في عمان هل هناك علاقة؟: مجلة دراسات المعلومات والتكنولوجيا، 2019.
26. مركز هدر، التنظيم القانوني والجرائم الإلكترونية ما بين حماية المعلومات وتقييد الحريات: القاهرة، 2018.
27. محمود سيد احمد عبد القادر عامر، اشكالية تحديد المسؤولية الجنائية للتحرش الإلكتروني كجرمة الكترونية والجهود الدولية لمكافحتها: رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2021.



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها

رمز I05L02UN260120190001

28. محمود عبد العزيز يوسف أبو المعاطي، وسائل التواصل الاجتماعي واثرها في انتشار خطاب الكراهية رؤية اسلامية: 2021.
29. صدام حسين ياسين العبيدي، جرائم الأنترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية: المنهل للنشر، 2019.
30. عمر شحادة وآخرون، جرائم اليوتيوب: منشورات حماة الوطن ، موقع الكتروني، <https://jordan-lawyer>، 2020.



التحريض عبر مواقع التواصل الاجتماعي

- فايسبوك أنموذجا -

Social media incitement mechanisms – Facebook -

د. قدوح نور الهدى

جامعة يحي فارس المدية

مقدمة :

من المذهل ما حققه العالم اليوم من تقدم تكنولوجي متطور في مجال التواصل الرقمي بين الأفراد و الجماعات ، حيث بات التواصل الرقمي مع الآخر ميزة هذه الألفية ، حيث حتمت علينا هاته الثورة التكنولوجية أن نكون جزءا من المنظومة الرقمية . لا ينحصر التواصل عبر مواقع التواصل بين الأفراد فقط ، و لكن أصبحت كل المؤسسات الرسمية و الغير الرسمية تلجأ لهاته المواقع للتقرب من الأفراد بشكل أسرع و أشمل بهدف الإعلام أو التحذير أو الإبلاغ لآخر المستجدات السياسية أو الاقتصادية أو الاجتماعية داخل المجتمع الواحد.

لأول مرة من عام 2004 أنشأ مارك زوكبيرغ موقعا للتواصل بين مجموعة من الطلبة ليسهل عليهم التواصل فيما بينهم أسماه فايسبوك . حقق هذا الموقع شعبية امتدت للعالم بأكمله حيث أصبح الموقع الأكثر استخداما لغالبية شعوب المعمورة ، الجزائر لم تكن الاستثناء . و هذا راجع لسهولة استخدامه حيث سهل لكل الأشخاص من مختلف الفئات و المستويات استخدامه لأهداف متعددة كالتعلم أو للترفيه و التسلية ، و بالرغم من الإيجابيات المتنوعة لهذا الموقع إلا أنه أصبح أيضا ملاذا للمتطفلين و للمعتدين و المحرضين . هذا ما سيقودنا في سياق هذا الطرح إلى جريمة التحريض و المساهمة في الجريمة ، حيث استغل العديد من الأشخاص ذو النوايا السيئة فايسبوك لتحقيق مآربهم الشخصية عن طريق جر فئة مستهدفة من الأفراد إلى انتهاج سلوك العنف و العدوان بدلا عنهم و لذلك أصبح التحريض عبر الفايسبوك من أكثر الأساليب تهديدا بالأفراد و المجتمعات ، يشمل التحريض الرقمي عدة أساليب منها التحريض على التطرف العقائدي أو السياسي أو حتى الاجتماعي أو التحريض بسبب الرياضة أو التحريض بالإحياء ، و التحريض على العنصرية و الجهوية و التحريض على الإدمان . حيث يهدف المحرض إلى نشر الفتنة و الفوضى و لزعة الاستقرار النفسي و الاجتماعي للفرد و الجماعات .

و في ظل ما تنامي هذه الظاهرة و هذا ما نلاحظه عبر مواقع التواصل الاجتماعي (فايسبوك) ، استنفر المشرع الجزائري لإعداد نصوص تشريعية لمجابهة هذا النوع من الجرائم الرقمية في ظل ثقافة عدم التبليغ من الضحايا أو للمتفاعلين مع هذه المنشورات التحريضية . لذلك عكفت الجهات الأمنية الجزائرية دائما على تنبيه و تحذير الأفراد من سوء استخدام هذه المواقع حماية لأنفسهم و لسلامتهم و لحريتهم المدنية على مختلف المستويات . لذلك من خلال مما سبق سنطرح الأسئلة التالية : ماذا نقصد بالتحريض عبر الفايسبوك ؟ و كيف يتمظهر ؟

لذلك سنتناول في فحوى هذه المداخلة المحاور الآتية :

1. ماهية الجريمة الإلكترونية

1.1. مفهومها

2.1. من هو الجاني المعلوماتي ؟ و ما هي سماته ؟



3.1. دوافع ارتكاب الجريمة الإلكترونية

2. ماهية التحريض

1.2. مفهوم التحريض

2.2. الفرق بين المحرض و الفاعل المعنوي

3.2. وسائل التحريض

3. مظاهر التحريض عبر وسائل التواصل الاجتماعي.

1. ماهية الجريمة الإلكترونية :

1.1. مفهوم الجريمة الإلكترونية : هي نشاط إجرامي يستعمل فيه التكنولوجيا الالكترونية (الحاسب الآلي و شبكة الأنترنت) بصفة مباشرة أو غير مباشرة ، للقيام بنشاط إجرامي معين.

(Mezaour nassima & others , 2021 : p .103)

عرفتها LeslieDBall بأنها فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية (قارة آمال ، 2001-2002 : ص 18)

كما عرفه Tidemann في كتابه fraude et autres délits d'affaires commis à l'aide d'ordinateurs عام 1984 هي كل فعل غير قانوني يرتكب بواسطة الحاسوب (قارة آمال ، 2001-2002 : ص 26)

و كذلك نجد تعريف parker الذي يتبنى مفهوما واسعا عن الجريمة الإلكترونية : كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق بالمجني عليه ، أو كسب يحققه الفاعل (نخلا المومني ، 2010 : ص 49) .

من خلال مما سبق ، نستنتج من التعاريف المقدمة أنها عرفت الجريمة المعلوماتية من خلال إساءة استخدام الحاسوب استخداما سلبيا مقصودا و لتحقيق أهداف شخصية ، و هذا هو موضوع الجريمة المعلوماتية و لكن العالم يتغير و حاليا أصبحت الجريمة الإلكترونية ترتكب بواسطة الحاسب و الهواتف الذكية و اللوائح الإلكترونية المبرمجة بأحدث البرامج التكنولوجية المزودة بشبكة الأنترنت .

** لذلك حسب ما لاحظته كباحثة أقدم تعريفا بسيطا حول الجريمة الإلكترونية ، هي استخدام الأجهزة الإلكترونية كالحواسيب الذكية و الهواتف الذكية و اللوائح الإلكترونية استخداما سلبيا مقصودا من قبل أشخاص يتمتعون بمعرفة تكنولوجية تمكنهم من إخفاء عناوينهم الإلكترونية مما يصعب من عملية القبض عليهم و هذه الفئة ما يطلق عليها CRACKRS و هي أعلى الجناة الإلكترونيين درجة يتسمون بالذكاء العالي في التعامل مع البرمجيات و صناعتها و اختراقها ، و أيضا فئة المؤثرين السلبيين الذين يتسمون بقوة التأثير و الإقناع على الآخرين للتغير بهم .

1. سمات المجرم الإلكتروني :

- يتمتع بالمهارة و الذكاء و المعرفة (نخلا المومني ، 2010 : ص 77) .

- تبرير سبب ارتكابه لجريمته

- هو إنسان اجتماعي

- الخوف من اكتشاف جريمته

- يتمتع بالسلطة اتجه النظام المعلوماتي (نخلا المومني ، 2010 : ص 80.79) .



3.1. دوافع ارتكاب الجريمة الإلكترونية :

- الرغبة في التعلم
- الربح المادي
- المتعة و التحدي و إثبات الذات
- الرغبة في الإنتقام (خلا المومني ، 2010 : ص ص 90.89) .

2. ماهية التحريض :

1.2. مفهومه :

هو دفع الغير على ارتكاب الجريمة . و يستوحى في ذلك أن يكون التحريض خالفا لفكرة الجريمة لدى الغير ، و التي لم تكن موجودة من قبل ، أو كان التحريض متمثلا في تشجيع الغير على تحقيق فكرة الجريمة و التي كانت موجودة لديه قبل التحريض (فهد العرفج ، 2006 : ص 35) .

أي أن التحريض يقوم على مبدأ الإيحاء ، أي كيف تتبلور فكرة الجريمة في مخيلته لغاية تنفيذها . ما يعني أن الفاعل أو المجرم به لديه مسبقا القابلية و الاستعداد النفسي للقيام بأفعال غير مشروعة يعاقب عليها القانون .

- الفاعل المعنوي :

هو الذي يكلف شخصا آخر غيره بارتكاب جريمة معينة نيابة عنه ، سواء كان هذا الشخص غير أهل للمسؤولية الجنائية أو بحسن النية ، و لكنه مجرد آلة في يد الفاعل المعنوي يسخره كيفما يشاء دون علم بمساهمة الجريمة و بالآثار الضارة المترتبة عليها كتاب التحري (فهد العرفج ، 2006 : ص 35) .

هنا نستنتج بأن المحرض يستخدم أو يستغل أشخاص آخرين للقيام بفعلته بطريقة غير مباشرة مستغلا فيهم سذاجتهم أو انعدام مسؤوليتهم الجنائية (القصر أو المختلين عقليا) أو قهورهم و اندفاعهم نحو بعض المواضيع كالدينية و السياسية و الاجتماعية ، حيث بدون علمهم و بطريقة غير مباشرة يقومون بفعل المساهمة الإجرامية .

2.2. الفرق بين المحرض و الفاعل المعنوي :

هناك بعض الفروق الأساسية بين المحرض و الفاعل المعنوي :

- توافر السيطرة على المشروع الإجرامي لدى الفاعل المعنوي ، فالجريمة ترتكب لحسابه ، لأن لديه ارتكاب الجريمة عن طريق استغلال شخص آخر غير مسؤول جنائيا أو لانعدام تميزه . أو لحسن نيته ، بينما المحرض لا تتوفر لديه هذه الإرادة . (فهد العرفج ، 2006 : ص 42) .

إرادة- الفاعل المعنوي يؤثر في إرادة غير معتبرة شرعا ، فيدفع صاحبها إلى ارتكاب الفعل ، بينما المحرض يؤثر في إرادة يعتد بها الشرع . لأنها شخص كامل الأهلية فيخلق لديه قرار ارتكاب الجريمة .

- الفاعل المعنوي لا يخلق القصد الجنائي في نفس و نية الفاعل . فالفاعل المباشر تنعدم لديه النية الإجرامية ، أما المحرض فهو يخلق هذا القصد الجنائي في نفس الفاعل (فهد العرفج ، 2006 : ص 43) .

3.2. وسائل التحريض :

1.3.2. التحريض بالهدية أو بالوعد :

تعتبر وسيلة تقديم الهدية من وسائل الترغيب التي من شأنها التأثير على نفسية المحرض ، بحيث يجعله أسير لما سُلم إليه و ما عُرض عليه من هدايا تتناسب مع جسامة الفعل موضوع التحريض



و تعرف الهدية : بأنها بذل قدر من المال المغربي أو غيره من الأشياء المستفزة لطمع الفاعل و تعتبر الهدية جمع الأشياء التي ينتفع بها الإنسان و يرغب بامتلاكها (فهد العرفج ، 2006 : ص 101) .

أستنتج من هنا صنف من أصناف الجناة و الضحايا على حد سواء و هو الطماع ، الذي يقوم بأي فعل مقابل أن يمتلك هاتف ذكي جديد أو أي جهاز إلكتروني متطور أو حتى سيارة على حسب جسامة الهدف المبتغى تحقيقه من قبل المحرض ، لذلك الجاني الإلكتروني — حسب هاته الدراسة هو مجرم غير مباشر فهو المدير و الفاعل المنفذ لجريمته بسلاسة و عن بعد . و حتى في بعض الأحيان ينتهك القانون أو يؤدي أشخاص آخريين بدون انتباهه .

2.3.2. التحريض بالتهديد : التهديد عبارة عن علاقة بين إرادتين تسيطر إحداها على الأخرى ، فيؤدي ذلك إلى أن يرتكب الفاعل الجريمة المخرض عليها خوفا مما سيحل به فيما إذا امتنع عن ارتكابها (فهد العرفج ، 2006 : ص 103) .

في هذه الحالة يكون الفاعل تحت طائلة تهديد المحرض إما لمعرفته بقيام الفاعل بفعل غير أخلاقي أو غير قانوني سابقا ، أو وضعه أمام خيارين يكون خيار ارتكاب الجريمة أخف الضررين بالنسبة للفاعل . هنا إذا أصبح الفعل الإجرامي محل متابعة قضائية القاضي وحده له السلطة التقديرية للفصل في ظروف التي جعلت من الفاعل يرتكب جريمته بتحت تهديد المخرض .

3.3.2. لمخادعة و الدسيعة :

يراد بها الغش و الخديعة و المكر ، أي كل الحيل الخبيثة و الوسائل المغرية و الأكاذيب و الأفعال المسيئة و المؤثرة على الفاعل (فهد العرفج ، 2006 : ص 105) .

مما نلاحظه في مجتمعنا الجزائري بما أننا جزء منه ، إقناع شخص بأن أحد محارمه (الوالدة أو الأخت أو الزوجة أو الإبن) يقمن بأفعال مخلة بالحياء ، مستغلين في ذلك التركيبة النفسية التي جُبل عليها الرجل الجزائري الحمية و العصبية أو بالدارجة ما يطلق عليه (النيف) ، فيرتكب أفعال عنيفة ضدهن (الجسدية على وجه الخصوص الضرب أو حتى القتل) مما يحقق لدى المخرض مبتغاه الذي كان يصبو إليه و هو التخلص من هذا الطرف الذي يزعجه أو يعيقه .

4.3.2. إساءة استخدام السلطة : الشخص الذي يستغل سلطة التأثير على إرادة من هو أدنى منه لدفعه إلى ارتكاب الجريمة ، شريطة التأكد من أن تأثير السلطة كان هو السبب في ارتكاب الجريمة (فهد العرفج ، 2006 : ص 107) .

5.3.2. إعلان النشاط التحريضي :

بعض التشريعات الجزائية جعلت من إعلان النشاط التحريضي سببا للتجريم على الفعل أو تشديد العقوبة المقررة له . و يقصد بهذه الوسيلة إيصال علم واقعة معينة أو تصرف معين إلى الناس إيصالا حقيقيا أو مفترضا (فهد العرفج ، 2006 : ص 108) .

إعلان النشاط التحريضي خطورته بالغة لما يلقاه من تجاوب أكبر بين أفراد المجتمع و من وسائل العلانية :

- الأعمال أو الإشارات أو الحركات إذا حصلت في طرق عام أو محفل عام أو مكان معرض لأنظار الجمهور .

- القول أو الصياح إذا حصل الجهر به أو ترديده في مكان عام

- الصحف و المطبوعات الأخرى و غيرها من وسائل الدعاية و النشر .

- الكتابة و الرسوم و الصور و الشارات و نحوها إذا عرفت في مكان أو وزعت أو بيعت إلى أكثر من شخص (فهد العرفج ،

2006 : ص ص 108.109) .

6.3.2. الإشاعة :

إطلاق شائعات على الآخرين بهدف تشويه سمعتهم و تنتشر بكثرة في المجال المهني (paula dugay,2004 : p.15)



و تهدف الإشاعة إلى التشهير بالآخرين لتدمير قواهم النفسية و الانفعالية للإقلال من شأنهم أو للحط من الجهود التي يعملون على تحقيقها وصولا لغاية رخيصة و هي إشاعة الفوضى و تحطيم الروح المعنوية (محمود دحان ، 1988 : ص 132)

3. مظاهر التحريض عبر وسائل التواصل الاجتماعي :

كوني باحثة ألحظ بالعين العلمية ما يدور في وسائل التواصل الاجتماعي و بالخصوص الفايسبوك من منشورات تحريضية ضد أشخاص أو ضد جماعات معينة كالإعتداء على الحريات العامة و الخاصة أو منشورات استفزازية ضد أنظمة سياسية أو إقتصادية ، هنا يجب أن نفرق بين الانتقاد و التعاليق البناءة التي يطمح أصحابها إلى تغيير أمر ما تغييرا إيجابيا يستفيد منه العامة ، و بين منشورات تحريضية يطمح أصحابها إلى نشر الفوضى أو التشكيك أو العنف المنظم .

و لكوني جزءا من المجتمع الرقمي الذي أصبح التفاعل من خلاله حتميا ، لاحظت و مازالت ألاحظ العديد من مظاهر التحريض و فئات عديدة من المحرضين . لذلك أقدم إليكم ما استنتجته بناء على ملاحظاتي الشخصية حول موضوع التحريض عبر الفايسبوك و مظاهره .

1.3. المحرضين من فئة المتطرفين :

و الذين يتميزون بالتطرف في طرح أفكارهم العقائدية أو السياسية أو الاجتماعية ، و الذين يحاولون فرض آرائهم بالقوة لمتبعي صفحاتهم أو مجموعاتهم الفايسبوكية . و يحاولون إقناعهم بأنهم على صواب و بأنهم يتفردون بالمعرفة و بالقدرة على تقييم الأمور . و يتسم متابعيهم بالمقابل بهشاشة تكوينهم النفسي و اندفاعيتهم المفرطة تجاه مثل هذه المواضيع الحساسة ، هذا ما استنتجته من قراءة بعض التعليقات ، و يتسمون أيضا بخلل عاطفي انفعالي خصوصا عندما يتعلق الأمر بالمسائل العقائدية المهمة . و يهدف المحرض من خلال ما ينشره إلى زعزعة الاستقرار الروحي و النفسي للمتابع لهذه المنشورات ، و هذا بتكرارها بصفة يومية ما يرسخ لديهم (المتابعين) فكرة التطرف و يتبنونها تدريجيا .

لاحظنا كما العديد من متصفح هذا التطبيق نشر فيديوهات أو مقاطع صوتية أو منشورات كتابية يحاولون فيها تشويه صورة الإسلام بإصدار فتاوى أو عرض أفكار متطرفة حول معنى الجهاد أو التشكيك في الذات الإلهية (جلي و علا) أو لإساءة الرسول الكريم (صلعم) أو لفرض آرائهم بالقوة لاستقطاب فئة معينة من المتابعين و هم فئة الانفعاليين ، حيث يهدف المحرض إلى تحسيسهم بالذنوب و التقصير تجاه دينهم بهذه الأساليب الملتوية .

و توجد أيضا فئة المتطرفين في آرائهم السياسية الذين يدفعون بمتبعيهم إلى نهج أسلوب العنف و الفوضى لتحقيق مآربهم الشخصية .

في الغالب هذه الفئة من المحرضين المتطرفين ، يقومون بعملهم بناء على خطة منظمة ذات أهداف مقصودة و محددة يتغنون من ورائها الدفع بالمغرب بهم إلى القيام بأعمالهم الإجرامية بدلا عنهم أو تحويلهم للخارج للمتاجرة بهم أو استخدامهم في أعمال عدوانية

2.3. فئة المحرضين بسبب الرياضة :

هذا ما يحدث يوميا في الصفحات الفايسبوكية المختصة في الرياضة من تلامس و تراشق للالتقائات و المعايير بهدف إضعاف الروح المعنوية للفريق الخصم و لمشجعيهم ، لزعزعة ثقتهم و الدفع بهم لممارسة العنف و الاعتداء على الأملاك و الأشخاص بغية لعاقبتهم من قبل الجهات المعنية .

3.3. فئة المحرضين بالنعدي على الحياة الخاصة للأفراد :



قد يستهين الناس بنشر تفاصيل حياتهم على شبكة الأنترنت و منها الفايسبوك بنتائج ذلك على حياتهم الواقعية ، إذ تجد من النسوة من ينشرن قصص نزاعتهن مع أزواجهن بحثا عن حلول لمعالجة المشكلة ، فإذا به يتلقين بالمقابل تعليقات محزنة إياهن بالطلاق و الخلع أو انتهاج أساليب العنف النفسي و اللفظي و الرمزي لمعالجة المشكلة ما قد يزيد من حدة العنف المنزلي المتبادل بين الطرفين .

4.3. فئة المخرضين على الإدمان :

لاحظت في العديد من الصفحات الفايسبوكية ، نشر أشخاص لمواد مضرّة بالصحة أو للمسكرات و المهلوسات بهدف بيعها و استقطاب المزيد من المستهلكين لهذه المواد ، أو نشر طرق تناولها أو مزجها مع مواد أخرى . ما قد يجعل المتتبعين يكتسبون طرق شرائها و كيفية تناولها ، و يقع على إثرها تحت عملية الإدمان التدريجي لهذه المواد ، الأمر الذي يفتح الطريق أمام أشخاص آخرين لتقليدهم خصوصا الأطفال و القصر (هنا يجب ذكر نقطة مهمة و هي ترخيص الوالدين لأولادهم القصر بفتح حسابات شخصية على الفايسبوك بحجة ضرورة مواكبتهم لروح العصر الرقمي الحديث متناسين أو غافلين بأن القصر يسهل التلاعب بهم و السيطرة عليهم ، بسبب محدودية تجربتهم الحياتية و انعدام تمييزهم ما يجعلهم الفئة الأكثر ترشيحا لاستهلاك هاته المواد المضرّة بالصحة النفسية و الجسدية ، حيث يبدو أن بالتدرج في سلم الإدمان خطوة بخطوة من تناول مواد بسيطة (كغبرة مشروب موجه للاستهلاك و مادة الغراء الاصطناعي) إلى المخدرات ، حيث تقوم فئة من الأشخاص بنشر صور و فيديوهات لتوعية الشباب و القصر بضرورة تفادي تناول هاته المواد ، و لكن هذه المنشورات توحى لآخرين بفكرة تناولها انطلاقا من مبدأ التجربة . لذلك يجب التبليغ على هذا النوع من المنشورات التي تهدف إلى تحطيم قيم الشباب و رميهم لمستمتع الأزمان النفسية و الإدمان .

5.3. فئة المخرضين على العنصرية و الجهوية :

يتميز المنتمين لهذه الفئة ، بنشر فيديوهات أو منشورات مكتوبة للتحريض على كراهية الآخر بسبب هويته الثقافية أو العقائدية أو المنطقة التي ينحدر منها ، أو السخرية من طريقة كلام منطقة معينة أو لباسهم أو مأكولاتهم . هذا النوع من التحريض يدخل ضمن ما يسمى بجرائم الكراهية . أي الإعتداء على حرية الآخر . و يهدفون من وراء ذلك لتوسيع رقعة الكراهية بين أبناء البلد الواحد لتفرقتهم و لزعة وحدتهم الوطنية .

6.3. التحريض بالإيحاء :

بما أن هدف التحريض هو خلق فكرة الجريمة لدى الفاعل ، فيتمظهر التحريض في هذه الفئة من خلال نشر فيديوهات عفوية هدفها تعليمي أو توعوي لكن بالنسبة لفئة من المتتبعين الذين يمتلكون النزعة الإجرامية ، فهو يوحي إليهم بفكرة الجريمة و بأساليبها و يسهل عليهم ارتكابها .

على سبيل المثال : شاهدنا الكثير من الفيديوهات حول أشخاص نسوا مفاتيح سياراتهم بداخلها . إذن كيف يتعاملون مع الأمر ؟ فيقوم الناشر بتوجيه نصائح مفصلة حول كيفية التعامل مع الأمر ذكرنا نوع السيارة و مميزاتها و هذا ما يوحي للمتتبع بفكرة الجريمة فتسهل عليه عملية سرقة السيارات دون إثارة الانتباه .

و بعض الصفحات ينشرون فيديوهات حول ابتكار أساليب الغش المثالية في الامتحانات حتى لا يتم كشفهم ، و لكي ينال الطلاب علامات عالية دون بذل أي جهد .

** بالنسبة للمخرض يكفي فقط غرس فكرة الجريمة و العنف أو التقليد لدى المتتبع . يتشابه المجرم المعلوماتي بما أسماه ساذرلاند جرائم الباقات البيضاء ، فهو يتسم بالمقدرة الذهنية و النفسية على التلاعب بعقل الفاعل و التأثير عليه تأثيرا بالغاً يحول به آلية



تفكيره ، و أيضا الفاعل أي القائم بالجريمة و بالسلوك العنيف و العدواني لديه ما أسماه دي تيليو بالاستعداد الإجرامي للقيام بالأفعال السالفة الذكر ، فتنفيذه لمثل هذه الأعمال يعني لديه نزعة إجرامية كانت تنتظر التحفيز للبروز .
حيث وقع هنا ما يسمى بتبادل الأدوار حيث الخرض مخفي و بعيد عن الأنظار و في غالب الأحيان غير معروفة هويته الأصلية فهو يختبئ وراء هوية إفتراضية تقمصها لهدف معين و الفاعل معروفة هويته و موقعه* .
*بتصرف الباحثة . بناء على ملاحظاتي الشخصية .

خاتمة :

** و في الأخير أختتم بما ذكرته روي جونسون خبيرة بمركز المعلومات الوطني لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة (قارة آمال ، 2001-2002 : ص 8) .

حيث أشاطرها الرأي ، الجريمة و الأساليب العنيفة أصبحت أكثر شراسة و متاحة و غير متحكم فيها ، حيث يمكن للجميع تعلم السلوكات السلبية و حتى العنيفة و اكتسابها من خلال ما يتصفحونه عبر الفايسبوك و بالتالي يقلدون ما اكتسبونه إما بدافع التجربة أو الفضول أو الرغبة في القيام بتلك السلوكات . و لا يمكن الجزم بأن مواقع التواصل الاجتماعي سيئة بقدر ما نلاحظ بأن كيفية استخدامها هي الفيصل في تحديد مساوئها وإيجابياتها.

قائمة المراجع :

- قارة آمال ، الجريمة المعلوماتية .(رسالة ماجستير تخصص القانون الجنائي و العلوم الجنائية) ، جامعة الجزائر ، 2001-2002 .
المومني عبد القادر نخلا ، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع ، الأردن ، ط2 ، 2010 .
دحان ولد أحمد محمود ، علاقة الإعلام بالمسائل الأمنية في المجتمع العربي ، المركز العربي للدراسات الأمنية و التدريب ، الرياض ، 1988 .
العرفج بن مبارك فهد ، التحريض على الجريمة في الفقه الإسلامي و النظام السعودي ، دراسة تأصيلية تطبيقية . (رسالة ماجستير تخصص السياسة الجنائية) ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2006 .
Mezaour Nassima & others ; Electronic crime ; Ijtihad journal on legal and economic studies ; volume 10 ; number 01 ; 2021 ; p 32-50 .
Dugay paula ; la violence au travail envers les enseignantes et les enseignants ; fédération des syndicats de l'enseignement ; canada ; 2004 .



المخدرات الرقمية: ادمان حديث عبر الفضاء الرقمي

Digital Drugs: a Modern Addiction In the Digital Space

د. رتيبي أسماء

ط. د. بخوش شيماء

جامعة بجي فارس المدينة

مقدمة:

إن التطور الذي شهده مجال الانترنت والتكنولوجيا يعد من أعظم الانجازات البشرية التي سهلت الحياة واستفاد منها البشر على المستوى الفردي والمجتمعي والدولي، لولا الجانب السلبي منها الذي استغله البشر نفسه لإيذاء نفسه وغيره، عن طريق ادخال الانترنت والتكنولوجيا بمختلف مزاياهم وخدماتهم إلى عالم الاجرام والانحراف، لتظهر الجرائم الالكترونية كواحدة من مفرزات الاستغلال السيئ للشبكة العنكبوتية، والتي تتنوع وتعدد هي الأخرى ليكون آخرها نوع حديث من الادمان عبر الفضاء الرقمي ألا وهي المخدرات الرقمية.

• الجانب المنهجي:

1. الاشكالية:

تعتبر المخدرات من أكثر الآفات الاجتماعية التي يعاني منها الشباب في المجتمعات المتقدمة والنامية على حد سواء، نظرا لتداعياتها السلبية على صحتهم أولا ثم على مستقبلهم واستقرار مجتمعاتهم، ولا تزال الدول والجهات الأمنية تحارب هذه الآفة وتتصدى لها بكل الطرق والوسائل الممكنة، ليظهر على الساحة نوع جديد من المخدرات يرتبط أساسا بالتكنولوجيا وشبكة الانترنت يطلق عليها المخدرات الرقمية أو الالكترونية.

والمخدرات الرقمية تعتبر مصطلحا تجاريا استخدمه مروجوه لترغيب واستقطاب الشباب لاستخدامها (أحمد و فوزي، 2020، صفحة 66)، وهي تمثل الشكل الأحدث للتعاطي والإدمان على المخدرات المنتشر بين أوساط الشباب، وهو ناجم أساسا على سوء استخدام الانترنت والتطبيقات الالكترونية الحديثة ويحكي في خطورته الإدمان على المخدرات التقليدية، حيث "لم يعد استهلاك المخدرات مقتصرًا على الوسائل التقليدية للتعاطي كالحقن، الشم، المضغ، والتدخين، وإنما تطورت أساليب استخدامها لتتحول إلى إلكترونية ورقمية، متمثلة في ملفات صوتية توصل لها بعض المختصين في الموسيقى وعملوا على نشرها، وهم في الغالب مدمنون مخدرات كونهم يعرفون تأثير كل مخدر تخليقي على المخ، فحاولوا الوصول لنتائج تقريبية أو مشابهة للمخدرات الطبيعية" (أحمد و فوزي، 2020، صفحة 66)، ومع التطور الهائل في مجال التكنولوجيا والانترنت كان الترويج لهذه المخدرات سهلا نوعا ما خاصة في البلدان الغربية، لتبدأ بعد ذلك في الانتشار تدريجيا وتصل للبلدان العربية على الرغم من كونها لا تزال غير معروفة تماما لدى العامة، بالإضافة إلى أن الدراسات التي اهتمت بالبحث والتقصي عن هذا النوع من المخدرات قليلة ومحدودة جدا.

ومن هنا جاءت هذه الدراسة للتعرف على المخدرات الرقمية وتداعياتها على الشباب، وعليه نطلق في دراستنا مجموعة من الأسئلة

التالية:

- ماهي المخدرات الرقمية؟



- ما مصدرها وما هي جذورها التاريخية؟
- ماهي آلية عمل المخدرات الرقمية وكيف تؤثر على الدماغ؟
- فيما تتمثل طقوس تعاطي المخدرات الرقمية؟ وما هي أهم أنواعها؟
- ما الأسباب والعوامل التي تؤدي بالفرد لتعاطي المخدرات الرقمية والإدمان عليها؟
- ماهي الآثار والأضرار التي تسببها المخدرات الرقمية؟

2. أهمية الدراسة:

1.2. الأهمية العملية: تنطلق أهمية هذه الدراسة من أهمية الموضوع الذي تدرسه وحداثته، ألا وهو المخدرات الرقمية التي استقطبت الاهتمام العالمي مؤخرا نظرا لانتشارها الواسع بين أوساط الشباب والمراهقين، كما أنها تساهم في تسليط الضوء على هذا النوع الحديث من المخدرات ولفت الانتباه إليه ولتداعياته وأضراره على الشباب، بالإضافة لكونها تعمل على توعية الأولياء أولا ثم أبناءهم للوقاية من المخدرات الرقمية وتجنبها، أيضا لها دور في توجيه الجهات الأمنية ومؤسسات الضبط الاجتماعي للتصدي لهذا النوع من المخدرات، وتوجيه صناع القرار لسن قوانين لردع وحماية جميع شرائح المجتمع من تعاطيها والإدمان عليها.

2.2. الأهمية العلمية: تعتبر هذه الدراسة إضافة للدراسات المحدودة في هذا الموضوع لتثري بذلك المكتبة العربية في مجال الدراسات الاجتماعية وأيضا في مجال دراسات الانحراف والجريمة بأحد أهم المواضيع التي يدرسها.

3. أهداف الدراسة: تهدف هذه الدراسة إلى مايلي:

- التعريف بالمخدرات الرقمية والإدمان عليها.
- تسليط الضوء على جذورها التاريخية ومصادرها.
- التعرف على طقوس تعاطيها وأنواعها وأسباب تعاطيها والإدمان عليها.
- لفت الانتباه لآثارها السلبية وأضرارها على متعاطيها.

4. مفاهيم الدراسة:

1.4. مفهوم المخدرات الرقمية:

تتمثل المخدرات في مجموعة من المواد التي تذهب العقل وتغيب وعي الفرد، كما أنها تسبب له الإدمان و تتلف جهازه العصبي، وهي غالبا عبارة عن مواد نباتية أو مصنعة (أدوية) تحتوي على عناصر تسبب النعاس والنوم أو مسكنة للألام، هذا ماهو متعارف عليه منذ آلاف السنين، لكن حاليا في عصر الرقمنة والتكنولوجيا ظهر للساحة نوع حديث من المخدرات يطلق عليها المخدرات الرقمية، والتي يمكن تعريفها كما يلي:

المخدرات الرقمية أو ما يعرف عالميا **Digital Drugs** عبارة عن مقاطع نغمات موسيقية يتم سماعها عبر سماعات الأذنين عالية الجودة، وذلك ببث ترددات معينة في الأذن اليمنى، وترددات منخفضة عنها بفارق محسوب في الأذن اليسرى أو يختلف فرق الترددات بين الأذنين بحسب نوع المخدرات المرغوب فيها، ويعمل تأثيرها من خلال اختلاف الترددات بين النغمات في الأذن اليمنى و اليسرى، والذي يستحث الدماغ على محاولة التوفيق بين تغير الإشارتين المترددتين، مما يظهر الموجة الثالثة التي تسمع وتكون ذات التأثير المشابه لتعاطي المخدرات، وهذه العملية تجعل الدماغ في حالة غير مستقرة كهرومغناطيسيا، ويحفز الخلايا العصبية لإفراز هرمونات متفاوتة بحسب نوع المخدر منها على سبيل المثال (الدوبامين) الهرمون المعني باعتدال المزاج، أو كما يسمى هرمون السعادة (صونيا و خالد، 2020، صفحة 43).



كما تعرف المخدرات الرقمية بشكل أدق أيضا "القرع على الأذنين Binaural Beats"، هي عبارة عن مجموعة من الأصوات أو النغمات التي يعتقد أنها قادرة على إحداث تغييرات دماغية، تعمل على تغييب الوعي أو تغييره على نحو مماثل لما تحدثه عملية تعاطي المخدرات الواقعية، مثال "الأفيون والحشيش والماريجوانا.. إلخ" (فوزي و علي، 2020، صفحة 163).

أيضا هي عبارة عن ملفات صوتية أحيانا تترافق مع مواد بصرية وأشكال وألوان تتحرك وتتغير وفق معدل مدروس، وتتم هندستها لتخدع دماغ الانسان، عن طريق بث موجات صوتية مختلفة التردد بشكل بسيط لكل أذن، ولأن هذه الأمواج الصوتية غير مألوفة يعمل الدماغ على توحيد الترددات من الأذنين للوصول إلى مستوى واحد بالتالي يصبح غير مستقر، وحسب نوع الاختلاف في كهربائية الدماغ يتم الوصول لإحساس معين يحاكي إحساس احد أنواع المخدرات أو المشاعر التي تود الوصول إليها كنشوة (نسبية و علي، 2020، صفحة 35).

إجرائيا: مجموعة من الملفات الصوتية مختلفة التردد لكل أذن، صممت للتأثير على دماغ الانسان والعمل على تغييب وعيه وتغييره على نحو مماثل لما تحدثه عملية تعاطي المخدرات التقليدية.

2.4. مفهوم الادمان:

هو حالة من السلوك الفعلي الذي يقوم به الفرد ويكرره وينتج عن تكراره رغبة شديدة في استمرار هذا التكرار وعدم انقطاعه، ويشمل ذلك السلوك تعاطي المواد المسكرة أو المخدرة وغيرها، التي توهم الفرد بتحقيق نوع من الراحة التي تسيطر على من يتعاطاها تدريجيا، ويعد الادمان من الأمراض والحالات المعقدة التي تشمل تغيرات فيزيولوجية ونفسية في الوقت ذاته (صبيحة و الزهرة، 2020، صفحة 117).

كما يعرفه "جواد فطائر" بأنه رغبة مرضية (ولع) من الانسان نحو موضوع معين قد يكون ماديا كالمواد المخدرة والخمر والسجائر...، وقد يكون حدثا كالقمار أو الجنس أو الحب للعمل أو التلفاز أو الانترنت (صبيحة و الزهرة، 2020، صفحة 117).

إجرائيا: هو حالة ناتجة عن تكرار فعل معين بصفة دائمة مما يولد الرغبة الشديدة في الاستمرار في ذلك الفعل وعدم انقطاعه، مثل تعاطي المواد المخدرة أو الانترنت أو التلفاز...

3.4. مفهوم الفضاء الرقمي:

الفضاء الرقمي أو العامل الافتراضي أو الفضاء السيبراني أو العامل الإلكتروني كلها مصطلحات نستخدمها بمعنى واحد، وهو الاتصال المستمر بين سكان الأرض على مستوى شبكة الإنترنت، مما يقتضي التزامية. كما يشير لكل ما يدور في فلك الشبكة العنكبوتية، بما في ذلك متصفح الويب الذي من خلاله يمكن الدخول إلى المواقع، أيضا المنصات الإلكترونية المختلفة، والشبكات الاجتماعية، مثل Facebook و Whats App و Twitter و Instagram، أيضا الصحافة والإعلام المكتوب والذي يكون عبر المدونات المختلفة (شيماء، 2021).

أو هو مصطلح يشير إلى عالم الكمبيوتر الافتراضي وهو العالم الذي تتلاقى فيه جميع شبكات الانترنت على مستوى العالم، وهو الذي يقوم بربط تلك الأجهزة مع بعضها البعض عن طريق خلق نوع من الاتصال بينها، وهكذا يتمكن البشر من التفاعل مع بعضهم من مختلف بقاع العالم (إيمان).

إجرائيا: يقصد به كل ما يتعلق بالأجهزة الإلكترونية وعالم الانترنت، الذي يقوم بربط الأفراد بعضها ببعض من مختلف بقاع العالم في فضاء افتراضي، يمكنهم من التواصل والتفاعل فيما بينهم.



الجانب النظري:

1. الجذور التاريخية للمخدرات الرقمية:

تعتبر ظاهرة المخدرات الرقمية (أو بشكل أدق تأثر الانسان بالموجات الصوتية) معروفة نوعا ما منذ القدم، لكنها كانت تستخدم كعلاج لبعض الأمراض، وبدايتها كانت عندما كان الانسان يستمع إلى دقات معينة ويتأثر بها ويتفاعل معها وتنقله من حالة إدراكية إلى أخرى، مثل رقص المطر عند الأفارقة، وعند المصريين القدامى أنشأ معهد طب للعلاج بالذبذبات الصوتية وذلك من خلال التعرض لأنواع معينة من الموسيقى التي تعمل على تحسين المزاج وتؤثر تأثيرا مباشرا على الجهاز العصبي، أما في المجتمعات اليونانية فقد تم الاعتماد على الموسيقى كعلاج صحي مبني على التفاعل مع الموسيقى من أجل تحقيق أهداف معينة في صحة الشخص، ولكن يجب أن يكون مؤهلا لذلك، كما تم الاعتماد عليها لطرد الأرواح الشريرة من جسم الانسان (صبيحة و الزهرة، 2020، صفحة 120).

ثم بعد ذلك ظهرت تقنية سميت قديما بـ "النقر بالأذنين" اكتشفها الفيزيائي الألماني "هينرش دوف" عام 1839، وقد اكتشف هذا العالم أنه إذا سلطت ترددتين مختلفتين قليلا عن بعضهما لكل أذن، فإن المستمع سيدرك صوت نبض سريع، ويعتقد أن بداية ظهورها كان في مدينة "أوكلاهوما" بالولايات المتحدة الأمريكية، وسميت هذه الظاهرة بـ binaural beat أي "النقر الوهمي"، وقد استخدمت هذه التقنية أيضا سنة 1970 لعلاج بعض الحالات النفسية، لعدد من المصابين بالاكتئاب والذين يرفضون العلاج الطبي الاستشفائي، ولهذا تم العلاج عن طريق ترددات كهرومغناطيسية لتعديل مزاج المصاب (نسبية و علي، 2020، صفحة 36). أيضا تعرف بعض الطوائف في البلاد العربية وغيرها من بلاد الهند ودول جنوب شرق آسيا موسيقى طربية أو ما تسمى بالشطحات على وقع نغمات متقابلة، ويبدأ الشخص في السماع والرقص حتى يصل به الوضع إلى الارتعاش ثم في الأخير الإغماء (سامية و ابتسام، 2018، صفحة 5).

أما إذا نظرنا إلى المخدرات الرقمية كواحدة من الظواهر السيبرانية السلبية والحديثة، فهي تعود إلى بداية التسعينات وتحديدًا سنة 1994، حين اكتشفت الباحثة والنفسانية الأمريكية "كمبرلي يونغ" ما يعرف بالإدمان على الفضاء السيبراني. وهناك مواقع متخصصة تقوم ببيع نغمات على مواقع الانترنت مثل (I-Doser) وموقع (digipill.com)، ولا توجد رقابة رسمية أو حظر لمثل هذه النغمات في الوقت الحالي، ويتم ترويجها عبر مواقع التواصل الاجتماعي أيضا مقابل القليل من الدولارات، إلى جانب إمكانية الحصول عليها عبر موقع يوتيوب بشكل مجاني. ثم بدأ انتشار هذا النوع من المخدرات الرقمية في شكلها الحالي عام 2010، عندما بثت بعض مواقع الانترنت موسيقى خاصة يتم الاستماع إليها عبر سماعات الرأس وفي غرفة مغلقة مع إغماض العينين والاسترخاء، وتعمل هذه الموسيقى على التأثير على دماغ المستمع تماما كما تؤثر المخدرات التقليدية على الدماغ (أحمد و فوزي، 2020، الصفحات 69 - 70).

في الوطن العربي ظهر هذا النوع من المخدرات على الساحة عام 2012، وتحديدًا في السعودية التي سجلت أول حالة وفاة جراء تعاطي المخدرات الرقمية، وأيضًا في لبنان التي دعت لحجب المواقع الالكترونية التي تقوم بتسويق وبيع هذه الموسيقى، كما تشير الاحصاءات إلى وجود 20 حالة إدمان في تركيا فضلا عن عدد آخر في كل من الأردن ومصر (أحمد و فوزي، 2020، صفحة 70)، أما في بلدنا الجزائر فقد كشف مسؤول فرقة حماية الأحداث بالقيادة الجهوية الأولى للدرك الوطني بالبلدية عن اكتشاف أولى حالات الإدمان على المخدرات الرقمية في ولاية البليدة، حيث تم تسجيل قرابة 15 حالة تم اكتشافها عندما توجه مجموعة من الشباب والقصر إلى فرقة حماية الأحداث قصد تلقي العلاج (أمين، 2015).



2. مصدر ومواقع توزيع المخدرات الرقمية:

وجدت المخدرات الرقمية راجعا هائلا بين الشباب ومستخدمي الانترنت، وقد تعددت المواقع الالكترونية التي تروج لها وتسهل طريقة الحصول عليها، بل تقوم أيضا ببيع كل مستلزماتها من الأقراص المضغوطة إلى الميكروفونات الخاصة وأجهزة وبرامج وحتى الستائر المناسبة والمخدرات والكراسي الملائمة للظروف المطلوبة للمخدرات الرقمية ولحصول مفعولها بالكامل، ومن أشهر هذه المواقع موقع BinauralBeats.com موقع Brainblogger.com وموقع I-Doser.com (سامية و ابتسام، 2018، صفحة 7) "الذي يقوم بعملية إغراء مكشوفة إذ يمنح مستخدميه تجربة مجانية في البداية ويشجع المروجين لبيع ملفاته عبر الانترنت لقاء عمولة تزيد على 20 ويتراوح سعر الملف الواحد بين 3 و 9 دولارات، بينما يكون الملف الأول للمستخدم مجانيا" (تركي، د.س، صفحة 10). فهذه المواقع إذا تعتمد سياسة دعائية قوية لجلب الزبائن من مختلف الأعمار، وتقدم دعاية احترافية ومؤثرة جدا عند التعرض المتكرر لها وبخاصة لدى الشباب والناشئة، زيادة على هذا فإن هذه المواقع توفر "ضمان للبضاعة المباعة" حيث تشير تلك المواقع إلى "النتائج المضمونة"، بل تقدم أكثر من هذا حيث تعد بأن ترجع قيمة البضاعة أو المنتج المباع في حالة عدم رضا الزبون على نتائج (مفعول) البضاعة أو المنتج، كما تقوم هذه المواقع بتوزيع وإيصال بضاعتها لجميع أنحاء العالم، وبسعر زهيد حوالي ثلاثون دولار فقط، وأيضا تقدم أوصافا لكل منتجاتها على اختلافها وطريقة استعمالها، وذلك من خلال الشبكة العنكبوتية أو وسائط التواصل الاجتماعي الأخرى (سامية و ابتسام، 2018، صفحة 7).

3. آلية عمل المخدرات الرقمية:

يدخل دماغ الإنسان عند سماعه هذه الترددات في حالة من عدم الاستقرار نظرا لبذله مجهودا كبيرا سعيا للمساواة بين الترددات اللذين يدخلان عبر الأذن اليمنى واليسرى ليكونا في مستوى واحد، فيكون الدماغ تحت تأثير الإشارات الكهربائية التي يتم إرسالها، فيصل الدماغ إلى حالة من النشوة نتيجة إفراز الدماغ لمواد منشطة للمزاج إلا أنه يصل إلى حد الإفراط فيدخل الإنسان بحالة هستيرية (عبير، 2019، صفحة 273).

وهكذا يختار المروجون لمثل هذه المخدرات نوع العقار الذي تريده، حيث أن كل نوع من المخدرات الرقمية يمكن أن يستهدف نمطا معيناً من النشاط الدماغي، ومن خلال دراسة حالة الدماغ وطبيعة الإشارات الكهربائية التي تصدر عن الدماغ بعد تعاطي نوع معين من المخدرات يمكن تحديد حالة النشوة المرغوبة (صبيحة و الزهرة، 2020، صفحة 121).

4. أنواع المخدرات الرقمية:

توجد عدة أنواع من المخدرات الرقمية تنقسم حسب تأثيرها على النشاط الدماغي، وحسب الحالة المرغوب الوصول إليها لدى متعاطي هذه المخدرات والتي قد تكون: حالة استرخاء، حالة فرحة ونشوة، حالة التوهم بالقدرة على الإبداع، حالة التحليق في عالم الخيال... (سامية و ابتسام، 2018، صفحة 08)، وغيرها، فنجد: (علي و جغدم، 2020، صفحة 54)

1.4. الأسطورة البلورية: وهي نوع من النعمات الهادئة التي تبعث على الاسترخاء والهلوسة والهدوء وتبعث في النفس من

النشوة من خلال توارد الذكريات الأليمة، كما أن نوع النعمة من النوع الدافعي الهادئ الذي يبعث أحلام اليقظة إلى الفرد، ويبعث في النفس البهجة.

2.4. الموجة العالية: وهي نوع من النعمات الصاخبة التي تتسبب في حدوث تحفيز لجميع خلايا الجسم والعقل وتعمل على تحفيز العقل بالصورة التي تزيد من نشاط الفرد بصورة مذهلة.



وهناك بعض من أنواع المخدرات الرقمية تقدمت على سابقتها في الاستخدام ونجد من بينها ما يستخدم لإنقاص الوزن ومسميات أخرى كأبواب الجحيم والمتعة في السماء (لمحاكاة المقدس)، الملاك الناعم (لمحاكاة الصعود للأعلى)، الدموي (لمحاكاة الخيال والأساطير)... وغيرها (تركي، د.س، صفحة 12).

5. شروط وطقوس تعاطي المخدرات الرقمية:

حتى يتحقق الهدف من تعاطي المخدرات الرقمية ويصل الفرد للحالة التي يرغب فيها، هناك مجموعة من الشروط والطقوس التي يجب اتباعها والتي اختلفت وتنوعت حسب الكتاب الذين تناولوا هذه الظاهرة، فمنهم من ذهب إلى أنه يكفي وضع ترددات موسيقية مختلفة في الأذنين مع سماعات، ومنهم من قال بأن أنواع معينة من الموسيقى تصلح للوصول إلى حالات الإدمان، ومنهم من حدد التردد الأعلى للموسيقى المستخدمة، فلا يجوز أن يزيد عن 1500 Hz لأن الدماغ بعدها سيصل إلى حالة الدمار، إلا أن الطقوس التي تكرر ذكرها عند الغالبية ممن كتبوا أو جربوا هذه المخدرات يمكن تلخيصها فيما يلي (سامية و ابتسام، 2018، صفحة 9):

- أن يخلق المستمع بيئة مثالية للاسترخاء، كأن يتم الجلوس في مكان هادئ خافت الإضاءة.
- أن يرتدي المستمع ملابس فضفاضة.
- أن يقوم المستمع بوضع عصبة على عينيه، وقد يشرب الماء.
- أن يضع المستمع سماعات عالية الجودة في الأذنين وفقا لترددات معينة حسب نوع المصدر المنشود الذي يجعل الدماغ في حالة غير مستقرة.

- أن يحرص المستمع على عدم تعرض جلسة الاستماع إلى أي مقاطعة خارجية.

6. عوامل وأسباب تعاطي المخدرات الرقمية:

هناك مجموعة من العوامل والأسباب التي تدفع بالمراهق أو الشاب لتعاطي المخدرات الرقمية والإدمان عليها، بعضها فردية تتعلق بشخصية الفرد المتعاطي، وأخرى خارجية تتعلق بالمحيط الخارجي للمتعاطي، نلخصها فيما يلي:

1.6. العوامل الفردية: (صبيحة و الزهرة، 2020، الصفحات 124 - 125)

- رفقاء السوء الذين يتأثر الفرد بهم وتوجهاتهم ومعتقداتهم فيقلدهم ويندمج معهم، خاصة في مرحلة المراهقة.
- ضعف الشخصية التي تجعل الشخص مسلوب الإرادة غير قادر على إدارة حياته بشكل مستقل عن الآخرين، فيكون هدفا سهلا للمروجين.
- الفضول وحب التجربة والاندفاع والتسرع دون اكتراث للنتائج المحتملة، خاصة في مرحلة المراهقة.
- الأوهام الخاطئة خاصة في ما يتعلق بقدرة المخدرات على زيادة القدرة الجنسية والجسدية.
- ضعف الوازع الديني والثقافة الدينية لدى معظم الشباب.
- الهموم والمشاكل الاجتماعية والعاطفية التي تواجه الشباب فيلجأ للمخدرات للهروب من واقعه.
- توفر الفراغ مع عدم توفر الأماكن الصالحة التي تمتص طاقة الشباب كالنوادي والمتنزهات. مما يؤدي لانعزالهم مع الانترنت وتوجههم نحو هذا النوع من الموسيقى.

2.6. العوامل الخارجية: (علي و جعدم، 2020، الصفحات 57 - 59)

- سهولة الحصول على المخدرات الرقمية وتعاطيها باستخدام الانترنت التي أصبحت متوفرة في كل الأماكن وكل الأوقات، فنظام الانترنت أصبح نظام حياة في متناول الجميع لا يمكن منعه ولا حجب.



- غياب الرقابة الأسرية وانشغال الآباء والإهمال من طرف الوالدين.
- نقص الوعي المفاهيمي للأسرة حول واقع وخطورة المخدرات الرقمية.
- قلة التكلفة المادية للحصول على المخدرات الرقمية، حيث أن أغلب المواقع المروجة توفر الجرعة الأولى بصورة مجانية، ثم باقي الجرعات بثمان زهيد يتراوح ما بين 3 و 9 دولارات، وهناك بعض المواقع المجانية بصفة دائمة.
- قلة الدور الذي تلعبه وسائل الإعلام في التوعية بمخاطر هذا النوع من المخدرات والتعريف به، بالإضافة للدور الذي تلعبه في الترويج لتعاطي المخدرات من خلال ما تعرضه من أفلام ومسلسلات عن أبطال وقادة يظهر على أنهم مدمني مخدرات.
- عدم وجود قوانين صارمة ضد هذا النوع من المخدرات.

7. أضرار المخدرات الرقمية:

لا تختلف آثار المخدرات الرقمية عن آثار المخدرات التقليدية، فكلتاها لهما أضرار جسيمة على صحة الفرد، سواء على دماغه وجهازه العصبي وعلى حالته النفسية والجسدية وأيضا من الناحية الاجتماعية، حيث نجد أن المخدرات الرقمية: (صبيحة و الزهرة، 2020، صفحة 122)

- تسبب الشعور برجفة وتشنجات بالجسم.
- تعمل على إبعاد المتعاطي وعزله عن الحياة الاجتماعية.
- تساهم في انخفاض الطاقة الانتاجية للفرد بسبب انعزاله عن الواقع الخارجي.
- الإصابة بالإدمان النفسي على مثل هذه الأصوات مما يدفع الفرد لاستنزاف نقوده للحصول عليها.
- إهمال الواجبات الاجتماعية والأسرية والوظيفية.
- التوتر والقلق الشديدين في حالة وجود أي عائق في الاتصال بالوسائل التكنولوجية التي يستعملها المدمن، قد تصل لدرجة الاكتئاب إذا طالت فترة الابتعاد عن الاتصال بهذه الوسائل.
- ضعف الانتباه والتركيز ونقص القدرة على التمييز بسبب التعرض المستمر للإشعاعات المنبعثة من الجهاز والتي بدورها تؤثر على القشرة المخية للفرد.
- ضياع القيم والمبادئ حيث يسعى المدمن للحصول على الجرعة مهما كانت الوسائل والطرق، مما يجعلهم يقعون في الانحراف ويرتكبون المخالفات والجرائم.
- تخريب الجهاز السمعي حيث أن الاستماع إلى الترددات المتباينة غير الصحية والأصوات الصاخبة يؤثر بالسلب على الأذنين والسمع ويسبب الارتخاف وعدم التوازن (أحمد و فوزي، 2020، صفحة 75).

8. طرق الوقاية من المخدرات الرقمية:

لا تختلف طرق الوقاية من المخدرات الرقمية عن غيرها من أنواع المخدرات الأخرى من حيث التوعية بمخاطرها الصحية الكبيرة وخطورها على الفرد والمجتمع كما يلزم على الأسرة القيام بدورها المنوط بها في الرقابة الذاتية على الأبناء خصوصا في مرحلة المراهقة، حيث ينصح الأولياء من أجل وقاية أبنائهم من الوقوع ضحية المواقع المروجة للمخدرات الرقمية بمائلي (أحمد و فوزي، 2020، الصفحات 75-76):



- يجب تشجيع الأبناء على الاندماج في أنشطة اجتماعية وتطوعية تفرغ طاقتهم بشكل ايجابي وتمنحهم شعور بتقدير الذات.
- يجب بناء روابط انسانية مع الأبناء خاصة في فترة المراهقة بما يضمن مصارحتهم لكم لتجارهم غير الآمنة دون خوف من العقاب.
- يجب توعية الشباب بأن موضوع المخدرات الرقمية هو مجرد وهم يؤدي لفقدان المال وإضرار الجهاز السمعي لا أكثر.
- يجب تشجيع الشباب على الاندماج في أنشطة اجتماعية وثقافية وترفيهية على أرض الواقع بدلا من الغرق في بحور العالم الافتراضي لاسيما في الجانب المظلم منه.
- تكثيف الرقابة الأسرية والحرص على أن يكون جهاز الحاسوب في مكان مفتوح سهل الرقابة.
- بالإضافة إلى ذلك يجب الحرص على: (عبير، 2019، صفحة 272)
- رصد وحجب هذه المواقع والمقاطع الصوتية قبل ترويجها والعمل على ضبط مروجيها من قبل الجهات المعنية.
- نشر وسائل التوعية للأسر عن طريق مد جسور التعاون بين المرشد التربوي والمدرسة وأسرة المراهق، وتدريبهم على كيفية فرض نوع من الرقابة الذاتية على أبنائهم.

خاتمة:

من خلال ما تم عرضه في هذا الموضوع يتضح مدى تأثير الانترنت وما تطرحه من ظواهر حديثة وغريبة على مجتمعاتنا من حين لآخر، كما يتضح مدى سيطرة التكنولوجيات على الأفراد وقدرتها على التحكم فيهم من خلال ما تصوره وتعرضه من اغراءات ينجر وراءها شبابنا دون وعي وإدراك لخطورتها، وظاهرة المخدرات الرقمية خير دليل على ذلك بالرغم من كونها لا تزال حديثة نوعا ما ومحدودة الانتشار، إلا أنه يجب دق ناقوس الخطر والتحرك فورا لمجابهتها والتصدي لها، بالإضافة لذلك يجب تكثيف الدراسات حول هذه الظاهرة والغوص أكثر في أعماقها من أجل الوقوف على مسبباتها واجتنابها، أيضا من أجل توجيه السياسيين وصناع القرار نحو سن قوانين رادعة لهذه الظاهرة، وزيادة الوعي لدى الأولياء بالخطر الذي يحيط بأبنائهم.

قائمة المراجع:

1. الزناتي شيماء. (30 11, 2021). ماهو الفضاء الرقمي؟ تاريخ الاسترداد 01 28, 2022، من مقال: <https://mqaall.com/what-is-digital-space>
2. بن عبد العزيز المتروك تركي. (د.س). المخدرات الرقمية علاج أم إدمان. مجلة وادي النيل للدراسات والبحوث الانسانية والاجتماعية والتربوية (د.ع).
3. بوخودوني صبيحة، و بن عاشور الزهرة. (2020). الإدمان على المخدرات الرقمية وعلاقتها بالانحراف والجريمة لدى الشباب. مجلة أنسنة للبحوث والدراسات، المجلد 11 (01)، الصفحات 115-130.
4. جلول أحمد، و فرحات فوزي. (08 مارس، 2020). المخدرات الرقمية: خطورتها وسبل الوقاية منها. مجلة الدراسات والبحوث الاجتماعية (العدد 01)، الصفحات 64-79.
5. شاوش أمين. (11 07, 2015). 15 طفلا يدمنون على المخدرات الإلكترونية في الجزائر. تاريخ الاسترداد 01 2022, 25، من <https://www.ennaharonline.com/15-طفلا-يدمنون-على-المخدرات-الإلكترونية/>



6. عزوز صونيا، و قريشة خالد. (2020). المخدرات الرقمية: مفهومها، جذورها التاريخية، كيفية تأثيرها، والحد منها. ملتقى وطني حول المخدرات والمجتمع: تشخيص الظاهرة وسبل الوقاية والعلاج.
7. فريجات نسبية، و العمارة علي. (2020). مقارنة مفاهيمية للمخدرات الرقمية. ملتقى وطني حول: المخدرات والمجتمع: تشخيص الظاهرة وسبل الوقاية والعلاج.
8. لوحيدي فوزي، و حامد علي. (2020). مخاطر المخدرات الرقمية وكيفية مواجهتها. ملتقى وطني حول المخدرات والمجتمع: تشخيص الظاهرة وسبل الوقاية والعلاج.
9. مامنية سامية، و حمادي ابتسام. (2018). المخدرات الرقمية. الملتقى الوطني: تعاطي المخدرات في المجتمع الجزائري، الأسباب، الآثار، طرق الوقاية والعلاج. قلمة: جامعة 8 ماي 1945.
10. ميهوب علي، و بن ذهبية جغدم. (2020). الأنثروبولوجيا الجنائية في مجال الهلوسة الإلكترونية "المخدرات السيبرانية نموذجاً". ملتقى وطني حول: المخدرات والمجتمع: تشخيص الظاهرة وسبل الوقاية والعلاج.
11. نجم عبد الله أحمد الخالدي عبير. (2019). المخدرات الرقمية وتداعياتها على المراهق وسبل الوقاية والعلاج. مجلة أبحاث البصرة للعلوم الانسانية ، المجلد 44 (04).
12. وشاح إيمان. (بلا تاريخ). ماهو الفضاء السيبراني. تاريخ الاسترداد 28 01, 2022، من الملف: <https://news.almlf.org/post/298266>



العملة الرقمية و الجرائم السيبرانية :

الدوافع الفاعلة في الفعل الاجرامي الرقمي-رؤية سوسيولوجية-

Digital globalization and cybercrime:

Digital crime motives - a sociological vision-

ط د مرازقية عادل

مخبر البحوث النفسية والاجتماعية جامعة الدكتور يحي فارس المدينة

Merazguia.adel@univ-medea.dz

مقدمة

إننا نعيش في عصر التقنية والحاسبات والانترنت في مختلف مجالات الحياة ، بل أصبح استخدامها ضرورة لاغنى عنها في جميع القطاعات الحكومية والخاصة في تبادل المعلومات وتقديم الخدمات ، مواكبة للتطور الهائل في مجال الاتصالات وأنظمة المعلومات. ان هذا التطور التكنولوجي الحديث افرز مجالات تفاعل افتراضية جديدة ناجمة عن الاستحداثات التكنولوجية، كما اسهم ايضا في بزوغ نجم العملة وتنوع الياتها و التي ازلت الحدود بين الشعوب.

هذا الاستمرار في التطور الرقمي السريع و الهائل في نظم المعلومات و الاتصالات زاد من حجم تدفق البيانات و المعلومات و فتح المجال لبروز شكل جديد من العملة يعرف بالعملة الرقمية والتي بدورها افرزت انماط جديدة من السلوكيات و الجرائم باتت تعرف بالجرائم السيبرانية. ومما لا شك فيه انه كلما تطورت ثورة المعلومات و الاجهزة التكنولوجية ظهرت انماط جديدة و اشكال مختلفة من الجرائم السيبرانية وهذا ما يفسر العلاقة المترابطة بين العملة الرقمية و الجرائم السيبرانية و مدى تر و تتداخل الدوافع الفاعلة في الفعل الاجرامي الرقمي.

-اسئلة الدراسة :

- ما العلاقة بين العملة الرقمية و الجرائم السيبرانية ؟

- ماهي فئات و اشكال الجرائم السيبرانية ؟

- ما هي الدوافع الذاتية و الموضوعية وراء ارتكاب الفعل الاجرامي الرقمي؟

-اهداف الدراسة :

تهدف هذه الدراسة الى الوقوف على مدى تأثير العملة الرقمية في الجرائم السيبرانية،وكيف تشكلت انواع و فئات مختلفة ومتعددة من الافعال الاجرامية الرقمية المرتبطة اساسا بعوامل متعددة.

-اهمية الدراسة :

تكمن اهمية الدراسة في تقديم رؤية سوسيولوجية للعوامل الدافعة لارتكاب الفعل الاجرامي الرقمي بسبب الانتشار الهائل للجرائم السيبرانية،والتي رافقت مخرجات العملة الرقمية و المتمثلة في التطور السريع والهائل لتكنولوجيات الاتصال و المعلومات على كافة الاعددة،الوطنية و الاقليمية و الدولية.



-التعريفات المفاهيمية و الاجرائية :

● تعريف العولمة :

أ- لغة : يعود لفظ عولمة الى الكلمة الانجليزية global والتي تعني عالمي او دولي او كروي (الوالي، 2002).

اما المصطلح الانجليزي globalization فيترجم الى الكوكبة وفي اللغة الفرنسية نستخدم مصطلح mondialisation مشتقة من كلمة monde وهي بذلك تعني الكون و الكونية.

فالعولمة في اللغة العربية اسم مصدر على وزن "فوعلة" مشتق من العالم وهي تعميم الشيء حيث تبين لنا هذه الصيغة على وجود فاعل يقوم بالفعل (القرضاوي، 2000).

وقد استخدمت في اللغة العربية للدلالة على هذه الظاهرة اربع كلمات وهي : العولمة و الكونية و الكوكبة و الشمولية وكانت الغلبة في النهاية لمصطلح العولمة.

ب- اصطلاحا :

يرى السيد ياسين ان صياغة تعريف دقيق للعولمة تبدو مسألة شاقة نظرا لتعدد تعريفاتها التي تتأثر أساسا بانخيازات الباحثين الايديولوجية واتجاهاتهم إزاء العولمة رفضا او قبولا، والتي حسب رأيه تتمثل في سهولة حركة الناس و المعلومات و السلع بين الدول على النطاق الكوني (سعيد، 1998).

كما عرفت بأنها إتجاه الحركة الحضارية نحو سيادة نظام واحد تقوده قوة واحدة، أو بعبارة أخرى إستقطاب النشاط السياسي و الإقتصادي في العالم حول إرادة مركز واحد من مراكز القوة في العالم (حجازي، 2003).

اما انطونيو جيدنز عرفها بأنها مرحلة جديدة من مراحل بروز و تطور الحداثة، تتكشف فيها العلاقات الاجتماعية على الصعيد العالمي، حيث يحدث تلاحم غير قابل للفصل بين الداخل و الخارج، ويتم فيها ربط المحلي و العالمي بروابط اقتصادية و ثقافية وسياسية وانسانية، حيث ان العولمة كإمتداد و كنتيجة هي اضافة بعد جديد للأبعاد المحلية حيث يصبح العالم الخارجي بنفس حضور العالم الداخلي في تأثيره على سلوكيات وقناعات وافكار الافراد (عبد الخالق ع، 1999).

كما يراها الكثيرون من المفكرين والكتاب هي سيطرة وغلبة ثقافة من الثقافات على جميع ثقافات العالم (شليبي، 1999).

التعريف الإجرائي :

مما سبق من التعريفات يمكننا ان نعرف العولمة بأنها عملية هندسة ثقافة عالمية موحدة تشمل جميع الميادين بحيث يتمكن منها الجميع بسهولة و دون مقاومة او معارضة.

● العولمة الرقمية :

يرى شيليرو بان العولمة الرقمية في القرن الواحد و العشرين تعززها التقنيات الرقمية، و تتميز بتسريع وزيادة تدفقات البيانات و المعلومات.

ففي عملية رقمنة الاقتصادات تتزايد تدفقات البيانات العالمية وتسمح المنصات الرقمية لمزيد من البلدان و الشركات بالمشاركة. فهو يرى بان التحول الرقمي للاقتصادات يغير طرق الاستهلاك و التجارة والاستثمار والتنفيذ للاعمال التجارية وادارة الحكومات، فهي تغير طرائق العلاقات الاقتصادية و التجارية بين الدول (Schilirò, 2020).



التعريف الاجرائي :

من خلال ماسبق يمكن ان نعرف العملة الرقمية بأنها عملية تحول رقمي عن طريق تسريع و زيادة تدفقات البيانات و المعلومات وذلك باستخدام تقنية المنصات الرقمية.

● الجريمة السيبرانية :

ان الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها، ففي البداية عرفت بمفهوم اساءة استخدام الكمبيوتر مروراً الى مفهوم احتيال الكمبيوتر، الجريمة المعلوماتية، جرائم الكمبيوتر، الجرائم المرتبطة بالكمبيوتر، جرائم التقنية العالية الى جرائم الهاكرز فجرائم الانترنت الى اخر المصطلحات الجرائم السيبرانية (عبد الله، 2017).

لا يوجد تعريف محدد للجريمة السيبرانية، فهناك من يعرفها بأنها نشاط اجرامي تستخدم فيه تقنية الحاسب الالى بطريقة مباشرة او غير مباشرة كوسيلة او هدف لتنفيذ الفعل الاجرامي المقصود (القرعان، 2018).

وهناك من يعرفها بأنها هي التي تتم بواسطة الكمبيوتر او احد وسائل التقنية الحديثة مع ضرورة توفر شبكة اتصال بينهما (احمد، 2007).

كذلك تعرف بذلك النوع من الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة هي الحاسب الألي عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة بجرائم الانترنت (الجهيني، 2004).

التعريف الاجرائي :

من خلال ما سبق يمكن ان نعرف الجريمة السيبرانية بأنها كل استخدام للأجهزة الالكترونية ، تكنولوجيا المعلومات، و شبكة الانترنت في انشطة اجرامية من طرف الافراد او الجماعات قصد الحاق الضرر المادي او المعنوي بالافراد او الجماعات او الحكومات للحصول على عائد منها.

● الفعل الاجرامي الرقمي :

-تعريف الفعل الاجرامي :

يعرف الفعل الاجرامي من المنظور القانوني بذلك الفعل الذي يعاقب عليه بموجبه القانون وبمعنى آخر هي ذلك الفعل او الامتناع الذي نص القانون على تجريمه ووضع عقوبة جزاء ارتكابه.

فالفعل الاجرامي من هذا المنظور له درجات تختلف حسب الجسامة، فالأخف يعرف بالمخالفة و المتوسط بالجناية والاشد جسامة بالجناية.

اما من الناحية السيكولوجية نجد ان علماء النفس ينظرون الى الفعل الاجرامي على انه فعل معاد للمجتمع Anti social behavior، وما هو الا نوع من السلوك الشاذ الذي يحتاج الى العلاج كما تحتاج الامراض العقلية للعلاج و الرعاية، كما يرون بان كل فعل اجرامي ماهو الا دلالة وتعبير عن صراعات نفسية تدفع صاحبها الى الوقوع في الجريمة (عبد الخالق ج.، 1999).

اما من المنظور السوسيولوجي فهي كل الافعال التي يترتب عليها الاخلال بالنظام السائد في الجماعة او الاضرار بمصالح او بحقوق افرادها او المساس بالقيم التي اصطلح الناس عليها علاقاتهم المختلفة والتزامهم باتباعها في الجماعة (اوهائية، 2007).

فمن المنظور السوسيولوجي نجد اتجاهين بشأن المعنى الاجتماعي للظاهرة الاجرامية، حيث الاتجاه الاول يعرفها بأنها كل فعل يتعارض مع المبادئ الخلقية فهو يربط بين الجريمة و قواعد الاخلاق، اما الاتجاه الثاني فيعرفها على اساس الربط بينها و بين القيم الاجتماعية، فهي كل فعل او امتناع يتعارض مع القيم الاساسية الخاصة بحفظ وبقاء المجتمع (عبد الخالق ج.، 1999).



• تعريف الفعل الاجرامي الرقمي :

التعريف الاجرائي :

من خلال التعاريف السابقة يمكن ان نعرف الفعل الاجرامي الرقمي بانه كل فعل باستعمال الوسائط الرقمية يتعارض مع القيم الاجتماعية و القواعد الاخلاقية الاساسية السائدة في الجماعة للاضرار بمصالح الافراد او الجماعات او النظام المجتمعي ككل.

1. العلاقة بين العولمة الرقمية و الجرائم السيبرانية :

تشير العولمة الى التحول العالمي او التداول المرتبط بالجوانب الاجتماعية و الاقتصادية و التكنولوجية و السياسية والثقافية من خلال وسائط مختلفة، كتبادل البيانات و المعلومات و التجارة عبر الانترنت للسلع و الخدمات (kellner, 2002) ، فهي اذن تشترك في تكامل المجتمعات المختلفة عن طريق الممارسات الثقافية و الاقتصادية و الابتكارات التكنولوجية مما ادى الى ترابط متبادل و معقد في نفس الوقت (Bosede Awoyemi, 2021).

ان هذا التحول الرقمي الهائل الذي خضع له عالم التكنولوجيا سعى لتحقيق اقتصاد رقمي في تطبيقات العالم الحقيقي مثل التعلم الذكي، الحوكمة الذكية و المدن الذكية، مما سمح لمختلف الابنية و الانظمة الاقتصادية كثيفة البيانات مثل الاتصالات و تكنولوجيا المعلومات و التصنيع و البنوك من التوجه الى وظيفية تطبيق البيانات الضخمة كطريقة لرقمنة اقتصاداتها. فمن خلال هذا التحول الرقمي المتسارع في وظائف الابنية و الانظمة و ادوارها المختلفة تعددت الابعاد و تعقدت في نفس الوقت، حيث انتجت نسق مترابط اجباري و ملزم من خلال الانتشار السريع للتقنيات التكنولوجية مثل الذكاء الاصطناعي AI و انترنت الاشياء IOT و الذي بات يعرف بالعولمة الرقمية.

ان العولمة الرقمية كعلامة مميزة للقرن الحادي و العشرين، غيرت بشكل كبير طرق و تفاعلات ممارسة الاعمال على مستوى العالم، فبخفض تكلفة الوصول الى الانترنت و السماح بالولوج المجاني الى منصات و تطبيقات التواصل الاجتماعي انتجت عددا لا يحصى من التحديات و المخاطر الجديدة و التي لم تفهم بالكامل بعد بالرغم من جانبها الايجابي، بحيث تعتبر الجرائم السيبرانية احدى هذه التحديات و المخاطر التي تهدد امن الافراد و الجماعات و كافة الابنية و الانظمة في العالم. فمجرمو الفضاء السيبراني يستفيدون من العولمة الرقمية بتنفيذ جرائمهم من الاماكن التي لا توجد فيها لوائح تنظيمية و تشريعية و قانونية خاصة من الناحية العملية، وايضا من الدول التي لا تطبق فيها القوانين.

اذن العلاقة بين العولمة الرقمية و الجرائم السيبرانية علاقة مترابطة حيث ان تقنيات المعلومات و الاتصالات الحديثة مع الشبكات و المنصات المتزايدة كغرار منصة ميتافيرس الغت جميع الحدود الافتراضية وانتجت بيئة رقمية تحفز التفاعلات و التكامل بين المجرمين و فتحت المجال بمصراعيه الى عولمة الجريمة السيبرانية والى تشكيل تهديد و مخاطر اكبر على امن الافراد و الجماعات و الدول.

2. الفئات و الاساليب الحديثة للجرائم السيبرانية :

هناك ثلاث فئات رئيسية تصنف فيها الجرائم السيبرانية وهي فئة الافراد و الممتلكات و الحكومات بحيث تختلف الاساليب المستخدمة و مستويات صعوبتها حسب كل فئة.

1.2. فئات الجرائم السيبرانية :

1.1.2. الفردية: تتضمن هذه الفئة من الجرائم السيبرانية فردًا واحدًا يوزع معلومات ضارة أو غير قانونية عبر الإنترنت، ويمكن أن يشمل ذلك المطاردة عبر الإنترنت وتوزيع المواد الإباحية والاتجار.

2.1.2. الملكية: هذا مشابه لمثال واقعي لمجرم يمتلك بشكل غير قانوني معلومات بنك أو بطاقة ائتمان لأحد الأفراد، يسرق المخترق التفاصيل المصرفية الخاصة بشخص ما للوصول إلى الأموال أو إجراء عمليات شراء عبر الإنترنت أو تنفيذ عمليات التصيد الاحتيالي



لحمل الأشخاص على الكشف عن معلوماتهم، ويمكنهم أيضًا استخدام برامج ضارة للوصول إلى صفحة ويب تحتوي على معلومات سرية.

3.1.2. الحكومية: هذه هي الجريمة السيبرانية الأقل شيوعًا ، لكنها أخطر الجرائم. تُعرف الجريمة ضد الحكومة أيضًا باسم الإرهاب السيبراني. تشمل الجرائم السيبرانية الحكومية اختراق المواقع الحكومية أو المواقع العسكرية أو توزيع الدعاية. هؤلاء المجرمون هم عادة إرهابيون أو حكومات معادية لدول أخرى (panda medeacenter, 2021).

2.2. تصنيفات الجرائم السيبرانية :

يمكن تصنيف الجرائم السيبرانية (Vadza, 2011) بشكل أساسي بطريقتين :

- استخدام الكمبيوتر كهدف لمهاجمة أجهزة الكمبيوتر الأخرى، على سبيل المثال قرصنة ، هجمات فيروسات / دودة ، هجوم DOS وما إلى ذلك.

- استخدام الكمبيوتر كسلاح لارتكاب جرائم حقيقية، على سبيل المثال الإرهاب السيبراني ، وانتهاكات حقوق الملكية الفكرية ، وعمليات الاحتيال على بطاقات الائتمان ، وعمليات الاحتيال عبر تحويل الأموال الكترونيا ، والمواد الإباحية ، إلخ. وعلاوة على ذلك، تم بتصنيفها على النحو التالي :

1.2.2. الدخول الغير مرخص: يعني أي نوع من الدخول الى ذاكرة او موارد وظيفية او نظام او شبكة كمبيوتر و ارشادها او التواصل معها دون إذن من أي من المالك الشرعي أو الشخص المسؤول عن الكمبيوتر.

2.2.2. القرصنة والاختراق: هو كل فعل يرتكب لاقتحام جهاز كمبيوتر و / أو الشبكة. حيث يقوم المتسللون بكتابة أو استخدام برامج الكمبيوتر الجاهزة لمهاجمة الكمبيوتر المستهدف. مثل سرقة معلومات بطاقة الائتمان ، وتحويل الأموال من الحسابات المصرفية المختلفة إلى حسابهم الخاص متبوعًا بسحب الأموال. كما يقومون بسرقة البيانات أو تعديلها أو إدراج فيروسات أو الديدان التي تلحق الضرر بالنظام عن طريق اختراق خادم الويب.

3.2.2. الاحتيال عبر الإنترنت : الشبكة هي نعمة للناس لممارسة الأعمال التجارية بفعالية وبسرعة كبيرة. غير انها اصبحت مفتوحة للمحتالين وأصبحت عمليات الاحتيال عبر الإنترنت تخرج عن نطاق السيطرة بشكل متزايد و التي منها :

- مواقع الويب المخادعة وتنبهات أمان البريد الإلكتروني.

- رسائل البريد الإلكتروني الحاملة للفيروسات.

- الاحتيال في اليانصيب.

- الانتحال و يعني التطفل غير المشروع باستعمال هوية غير الهوية الحقيقية.

- احتيال بطاقات الائتمان.

4.2.2. السرقة الإلكترونية: سرقة المعلومات المالية و / أو الشخصية من خلال

استخدام أجهزة الكمبيوتر.

5.2.2. الإرهاب السيبراني: وهي الهجمات المستهدفة للمنشآت العسكرية ومحطات الطاقة ، ومراقبة الحركة الجوية والبنوك ومراقبة حركة المرور وشبكات الاتصالات. وآخرون يحبون الشرطة والأنظمة الطبية وأنظمة الإطفاء والإنقاذ وما إلى ذلك.

6.2.2. تدفق الفيروسات ، حصان طروادة ، الدودة والقنابل المنطقية : وهي برامج تحمل فيروسات تعمل على اتلاف نظم التشغيل و كذا المعلومات المخزنة في ذاكرة الكمبيوتر.



7.2.2. المواد الإباحية على الإنترنت: هي وصف أو إظهار أفعال جنسية بتنسيق من أجل الإثارة الجنسية عن طريق الكتب والأفلام .. إلخ. " وهذا يشمل المواقع الإباحية ؛ والمواد المنتجة باستخدام أجهزة الكمبيوتر والإنترنت لتنزيل ونقل مقاطع الفيديو والصور الإباحية.

8.2.2. التشهير : يمكن فهم التشهير على أنه انتهاك متعمد لحق شخص آخر في سمعته الجيدة.

9.2.2. المطاردة عبر الإنترنت: يمكن تعريف المطاردة عبر الإنترنت على أنها الأفعال المتكررة المضايقة أو السلوك التهديدي لمجرم الإنترنت تجاه الضحية باستخدام خدمات الإنترنت. فالمطاردة تنطوي على متابعة تحركات الشخص عبر الإنترنت عن طريق نشر رسائل (تهديد في بعض الأحيان) على لوحات الإعلانات التي يتردد عليها الضحية ، ودخول غرف الدردشة وقصف الضحية باستمرار برسائل البريد الإلكتروني وما إلى ذلك.

10.2.2. البريد الإلكتروني و المحادثات عبر الانترنت المتصلة بالجريمة.

11.2.2. البريد العشوائي: يغمر البريد العشوائي الإنترنت بنسخ عديدة من نفس الرسالة، في محاولة لفرض الرسالة على الأشخاص الذين لن يختاروا تلقيها بطريقة أخرى.

حيث يجمع مرسلو البريد العشوائي عناوين البريد الإلكتروني من غرف الدردشة والمواقع الإلكترونية لقوائم العملاء ومجموعات الأخبار والفيروسات التي يتم حصادها في دفاتر وعناوين المستخدمين ويتم بيعها لمرسلي البريد العشوائي الآخرين.

12.2.2. هجمات رفض الخدمة: وهي إغراق موارد الكمبيوتر بطلبات أكثر منه ويمكن التعامل مع هذا يؤدي إلى تعطل الموارد وبالتالي رفض الوصول إلى الخدمة للمستخدمين المصريح لهم.

13.2.2. التزوير: تزوير الأوراق النقدية والطوابع البريدية والإيرادات المزيفة ،

كما يمكن تزوير أوراق العلامات وما إلى ذلك باستخدام متطور أجهزة الكمبيوتر والطابعات والمساحات الضوئية ، كما يعتبر انتحال شخصية شخص آخر تزويرًا.

14.2.2. انتهاكات حقوق الملكية الفكرية: وتشمل قرصنة البرامج ، وانتهاك حقوق النشر ، انتهاكات العلامات التجارية ، وسرقة شفرة مصدر الكمبيوتر ، انتهاكات براءات الاختراع .. إلخ .

15.2.2. التجارة الإلكترونية / الاحتيال في الاستثمار: وهي عمليات الاحتيال في المبيعات و الاستثمارات عن طريق تقديم مطالب احتيالية أو شراء باستخدام أوراق مالية مزورة أو عدم تسليم أو استخدام البضائع و الخدمات المتعاقد عليها مع الافراد عن طريق الانترنت.

16.2.2. بيع المواد غير القانونية: ويشمل ذلك تجارة المخدرات والأسلحة وما إلى ذلك ، من خلال نشر المعلومات على مواقع الويب والمزادات أو ببساطة عن طريق استخدام البريد الإلكتروني لعرض منتجات محظورة أو غير قانونية للبيع.

17.2.2. لعب القمار على الانترنت: هناك الملايين من المواقع التي تقدم المقامرة عبر الإنترنت. في الواقع أن العديد من هذه المواقع هي واجهات لغسيل الاموال.

18.2.2. العبث بالبيانات : ينطوي هذا الفعل على تغيير البيانات قبل أو أثناء الإدخال إلى الكمبيوتر. فيتم تغيير المعلومات بواسطة شخص يكتب في البيانات ، أو فيروس مرمج يغير قاعدة البيانات أو التطبيق .

19.2.2. الإتلاف المادي لنظام الكمبيوتر: وهو إلحاق الضرر المادي بجهاز الكمبيوتر أو الأجهزة الطرفية الخاصة به عن طريق الصدمة أو الحريق أو التيار الكهربائي الزائد وما إلى ذلك.



20.2.2. خرق الخصوصية والسرية: تشير الخصوصية إلى حق الفرد / الأفراد في تحديد متى وكيف وإلى أي مدى يمكن مشاركة بياناتهم الشخصية مع الآخرين.

21.2.2. القرصنة لتعدين العملات المشفرة : هي احد انماط الجريمة السيبرانية التي يستخدم في اطارها المجرمون سرا طاقة حاسوب الضحية لتعدين العملات المشفرة، وتحدث عادة عندما تنصب الضحية بشكل عرضي برنامجا يحتوي على برامج نصية خبيثة تتيح لمركبي الجرائم السيبرية الولوج إلى حاسوبكم أو إلى أي جهاز آخر موصول بالإنترنت عبر النقر مثلا على وصلة مجهولة المصدر في بريد إلكتروني أو عبر زيارة موقع إلكتروني موبوء. ويستعين الجناة ببرامج تُسمى تعدين العملات coin miners لاستحداث أو تعدين عملات مشفرة.

3. الدوافع الفاعلة في الفعل الاجرامي الرقمي :

ان ظاهرة الفعل الاجرامي الرقمي ظاهرة معقدة ومتشابكة لها علاقة ببعض المتغيرات الاجتماعية والاقتصادية والثقافية والذاتية، ولها ايضا اسبابها ودوافعها الكفيلة بان تكشف لنا السياق الاجتماعي والثقافي لانتشار الظاهرة.

1.3. الدوافع الذاتية :

تتباين الدوافع الذاتية لارتكاب الفعل الاجرامي الرقمي بتباين توجهات واهداف مرتكبيه ويمكن ان نحددها فيمايلي :

1.1.3. الرغبة في التعلم : ان الفعل الاجرامي الرقمي لا يعتمد على المستوى التعليمي الاكاديمي فقط بل يتعدى الى عملية التعلم، فهو اذن تعلم مكتسب من خلال الاختلاط بالنماذج الاجرامية في ذات النمط الاجرامي، وهذا ما اكده "ساذرلاند" في نظرية المخالطة الفارقة.

فقرصنة الانظمة يعلنون ان هدفهم من الوصول الى المعلومات ودخولهم للشبكات و الحواسيب هو التعلم فقط، فهم يتعاونون في شكل افراد او جماعات ويتشاركون المعلومات التي يتحصلون عليها قصد الاستفادة منها في انشطة هادفة ولو بطرق غير مشروعة، غير ان مرتكبي هذا الفعل الاجرامي الرقمي ذوي المستويات التعليمية الجامعية او ما بعد التدرج يتناقض مع طبيعة التعليم كونه يهذب الشخص ويوجه سلوكه نحو الالتزام بقوانين المجتمع ومعايير و تقاليده ويحوله الى دافع للاجرام لمن لديه الاستعداد للجريمة حيث يزيد من الخطورة الاجرامية للفرد.

غير ان عملية التعلم تكمن اهميتها في بعض الانماط الاجرامية كاختراق الحسابات البنكية او الابتزاز، اما القذف و الشتم و التشهير لا تتطلب تعليما متخصصا بل مهارات التعامل مع الانترنت فقط.

2.1.3. الرغبة في الثراء : ان الطمع، حب الثراء، والرغبة في تحقيق النجاح المادي، بالاضافة الى القدرة على ارتكاب الفعل الاجرامي الرقمي تجعل من المجرم السيبراني يبتكر طرق و اساليب لتحقيق الهدف المرغوب فيه بطرق غير مشروعة، وهو مايتفق مع الاستجابة الابتكارية لروبرت ميرتون.

فالمجرم السيبراني يبتكر وسائل غير مشروعة كوسائل بديلة عند تعذره لتحقيق الاهداف بوسائل مشروعة لتحقيق الثراء او النجاح المادي وهذا ما اكده ميرتون عن الانومي او اللامعيارية في تفسير السلوك الاجرامي.

لذا يعتبر الدافع المادي من اكثر الدوافع التي تحرك الجاني لاقتواف الفعل الاجرامي الرقمي، لان الربح الممكن تحقيقه يدفع المجرم السيبراني الى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية ثم يستغل الفرص المتاحة ويسعى الى الاحتراف حتى يحقق اعلى المكاسب وبأقل جهد ممكن دون ان يترك دليل رقمي يدينه.



3.1.3. الرغبة في الانتقام : لعل اهم العوامل الذاتية الدافعة للفعل الاجرامي الرقمي هو الانتقام لدوافع اجتماعية او نفسية، فغالبا مايصدر عن شخص يملك معلومات كبيرة عن المؤسسة او الشركة التي يعمل بها، وغالبا مايكون هذا الدافع لا سباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية او الطرد من الوظيفة فيتولد لديه الرغبة في الانتقام من رب العمل. كما يتجسد ايضا فعل الانتقام في المساس بأعراض بعض الاسر او التشهير ببعض افرادها، ايضا بث الصور و الموضوعات التي تسبب التفكك الاسري و الخلافات، ومنه يصبح الانتقام هنا عبارة عن احد اساليب التخفيف عن الطاقات المتولدة في النفس جراء الاحباطات المتتالية، كما اكده جون دولار في نظرية الاحباط و العدوان. وعليه فان الفعل الإجرامي الرقمي بدافع الانتقام ماهو الى رد فعل عدواني بسبب وجود احباطات مسبقة لم تصرف او تخفف بأسلوب معقول حيث يقوم الجاني بتحويلها الى سلوكيات انتقامية عدوانية للإحراق الضرر المادي و المعنوي بالضحية.

2.3. الدوافع الموضوعية :

1.2.3- التحولات و التغيرات في البناء الاجتماعي :

لقد ظهرت أنماط مستحدثة من الجرائم بأشكال و طرق متباينة تختلف في طبيعتها وأنماطها عن الجرائم التقليدية، حيث مارست التحولات و التغيرات التي طرأت على البناء الاجتماعي في الجزائر تأثيراتها على الشباب باختلاف فئاتهم العمرية وانتماءاتهم الفكرية لان التغير الاجتماعي حقيقة متأصلة في طبيعة المجتمعات والذي يقصد به كل تحول يحدث في النظم والأنساق والأجهزة الاجتماعية سواء البنائية أو الوظيفية خلال مدة زمنية محددة (الخشاب، 1977، صفحة 188)

إن الأوضاع الجديدة التي طرأت على البناء الاجتماعي و النظم و العادات وأدوات المجتمع أوجدت من حقق أهدافه بطرق و أساليب مشروعة وينعم بمستوى معيشي مقبول في العالم الفيزيقي نجد بالمقابل من يكابد الحرمان وإشباع احتياجاتهم الأساسية، وعليه يقومون باستغلال العالم الافتراضي واستعمال طرق ووسائل غير مشروعة كالجرائم السيبرانية لتحقيق النجاح المادي و المعنوي.

فإذا تعارفنا بان الفعل الإجرامي الرقمي موجود على مستوى البنيات الاجتماعية والذي هو أساسا مرتبط بثقافة مجتمعية، فيجدر بنا تقديم تحليل موضوعي للظاهرة يتجاوز نظرة تقديم تبريرات فقط. فإذا كان التغير الاجتماعي مرتبط أساسا بالجانب التفاعلي لأفراد جميع البنيات الاجتماعية فيستوجب علينا فهم الجوانب المحركة و الدافعة لهذا الفعل الإجرامي من خلال بعده الماكر و سوسيولوجي. فانطلاقا من التغير الاجتماعي الذي حتما يؤدي الى تغيرات في السلوك المتوقع و النماذج الاجتماعية السائدة وذلك بتجريب قواعد ومقاييس جديدة وبالتالي تتغير التوقعات الاجتماعية وتغير النماذج ويزداد البناء الاجتماعي تعقيدا وهذا ما نلاحظه في السلوكيات الإجرامية الغير متوقعة والنماذج المختلفة للفعل الإجرامي الرقمي و التي عقدت التفاعلات داخل البنيات الاجتماعية. كذلك الثورات الرقمية التي يتعرض لها المجتمع تعتبر من العوامل التي تعجل بحدوث التغير الاجتماعي وذلك لما يترتب عنها من تغيير سريع في كل الأوضاع والنظم الاجتماعية السائدة.

وعليه يمكن أن نستبق المخرجات الغير مرغوب فيها بسبب التغير الاجتماعي وذلك بدراسته وفق خطط و استراتيجيات ومعايير تجعل من الفعل الاجتماعي عقلانيا و مشروع يحقق الاحتياجات و الإشباعات والتطلعات لجميع الكتل الاجتماعية على مستوى النظام الاجتماعي ونكون بذلك ساهما في الحد من الفعل الإجرامي الرقمي عند بدايته.

2.2.3. العولمة الرقمية و شبكات التواصل الاجتماعي :

لقد اجتاحت المجتمعات في الآونة الأخيرة تحولات و تغيرات في مناحي الحياة، الأمر الذي انعكس بدوره على بنيتها وقيمتها. فالتغيير في بنية العلم و التكنولوجيا والاتصالات و الثورة الرقمية العابرة للقارات تطورت بشكل مذهل وغير متوقع لم تستطع الثورات الأخلاقية و الدينية مجاراتها وحتى التوازن معها (مرتضى، 2002، صفحة 52)، فلم يعد العالم كما كان عليه بعد ثورة الاتصالات و المعلومات



سواء في مشهده ونظامه أو في قيمه ومفاهيمه وأدواته و وسائطه، لقد دخلنا عصر كوني جديد ظهر فيه فاعلون جدد أبرزهم العاملون في مجالات تقنية المعلومات، عصر متعدد اللغات والمجالات، متداخل الأنظمة والمستويات، بقدر ماهر تقني فهو رقمي والذي بات يعرف بالعملة الرقمية، هذا الانفتاح الرهيب على عالم المعلوماتية و الرقمية جعل المجتمعات أمام مجتمع المخاطرة بكل ما يحمله من أفكار وسياسات وممارسات وهذا ما أكدته اورليش بيك بقوله أن مرحلة العملة هي مرحلة الشكوك أو اللايقينيات المصطنعة و اللامسؤولية الممنهجة (wendy & tony, 1997).

فشبكات التواصل الاجتماعي تشكل مستخدميه في اتساق جديد يساهم في تشكيل جماعات إجرامية افتراضية تجمع بين ذوي الاهتمامات المشتركة لتبادل أساليب و طرق الفعل الإجرامي الرقمي المختلف، وهذا ما يزيد من نسب الجرائم السيبرانية والتي تؤدي إلى حالة اللا امن و اللا استقرار للفرد و المجتمع على حد سواء. ففي ظل تكنولوجيا المعلومات والياتها و ضغوطاتها وممارساتها وفي ظل ما ينجم داخل المجتمعات من ميكانيزمات دفاعية او مؤيدة للممارسات الفعلية تتجلى تأثيرات العملة الرقمية وشبكات التواصل الاجتماعي على الحياة الاجتماعية والثقافية للفرد و المجتمع كمجتمع مخاطرة.

إن الدوافع الموضوعية لارتكاب الفعل الإجرامي الرقمي متعددة الأبعاد غير أنها تختلف من مجتمع إلى آخر حسب خصوصياته وقيمه و معاييرها ومنها :

- الأسرة و طبيعة الحياة.
- التعليم و الميول الاجرامية.
- ثقافة الاستهلاك و الطموح الزائد للشباب.
- البطالة والضغط الاقتصادي.
- المهنة وبناء الفرص الاجرامية.
- اختلال القيم الثقافية.

كل هذه العوامل متداخلة و متشابكة و تحتاج الى بحوث سوسيولوجية ميدانية معمقة والى تحليل منطقي للوقوف على مدى فاعليتها ودورها في تشكيل وبناء السلوك الاجرامي الرقمي لدى المستخدم من اجل بناء وتبني استراتيجيات على جميع المستويات تكون كفيلة بالحد او التقليل من ظاهرة الفعل الاجرامي الرقمي.

نتائج الدراسة :

- وجود علاقة مترابطة ومتكاملة بين العملة و الجرائم السيبرانية.
- تنوعت انماط الجرائم السيبرانية من السب و القذف و التشهير الى تعدين العملات المشفرة.
- ابرز الدوافع لارتكاب الفعل الاجرامي الرقمي هي الطمع وحب الثراء والرغبة في تحقيق النجاح المادي.
- يوجد اختلاف كبير بين الابعاد التي تتحكم في ظاهرة الفعل الاجرامي الرقمي.
- يمثل الفعل الاجرامي الرقمي تهديدا لأمن الافراد والمجتمعات مهما تنوعت دوافعه.

توصيات :

يوصي الباحث بمايلي :

- انشاء مراكز بحوث مشتركة بين جميع التخصصات لدراسة الجرائم السيبرانية من جميع الجوانب.
- التركيز على البحوث الميدانية خاصة السوسيولوجية و تمويلها قصد الوقوف امام واقع الجرائم السيبرانية.



- انشاء مراكز استقبال متخصصة لجميع البلاغات المتعلقة بالجرائم السيبرانية.
- تكوين خبراء و متخصصين في مجال الامن السيبراني و التحقيق الرقمي.
- اعادة صياغة القوانين و النصوص التشريعية وفق تطور الجرائم السيبرانية.
- العمل على توعية افراد المجتمع بجميع شرائحه بمدى خطورة الجرائم السيبرانية مع نشر ثقافة امنية تتماشى مع تطورات الاجهزة التكنولوجية و العالم الافتراضي عن طريق الوسائل الاعلامية وكافة مؤسسات التنشئة الاجتماعية.
- ضرورة تبني استراتيجيات ناجعة لمواجهة خطر الجرائم السيبرانية.

الخاتمة:

ان ازدهار الحضارة وانتشار التقدم التقني ساعد في تسهيل الكثير من امور حياتنا ولكنه في نفس الوقت جلب لنا العديد من المخاطر والاضرار و التحديات المتعلقة بالتقنيات الحديثة و الانترنت والتي تتمثل في الجرائم السيبرانية، والتي تعتبر ظاهرة اجتماعية قبل ان تكون حالة قانونية، وانطلاقا من هذا المفهوم نوى بانها تعبر عن موازنة بين القيم الاجتماعية والضغوط المختلفة من قبل المجتمع. ومما لا شك فيه بان الجرائم السيبرانية في المجتمع الجزائري مهما اختلفت انواعها و ابعادها واسبابها وعواملها فهي مرتبطة بالسلوك ومخرجاته التي تتمثل في افعال افراد المجتمع، وعليه يجب على كافة المختصين و الباحثين والعلماء من شتى التخصصات والميادين وخاصة علم الاجتماع التعامل معها بموضوعية و العلمية اللازمة والبحث عن حلول ناجعة بناء على المعطيات المتوفرة على مستويات البناءات الاجتماعية للحد من مخاطر هذه الظاهرة الخطيرة لان لها تداعيات على امن المواطن و الوطن .

قائمة المراجع :

- Bosede Awoyemi, O. O. (2021). GLOBALIZATION AND CYBER CRIMES. *International Journal of Multidisciplinary Research and Modern Education (IJMRME)*, 18.
- kellner, d. (2002). theorizing globalization. *sociological theory*, 20(03).
- panda medeacenter. (2021, april 26). Retrieved from <https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/>
- Schilirò, D. (2020). Towards digital globalization and the covid-19 challenge. *MPRA Paper No. 100504t* <https://mpira.ub.uni-muenchen.de/100504/>, 03.
- Vadza, K. (2011). Cyber Crime & its Categories. *Indian Journal of Applied Research* 3(5).
- wendy, h., & tony, j. (1997, juin). the risk society in age of ansxiety situating fear of crime. *british journal of sociology*, 4(2), 258.
- احمد هـ. ع. (2007). جرائم المعلوماتية عابرة للحدود، اساليب المواجهة وفقا لاتفاقية بودابست (1 ed.). القاهرة: دار النهضة العربية للنشر.
- الجهيني م. م. (2004). جرائم الانترنت. الاسكندرية-مصر: دار الفكر الجامعي.
- الحشاش م. (1977). دراسة المجتمع. الاسكندرية: الانجلو المصرية.
- القرضاوي، ي. (2000). المسلمون و العولمة. القاهرة: دار التوزيع و النشر الاسلامية.
- الوالي، ع. ا. (2002). جدلية العولمة بين الاختيار و الرفض. مجلة المستقبل العربي، 58،
- اوهابية، ع. ا. (2007). شرح قانون العقوبات الجزائري، القسم العام. الجزائر: مومف للنشر و التوزيع.



فرقة مشروع البحث التكويني الجامعي P.R.F.U الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها

رمز I05L02UN260120190001

- بن غرم الله عبد الله. (2017). جرائم الانترنت وعقوباتها وفق نظام مكافحة جرائم المعلوماتية السعودي. السعودية: دار الكتاب الجامعي.
- جلال الدين عبد الخالق. (1999). الجريمة و الانحراف الحاسوب و المعالجة (الإصدار دون طبعة). الاسكندرية، مصر: دار المعرفة الجامعية.
- حجازي، ا. م. (2003). الثقافة العربية في زمن العولمة. القاهرة: دار قباء.
- سعيد، أ. ز. (1998). العولمة، ماهيتها، نشأتها، أهدافها. عمان: دار البيارق.
- شليبي، أ. (1999). الدين و العولمة. المجلة العربية.
- عبد الخالق، ع. ا. (1999). العولمة: جذورها و فروعها وكيفية التعامل معها. مجلة عالم الفكر الكويت. 54 ,
- محمود احمد الفرعان. (2018). الجرائم الالكترونية (الإصدار الاول). عمان: دار وائل للنشر و التوزيع.
- مصطفى مرتضى. (2002). الواقع العربي في عصر العولمة. مصر: حويلات كلية الاداب جامعة عين شمس.



قراءة سوسيولوجية للدراسات العربية في مجال مكافحة الجرائم الالكترونية A sociological reading of Arabic studies on combating cybercrimes

د. أسامة باحمد

د. الزهرة بن عاشور

BAHMEDOUSSAMA79@GMAIL.COM

مقدمة

إن ظاهرة الانحراف والجريمة من الظواهر التي تواجه جميع المجتمعات النامية والمتقدمة ، وعلى الرغم من الجهود التي تبذل لمواجهتها إلا أنها لا تزال في تزايد مستمر ، والاحصائيات الخاصة بالانحراف والجريمة تشير الى الزيادة الكبيرة في عدد حالات السلوك المنحرف ولأن أبسط مفهوم لها عدوان فإن اهتمام المجتمعات بأمرها وأمر مرتكبيها قديم يرتد الى التاريخ الذي وجدت فيه هذه المجتمعات، ولم يتخذ هذا الاهتمام بطبيعة الحال شكل الدراسة العلمية الرامية الى تفسير الظاهرة الاجرامية واستقصاء أسبابها ووسائل مكافحتها وإنما اتخذ شكل الأفكار حول الظاهرة الجريمة دون التعمق في دراسة الظاهرة نفسها لاستجلاء أسبابها ووسائل مواجهتها. وتعتبر الجريمة المعلوماتية " الابن الغير اشعري " الذي جاء نتيجة لتزاوج بين ثورة تكنولوجيا المعلومات والعمولة " وإن حماية المجتمع من هذا النوع من الجرائم يقتضي وضع تشريعات فاعلة تواجه هذه الظاهرة الاجرامية ، وملاحقة مرتكبيها وانزال العقوبات المناسبة بحقهم (الرواشدة ، دس.ص 11)

كما أن من أكبر المشاكل التي تواجه عملية مكافحة الجريمة المعلوماتية والتي تشكل قلقا للأفراد والدول هي اكتشاف النشاط الإجرامي ، وتحديد الفاعل ، والملاحقة الجزائية لمرتكبي هذه الجريمة .

ومن أجل هذه الطبيعة الخاصة للجرائم المعلوماتية وخصوصية اساليبها على مستوى الموضوع والاجراء أصبح لا بد من وجود نصوص تشريعية خاصة بالتجريم والعقاب لمكافحة هذه الجريمة (اليحي ، تركي بن محمد، دس، ص 254) مما أوجب تطوير البنية التشريعية الجزائية الوطنية بذكاء تشريعي تعكس فيه الدقة الواجبة على المستوى القانوني مع ضرورة احترام مبدأ شرعية الجرائم والعقوبات من ناحية ، ومبدأ الشرعية الاجرائية من ناحية أخرى (الشوابكة ، محمد أمين، 2011 ، ص 7)

ومن جملة ما ذكر يمكن القول ان الجريمة المعلوماتية هي " كل فعل أو امتناع معاقب عليه بموجب القانون والمتعلق باستخدام نظم وشبكات ووسائل المعلومات والبرمجيات والحواسيب والانترنات والنشطة المتعلقة بها استخداما مجرما " (طه ، ابراهيم قاسم السيد محمد، 2015 ، ص 2).



1. الدراسات العربية:

1.1. الدراسة الأولى:

1.1.1. اسم الدراسة:

الجرائم الالكترونية الموجهة ضد مستخدمي الإنترنت

دراسة مسحية لبعض مستخدمي الإنترنت بالمملكة العربية السعودية، مقدمة لنيل شهادة ما جستير في العلوم الاجتماعية جامعة الامام محمد بن سعود الاسلامية - السعودية - الرياض - سنة 2010، من اعداد: فيسي نوال بنت علي بن محمد،

2.1.1. اشكالية الدراسة:

قد تمحورت إشكالية الباحثة فيما يلي : تحديد حجم أهم جرائم الإنترنت شيوعا بين مستخدمي الإنترنت في المجتمع السعودي وخاصة فيما يتعلق بالجرائم الجنسية ، جرائم الاختراقات ، جرائم القرصنة والجرائم المادية وجرائم الارهاب الالكتروني ، مع تحديد أهم المشكلات التي تسببها لمستخدمي الإنترنت في المجتمع السعودي وقد أُندرجت تحتها تساؤلات فرعية وهي كالآتي :

- ما حجم الجرائم الجنسية ، جرائم الاختراقات ، والجرائم المالية ، وجرائم القرصنة ، وجرائم الإرهاب الإلكتروني الموجهة ضد مستخدمي الإنترنت بالمملكة السعودية ؟ ما حجم المشكلات التي تواجههم ؟

3.1.1. منهج الدراسة:

أما منهج المستعمل في هذه الدراسة قد استعملت الباحثة منهج المسح الاجتماعي لعينة من مستخدمي الإنترنت في المملكة العربية السعودية ، واستخدمت أداة الإستبانة لجمع المعلومات الميدانية لهذه الدراسة ، والتي تم تطويرها خصيصا لأغراض هذه الدراسة.

4.1.1. العينة:

تم اختيار عينة الدراسة من مستخدمي الانترنت بالمملكة العربية السعودية من 15 موقعا ليلبلغ عدد العينة 155 ألف مستخدم.

5.1.1. أهم النتائج وعلاقتها بالدراسة :

- أن عددا كبيرا من أفراد العينة وجهت لهم دعوات من المواقع الجنسية عبر الانترنت .
- عدد كبير تعرضوا للتشهير من قبل الأشخاص على صفحات الإنترنت .
- عدد كبير تعرض اقاربهم ومعارفهم للتشهير من قبل الأشخاص على صفحات الأنترنت .
- تعرضوا لدعوات من إحدى المواقع لنشر المواد المقرصنة .
- تعرضوا لإتلاف بسبب المواد المقرصنة .
- تعرضوا لمنضمات وجماعات تنشر أفكار ومبادئ متطرفة .

2.1. الدراسة الثانية

1.2.1. اسم الدراسة:

الجريمة الالكترونية وسبل مواجهتها في الشريعة الاسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، كلية الشريعة والقانون، طنطا، 1436 / 2015م. من اعداد: إبراهيم رمضان إبراهيم عطايا.

2.2.1. اشكالية الدراسة:

إن الجرائم بطبيعتها توجد بوجود الانسان وتتطور بتطوره ، وبما أنَّ الإنسان دائما في تطور مستمر بفضل ثورة المعلومات والتكنولوجيا المتطورة فإننا نجد العلماء والصالحون يحاولون الاستفادة منها ، وبالمقابل نجد أن المجرمين يحاولون الاستفادة أيضا من التقدم التقني



فأصبحت التكنولوجيا كلاً مباحاً للجميع الصالح والطالح ، بل أن المجرمين كثر ، واستطاعوا اكتساب خبرات ومهارات أكثر في تعاملهم مع الأنترنت وارتكابهم للجرائم الإلكترونية عبر الأقمار الصناعية ، ولم تعد جرائمهم تقتصر على اقليم دولة واحدة بعينها بل تجاوزت حدود الدولة ، وهي جرائم مبتكرة ومستحدثة تمثل ضرباً من ضروب الذكاء الاجرامي ، استعصى ادراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية ، مما أوجب تطوير الأنظمة التشريعية الجنائية الوطنية بذكاء تشريعي مماثل لذكاء الاجرامي تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب تلك التقنيات وأبعادها الجديدة ، بما يضمن في كافة الأحوال احترام مبدأ شرعية الجرائم والعقوبات من ناحية ، ومبدأ الشرعية الإجرائية من ناحية أخرى ، وتتكامل في الدور والهدف مع المعاهدات والأنظمة الدولية ، وبهذا كله يمكن الوصول الى سبل مواجهة هذه الجرائم الالكترونية من خلال تعاون الأنظمة الدولية وفهمها لسبل الشرعية والعمل بها في مكافحة هذا النوع من الجرائم المبتكرة والمستحدثة ، فتكثر الاستفادة من هذه الوسائل والأجهزة الإلكترونية ، ويقل خطرها فيسعد وينعم المجتمع ويعيش الجميع في أمان وسلم وسلام .

وتمكن اهمية الموضوع وسبب اختياره فيما يلي :

1. هذا الموضوع أهمية من الناحية النظرية والعملية لكونه يمس كثيراً من مصالح المجتمع ، وعلى وجه الخصوص المصارف من خلال التعامل الإلكتروني والسحب من الأرصدة بواسطة البطاقة الممغنطة أو الدفع الإلكتروني.
2. أيضاً هذا الموضوع يعالج قضية المساس بالحياة الخاصة للأفراد عن طريق التسجيل وغيرها من المجالات التي تدخل في استعمال الحاسوب الآلي .
3. التعرف على أدلة اثبات الجرائم الالكترونية في الشريعة الاسلامية والانظمة الدولية .
4. وفي هذا الموضوع تتجلى عظمة الشريعة الإسلامية في كونها أسبق من النظم الدولية في وضع سبل لمواجهة هذا النوع من الجرائم المبتكرة والمستحدثة ، وفي هذا كله بيان أن الاسلام دين شامل يتناول جميع مظاهر الحياة ، فهو كاف وواف ، وليس في حاجة الى استيراد أنظمة غريبة ، وما على الأنظمة الدولية الا اكتشاف جوهر هذا الدين والعمل بما فيه .

1.2.3. المنهج المتبع:

أما منهج البحث لقد اتبعت هذه الدراسة المزج بين المنهج الوصفي التحليلي والمنهج التاريخي حيث قمت ببيان مفهوم الجريمة وخصائصها ومظاهرها والتحديات التي تقف امام القضاء عليها ، وتوضيح الحكم الشرعي فيها ، مع تحليل المادة العلمية والتعقيب عليها ، مع تتبع المراحل التاريخية لمواجهتها من خلال الأنظمة الدولية .

1.2.4. أهم نتائج الدراسة:

ومن أهم نتائج البحث والتوصيات المقترحة وهي كما يلي :

1. إن الشريعة الاسلامية تمتاز بانها شريعة عالمية تواكب كل زمان ومكان ولا توجد هذه الميزة في غيرها من الشرائع وكذلك الفقه الاسلامي يمتاز بمرونة نصوصه مما يجعله قادراً على استيعاب ما استحدثت من أمور في المجتمعات الحديثة ونلمس ذلك من خلال البحث في مواجهة الفقه الاسلامي للجريمة الإلكترونية وسلامته من العيوب التي لحقت بالأنظمة الدولية التي عنيت بهذا الشأن .
2. الحاسب الآلي والأنترنت لهما إيجابيات وسلبيات والعامل والمنضبط بتعاليم الاسلام وقواعده الفقهية يمكنه كسب هذه الإيجابيات والبعد قدر الامكان عن هذه السلبيات .



3. مرتكب الجريمة الالكترونية في الغالب شخص يتميز بالذكاء والدهاء وذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في نظام الحاسب في حين أن مرتكب الجريمة التقليدية شخص امني بسيط متوسط التعليم .
4. مرتكب الجريمة الالكترونية قد يكون منسجما اجتماعيا وقادرا ماديا إلا أن باعته من ارتكاب جرمته في كثير من الأحيان رغبتة في قهر النظام ، وهذه الرغبة قد تزيد عنده على رغبتة في الحصول على المال في حين أن مرتكب الجريمة التقليدية في الغالب يكون غير منسجم اجتماعيا ، ورغبتة في الحصول على المال تفوق بكثير أي رغبة أخرى .
5. الجريمة الإلكترونية ذات بعد دولي أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية على أساس أن تنفيذها يتم عبر الشبكة المعلوماتية ، وهو ما يثير في كثير من الأحيان تحديات قانونية ادارية فنية بل وسياسية بشأن مواجهتها ، لا سيما في ما يتعلق بإجراءات الملاحقة الجنائية .

3.1. الدراسة الثالثة:

1.3.1. اسم الدراسة:

خصوصية الجرائم المعلوماتية، شهادة الماجستير في القانون العام، كلية دراسات العليا في جامعة النجاح الوطنية في نابلس فلسطين، تحت اشرف فادي شديد ، 2017، من اعداد: نداء نائل فايز المصري.

2.3.1. اشكالية الدراسة:

لقد تناولت الباحثة هذا الموضوع لما له من خصوصية على مستوى التجريم والعقاب ، حيث تكمن هذه الخصوصية بعدم قدرة التشريعات التقليدية على احتواء هذا النوع من الجرائم ، بسبب ما يميز هذه الجرائم من طبيعة متجددة ومتغيرة فهي مرتبطة بتطور التقنيات ، ومن حيث أركانها فهي تختلف عن الجريمة التقليدية في أركانها الأساسية المكونة للجرم وفي طبيعة ونوع العقوبات الرادعة لهذه الجريمة ، أما بالشق الاجرائي كان لهذه الخصوصية الأثر الواضح في عدم اتساع قوالب التشريعات الإجرائية التقليدية في مواجهة هذا النوع من الجرائم بحيث يواجه رجل القانون الكثير من الصعوبات في مرحلة التحقيق الابتدائي سواء من حيث الاجراءات أو بما يتعلق بالدليل الرقمي ومن الجدير ذكره أنه هناك خصوصية على مستوى التحقيق النهائي تبرز في قواعد الإختصاص القضائي المتعلقة للجريمة المعلوماتية فهي جرائم عابرة للحدود وفي سلطة القاضي في قبول الدلة الرقمية حيث أنّ هناك العديد من المواقف الفقهية والتشريعات المختلفة التي تناولت مسألة الإثبات بالدليل الرقمي وعليه تعتبر هذه الدراسة بمثابة تحليل للنصوص القانونية التقليدية المطبقة على الجرائم المعلوماتية وبيان أوجه القصور في هذه النصوص ومحاولة وضع خطوط ريفية يجب أن يلتفت اليها المشرع عند اعداد او صياغة اي تشريع يتعلق بالجرائم المعلوماتية .

وتنبع الأهمية النظرية للدراسة من الجدل الفقهي القائم حول اعتناق تشريع خاص للحد من الجريمة المعلوماتية فالبعض يرى أن هناك حاجة ملحة لوجود تشريع خاص بالجرائم المعلوماتية يعالج الجانب الموضوعي من جهة والجانب الإجرائي من جهة أخرى والبعض الآخر يرى إن الطريقة الفضلى هي دمج نصوص في قانون العقوبات التقليدي من خلال طرق مختلفة، بالإضافة الى أهمية الموضوع المنوي تناوله وهو الجريمة المعلوماتية ، فتبرز أهميته في مدى الخطورة التي باتت تشكلها تلك القضية من خطر كبير على أعمال مؤسسات والمنظمات حتى على الشخصا ، حيث أن تلك الجريمة باتت تطل جميع شرائح المجتمع ، ولا بد من وجود قواعد تشريعية موضوعية واجرائية للحد من هذه الظاهرة .

أما أهداف الدراسة فحاولت هذه الدراسة تحقيق الأهداف التالية :

1. التركيز على خصوصية الجريمة المعلوماتية ومدى اختلافها عن الجريمة التقليدية .
2. الوصول الى قوانين مستحدثة تتسع لقوالب الجريمة المعلوماتية.



3. إيجاد حلول قانونية لتحقيق التوازن بين مصلحة المجتمع في الاستفادة من الثورة المعلوماتية من جهة ، وحق الفرد في حماية خصوصيته من جهة أخرى .

1.3.3. المنهج المتبع:

أما منهج الدراسة فقد اتبعت الباحثة منهجا تأصيليا وتحليليا ومقارنا ، فهو أولا منهج تأصيلي يرجع بالنقاط التفصيلية الى اصولها النظرية، فعند معالجة أي صورة من صور الجريمة المعلوماتية نردها الى الأركان العامة في التجريم كالتحقيق مثلا فنرده الى النظرية العامة لتحقيق، أما المنهج التحليلي الذي اتبعته الباحثة فهو قائم على التحليل النصوص القانونية ذات الصلة ، بالإضافة الى شرح وجهات النظر الفقهية والقانونية المختلفة، كذلك لقد استعانت الباحثة بالمنهج المقارن من خلال عرض مواقف عدة دول المتمثلة في التشريعات المختلفة لمعالجة الجرائم المعلوماتية .

تمحورت مشكلة الدراسة حول الجرائم المعلوماتية ، وترى مع انتشار الجريمة المعلوماتية تزداد خطورة هذه الجريمة ، وتتسع الآثار السلبية لثورة تقنية المعلومات ، ويزداد الجناة اجراما في ما تتعاضم خسائر المجنى عليهم من هنا جاءت هذه الدراسة لمحاولة التعرف على أكثر الجرائم حداثة في هذا العصر ، وقد أثار البحث تساؤلات عديدة منها :

ما مفهوم الجريمة المعلوماتية والأركان العامة لهذه الجريمة ؟

ما العقوبات اللازمة للحد من هذه الجريمة ؟

ما الاجراءات الواجب تتبعها عند وقوع جريمة معلوماتية ؟

وعليه تبلورت الاشكالية الجامعة المانعة لهذه الدراسة والمتمثلة في :

ما هي خصوصية التنظيم القانوني لجريمة تقنية المعلومات ؟

وقد أجابت على هذه الإشكالية على مستوى التجريم والعقاب وهذا في (الفصل الاول) ، ومن ثم على مستوى التتبع والملاحقة وهذا في (الفصل الثاني)

1.4.3. أهم نتائج هذه الدراسة:

أما في الأخير توصلت هذه الدراسة أن الجريمة المعلوماتية أهمية كبيرة لدى المشرعين ، فهي موضوع العصر في القانون الدولي والإقليمي ، حيث كان لهذا البحث أهمية كبيرة في تسليط الضوء على بعض الجرائم المعلوماتية وكذلك اجراءات التحقيق بشقيه الابتدائي والنهائي ، لذلك تعتبر هذه الدراسة بمثابة تقييم للنصوص القانونية التقليدية ، وفيما يلي عرض لأهم النتائج والتوصيات التي توصل اليها الباحث :

1. إن الجرائم المعلوماتية أصبحت تمثل أهمية كبرى للمجتمع وخصوصا بعد ظهور أنماط جديدة منها ، بالإضافة الى أن هناك أنماط شائعة إلا أنها تتمتع بخصوصية ومن أبرزها جريمة الدخول الالكتروني ، وجريمة التلاف البيانات الإلكترونية ، وجريمة التزوير.

2. تثير الجرائم المعلوماتية الكثير من الصعوبات في مجال الحصول على الأدلة الجنائية ، فالحقق إعتاد على كون محل الجريمة شيء مادي وملسوس ، على عكس البيئة المعلوماتية ذات الطبيعة المعنوية التي يصعب معها تطبيق اجراءات ووسائل الاثبات التقليدية .

3. يتسم التحقيق بالجرائم المعلوماتية بصعوبة وتعقيد بالغين وذلك لعدم إلمام رجال الشرطة والمحققين بمجالات الحاسب الآلي والأنترنت ، وعدم تدريبهم على آليات الوصول الى الأدلة المعلوماتية والحفاظ عليها من التلف والضياع .

4. يوجد قصور في القواعد والتشريعات الاجرائية الواجب اتباعها في مرحلة التحقيق الابتدائي ومرحلة المحاكمة .



5. ضعف قدرة القاضي على التقدير أو ما يسمى القناعة الوجدانية لأن ثقافته لا تسعفه على ادراك أو استنتاج الحقائق المتعلقة بأصالة الدليل الالكتروني .

1.4.4. الدراسة الرابعة:

1.4.1. اسم الدراسة:

دراسة مقارنة التحقيق في الجريمة الالكترونية وإثباتها في فلسطين، كلية الحقوق والادارة العامة، جامعة بيرزيت، رام الله فلسطين، 2016، من اعداد: مصطفى عبد الباقي.

1.4.2. اشكالية الدراسة:

لقد تمحورت هذه الدراسة في التحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة الرقمية وجعلها من الموضوعات المستجدة في فلسطين وغيرها من دول العالم ، كما أن طبيعة الادلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات ذات الأهمية القانونية والعملية ، ويقوم بالتحقيق في الجرائم الالكترونية نيابة متخصصة وفقا لإجراءات وقواعد إثبات خاصة . يساعدها في ذلك ضابطة قضائية متخصصة بالجرائم الالكترونية ، على عكس الجرائم التقليدية التي تختص بالتحقيق فيها النيابة العامة تساعدها الضابطة القضائية ذات الاختصاص والإثبات التقليدية .

ويعترض عمل النيابة العامة والضابطة القضائية العديد من الصعوبات من أهمها القصور التشريعي وضعف التخصص لدى القائمين على التحقيق وجمع أدلة من هذا النوع من الجرائم ، إنّ تعزيز وتقوية التحقيق في الجرائم الإلكترونية يقوم على وضع إجراءات إدارية لقسم التحقيق لضمان السيطرة الفعّالة على قضايا الجرائم الالكترونية ، إضافة الى وضع مبادئ توجيهية للأدلة الإلكترونية الجنائية وصولا الى تحقيق نجاح وفعّال للجرائم الإلكترونية

أما أهمية الدراسة وأهدافها، فتأتي هذه الدراسة في الشق الاجرائي الشكلي استكمالا لدراسة سابقة للمؤلف (باللغة الانجليزية) في الشق الموضوعي للجرائم الالكترونية ، وتتبع الدراسة اهمية من أهميات الموضوع التي تعالجها، فالتحقيق في الجرائم الالكترونية وكيفية ضبط الأدلة الرقمية وجمعها من الموضوعات المستجدة في فلسطين ، كما أنّ طبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات ذات الأهمية القانونية والعملية ، لذلك تسلّط هذه الدراسة الضوء على كيفية التعامل القاضي مع الأدلة الرقمية وكيفية وزنه لها وتحديد قيمتها في الإثبات الجزائي ، كما تتبع أهمية الدراسة من معالجتها لجوانب النقص في النظام القانوني والتطبيق العملي في فلسطين .

وتهدف الدراسة الى الخروج بتوصيات للمشروع الفلسطيني لتعديل القوانين ذات العلاقة ، أما فيما يتعلق بالتحقيق الجزائي والقاضي فتهدف الدراسة الى تقديم توصيات وإرشادات تساهم في تحسين الأداء ، كما تهدف هذه الدراسة الى تسهيل إجراءات التحقيق وموائمة السياسات وصولا الى تحقيق فعال في الجرائم الإلكترونية ، كذلك تهدف الدراسة الى فحص وتحديد العوامل المؤثرة في الوصول إلى تحقيق جنائي ناجح والتغلب على الصعوبات والمعضلات التي تعترض طريقه.

أما إشكالية الدراسة، فقد أنشأت في الشرطة الفلسطينية مؤخرا وحدة تحقيق في الجرائم الإلكترونية وجمع أدلتها ، قوامها عدد محدود من الكوادر والأجهزة والبرامج ، يعترض عمل هذا القسم العديد من الصعوبات ، من أهمها القصور التشريعي وعدم ملائمة نصوص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 لتحقيق وجمع أدلة من هذا النوع من الجرائم ، فالقانون المذكور لا يشمل على نصوص توضّح كيفية التعامل مع الأدلة الالكترونية (الرقمية / غير المادية) خاصة ما يتعلق بضبط وتخزين الأدلة الرقمية ، أو قيمتها في الإثبات ، كما لا يتوافر في النظام القانوني الفلسطيني تعليمات أو إرشادات أو إجراءات معيارية تبين كيفية ضبط وتخزين هذه الأدلة ، كل هذا يشكل عقبة في وجه مأموري الضبط القضائي والنيابة العامة في سبيل القيام بالتحقيق في الجرائم الإلكترونية



وضبط الأدلة الرقمية وجمعها وتحريزها وتسليمها للجهات المختصة ريثما يتم عرضها على المحكمة صاحبة الاختصاص في التثبت من صحتها ووزنها وتقدير قيمتها في الدعوى المنظورة أمامها .

أما أسئلة الدراسة، فقد كان السؤال الرئيسي هو كيف تقوم النيابة العامة والضابطة القضائية في فلسطين بالتحقيق في الجرائم الإلكترونية ؟

وكيف يتم تطوير نصوص قانون الإجراءات الجزائية المخصصة للتحقيق في الجرائم التقليدية وضبط الأدلة المادية وتحريزها لتطبق على التحقيق في الجرائم الإلكترونية وضبط الأدلة الرقمية ؟

هل يأخذ التحقيق في الجرائم الالكترونية بعين الاعتبار سلامة الدليل ، وحماية الحياة الخاصة للمتهم ، وسرية المعلومات التي يحتويها الكمبيوتر وأجهزة الاتصال الذكية ؟.

هل يتوجب على الضابطة القضائية عند قيامها بضبط الأدلة الرقمية أن تستصدر مذكرة تفتيش من النيابة العامة ، أم يجوز لها القيام بذلك دون مذكرة في أحوال الاستثنائية ؟

كيف يتمكن القاضي الفلسطيني من تحقيق الأدلة الرقمية ووزنها وتقدير قيمتها في الإثبات ؟

1.4.3. المنهج المتبع:

أما منهجية الدراسة فقد اعتمدت الدراسة على المنهج الوصفي التحليلي المقارن ، حيث تقدم وصفا للنظام القانوني الفلسطيني المتعلق بالتحقيق في الجرائم الالكترونية وإثباتها ، وتعتمد الدراسة الى استعراض النصوص القانونية المتعلقة بالتحقيق في الجرائم التقليدية وجمع أدلتها ، ومن ثم تحليل تلك النصوص وبيان مدى انطباقها على إجراءات التحقيق في الجرائم الإلكترونية ، وكذلك تبين الدراسة مدى انطباق وسائل جمع أدلة الجرائم التقليدية وإثباتها على تلك المتعلقة بالجرائم الإلكترونية ، كل ذلك من خلال المقارنة مع أنظمة قانونية لدول متقدمة في هذا المجال .

1.4.4. أهم نتائج الدراسة:

وتوصلت الدراسة أن الكمبيوتر والأنترنت خلال الثلاثين سنة الأخيرة روح العصر ومحرك عجلة التنمية ووسيلة الرقي والتقدم في كافة العلوم ، كما يعتبر الكمبيوتر والأنترنت كاتم أسرار قطاعات واسعة من شرائح المجتمع ووسيلة التواصل الرئيسية عبر العالم ، إلا أنهما في المقابل أصبحا للأسف وسيلة ارتكاب جرائم خطيرة عابرة للدول والقارات ، وهي الجرائم الالكترونية ، إن من أهم وسائل مكافحة الجرائم الإلكترونية تجريمها والكشف عنها وعن مرتكبيها وتقديمهم للقضاء بعد جمع أدلة هذه الجرائم ، إلا أن من أهم التحديات التي تواجه المشرع في المستقبل موضوع التجريم والعقاب ، إذ يتوجب الانتباه الى معظم الجرائم الالكترونية مصنفة في كثير من دول العالم على أنها جنح ، وبالتالي الاهتمام بها يقل لمصلحة الجنايات الأشد خطورة وجسامة ، هذه النظرة بدأت تتغير مؤخرا بشكل كلي مع نمو ظاهرة الجريمة الالكترونية وتشعبها ، وكذلك بسبب إنشاء مؤسسات وأقسام تختص بملاحقة وتحقيق في الجرائم الإلكترونية والتي ساهمت إيجابيا في زيادة الوعي بخطورة الجرائم الإلكترونية .

ومن أهم التحديات التي تواجه المحقق الجزائري مسألة الخصوصية ، حيث لا يجوز للمحقق ضبط وتفتيش أجهزة الكمبيوتر وأجهزة الاتصال الذكي التي تعود للمتهم إلا وفقا لقيود وضوابط ، وخلال هذه الفترة اللازمة للحصول على الإذن المطلوب يخشى ضياع تلك الأدلة الرقمية ، خاصة أنها من النوع السريع التغير والتلف ، فقد ألزمت اتفاقية بودابست الدول الأطراف عند تطبيق النصوص الإجرائية المتعلقة بالتحقيق في الجرائم الإلكترونية وجمع أدلتها الخضوع للشروط والضمانات المتعلقة بحقوق الإنسان والحريات المنصوص عليها في قوانينها الداخلية ، وفي الاتفاقية الأوروبية لحقوق الإنسان لعام 1950 ، والعهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966 والمعاهدات والمواثيق الأخرى ذات العلاقة .



إلا أن الاتفاقية ألزمت الدول الأعضاء أيضا اعتماد التشريعات والمعايير الأخرى الضرورية لتمكين السلطات المختصة الطلب من المشترك تسليم المعلومات الرقمية الضرورية التي يحوزها في جهاز الكمبيوتر الخاص به أو أي من أدوات تخزين المعلومات ، وكذلك من مزود الخدمة لتقديم معلومات تتعلق بالمشترك ، من قبيل نوع الخدمة المقدمة للمشارك ، الشروط التقنية ، مدة اشتراكه في الخدمة ، هويته ، عنوانه الجغرافي والبريدي ، رقم هاتفه ، طريقة الدفع ، وأية معلومات أخرى متوفرة من خلال عقد اشتراك أو من خلال جهاز تزويد الخدمة ، ويشهد العالم في الآونة الأخيرة تعاظم سطوة مؤسسات إنفاذ القانون في دول العالم قاطبة على حساب حريات وخصوصيات الأفراد ، فمثلا ، بموجب قانون باتريوت " في الولايات المتحدة ، أعطيت مؤسسات إنفاذ القانون صلاحيات واسعة للتصنت والمراقبة واسترجاع المعلومات ذات العلاقة بالتمهين والأمر بفك الشيفرة .

وبالتركيز على الواقع التشريعي والعملي في فلسطين، تم الوصول الى الاستنتاجات التالية :

1. يعاني التحقيق الإلكتروني في فلسطين من الفراغ التشريعي ، فغياب أو النقص في التشريعات والمبادئ التوجيهية المتعلقة بالتحقيق في الجرائم الإلكترونية يقود الى تدني مستوى أداء قسم التحقيق في الجرائم الإلكترونية في الشرطة .
2. عدم ملائمة نصوص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 للتحقيق وجمع أدلة الجرائم الإلكترونية . فالقانون المذكور لا يشتمل على نصوص توضّح كيفية التعامل مع الأدلة الإلكترونية الرقمية ، خاصة ما يتعلق بضبطها وتخزينها ، أو قيمتها في الإثبات ، كما لا يتوافر في النظام القانوني الفلسطيني تعليمات أو إرشادات أو إجراءات معيارية تبين كيفية ضبط وتخزين هذه الأدلة . من ناحية أخرى ، لم يعالج قانون الإجراءات الجزائية الفلسطيني التفتيش عن بيانات الحاسوب وبيانات مرور أجهزة الإتصال السلكي واللاسلكي سواء بمذكرة أو بدون مذكرة .

1- لا يوجد حتى الآن قانون يتعلق بالخصوصية في فلسطين ، ولا توجد نصوص قانونية تتناول خصوصية الفضاء الإلكتروني أو تنظيم الخصوصية في الفضاء الإلكتروني ، وإن كان هناك بعض النصوص المتناثرة في قوانين مختلفة ، إلا أن أيًا منها لا يشكل نظاما كافيا وشاملا .

2- على الرغم من أن الأدلة الرقمية تلعب الآن أدوارا متعاظمة في إثبات الجرائم في الدول المتقدمة مع تنامي ظاهرة الجرائم الإلكترونية وتطور وسائل مؤسسات إنفاذ القانون في الإثبات ، إلا أن الوضع في فلسطين على عكس ذلك ، حيث لا تزال الأدلة الرقمية غريبة عن النظام القانوني الفلسطيني ، وبالتالي غير معمول بها بشكل جدي حتى الآن فالقوانين المعمول بها في فلسطين قد وضعت لتناسب الأدلة المادية فقط

3- إن مبدأ حرية إثبات ومبدأ القناعة الوجدانية للقاضي ، الذين ورد النص عليهما في قانون الإجراءات الجزائية الفلسطيني يعطيان للقاضي الجزائي مكنة الأخذ بالدليل الإلكتروني ، فالقاضي الجزائي ، على عكس القاضي المدني ، غير مقيد بأدلة إثبات محددة ، إنما يستطيع أن يلجأ إلى أي دليل ، بما فيها الأدلة الإلكترونية ، طالما كانت أدلة قانونية وتم الوصول إليها بطرق قانونية وتم طرحها في جلسات المحاكمة ومكّن الخصوم من مناقشتها ، هذا من ناحية ، وطالما اقتنع بها القاضي ، من ناحية أخرى



5.1. الدراسة الخامسة:

1.5.1. اسم الدراسة:

الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها

قطر، 2015، من اعداد: عبد الرحيم

2.5.1. اشكالية الدراسة:

تكمن أهمية الدراسة الى أنها:

1. تتناول موضوعا من الموضوعات الحيوية التي لها تأثيراتها وعواقبها المباشرة وغير المباشرة على الأفراد والمؤسسات ، فكل من يستخدمون تكنولوجيا المعلومات والاتصالات هم عرضة وهدف للجرائم الإلكترونية .
 2. تعمل على تشخيص الوضع الراهن للجرائم الإلكترونية في دول مجلس التعاون الخليجي للوقوف على ظواهرها وأسبابها الحقيقية .
 3. تبحث في كيفية تحقيق التكامل بين دول مجلس التعاون الخليجي من أجل توفير حماية إلكترونية على درجة عالية لتخفيض الجريمة الإلكترونية والهجمات التي تتعرض لها المواقع الإلكترونية .
 4. تركز على موضوع الجريمة الإلكترونية وكيفية مواجهتها في ضوء المعطيات الحالية التي ادت إلى زيادة انتشار الجريمة الإلكترونية وارتفاع تكاليف معالجتها.
 5. تقوم بتحليل الموضوع من زوايا وأبعاد مختلفة للوصول إلى الدوافع الكامنة والمسببات الرئيسية التي تدفع وتشجع مجرمي الانترنت على ارتكاب هذه النوع من الجرائم .
- أما أهداف الدراسة، فتهدف الدراسة الى وضع تصور لاستراتيجية لمواجهة الجريمة الإلكترونية والمساهمة في تخفيضها وتقليل الآثار السلبية المترتبة عن حدوثها في دول مجلس التعاون الخليجي . بحيث تتضمن الاستراتيجية ما يلي :
- الأهداف الاستراتيجية المطلوب تنفيذها .

- الآليات والأدوات والمنهجيات العلمية التي سيتم استخدامها في تحويل الاستراتيجية الى واقع ملموس .
 - وضع آلية لتوعية مستخدمي الإنترنت بكيفية حماية أنفسهم من الوقوع تحت سيطرة الجريمة الإلكترونية
 - صياغة تصور لتحقيق التكامل والتعاون بين دول المجلس لضمان تنفيذ الاستراتيجية
- أم مشكلة الدراسة كانت تتمحور على أن هناك خطرا دائما وجرائم مستمرة تواجه مستخدمي شبكة الإنترنت ، وقد تأخذ هذه الجرائم اشكالا متعددة مثل التخريب للأجهزة أو سرقة البيانات أو الأموال أو الاحتيال أو غسل الأموال أو غيرها ، وأيا كان الشكل الذي تتشكل فيه الجريمة الالكترونية فإنه في النهاية يمثل تهديدا وضرا بالغا بضحايا هذه الجريمة .
- وتشير الدراسة التي قام بها معهد أمن الكمبيوتر في أمريكا computer security Institute في عام 2003 بالتعاون مع مكتب التحقيقات الفدرالي الأمريكي FBI والتي شملت 530 متخصصا في أمن المعلومات في الولايات المتحدة الأمريكية ، أن الأنظمة الإلكترونية في المؤسسات التي يعملون بها تعرضت لاختراقات خلال 12 شهرا التي سبقت الدراسة ، كما أوضحت الدراسة أن الخسائر المالية الناتجة عن الجرائم الإلكترونية خلال هذه الفترة بلغت . 797.340 201 دولار أمريكي ، (Richardson . 2003) .

ويشير تقرير Kasperlab أن الهجمات الإلكترونية الخطيرة تكلف الشركات الكبيرة في المتوسط حوالي 649000 دولار والشركات المتوسطة الحجم تتكلف فاتورة العلاج حوالي 50000 دولار . ففي بريطانيا على سبيل المثال تشير الإحصائيات إلى



أن 18 من المشتركين في خدمة الإنترنت المنزلي قد تعرضوا إلى مثل هذه الجرائم عام 2000 ، بينما ارتفعت هذه النسبة إلى 27 بالمئة عام 2004 ، وإلى 62 بالمئة عام 2006.

وتتعدد الآثار السلبية لهذا النوع من الجرائم ، فمن الناحية الاقتصادية تكلف الدول أموالا طائلة حيث قدرت الخسارة العالمية الناجمة عن تلك الجرائم عام 2007 بنحو 200 مليار دولار ، وتقدر خسائر الأمريكيين وحدهم بحوالي 240 مليون دولار . وأثبتت دراسة عالمية حول " تكلفة الجرائم الإلكترونية عام 2013 " ، أجراها معهد ponemon برعاية شركة hp أن تكلفة وتكرارية الهجمات الإلكترونية في حالة تصاعد

والحقيقة أن توجهات الاقتصاد العالمي المعاصر تميزت بإنتاج مشاريع الكترونية والكهربائية وظهرت أقطاب عالمية جديدة كالصين ، والهند ، وماليزيا ، وتركيا ، ومصر وبعض الدول الأوروبية كإسبانيا ودول أخرى ، والتي رسمت سياسة جديدة للإنتاج هذه المعدات ، اتسمت برفع الكميات المنتجة من جهة وتقليص مدة صلاحيتها من جهة أخرى ، مما طرح في الأسواق مزيد من نفايات هذه الأجهزة ، الشيء الذي أصبح معه من الضروري الوقوف عند هذه الظاهرة ودراسة تأثيرها من الناحية الاقتصادية ، البيئية ، الاجتماعية والقانونية .

وتم عرض في صفحات القليلة السابقة لموضوع الحماية الجنائية للبيئة من النفايات الالكترونية كأحد النفايات الخطرة حيث عرضنا لمفهوم النفايات الخطرة وكذلك المقصود بالنفايات الالكترونية وتدويرها مرور بالحماية الجنائية المقررة للبيئة من النفايات الالكترونية.

1.3.5. أهم نتائج المتعلقة بالدراسة:

خلصت هذه الدراسة الى جملة النتائج وتوصيات على النحو التالي :

1. مشكلة التلوث البيئية وتحديد النفايات الإلكترونية تعد جزء من مشكلة التنمية ولا يمكن إحداث تنمية حقيقية في بيئة تتعرض للتدمير والفساد ، ولذلك فإن شكل الحماية الجنائية يعد مساهمة في إنقاذ البيئة ويعد أيضا شكل من أشكال التنمية الضرورية .
2. النفايات الإلكترونية من القضايا البيئية الخطيرة التي أصبحت تهدد مسيرة الحياة وهي مشكلة مواكبة لكل تطور ونمو عمراني وصناعي فضلا عن كونها من المشاكل العالمية التي تهدد كل دول العالم .
3. التلوث بالنفايات الالكترونية لا يقتصر على جزء من إقليم دولة واحدة ، بل يمتد أثره ليتعدى حدود أكثر من دولة ، فالتلوث لا يعترف بالحدود الدولية .
4. إن مسألة سلامة تناول النفايات الخطرة وتركها وتخزينها ثم التخلص منها هي من أكبر التحديات التي ستواجه الصناعة والحكومات في العقود القادمة .
5. أن إقرار المسؤولية الجنائية والمدنية عن أضرار التلوث الناتج من النفايات الإلكترونية بإعتبارها أحد النفايات الخطرة على مستوى القانون الداخلي والدولي يحقق التكامل بين الأنظمة الداخلية والقانون الدولي .
6. أن النصوص القانونية وتحديد الجنائية على درجة عالية من الإحكام والإتقان إلا أنها ما زالت قاصرة عن مواجهة المشكلات البيئية عامة والمشكلات الخاصة بالنفايات الإلكترونية خاصة .



2. الدراسات الجزائرية:

1.2. الدراسة الأولى:

1.1.2. اسم الدراسة:

الاسرار المعلوماتية وحمايتها الجزائرية

أطروحة مقدمة لنيل شهادة الدكتوراه علوم، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، من إعداد الطالبة راجحي عزيزة، تحت إشراف أ. د. تشوار جيلالي، 2018

2.1.2. اشكالية الدراسة:

لقد تمحورت هذه الدراسة على الأسرار المعلوماتية في البيانات السرية المعالجة آليا وهي ما نعبر عنه بالمعلومات ، ولا يدخل في نطاق المعلومات بالمفهوم الحديث كل ما يمكن أن يطلق عليه مجازا معلومات ، فالمعلومة محل الحماية القانونية الجزائرية ، لا بد من أن تتصف بالسرية . وبالتالي ، فإن موضوع الحماية الجزائرية للأسرار المعلوماتية يشمل حماية كل الأسرار المعالجة آليا من كل أنواع الاعتداءات ما تعلق منها بالاطلاع المجرد أو استعمالها لأغراض غير مشروعة كالإفشاء والسرقة أو اعتراض طريقها وغير ذلك من السلوكات المستحدثة الماسة بحق صاحب المعلومة في الحفاظ على سريتها ، طبعاً بالوسائل الفنية ذات الحدين التي تعتبر من جهة أهم وسائل المعالجة والتخزين والارسال ومن جهة أخرى هي ذاتها الوسائل التي سهلت انتهاك سرية المعلومات . وعليه تهدف هذه الدراسة الى التعرف على سلوكيات الجريمة الماسة بأسرار المعلوماتية وكيفية إثباتها خاصة إذا كانت عبارة للحدود ، وماهي التحديات التي فرضتها هذه الأخيرة على جهات التحقيق والحكم التي تعتبر خط الدفاع الاول في مواجهة ظاهرة الجريمة ، والتي تعمل على تنمية قدرتها وتطوير إمكانياتها بصورة تواكب تطور أساليب الجريمة وتنوعها . وللإجابة على التساؤلات السالفة.

3.1.2. المنهج المتبع:

هذه الدراسة اتبعت منهجين يتم الاعداد عليهما هما المنهج التحليلي والوصفي ، حيث أنه تم اعطاء بعض الشروحات لبعض المفاهيم كما هو الحال بشأن مفهوم السرية والمعلوماتية والجريمة المعلوماتية هذا من جهة ، ومن جهة أخرى سيتم الاعتماد منهج تحليلي من أجل محاولة التدقيق في الجرائم الماسة بالسرية دون غيرها من الجرائم المعلوماتية . وفي بعض المخطات تناولت هذه الدراسة سيتم الاعتماد على المنهج المقارن ، وسبيل بيان الأهداف المنشودة.

4.1.2. اشكالية الدراسة:

من هذا البحث تمت معالجة إشكالية الدراسة وفق لخطة ثنائية تم تقسيمها إلى بابين :

الباب الأول : الاحكام العامة للأسرار المعلوماتية .

الباب الثاني : الجرائم الواقعة على أسرار المعلوماتية في القانون الجنائي وآليات مكافحتها.

إضافة إلى أن المشرع الجزائري اصطلح على الجريمة المعلوماتية بالجرائم الماسة بالأنظمة المعلوماتية وليس هو الوحيد في ذلك ، فهو اختلاف في المصطلحات كما سيتم التفصيل أدناه ، فالجرائم الماسة بالأنظمة المعلوماتية وان كانت تختلف في أركانها وعقوبتها ، إلا أن ما يجمعها أنها تحقق حماية جزائية لنظم المعالجة الآلية للمعطيات ، أي أن القاسم المشترك بينها هو نظام المعالجة الآلية . ويشمل نطاق هذا البحث دراسة الجرائم الماسة بالسرية المعلوماتية التي تقع بواسطة النظام المعلوماتي وعلى النظام محاولين تخطي التقسيمات الفقهية للجريمة



كذلك شملت هذه الدراسة نظام المعلوماتي للحاسب الآلي دون الهاتف الذكي ، نظرا للتشابه الكبير بين الجرائم الماسة بالأسرار المعلوماتية بواسطة الحاسب الآلي والهاتف الذكي ، حيث أن إمكانيات الهاتف الذكي الذي يصلح لارتكاب الجرائم المعلوماتية يعتبر في حكم الحاسب الآلي ، وأيضا على أساس أن الأنظمة المعلوماتية الغالبة حاليا على مستوى الحياة الخاصة والعامة على وجه العموم هي الأنظمة المعلوماتية للحاسب الآلي ، وعلى هذا الأساس أصلا سميت جرائم المعلوماتية باسم الحاسب الآلي أو ارتبطت به كتسمية جرائم الحاسب الآلي والانترنت .

ففي وقت مضى كانت أسرار الشخص تحفظ بوسائل تقليدية ، بينما اليوم تحفظ بوسائل متقدمة لها القدرة العالية على حفظها وعدم المساس بها ، باعتبارها وسائل معلوماتية لا تزال في تطور دائم لخدمة الشخص ، ومع كل ما تتميز به هاته الوسائل من قدرات هائلة على الحفظ فهل ستبقى بها المعلومات في مأمن من أيدي مجرمي المعلوماتية ، هؤلاء الذين يودون انتهاك الأسرار المعلوماتية ولكل منهم دوافعهم .

كان لهذا الموضوع له أهمية كبيرة جدا نظرا لحجم الانتهاك والاختراقات الواقعة على الأنظمة المعلوماتية التي نشهدها يوميا في ظل التطورات التكنولوجية وتزايد المعرفة بالتقنية الحديثة وظهور ما يسمى بالمجرم المعلوماتي ، كذلك يمكن للمعلومات أن تنقل بواسطة الحاسوب والانترنت من أدنى بقاع الأرض إلى أقصاها في ثوان ، حيث يمكن تبادلها بيسر كبير بين الحاسبات الآلية وتصبح هذه المعلومات مادة أولية للإضرار بأصحابها خاصة من حيث الافشاء والابتزاز وغيرها من السلوكيات المجرمة .

5.1.2. أهم نتائج الدراسة:

وتوصلت هذه الدراسة الى تراجع قدرة الشخص على التحكم في سرية معلوماته في ظل قدرات أجهزة الحاسوب على تخزين واسترجاع قدر كبير من المعلومات في وقت قصير عن مختلف أوجه الحياة ، فالقدرة الهائلة للحاسوب في تخزين المعلومات في أقل فترة ممكنة وفي أضييق حيز ممكن وحفظها داخل الذاكرة الحاسب بصفة دائمة.

2.2. الدراسة الثانية:

1.2.2. اسم الدراسة:

التحقيق الجنائي في الجرائم الإلكترونية.

أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، تخصص قانون، جامعة مولود معمري تيزي وزو، تحت إشراف د. اقلولي محمد، 2018 ، من اعداد: براهيم جمال.

2.2.2. اشكالية الدراسة:

لقد تناولت هذه الدراسة أشكال الإجرام الجديدة التي أفرزتها بيئة المعالجة الآلية للمعطيات والتنبه لأثارها السلبية ، بدأت مهمة معالجتها تحظى باهتمام متزايد من الحكومات وحتى العديد من الهيئات الدولية ، فأخذ الفنيون وخبراء الحسابات والإعلام الآلي ، يركزون جهودهم البحتة وتجاربهم العلمية على سدّ ثغرات الأنظمة الأمنية وتحسين وتطوير أساليب الحماية الفنية للنظم والبرامج المعلوماتية لتصل إلى أقصى درجة ممكنة من الفعالية تجنباً لوقوع اعتداءات عليها و بواسطتها ، وتكفل الفقهاء الجنائي بإبراز أوجه القصور التي تعترى تطبيق النصوص الإجرائية للتشريعات التقليدية القائمة على النمط الإجرامي الجديد الذي أسفرت عنه المعلوماتية ، وسعى المشرع إلى تدارك هذا القصور باستحداث نصوص قانونية إجرائية تحمل معها طرقا إجرائية مدعّمة من قبل التقنية ذاتها ، تمكن رجال العدالة الجنائية من البحث والتحقيق واستنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم . ومن ثم تحقيق التوازن بين الضرورة الملحة في عصرنا إلى الاستفادة من إمكانيات الحسابات وتقنيات التكنولوجيا الحديثة ، وبين الحاجة الفردية والاجتماعية إلى الحماية الجزائية من انعكاسات هذه التقنيات .



من هنا ظهرت أهمية موضوع " التحقيق الجنائي في جرائم الالكترونية " وسبب اختيارهم له رغم ما يكتنفه من صعوبات ترجع في الأساس الى حداثة هذا الموضوع وما يتسم به من صبغة علمية بحثية جديدة غريبة في تصورنا على رجال القانون ، إذ لم ينل حظه بعد من البحث والتمحيص على المستوى الفقه الجنائي ، كما أن معظم الدراسات والأبحاث القانونية التي عنيت بالجرائم الالكترونية تركزت على الجانب الموضوعي فقط ، ما نتج عنه قلة وندرة المراجع والمؤلفات التي تعرضت للجانب الإجرائي . وهو ما أثار اهتمام للبحث وإثراء النقاش القانوني في هذا الموضوع ، من خلال تحقيق مقصدين أساسيين، المقصد الأول فهو نظري ، نسعى من خلاله إلى التعرف على طرق وآليات التحقيق في مثل هذه الجرائم ، وما هي العقوبات الاجرائية التي تصطدم بها سلطات البحث والاستدلال في التعامل معها ، ثم اقتراح الحلول القانونية المناسبة والممكنة لتجاوز هذه العقوبات . للاستفادة منها في المواجهة الفعالة للجرائم الالكترونية ومواكبة تطوراتها.

وأما المقصد الثاني فهو تطبيقي ، ينبع من كون هذه الدراسة تأتي في وقت تهم فيه عدة دول بما فيها الجزائر إلى إعادة النظر في قوانينها في إجراءات الجزائية ، مما يتيح لهذا البحث المتواضع في توجيه أنظار المشرع في هذه الدول إلى ضرورة مسايرة تشريعاتها للتطورات التكنولوجية وما تطرحه من مشاكل ، واستدراك وتغطية الفراغ التشريعي الملحوظ في هذا المجال ، وإلزامه ببعض المقترحات التي نوردتها بعد تسليط الضوء على آخر ما توصلت إليه الدول المتقدمة في علم القانون لمواجهة الإجرام الإلكتروني المتطور .
وأما عن الإشكالية التي يطرحها موضوع دراسة، فتصب أساسا حول إبراز إلى أي مدى يمكن الاعتماد على إجراءات التحقيق التقليدية لإثبات جرائم إلكترونية ارتكبت في عالم افتراضي غير ملموس ، وهل تطبيق هذه الإجراءات كافيا وفعالا لاحتواء متغيرات هذا النمط المتجدد والمتطور من الجرائم ، أم أن ذلك سيؤدي إلى عدم الوفاء بمتطلبات مبدأ الشرعية الإجرائية وما ينجر عن ذلك من عقبات؟

3.2.2. المنهج المتبع:

وللاجابة عن هذه الإشكالية اعتمدوا على المنهج الوصفي التحليلي ، لأن دراسة تركزت على وصف المفاهيم العامة الخاصة بالإجراءات المتبعة للبحث والتحقيق في جرائم الالكترونية لاستخلاص الدليل والعقوبات التي تعترها وتحليلها، لأنها تستعرض أهم الإشكالات القانونية التي تطرحها المواجهة الإجرائية للجريمة الالكترونية ، ثم مناقشتها وتحليلها بشكل من التفصيل والتشريح بالخوض في جزئياتها ، من ثمة تقديم الحلول المناسبة على ضوء ما توصل إليه الفقه والتشريع والقضاء المقارن، وأتبع في ذلك خطة تتضمن بابين الأول تحليل آليات التحقيق في الجرائم الإلكترونية ، من خلال التأكد في الفصل الأول من محدودية سريات إجراءات التحقيق المألوفة على الجرائم الإلكترونية ، أما الفصل الثاني استعراض إجراءات التحقيق المستحدثة . وأما الباب الثاني فقوامه إبراز عقوبات التحقيق في الجرائم الإلكترونية والحلول المقترحة لتجاوزها، من خلال التركيز في الفصل الأول على تبيان عقوبات التحقيق في الجرائم الالكترونية ، وتخصيص الفصل الأول على تبيان عقوبات التحقيق في الجرائم الالكترونية ، وتخصيص الفصل الثاني لاقتراح الحلول الممكنة لتجاوز هذه العقوبات .

وتتضمن هذه الدراسة في متنها إيضاحا لرؤية إجرائية تتناول مسألة البحث والتحقيق الجنائي في الجرائم الإلكترونية ، والمشكلات الإجرائية المترتبة عليها ، وكذا الحلول الممكنة المقترحة لمعالجة تلك المشكلات .

4.2.2. أهم نتائج هذه الدراسة:

وقد اتضح في هذه الدراسة أن الجرائم الإلكترونية تعد من الأنماط الإجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد ، والتي تتميز بخصائص مختلفة تماما عن الجرائم التقليدية ، وأنا من المستجدات التي لم تكن معروفة في القانون الجزائي بشقيه الموضوعي والإجرائي ، ومن ثمة فأي محاولة للتعامل إجرائيا مع هذا النمط الإجرامي الجديد في إطار عملية البحث



والتحقيق سوف يخلق إشكالات إجرائية أمام السلطات المكلفة بهذه العملية، وتتجلى أولى هذه الإشكالات في القصور الذي يعتري النصوص الجزائية الاجرائية القائمة في مواجهة مثل هذه الجرائم ، لأن أحكام هذه النصوص إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها مع خضوعها لمبدأ حرية القاضي الجزائري في الاقتناع.

وقد تبين أنه من أجل تغطية وتلافي هذا القصور من جهة ، وتفادي إفلات المجرم الالكتروني من المتابعة الجزائية والعقاب ، بادر المشرع في الكثير من الدول إلى إعادة النظر في بعض القواعد الإجرائية المتعلقة باستخلاص الدليل كالتفتيش والضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية الالكترونية، فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع الطبيعة الخاصة التي يتميز بها هذا النوع من الجرائم ، كالمراقبة الالكترونية واعتراض المراسلات والتسرب الالكتروني ، وهو ما أقدم عليه المشرع الجزائري .

وقد أظهرت الدراسة كذلك أنه من المشكلات التي تواجه سلطات البحث والتحقيق ما يتعلق بالقيمة القانونية للأدلة الالكترونية المتحصل عليها في عملية الإثبات الجنائي أو بمعنى آخر مدى قبول هذه الأدلة كوسيلة إثبات من طرف القاضي الجزائري، إذ أن عملية استخلاص الدليل الإلكتروني سواء بالطرق الإجرائية التقليدية أو المستحدثة ليست بالسهولة بما كان، بل تعيقها في غالب الأحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الالكتروني أو بالعامل البشري، كما أن مجرد وجود دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين قد لا يكفي للتعويل عليه ، بل يلزم أن يكون لهذا الدليل قيمة قانونية ، التي تتوقف على مسألتين ، الأولى هي مشروعية الدليل ، والثانية هي حجيته على الوقائع المراد إثباتها .

فالأدلة الالكترونية وإن كانت تتمتع بقيمة علمية قاطعة في الدلالة على الحقائق التي تتضمنها ، إلا أنّ ذلك لا يغني عنها أن تكون مشروعة ، سواء من حيث الوجود ، بأن تكون من ضمن الأدلة المقبولة قانونا كوسيلة إثبات . أو من حيث التحصيل ، وذلك بأن يتم الحصول عليها بالطرق القانونية وأن تقدم للمحكمة على الهيئة نفسها التي تم جمعها عليها ، بدون أن يطرأ عليها أي تغير أو تحريف خلال فترة حفظته .

وقد استخلصت في نهاية هذه الدراسة أيضا بأن مسألة قبول الدليل الالكتروني من عدمه إنما تخضع لمطلق تقدير القاضي الجزائري ، الذي يتمتع بدور إيجابي في مناقشة وموازنة القيمة القانونية للدليل الالكتروني قبل أنّ يطمئن إليه ، شأنه شأن باقي الأدلة ، ولكن أكدنا في الوقت نفسه أنه لا يجب الخلط بين القيمة العلمية القاطعة للدليل الالكتروني ، التي لا يملك للقاضي الفصل فيها لأنها مسألة فنية بحتة والقول فيها هو قول أهل الاختصاص ، وبين الظروف والملابسات التي تحيط بالدليل ، والتي يجوز للقاضي أن ينصب نفسه فيها مكان الخبير وي طرح رأيه وفق أسباب سائغة مقبولة ، وله في ذلك أنّ يرفض هذا الدليل إن لم يقتنع بظروف القضية وملابساتها، بالموازاة مع ذلك اتضح أن عملية البحث والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الحديثة تتخللها عقبات كثيرة ، يعود البعض منها إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم ، فالطابع العابر للحدود الذي تتسم به الجريمة الالكترونية قد يثير العديد من المشاكل القانونية ، من بينها تحديد الدولة التي يتخصص قضاءها بملاحقة مرتكب هذه الجريمة ، والمعيير المعتمد في ذلك ، ناهيك عن مشكلة احترام سيادة الدولة التي تقف حاجزا أمام سلطات التحقيق عندما يستوجب البحث عن أدلة إثبات جريمة إلكترونية خارج الإقليم الوطني وفي أقاليم عدة دولية أجنبية ، خاصة إذا اقترن ذلك بغياب وسائل وآليات دولية فعالة تضمن التعاون الفضائي والأمني بين الدول في هذا المجال، إضافة قصور القواعد الإجرائية عن مواكبة تطورات ومتغيرات الجرائم الالكترونية المتسارعة ، ما قد يقف حجر عثرة في سبيل الاستفادة من معطيات التكنولوجيا الحديثة في الكشف عن الجرائم الالكترونية وملاحقة مرتكبيها.



3.2. الدراسة الثالثة:

1.3.2. اسم الدراسة:

آثار استعمال التكنولوجيات الحديثة على أفراد الأسرة الجزائرية دراسة التأثيرات النفسية والاجتماعية والأخلاقية والصحية لاستعمال الأنترنت على بناء الأسرة الجزائرية نموذجاً دراسة على عينة مراهقين مستخدمين للأنترنت بمدينة أم البواقي - الجزائر -، كلية العلوم الاجتماعية قسم علم النفس، أطروحة لنيل الشهادة دكتوراه في علم النفس الاسري، اشراف ميموني معتصم بدر، 2016 من اعداد، صافية أمينة.

2.3.2. اشكالية الدراسة:

هدف هذا البحث إلى دراسة تأثير الأنترنت على المراهقين المستعملين له وذلك على جميع المجالات ؛ النفسية ، الاجتماعية ، الأخلاقية وكذا الصحية ، متطرقين إلى كل من التأثيرات الإيجابية والسلبية تبعا للمتغيرات التالية : الجنس ، مدة الاستعمال ، فترات الاستعمال ، وعدد ساعات الاستخدام اليومي .

3.3.2. المنهج المتبع:

وذلك باستخدام المنهج الوصفي التحليلي من أجل وصف المتغيرات وكل ما يتعلق بالدراسة عينة الدراسة: تمت الدراسة على عينة حجمها 200 تلميذا من تلاميذ المرحلة المتوسطة من مدينة أم البواقي يتراوح سنهم ما بين 13 و 15 سنة من الجنسين ومن معتادي استعمال الأنترنت ، مستخدمين فيها أداتين بحثيتين تتمثل الأولى في استمارة معلومات وبيانات حول عادات استعمال الأنترنت عند التلميذ المراهق ، وتمثلت الثانية في مقياس الآثار النفسية والاجتماعية والأخلاقية والصحية من إعداد الباحثة ، وبعد تمرير الأداتين من خلال المقابلة تمت معالجة المعطيات المحصل عليها بطريقة إحصائية عن طريق SPSS وتم دعم النتائج المحصل عليها بعرض مفصل لمقابلات تمت مع ثلاث حالات من مراهقي العينة المستخدمين للأنترنت كما خضعت الدراسة لمجموعة من الأساليب الإحصائية : النسب المئوية ، التكرارات ، T - test ، وتحليل التباين الأحادي one way anova .

4.3.2. أهم نتائج الدراسة:

حيث جاءت نتائج البحث كالآتي :

✓ لقد أثبتت الأنترنت وجوده داخل الأسرة الجزائرية من خلال استخدامه من طرف أبناءها المراهقين وذلك عند كلا الجنسين وباختلاف مدة الاستعمال وفتراته وعدد ساعاته.

✓ توجد فروق في التأثيرات النفسية والاجتماعية والأخلاقية والصحية لدى المراهقين المستعملين لشبكة الأنترنت تبعا لمتغير الجنس ومتغير مدة الاستعمال ، وتبعا لمتغير فترة الاستعمال ، وكذلك تبعا لمتغير الحجم الساعي اليومي .

✓ اختلفت النتائج بين مستويات شدة التأثير في جميع المجالات (النفسية والاجتماعية والأخلاقية وحتى الصحية) على المراهقين المستعملين للأنترنت بين مرتفع ومتوسط ومنخفض وفي كلي الاتجاهين، الإيجابي والسلبي (

وخلصت الدراسة الى التوصيات التالية أهمها الاهتمام بالمراهق وإشباع حاجياته الاتصالية داخل أسرته عن طريق بناء علاقات أسرية قوية مع توفير المناخ الأسري المناسب ليكون جوّه الاجتماعي الصحيح والحقيقي ليحول دون الإفراط في استخدام الانترنت وخلق جو اجتماعي افتراضي.

سهيل وبارجيز يعود إلى سن عينة البحث ، فسن عينة الدراسة الحالية صغير (13 - 15) مقارنة مع دراسة سهيل وبارجيز (طلاب جامعة) فهذا جعل من أفراد عينة دراستنا لا يبرزون هذه المشاكل الصحية ويوحون بها خوفا من فقدان الموضوع المحبوب وهو الأنترنت



، ونظرا لتعلقهم به مع تفكيرهم المحدود أنه ربما إذا كشف عن آثاره السلبية فسوف يختفي ويذول ، لذا لم يتم الكشف عنها والافصاح عنها .

فمن خلال ما تقوله الباحثة النفسية داليا حنفي " أردنا معرفة تأثير استخدام تقنيات الاتصال على السلوك الاجتماعي فلا يمكننا اصدار حكم عام فالأمر يعتمد أساسا وبالدرجة الأولى على حجم الاستخدام وعدد الساعات التي يقضيها الفرد مستخدما لشبكة الأنترنت".

وهكذا ومن خلال هذه الدراسة التي حاولوا من خلالها التقرب من الاسرة ومحاولة مساعدتها في حل أكبر المشاكل التي تعاني منها من خلال التقرب من ذلك المراهق الذي أصبح يستعمل التكنولوجيات الحديثة وعلى رأسها الأنترنت في حياته اليومية وبذلك أصبح يعد موضوع قلق وتوتر بالنسبة لأسرته من جراء هذا الاستعمال فكان هذا البحث على هذه الشريحة الحساسة داخل أسرتها ومجتمعها ككل، وذلك من خلال دراسة مختلف التأثيرات على جميع المستويات النفسية والاجتماعية والأخلاقية وكذا الصحية التي تطرأ عليه من جراء هذا الاستعمال ، فاتضح من خلال هذه الدراسة مدى أهمية هذه التكنولوجية الحديثة عند أبناء الأسرة الجزائرية ومدى تعلقهم بها محاولين بذلك إخفاء جميع تأثيراتها السلبية وإبراز تأثيراتها الايجابية وذلك بتفاوت في شدة التأثيرات على جميع المجالات والأبعاد كما قد تبين وجود اختلاف في التأثيرات في بعض المجالات تبعا للمتغيرات التالية، الجنس ومدة الاستعمال وفتراته والحجم الساعي المستغرق في ذلك يوميا ولم يتضح وجود أية اختلافات في التأثيرات في مجالات أخرى تبعا لنفس المتغيرات ، وبهذا يمكننا استخلاص من هذه الدراسة وعلى حسب قول الباحثة النفسية أ/ داليا حنفي " إن الحد الفاصل بين ايجابية وسائل الاتصال الحديثة وسلبياتها يتحدد وفقا لطبيعة الاستعمال واذا ما كان في حدود الطبيعة أم ادمانا ... " وانتهت الدراسة ببعض الاستنتاجات نذكر منها ما يلي :

- الاهتمام بالمراهق بمحاولة توفير المناخ الأسري المناسب ليكون جوّه الاجتماعي الصحيح والحقيقي ليحول دون الإفراط في استخدام الانترنت وخلق جو اجتماعي افتراضي.

- بناء علاقات أسرية قوية مع المراهق خاصة (المراهقة المبكرة) من اجل اشباع حاجياته الاتصالية داخل أسرته .

- ضرورة اهتمام الوالدين بالارتقاء بمستواهم العملي والتثقيفي لمسايرة متطلبات المراهقين في هذه المرحلة

3. تفسير السوسيولوجي للدراسات السابقة:

لقد اتفقت هذه الدراسات السابقة في العديد من الجوانب العلمية لدراستنا، ابرزها الجريمة الإلكترونية، وآثارها على الفرد والمجتمع، من خلال الربط بين الجريمة التقليدية بوجه عام والإلكترونية منها بوجه خاص ، فالجريمة مهما كان نوعها فهي ناتجة عن مخالفة الفرد لمجموعة من القواعد التي تنظم سلوك الأفراد في المجتمع والأهداف ، على حساب الهدف الحقيقي هو تنظيم العيش في جماعة بقصد تحقيق الأمن والاستقرار للجميع، لأن الظاهرة الاجرامية هي الحدث اجتماعي موجودة في المجتمع، المرتبطة بالحياة الاجتماعية وظواهرها المختلفة وتستمد مضمونها من الظروف الواقعية للحياة، وقد اختلفت هذه الدراسات حول تحديد نوع العوامل الإجرامية فذهب رأي على أن هذه العوامل فردية دائما تكمن في شخص المجرم سواء تعلقت بتكوينه العضوي حيث يتصف المجرم بسمات معينة أو تعلقات بتكوينه النفسي، وهناك اتجاه آخر يركز على الإجرام أو عوامل الإجرامية لا تعد وأن تكون عوامل بيئية اجتماعية إقتصادية أو سياسية وأسباب هذا التنوع والتعارض فالسلوك الاجرامي يقع على مفترق الطرق مختلف العلوم الإنسانية فهي تم عالم الاجتماع وعالم القانون وعالم النفس والمرئي والطبيب وتدخل إختصاص كل منهم، بحيث أنّ العوامل الاجرامية مزيج من عوامل فردية تتعلق بشخص المجرم وعوامل بيئية تتعلق بالحيث الذي يعيش فيه إذ يتفاعل نوعا العوامل فيتولد عن تفاعلها حدوث الجريمة.



وعليه يمكن القول أن الجرائم الإلكترونية تهدد الكثيرون وهناك عدة طرق لحماية البيانات الشخصية خاصة على الأجهزة الالكترونية ومن هذه الطرق ، تتمثل في المحافظة على تحديث نظام التشغيل والبرنامج لان هذا يجعلنا نحصل على تصحيحات حديثة للأمان ، وهذا يحمي الأجهزة الالكترونية الخاصة بن، و. العمل على استخدام برنامج لمكافحة الفيروسات وجعله محدث، لان استخدام هذا البرنامج يساعد في الحل الكامل لأمن الإنترنت مثل Kaspersky Total Security ، وهي طريقة تعمل على حماية النظام الخاص بك من الهجمات، ويقوم برنامج مكافحة الفيروسات بالسماح لك بفحص واكتشاف وإزالة التهديدات قبل حدوث أي مشكلة ، وأيضا القيام باستخدام كلمات مرور قوية حتى لا يكون من السهل تخمينها ولا القيام بتسجيل تلك الكلمات في مكان آخر أو القيام باستخدام مدير لكلمات يكون حسن السمعة للعمل على إنشاء كلمات مرور قوية بصورة عشوائية..

اما الآثار الاجتماعية تكمن في القيام مجرمون الإنترنت بالاستفادة من الترابط الذي يقوم بتوفير الإنترنت واختفاء السرية والهوية ، ولهذا يقومون بالهجوم على المجتمع الخاص بالمعلومات الحديثة ، لذلك تحتوي الجرائم الإلكترونية على فيروسات الكمبيوتر وشبكات الروبوتات والتسلط من خلال الإنترنت والإرهاب السيبراني والمطاردة عبر الإنترنت وهجمات رفض الخدمة والمواد الإباحية السيبرانية والبرامج الضارة والقرصنة والبريد العشوائي وسرقة الهوية قام المسؤولين بالإنقاذ لقانون المراقبة لمجرمي الإنترنت.

قائمة المراجع:

- 1/- الرواشدة ، سامي حمدان ، مكافحة الجريمة المعلوماتية بالتحريم والعقاب : القانون الانجليزي نموذجا ، المجلة الردينية في القانون والعلوم السياسية مجلد 1 ، العدد 4 دار المنظومة . ص 11.
- 2/- البحي ، تركي بن محمد ، بن عبد الله ، مكافحة الجرائم المعلوماتية في المملكة العربية السعودية ، مجلد2 ، العدد 7 ، دار المنظومة ، ص254.
- 3/- الشوابكة ، محمد أمين ، جرائم الحاسوب والانترنت دار الثقافة للنشر والتوزيع ، طبعة 4 ، 2011 ، ص7.
- 4/- طه ، ابراهيم قاسم السيد ، محمد ، شرح قانون جرائم معلوماتية ، ط2 ، 2015 ، ص2.



تظاهرات العنف والسلوك الاجرامي الرقمي عبر المنصات الالكترونية بالمجتمع الجزائري

على ضوء دراسة استطلاعية ميدانية.

Cybercriminal and violent behavior characterizations on electronic platforms in Algerian society based on a field survey.

ط.د قطاب نورالدين

noureddine.guettab@cu-relizan.dz

ط.د بخيرة أحمد

Ahmed.bekheira@univ-relizan.dz

مقدمة :

إن التقدم الحضاري الذي اجتاحت العالم في العصر الحديث أثر في كافة مناحي الحياة الإنسانية من سلوكيات وغيرها، مخلفا تغيرا اجتماعيا نتيجة الانصهار في مظاهر الإغواء وأشكال الإثارة الحديثة، في ظل تطور تكنولوجي وثورة معلوماتية سهلت العملية التواصلية التفاعلية بين البلدان والأشخاص، إذ نجد عالم اليوم وثيق الصلة بالبيئة الرقمية التي مازال عدد المنتسبين إليها في منحنى متصاعد، ما تسبب في توظيف السلوك الإجرامي والعنف من طرف بعض المستخدمين عبر المنصات الالكترونية والمواقع التابعة لهذا الفضاء من خلال مشاركة مضامين هدفها إلحاق الأذى بالغير أو الإخلال بالنظام العام وغيرها من السلوكات العدائية الموجهة للمجتمع، ويشار إلى أن الأفعال الإجرامية لم تعد تقليدية (مادية) مثلما كانت عليه في السابق وإنما أصبحت ترتكب في عالم افتراضي أصبح المرسل فيه مستقبلا في آن واحد، حيث لم يسلم المجتمع الجزائري كغيره من المجتمعات الأخرى من هذه الظاهرة حين نسمع ونرى ونقرأ يوميا عن سلوكات عنف وإجرام رقمي يرتكب باستخدام مواقع التواصل الاجتماعي، التي أصبحت تستعمل استعمالا سلبيا أثر على الأمن المعنوي للأشخاص، وهذا نظرا لارتفاع معدلاتها التي أكدت كل الدراسات المتخصصة وأشارت إلى دق ناقوس الخطر في الوقت الراهن.

1. تحديد الإشكالية :

تميزت السنوات الأخيرة بظهور نوع جديد من الجرائم والسلوكيات العنيفة عبر الفضاء الافتراضي، وهذا راجع إلى التطور التكنولوجي السريع الذي أفرز بدوره تطبيقات تسهل عملية التواصل بين الأشخاص ونذكر منها المنصات الالكترونية ومنصات شبكات التواصل الاجتماعي بمختلف أنواعها التي ألغت الحواجز الجغرافية والمكانية حين أصبحت السلوكات العدائية عابرة للحدود بلا استئذان، حين أصبح الاستعمال السليبي لها باستخدام الشبكة العنكبوتية من طرف المستخدمين يقدم صورا جديدة من جرائم العنف الرقمي المرتبطة بالتقنيات الحديثة التي شكلت العامل الأساسي في إحداث ثورة هائلة في مجال الاتصالات واستخدامات الحاسب الآلي والهاتف النقال لأغراض مختلفة، وفي نفس الوقت ساهمت في إنتاج وتطوير كثير من السلوكيات التي تعتبر عنفا وإجراما وفقا لقوانين وقواعد التحريم، ولا شك أن لها الأثر البالغ على حياة أفراد مجتمعات العالم وعلى القطاع العام والخاص على غرار المجتمع الجزائري الذي أضحى يواجه العديد من المشاكل التي تجلت في سلوكات إجرامية ومظاهر عنف على المنصات الالكترونية المتضمنة الشبكات والحسابات والمواقع الالكترونية والصفحات المساعدة على التواصل الاجتماعي كالفيس بوك، التويتر، واتس آب، اليوتوب، الفاير، الماسنجر، السكايب، السناشات وغيرها من التطبيقات المختلفة التي سهلت عملية بروز ظاهرة جديدة تعرف بالجريمة الالكترونية



التي تتضمن مجموعة من الأفعال الاجرامية المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب (أمير فرج، 2009 : 106-107) ، ومع الانتشار الواسع للشبكات الاجتماعية في شتى مجالات الحياة وتقييم تأثيراتها السلبية فقد وُصفت منصات التواصل الاجتماعي بالميكانيزمات الافتراضية لنشر الإرهاب والكراهية (بوعمامة، 2016) ، وبالنظر إلى الواقع المعاش نرى أن المجتمع الجزائري يأخذ حقه من ظاهرة السلوكات المضادة للمجتمع المنتشرة بالبيئة الرقمية وبناء على ما تم توضيحه يمكن طرح الإشكال الرئيسي التالي: ماهي تجليات العنف والسلوك الإجرامي عبر المنصات الالكترونية بالمجتمع الجزائري؟ وانبثقت عنه التساؤلات الفرعية التالية:

- 1- ما هي الأنواع وأشكال العنف والسلوك الاجرامي بالمنصات الالكترونية؟
 - 2 - ما هي الأسباب الرئيسية في انتشار العنف والسلوك الإجرامي عبر المنصات الالكترونية بالمجتمع الجزائري؟
 - 3- ما نوع التطبيقات الشائعة والأكثر استعمالا في نشر العنف والسلوك الإجرامي على مواقع التواصل الاجتماعي؟
 - 4- هل النزعة المادية في كسب المال لمستعملي الأنترنت سبب في انتشار العنف والسلوك الإجرامي عبر المنصات الالكترونية؟
 - 5- ما هي السلوكات العدائية والأكثر انتشارا في الفضاء السيبراني؟
- وتبعت التساؤلات فروض فرعية هي كالتالي:

- 1 - من أشكال العنف والسلوك الإجرامي بالمنصات الالكترونية هي النصب والاحتيال.
 - 2- من الأسباب الرئيسية في انتشار العنف والسلوك الإجرامي عبر المنصات الالكترونية بالمجتمع الجزائري ضعف الرقابة الوالدية لأبنائهم خلال استعمالهم للأنترنت.
 - 3- من التطبيقات الشائعة لنشر العنف والسلوك الإجرامي بالمنصات الالكترونية في المجتمع الجزائري هي الفايسبوك.
 - 4- تعد محاولة الكسب غير المشروع للمال سببا في انتشار العنف والسلوك الإجرامي باستعمال الأنترنت.
 - 5- يعد التشهير بالصور والفيديوهات ضد الأشخاص من أكثر السلوكات العدائية الموجهة للغير بالفضاء السيبراني.
- ## 2. أهمية الدراسة :

- معرفة مظهرات العنف والسلوك الاجرامي وتحليلاتها عبر المنصات الالكترونية.
- معرفة أسباب هذه الظاهرة مع توضيح حجمها عبر المنصات الالكترونية بالمجتمع الجزائري.
- معرفة خصائص ودور المنصات الالكترونية ومنصات شبكات التواصل الاجتماعي في انتشار السلوكات المضادة للمجتمع.
- معرفة الأنواع والأشكال المختلفة للسلوك الإجرامي عبر منصات شبكات التواصل الاجتماعي.
- تقديم توصيات اقترح حلول للمشكلات المرتبطة باستخدام وسائل التواصل الاجتماعي بناء على نتائج الدراسة المتوصل إليها.

3. المصطلحات الإجرائية :

3.1. المنصات الالكترونية : هي أرضيات تتمن مواقع من أجل الاتصال والتواصل بين الشركات أو بين الأشخاص عن بعد، وهي قائمة على تكنولوجيا الويب، إذ تعتبر ساحات بواسطتها يتم التفاعل وتبادل الآراء والأفكار والملفات والقيام بأنشطة مختلفة، حيث تنقسم إلى منصات مغلقة تتكون من مجموعة من الأشخاص يمثلون مجتمعا مغلقا أو خاصا كأفراد الشركات أو المنظمات وهناك منصات مفتوحة وهي عبارة عن مواقع متاحة لجميع مستخدمي الأنترنت وهي مصممة خصيصا لجذب المستخدمين للشبكة بحيث يسمح للكثير منهم المشاركة في أنشطة المنصة بمجرد أن يقدم المستخدم نفسه للموقع (هالة عبد القادر، 2019 : 66-67) ، أما إجرائيا فيقصد بها الأرضيات التي تعبر عن المنصات التجارية المملوكة أو المغلقة أو المنصات الحرة المفتوحة المصدر مثل



منصات / شبكات التواصل الاجتماعي التي تتضمن مجموعة من التطبيقات التي تساهم في تنظيم الأنشطة الفردية والجماعية و التي تنتشر عبرها و بواسطتها سلوكات العنف والإجرام.

2.3. الشبكات الاجتماعية : هي تلك الوسائل الحديثة للاتصال والتواصل بين الأشخاص حين تقرهم من بعضهم البعض، وهي متمثلة في الفاييس بوك، التويتر، الواتساب، يوتيوب (بلقرع، 2017: 26) ، أما إجرائيا فيقصد بها كل التطبيقات والمنصات المتضمنة الشبكات الالكترونية التي تسمح للمستخدمين بالتواصل الافتراضي سواء كان مرئي، كتابي، صوتي، بغرض بناء علاقات افتراضية تساعدهم على تبادل الآراء والأفكار والتخطيط للقيام بأنشطة مختلفة و المساهمة في نشر العنف والسلوك الإجرامي بالبيئة الرقمية.

3.3. الجريمة الالكترونية : هي تلك الجرائم التي يكون دور الحاسوب فيها ايجابيا أكثر منه سلبيا (عبد الفتاح، 2006: 24) وهي تعبر أيضا عن النشاط الاجرامي الذي يتم ارتكابه باستخدام الانترنت (Mshana, 2008: 3) أما إجرائيا فيقصد بها مجمل سلوكات العنف والاعتداءات والجرائم المرتكبة بالمجتمع الجزائري باستعمال التكنولوجيا الحديثة سواء الحاسوب أو الهاتف الذكي هذا عبر المنصات الالكترونية ومنصات شبكات وسائل التواصل الاجتماعي.

4.3. المجرم الالكتروني : هو شخص لديه كفاءة وخبرة في استعمال التكنولوجيا الحديثة، بحيث يتميز بالمهارة التقنية والتحكم الجيد في نظام الحاسبات الآلية، أما إجرائيا فيقصد به الشخص يوجه سلوكات إجرامية وأعمال عنف عبر الأنترنت وباستعمال المنصات الالكترونية ومنصات شبكات التواصل الاجتماعي.

5.3. الضحية : تمثل شخص طبيعي أو معنوي يمثل مؤسسة أو قطاع مالي أو شركة ضخمة، أو مجموعة من الأشخاص أصيبوا بضرر فردي أو جماعي بما في ذلك الضرر البدني والمعنوي المؤدي إلى المعاناة النفسية أو الخسارة الاقتصادية أو الحرمان بسبب ممارسات إجرامية منفذة ضدهم بالاعتماد على الانترنت، أما إجرائيا نقصد به ذلك الشخص المجني عليه وهو الذي تفاعل مع المجرم بشكل مباشر أو غير مباشر قبل تنفيذ جرمه عليه، بحيث سهلت عملية التنفيذ استخدامهما للمنصات الالكترونية أو منصات شبكات وسائل التواصل الاجتماعي، إذ تكون الضحية تحمل صفة شخصية معنوية أو شخصية طبيعية، أو هيئة ، كيان ، قطاع ...

4. أنواع جرائم الأنترنت :

1.4. صناعة الفيروسات والتخريب الالكتروني: تستعمل طرق التخريب من قبل قراصنة الحاسب من خلال القنابل الالكترونية ونشر الرسائل المفخخة وإتلاف المعلومات والبيانات وتشويهاها وتعطيل الحواسيب.

2.4. جرائم الملكية الفكرية : وهو ما يعرف بالقرصنة وتشمل نسخ البرامج بطريقة غير قانونية وسرقة البرمجيات التطبيقية.

3.4. تهديد الامن القومي والعسكري.

5. الأشخاص الأكثر عرضة للجرائم عبر المنصات الالكترونية :

تتمثل الخصائص الشخصية لضحايا الجرائم من خلال استعمال وسائل التواصل الاجتماعي بما يلي:

- الأشخاص المصابين بأمراض عقلية.
- الأشخاص ذوي المستوى التعليمي المتدني و الغير المتعلمين.
- الأشخاص الجدد في المدينة.
- الأشخاص الساذجين الذين تنقصهم التجربة في الحياة.
- صغار السن (الأحداث) و العجزة (المسنين).
- أطفال الشوارع.



- السواح الأجانب.

لا تقتصر خصائص الأشخاص الأكثر تعرضا للجريمة على العوامل الشخصية فقط لمستخدمي وسائل التواصل الاجتماعي ، بل هنالك عوامل ظرفية ومكانية تقتزن مع الخصائص الشخصية للشخصية. (البشري، 2005 : 60)

6. أسباب انتشار الجريمة عبر المنصات الالكترونية و منصات/ الشبكات الاجتماعية :

- الانتشار الواسع للإنترنت وسهولة استخدام المنصات الالكترونية وشبكات التواصل الاجتماعي بعيدا عن الرقابة.
- تعدد تطبيقات ومواقع التواصل الاجتماعي، والتي سهلت من عملية التفاعل فيما بين الأشخاص وهي بمثابة أدوات لتنفيذ الجريمة.
- الرغبة في تحقيق مكاسب مالية من الآخرين لأن مرتكبي الجرائم يعلمون بأنه لا يمكن الوصول إليهم والكشف عن هويتهم وبالتالي صعوبة ملاحقتهم قانونيا (Dashora , 2011:240).

- الرغبة في الانتقام من بعض الأشخاص ماديا و معنويا من خلال ابتزازهم و تهديدتهم بنشر معلومات، صور أو فيديوهات تلحق الأذى بهم.

- ارتفاع نسبة البطالة بين الشباب ما يدفعهم إلى استخدام الانترنت وتطبيقاته الحديثة لتحقيق مكاسب مادية تساعد على كسب معيشتهم (Kamal , 2012 : 16)

- غياب الوازع الديني وانحطاط الأخلاق في المجتمعات المتقدمة والنامية حيث ساهمت هذه الأخلاق على تنفيذ الجريمة (Little : 8 , 2011 wood)

- قلة التوعية داخل المجتمع حول طرق وكيفيات الاستخدام الآمن لوسائل التكنولوجيا الحديثة من قبل الأشخاص.
- غياب قوانين وعقوبات صارمة تجرم مثل هذه الأفعال، وتعاقب بالسجن لأصحابها مع تغريمهم مبالغ مالية حسب نوع وحجم الجريمة ساهم في انتشار الجريمة عبر مواقع التواصل الاجتماعي.

7. بعض الجرائم الشائعة على المنصات الالكترونية :

- اختراق حسابات الآخرين استعمال حسابات مزيفة من أجل الاعتداء على الآخرين.
- التحرش الالكتروني من خلال تعطيل حواسيب الآخرين ونشر الفيروسات والقنابل الالكترونية.
- النصب والاحتيال من خلال التسويق الرقمي.
- الترويج بالأسلحة المحضرة والمخدرات والتشهير بها.
- نشر الإشاعات والدعاية والأخبار الكاذبة التي تمس النظام وهذا بهدف خلق البلبلة وتضليل الرأي العام.
- ابتزاز الفتيات وتهديدهن بنشر الصور وفيديوهات خاصة بهن.
- الدعوة للتطرف و الانخراط في شبكات إجرامية وإرهابية.
- التشجيع على الفسق وممارسة الدعارة.
- سرقة ملفات الآخرين وكلمات السر الخاصة ببطاقات الائتمان واختراق الحسابات البريدية واختلاس الأموال.
- الدعوة للهجرة السرية وتشجيع الشباب عليها.
- استدراج الضحايا من خلال الحسابات الوهمية.
- نشر فيديوهات مخالفة للنظم و القواعد التي تنظم المجتمع.
- إفشاء أسرار تمس الأمن الاجتماعي.
- نشر إعلانات وصور وفيديوهات تنقص من معنويات الجيش وتشوه سمعة البلد.



- المتاجرة بالمخدرات والأطفال.
- التجسس على الغير.
- الدعوة على التجمهر الغير المشروع.
- عرض الصور والفيديوهات المخلة بالحياء كعرض الأفلام الجنسية.
- الدعوة للتكفير ونشر الأفكار المنافية لتعاليم الدين.
- نشر ألعاب الكترونية خطيرة على الأطفال والمراهقين.
- الوشاية وقذف الآخرين والإساءة إليهم.
- استدراج الأشخاص بهدف إلحاق الضرر المادي والمعنوي بهم .
- السب والشتم بواسطة الرسائل النصية.

8. خصائص المنصات الالكترونية ومنصات شبكات التواصل الاجتماعي (الشبكات الاجتماعية):

- التواصل الفعال والمستمر بين الأشخاص، وليس فقط تواصل مباشر وإنما وصول نشاطاتهم وأخبارهم لبعضهم البعض بشكل آلي وإبداء الرأي عليها ومناقشتها.
- التحوار الكتروني: النصي والصوتي والمرئي المتعدد الاتجاهات بين الأشخاص.
- التشارك بين الأشخاص في صنع المحتوى وتشكيل المجموعات لأداء أنشطة مختلفة.
- التفاعلية بين الأشخاص والشبكات والمنظمات.
- بناء المحتوى والقدرة على التحكم فيه.
- الاهتمامات المشتركة للمستخدمين سواء كانت اهتمامات اجتماعية، اقتصادية، سياسية، تعليمية.
- التشبيك إذ تهدف الشبكات الاجتماعية إلى التعارف والترابط والتشاور، وهي تنمو بفعل الترابط فيما بينها بفعل الوصلات الالكترونية.
- الفاعلية إذ أن كل مستخدم هو شخص نشط وفعال مادام يكتب، ويقرأ، وينشر ويرسل معلومات ويشارك ويضيف ويعدل ويحذف ويطور المحتويات.
- سهولة الاستخدام إذ تتميز عملية التسجيل بهذه المواقع بالبساطة والسهولة المجانية.
- إعتماها على شبكة الأنترنت. (هالة عبدالقادر، 2019 : 71-72)
- العالمية بحيث يستطيع الشخص التواصل مع شخص أو مجموعة من الأشخاص من أي بلد كان.
- تعدد الاستعمالات إذ يستخدمها المستقبل لتلقي الخدمة والمرسل للتواصل مع الآخرين (www.alukah.net).

9. خصائص الجريمة الالكترونية :

- صعوبة إثباتها لأنها تفتقر إلى الدليل المادي التقليدي مثل البصمات.
- النعومة لان ارتكابها لا يتطلب مجهود عضلي بل تعتمد على مجهود ذهني محكم.
- عدم التبليغ لأن الضحية يخاف على سمعته، ومكانته (طالة، سلام، 2020 : 75-76).
- العالمية: لأنها تتعدى الحدود الجغرافية للدول، إذ يمكن أن يكون الجاني من بلد والمجني عليه من بلد آخر. (مراد، 2007: 42)



10. نماذج وصور من منصات / الشبكات الاجتماعية :

1.10. الفيس بوك – face book : يعد هذا الموقع من أشهر المواقع على شبكة الانترنت ورائد في التواصل الاجتماعي، حيث يتعامل به كل شرائح المجتمع شيئا وشبابا وبمختلف الاعمار، إذ يساعد على تكوين علاقات بين المستخدمين وتبادل المعلومات والملفات والصور الشخصية ومقاطع الفيديو، ووضع تعليقات، عرض المنشورات و كل هذا يتم في عالم افتراضي يقطع حاجز الزمان والمكان.

2.10. التويتر – Twitter : موقع للتواصل الاجتماعي يقدم خدمة تسمح لمستخدميه بإرسال تغريدات وتحديثات Tweets عن حالتهم من خلال رسائل أو رسائل قصيرة S.M.S أو برامج المحادثة الفورية وغيرها.

3.10. المدونات – Weblogs : هي مواقع شخصية على الأنترنت تساعد المستخدمين على التفاعل من خلال المشاركة وتبادل الأفكار والمعلومات.

4.10. واتسب – Whatsapp: هو شبكة الكترونية تسمح للمستخدم إنشاء موقع خاص به، مع إمكانية ربطه بالمواقع الأخرى التابعة للأصدقاء، وهو برنامج يعمل على الهواتف الذكية. (<http://ljk599.blogspot.com>).

11. الاستخدامات السلبية للمنصات الالكترونية والشبكات الاجتماعية : نذكر بعض الصور للاستخدامات السلبية للمنصات

الالكترونية بما فيها منصات / شبكات التواصل الاجتماعي وهي كالاتي :

- بث الأفكار الهدامة والدعوات المنحرفة والتجمعات المخالفة للقيم والقانون.

- عرض المواد الإباحية والفاضحة الخادشة للحياء العام.

- التشهير والمضايقة وبث الإشاعات.

- التحايل والابتزاز والتزوير.

- إنتهاك الحقوق الخاصة والعامة.

- الاستغلال الجنسي للأطفال. (البادي وآخرون ، 2016 : 53).

الجانب الميداني :

1. **منهج البحث :** اعتمدنا على منهج تحليل المحتوى وهو من الأساليب البحثية التي تستخدم بهدف الوصف الدقيق والمنظم لمحتوى النصوص المكتوبة أو المسموعة أو المرئية، حيث جسدنا هذا في دراستنا من خلال التحري والبحث عن مظهرات العنف والسلوك الإجرامي الرقمي عبر المنصات الالكترونية والشبكات الاجتماعية المتضمنة وسائل التواصل الاجتماعي والمعبّر عنها في وسائل الإعلام والانترنت والجرائد والوثائق وغيرها من المصادر الأمنية والقضائية.

2. **أدوات البحث :** المقابلة الموجهة : اعتمدنا على هذه التقنية وباستعمال دليل المقابلة بغرض رصد أشكال العنف والسلوك الإجرامي الرقمي المنتشر عبر المنصات الالكترونية من خلال إلقاء أسئلة مباشرة على أفراد من مصالح الأمن والدرك والجهات القضائية (محكمة وادي رهيو - غليزان) بحيث كانت الإجابات بتحفظ شديد نظرا لسرية وحساسية الموضوع من جهة، وحدائته من جهة أخرى، وسنوضح في مايلي إجراءات البحث.

* **دليل المقابلة:** تم إجراء مقابلات موجهة تعتمد على طرح أسئلة مباشرة تركز على السلوكات العدائية والإجرامية المنتشرة باستعمال الانترنت مع تسجيل إجابات محددة تخدم أهداف البحث حيث اعتمدنا في بحثنا على الأسئلة التالية:

1- حدثني عن أشكال العنف والسلوك الإجرامي بالمنصات الالكترونية.

2- ما هي الأسباب الحقيقية في انتشار العنف والسلوك الإجرامي بالمنصات الالكترونية؟



- 3 - حدثني عن حيثيات قضايا حول العنف والسلوك الإجرامي سجلت بالمنصات الالكترونية.
 - 4 - هل ممكن تقديم تواريخ حول حدوث قضايا عنف وسلوكات إجرامية بالفضاء السيبراني؟
 - 5 - ما هي التطبيقات الشائعة في تفريغ النزوات العدوانية لدى مستعملي الأنترنت؟
 - 6 - ما هو العدد الكلي للقضايا التي تتعلق بالعنف والسلوك الإجرامي بالمنصات الالكترونية؟
 - 7 - في رأيكم ما هي العراقيل والصعوبات التي تحول دون محاربة العنف والسلوك الإجرامي بالمنصات الالكترونية؟
 - 8 - ما هي اقتراحاتكم للحّد من ظاهرة انتشار العنف والسلوك الإجرامي بالفضاء السيبراني؟
- وسنوضح أكثر عن استعمال أداة المقابلة الموجهة لجمع البيانات حول تحليلات العنف والسلوك الإجرامي بالمنصات الالكترونية من خلال الجدول (1).

جدول (1) : مصادر جمع البيانات حول ظاهرة العنف والسلوك الإجرامي عبر المنصات الالكترونية باستعمال المقابلة الموجهة

المصدر	المصادر الأمنية		المصادر القضائية		المصادر الإعلامية		مصادر البحث الالكتروني
	الأمن الوطني	الدرك الوطني	المحكمة		الجرائد	التلفزيون	الانترنت
تحديد نوع سلوك العنف والإجرام بالفضاء السيبراني							
ذكر الأسباب الحقيقية في انتشار العنف والسلوك الإجرامي							
تحديد نوع التطبيق المستعمل في تنفيذ السلوك الإجرامي							
ذكر العدد الكلي لقضايا العنف والسلوك الإجرامي المرتكبة باستعمال الأنترنت							



3. عرض وتحليل نتائج البحث :

توصلنا في دراستنا إلى مايلي:

- من مظاهر العنف والسلوك الإجرامي عبر المنصات الالكترونية وخاصة منصات / شبكات التواصل الاجتماعي هي الجرائم التي تحدث فعلا على أرض الواقع، وتتعلق بمواقع التواصل الاجتماعي، منها ما وقفنا عليه بواسطة ما تتحراه مصالح الأمن وتحقق فيه جهات قضائية ومنها ما نراه وما نسمعه عنها وما ينشر عبر شاشة التلفزيون أو ما ينشر عبر الجرائد من جهة أخرى، بحيث نذكر منها:

- الخبر الذي نشرته جريدة النصر عن موظفة تم سرقة صورها من هاتفها من مقر عملها من طرف زميل لها حيث قام بابتزازها وتهديدها بنشرها عبر منصات شبكات التواصل الاجتماعي إذا لم تنصع لرغباته الجنسية (لبوزيد، 2017، العدد 15285)، فالجرم هنا استغل عدم حرص زميلته على هاتفها بحيث استغله ضدها، واستغل أيضا خوفها من الفضيحة على منصات مواقع التواصل الاجتماعي.

- خبر آخر نشرته جريدة الشروق اليومي حول فتاة تم قرصنة حسابها الشخصي على منصات شبكات التواصل الاجتماعي في موقع الفاييسبوك وابتزازها بنشر صورها من طرف شخص مجهول إذا لم تنصع لرغباته المادية (عنشر، 2017، العدد 5418)، نجد هنا أن المجرم يقوم باستغلال خصوصيات الأشخاص مع الابتزاز والتهديد إذ لم يحصل على مبالغ مالية ويستغل المنصات الالكترونية كأداة تهديد.

- خبر آخر نشرته الجريدة الخبر عن رجل له حساب الكتروني وهمي مزيف على موقع الفاييسبوك باسم فتاة قاصرة حيث استدرج به العديد من الفتيات سنهن ما بين 13 و 14 وشجعهن على إرسال وتبادل صور وفيديوهات وهن في وضعيات مخلة بالحياء (حريشان، 2017 ، العدد 8484)، فهذا يعتبر مجرم الكتروني شاذ جنسيا، حيث قام باستغلال تواجد فتيات قاصرات على الشبكات الاجتماعية بدون رقابة والدية وبسبب قلة وعيهم وسذاجتهن وخبرتهن في الحياة وفي التعامل في مثل هذا النوع من المواقف تمكن من تنفيذ جرمته بسهولة.

- خبر آخر نشرته جريدة الفجر عن طالب جامعي استدرجه شخص تعرف به على الفاييسبوك للقاء به في مكان مهجور وتم اللقاء ليفاجئ الطالب بوجود أشخاص آخرين قاموا بسرقة وتجيده من ملابسه والتقاط صور مخلة بالحياء له وهددوه بعدها بنشرها على الأنترنت إن لم ينصع لرغباتهم المادية (مجيد ، 2017 ، العدد 5011) ، فالجرم استغل سذاجة الضحية وقلة حذره وحييطته تجاه نفسه أرادوا ارتكاب جرم الكتروني ضده.

- خبر آخر نشرته جريدة البلاد حول تفكيك شبكة تجنيد دولية للإرهابيين من أجل الانضمام إلى صفوف التنظيم الإرهابي داعش بحيث استخدمت الشبكة المنصات الالكترونية المتمثلة في شبكات التواصل الاجتماعي من أجل التجنيد واصطياد الأشخاص ذوي الأفكار المتطرفة والمتشددة التي تخدم مصالح التنظيم (بهاء الدين ، 2017 ، العدد 5287)، فالشبكة اعتمدت على مواقع التواصل الاجتماعي من أجل نشر أفكارها المتطرفة في أوساط الشباب وتعد هذه العملية من الجرائم الالكترونية الهادفة إلى استغلال الشباب والتضليل بهم ونشر العنف والسلوك الإجرامي بالبلدان وخلق اللااستقرار بها.

- في سنة 2021 سجلت محكمة وادي رهيو سبعة (7) قضايا عنف وإجرام مرتبطة باستخدام المنصات الالكترونية خاصة عبر منصات شبكات التواصل الاجتماعي، لأشخاص ذوي نوازع إجرامية نعددها على النحو الآتي:

1 - إضعاف الروح المعنوية للجيش.

2 - التحريض على التجمهر المسلح.



- 3- التهديد بالتشهير بواسطة الماسنجر
- 4 - الإشادة بأعمال إرهابية.
- 5 - ابتزاز وتهديد فتاة قاصر على نشر صورها وهي في وضعية مخلة بالحياء.
- 6 - التشجيع على الهجرة غير شرعية.
- 7 - التشهير بالصور لضرب سمعة الغير، حيث وقعت معظم هذه الجرائم على مستوى منصة الشبكات الإجتماعية وخاصة عبر صفحات الفايسبوك.

لهذا يمكننا القول أن الاستعمال الواسع لهذا التطبيق من طرف مستخدمين وسط المجتمع الجزائري نتج عنه مجرمين وضحايا بما يسمى الحدث الإجرامي حيث أن العملية التفاعلية التي تنمو بين الأشخاص أسفرت على بروز نموذج جديد لميكانيكية الجريمة إذ تأخذ في الاعتبار المبادرات الفردية والاستجابة لها - وهذا يتطابق مع أشرنا إليه في الجانب النظري - يعني الإشارات التي تصدر من الضحية يلتقطها المجرم وبناء عليها يخطط لارتكاب جريمته سواء كانت هذه الإشارات شخصية لدى الضحية أو تتعلق بالمكان الذي يتواجد فيه، فالفايسبوك بصفته منصة الكترونية تميز بالتطبيق الشائع الذي بواسطته تقع الجرائم وهو يحتل المرتبة الأولى حيث يساعد على تبادل الرسائل النصية والصور والفيديوهات إضافة إلى أنه يساعد المجرم على أخذ المعلومات اللازمة كي ينفذ جرمه بسهولة دون أن تحوم حوله الشبهات بحيث يمكنه التملص من العقاب، نفهم من هذا أن المنصات الالكترونية بما فيها منصات شبكات التواصل الاجتماعي تسهل تلك العملية التفاعلية بين المجرم والضحية، وتساعد على عرض نواذره الإجرامية، لأن تلك الشبكات تكون محاطة بخصوصية كبيرة وبدون رقيب أو شهود، بالإضافة إلى انعدام الردع من خلال الدراسات القانونية في مجال ضبط عملية استعمال منصات شبكات / مواقع التواصل الاجتماعي في الجزائر نظرا لحدثة هذه الأفعال وضعف التحكم فيها.

أصبحت الوسائل التكنولوجية الحديثة مثل المنصات الالكترونية بمختلف أنواعها و تطبيقاتها تلعب دورا هاما في انتشار الجريمة لأنها قد تلبي احتياجات الشباب والفئات المهمشة اجتماعيا التي تعيش تحت طائلة الفقر والبطالة والعنف والعزلة و التهميش ، حيث تشير الأدلة إلى أن هناك شبكات دولية بالخارج تعتمد على الإغراء المادي حين توظف مهنين شباب مقابل أجر وهناك متطوعين يعملون بدون أجر، ومن جهة أخرى تساهم الشبكات الاجتماعية في ازدياد المعلومات والتواصل بين العصابات لينتج عن هذا تدهور الأوضاع الأمنية للبلدان المستهدفة، وأيضا عملية نشر الإعلانات المحرصة والصور والفيديوهات على نطاق واسع يخلق الفوضى وأعمال الشغب داخل البلاد، وغيرها من الأحداث والمشاكل المتعلقة باستعمال المنصات الالكترونية للتواصل في الجزائر وفي العالم ككل، حيث توسعت سلوكيات العنف والجريمة عبرها، وفي نفس السياق نذكر قضية اختطاف فتاة قاصر من طرف رجل بالغ الذي اعتمد على الفايسبوك لرصد تحركات العائلة، وهذا راجع للفتاة التي كانت تنشر كل تفاصيل عائلتها على موقع الفايسبوك، إضافة إلى التجارة بأعضاء البشر وضحايا الشركات الوهمية التي تعمل على تسويق المنتجات المختلفة وتعد بإيصال المنتج ولكنها في الأخير تنصب على الزبائن وتحتفي ولا تعيد الأموال لأصحابها، بما يسمى ببيع الوهم بالبيئة الرقمية وهناك حالات عديدة من محاولات الانتحار أو الانتحار خاصة لدى المراهقين بسبب تعرضهم للابتزاز والتنمر من طرف أقرانهم أو من طرف أشخاص يكيرونهم سنا على مواقع التواصل الاجتماعي، وغيرها من الحوادث التي نقرأ عنها بشكل يومي وآخرها قضية النصب والاحتيال على الطلبة من طرف شركتين وهميتين وصاحب وكالة سياحية الذين قدموا عروضاً لهم تمثلت في حصولهم على منح للدراسة في الخارج مقابل دفع مبالغ مالية تراوحت بين 30 و 500 مليون سنتيم والتي سلبت منهم باستعمال مؤثرين على منصات الشبكات الاجتماعية لجلب وكسب الزبائن -الضحايا- الذين وجهت لهم تم الانتحار بالبشر والنصب والاحتيال الموجه للجمهور، ومخالفة التشريع الخاص بحركة الأموال من وإلى الخارج، وهنا نجد أن هؤلاء المؤثرين استعملوا للتأثير على الطلبة وكسب ثقتهم نحو تقبل هذا المشروع الوهمي عبر



شبكات التواصل الاجتماعي التي أصبحت بمثابة الأرضية الخصبة والمساعدة لحدوث الجرائم في البيئة الافتراضية وفي هذه الحالة استعملت المنصات الإلكترونية استعمالا سلبيا.

ومّا سبق يتضح لنا سويّا أنّ كلّ شخص مشترك في هذه المنصات الالكترونية أو المواقع معرض لخطر التعرض لاعتداءات العنف والجريمة الالكترونية عبرها وخاصة على منصات الشبكات الاجتماعية كون هذه الأخيرة فضاء كبيرا يجمع بين مختلف الفئات والثقافات والمستويات والأعمار، إذ يقع التفاعل بينهم بسهولة في عالم افتراضي جديد ومناسب لتفريغ نوازع الإجرام وممارسة الشذوذ وكل أنواع العنف بعيدا عن الرقابة (خطاب، 2017)، وماهي إلا عبارة عن جرائم تقليدية ترتكب بأسلوب الكتروني، بما يسمى الجرائم السيبرانية وهي أنشطة غير مشروعة تنشأ في الانترنت مثل شبكات ومواقع التواصل الاجتماعي وغرف المحادثة، أو البريد الالكتروني، ويمكن أن تشمل جرائم الانترنت باستخدام وسائل التواصل الاجتماعي إلى اقتحام حسابات الأشخاص والتسلل إلى ملفات الغير من صور وفيديوهات واستعمالها بغرض الابتزاز والتشويه، بالإضافة إلى سرقة هوية الغير وانتحال شخصيات مزيفة عبر شبكات التواصل الاجتماعي فالجرائم المرتبطة بشبكة الانترنت تتنوع وتتعدد حسب أهدافها مابين جرائم ذات دافع سياسي أو ذات ارتباط بالأمن القومي أو العسكري، وبين جرائم ذات طبيعة جنائية والتي بدورها تتنوع ما بين جرائم ذات طابع اقتصادي أو جرائم متعلقة بأمن وسلامة الأشخاص من أهمها جريمة القرصنة والاحتيايل المعلوماتي، الجرائم المخلة بالآداب، السب والشتم باستخدام وسائل التواصل الاجتماعي، الجرائم المتعلقة بتعطيل أو إفساد حسابات شخصية أو الاستيلاء على معلومات الغير، جرائم السرقة واستدراج القصر، نستنتج من ذلك أنّ التنامي المستمر لمنصات شبكات الاتصال الاجتماعي في الجزائر بصفة خاصة والمنطقة العربية بصفة عامة واستعمالها الدائم والسلس من طرف فئة الشباب قد أفرز مشكلة أخرى تتمثل في الإدمان على استعمالها، الأمر الذي يتطلب الدراسة نظرا للعلاقة الايجابية بين كثرة الاستعمال وزيادة احتمالية وقوع الجريمة الالكترونية، وهذا ما يحتاج إلى تكاتف جميع مؤسسات التنشئة الاجتماعية ومؤسسات المجتمع المدني ووسائل الإعلام للتصدي لمثل هكذا ظواهر.

4. استنتاج عام :

ما أفرزته نتائج البحث النظري و الميداني، هو بمثابة إجابة عن التساؤل الرئيسي وجميع التساؤلات الفرعية للبحث، كذلك تم التحقق من صحة جميع الفرضيات، حيث أشارت النتائج إلى أنّ هناك العديد من أشكال العنف والسلوك الإجرامي المنتشرة عبر المنصات الالكترونية على غرار نصب والاحتيايل الذي يقع على الأشخاص، مما يؤكد تحقق صحة الفرضية الأولى، ومن جهة أخرى سجلنا عدة معلومات حول ضعف الرقابة الوالدية وغياب السلطة الأبوية الضابطة للسلوك وسط الأسرة، وكانت من الأسباب الرئيسة لوقوع أبنائهم ضحية اعتداءات وإغراءات مادية وجنسية خاصة القصر، بحكم قلّة وعيهم بما يحيط بهم من ذئاب بشرية تصطاد في الفضاء الأزرق، ممّا يدل على تحقق صحة الفرضية الثانية، وقد تمّ أيضا التصريح من جهات قضائية وأمنية وإعلامية بتسجيل قضايا عنف وقعت بالفضاء السيبراني سببها استعمال وسائل التواصل الاجتماعي وبالدرجة الأولى استخدام تطبيق الفايسبوك بمعنى أنّ معظم الجرائم وسلوكات العنف سجلت على الفايسبوك، نظرا لسهولة تحميله والتواصل في ما بين الأشخاص أو الهيئات المختلفة و هذا ما أشارت إليه الفرضية الثالثة التي تضمنت أنّ تطبيق الفايسبوك هو الشائع والأكثر استخداما من طرف مستخدمي الشبكة العنكبوتية بالمجتمع الجزائري وهو المساعد في نشر العنف والسلوك الإجرامي بالمنصات الالكترونية، ما يرمز إلى تحقق هذه الفرضية أيضا، أما الفرضية الرابعة التي أشارت إلى محاولة الكسب الغير المشروع للمال يعد سببا في انتشار العنف والسلوك الإجرامي باستعمال الأنترنت فقد تمّ اختبار صحتها، لأن العديد من قضايا التهديد والابتزاز، النصب والاحتيايل عبر المنصات الالكترونية والتي يتم تسجيلها والتحقيق فيها كان من ورائها طلب أو أخذ مبالغ مالية من الضحايا و الاستيلاء عليها، وبالنظر إلى النتائج التي أفرزتها الدراسة النظرية والميدانية فإن الفرضية الخامسة التي تشير إلى أنّ من أكثر السلوكات العدائية الموجهة للغير بالفضاء السيبراني



هي التشهير بالصور والفيديوهات قد تحققت وهذا استنادا بما تمّ عرضه من قضايا وأخبار من مصادر مختلفة حول التشهير بالصور وفيديوهات الأشخاص من أجل ضرب سمعتهم أو تقزيمهم في رأى الآخرين، ومن جهة أخرى يكون تهديدهم لأجل أغراض مادية أو جنسية أو انتقامية، وفي الأخير نستخلص أن المنصات الالكترونية أصبحت فضاء جديدا وأرضية خصبة لممارسة الشذوذ وانتشار العنف والسلوك الإجرامي بشتى أشكاله، وعليه فلا بد من أخذ الاحتياطات اللازمة حين استخدامها.

خاتمة:

تعد المنصات الالكترونية فضاء مهما لتبادل المعارف والتواصل بين الأفراد، والترويج للمشاريع التجارية عبرها، لكن استعمالها السلبي في وقتنا الحالي يطرح مشاكل كبيرة لأنها أصبحت مكانا لتوظيف بعض الأشخاص لنزواتهم العدائية على الآخرين بطرق متعددة، وبواسطة صفحات مختلفة كالفيسبوك، الواتساب، الانستغرام والفابريكس والتويتير واليوتيوب...، إذ أنها تساهم في انتشار العنف وارتكاب الجرائم بكل أنواعها خاصة الجريمة الالكترونية حين تنتهك فيها خصوصيات الأفراد والاستلاء على معلوماتهم وملفاتهم الشخصية وابتزازهم بنشر الصور والفيديوهات، ولهذا يجب أن تكون هناك سياسة واضحة وسليمة للحد من هذه الممارسات حتى لا يقع أبناءنا وبناتنا ضحايا استعمال التكنولوجيا الحديثة في الفضاء الافتراضي، وهذا ما أفرزته دراستنا هاته من خلال القضايا والمسائل الجوهرية التي يجب أن تؤخذ بعين الاعتبار حتى يتقلص حجم الاعتداءات بالبيئة الرقمية التي أصبحت تغذي السلوكات الشاذة والمضادة للمجتمع، وقد ساهمت أيضا في تعليم طرق الإجرام الالكتروني عند أشخاص همهم الوحيد هو إيذاء الآخرين ونشر الأفكار الهدامة والدعوة للهجرة الغير الشرعية وهذا راجع إلى نقص التوعية السياسية على مستوى مؤسسات التنشئة الاجتماعية، خصوصا المدرسة والجامعة، حيث تفتقر المساقات المدرسة في الكثير من التخصصات، الى تعزيز المفاهيم المواطنة السياسية؛ وهو ما يجعل الولاء والانتماء يتراجع أمام بريق الأفكار المعادية، حيث يتحول الشاب فجأة الى باحث عن الولاء والانتماء خارج وطنه، ويصبح حينها في وضعية "تهريب للولاء" وهي أخطر حالة تشهدها المنطقة العربية اليوم (زقاوة، 2016)، ومن جهة أخرى لا ننسى بأن للمنصات الالكترونية ولوسائل وشبكات التواصل الاجتماعي دور آخر إيجابي حيث تعرض في شقها الآخر نماذج وتجارب ناجحة نظير استخداماتهم الإيجابية للمنصات الالكترونية وللشبكات الاجتماعية سواء كانت لأغراض علمية وتعليمية أو دعوية، اجتماعية أو اقتصادية.

التوصيات والاقتراحات :

شكل الاستعمال السلبي للمنصات الالكترونية ومنصات شبكات التواصل الاجتماعي خاصة بؤرا للمشاكل وسط المجتمع الجزائري، إذ ظهرت عبرها الاعتداءات الموجهة للغير وتفشت الجريمة بكل أنواعها وتفككت الأسر بسبب اضطراب العلاقات الزوجية مع تزايد الهوة بين أفراد العائلة والمجتمع الواحد، لذا يتوجب ضبط أخلاقيات لاستعمال هذه الوسائل بمختلف أنواعها وتقنياتها و التعامل الجيد مع تقنياتها ومحتوياتها، ومما تمّ طرحه سابقا نقدم بعض التوصيات في شكل نصائح وإرشادات بهدف التوعية والتحسيس والوقاية على النحو الآتي:

- 1 - تشريع قوانين مكافحة العنف والجريمة الالكترونية وفق دراسات علمية متخصصة وحديثة.
- 2 - ضرورة المراقبة الوالدية للهواتف وكل وسائل التواصل الاجتماعي المتاحة داخل المنزل المستخدمة من طرف الأبناء.
- 3 - ضرورة التوعية الأمنية ضد الجريمة الالكترونية، من خلال الحملات التوعوية والمحاضرات وإعداد برامج دراسية قائمة على الأمن السيبراني .
- 4 - تأمين استعمال جهاز الكمبيوتر وهذا من خلال وضعه في مكان يمكن مراقبته بسهولة، مع الكشف عن الصفحات على مستوى ذاكرة الملفات أو المواقع التي تم تصفحها من طرف الأبناء خلال استعمالهم للإنترنت مع حجب كل المواقع الغير المناسبة.



- 5- إنشاء معهد خاص بالفضاء السيبراني يتم فيه معالجة المشكلات التي تقع باستخدام شبكة الانترنت.
 - 6 - ضرورة التعاون الدولي للرفع من القدرات الخاصة في مجال العدالة الجنائية، وتطوير التحقيقات الجنائية في مجال الجريمة والأدلة الرقمية من خلال التدريب والتأهيل المناسب.
 - 7- تشجيع البحث والتطوير في مجال الحماية من الجريمة الالكترونية ورصد انتهاكاتها، وضبط أدلتها ومرتكبيها.
 - 8 - استعمال كلمات مرور لا يمكن الوصول إليها من طرف مستعملي المنصات الالكترونية.
 - 9- ضرورة بعث ثقافة التبليغ، من خلال الاتصال بالجهات الرسمية عند وقوع المستخدم ضحية للتجسس أو اختراق أو اعتداء وقع ضده من طرف شخص آخر باستعمال شبكة الأنترنت.
 - 10- ضبط التعامل مع المنصات الالكترونية ومنصات الشبكات الاجتماعية، خاصة وضع الصور والفيديوهات الشخصية بها.
- قائمة المراجع :

- المراجع باللغة العربية :

- 1- أمير فرج يوسف (2009)، الجرائم الالكترونية على شبكة الأنترنت ، دار المطبوعات الجامعية ، الاسكندرية.
- 2 - بلقرع أحمد (2017)، مواقع التواصل الاجتماعي و دورها في التعريف بالمعالم السياحية لولاية برج بوعريريج ، دراسة ميدانية على طلبة جامعة البشير الابراهيمية، مذكرة مكملة لنيل شهادة الماستر 2 في علوم الإعلام و الإتصال، جامعة المسيلة.
- 3 - بوعمامة، العربي (2016)، منصات التواصل الاجتماعي كميكانيزمات افتراضية لنشر خطاب الإرهاب والكراهية، المؤتمر العلمي، دور الشريعة والقانون والإعلام في مكافحة الإرهاب - مجلة جامعة الزرقاء- الأردن، 2، 465-479.
- 4- هالة، عبد القادر، سعيد، السنوسي(2019)، أدوار المنصات الالكترونية والشبكات الاجتماعية كميثات تعلم تواصلية تشاركية في التعليم الالكتروني في ضوء خبرة الطالبة، مجلة الكلية العربية، جامعة الأزهر، العدد 181، ج3، يناير، (57-89).
- 5- زقاوة، أحمد (2016) قيم المواطنة وخطاب العولمة، فصل في كتاب جماعي: دور وسائل الاتصال المحلية في تنمية قيم المواطنة وثقافة الحوار في الجزائر، منشورات مخبر الدراسات الاجتماعية والنفسية والانثروبولوجية، جامعة غليزان.
- 6 - حسام، حريشان، جريدة الخبر، العدد 8484 تاريخ النشر: 01 - 04 - 2017.
- 7 - خطاب، حاجة خيرة، مجلة دراسات و أبحاث 9751-1112، مواقع التواصل الاجتماعي ... فضاء جديد للجريمة، العدد 28 سبتمبر 2017، (411 - 421)، جامعة وهران.
- 8 - لامية، طالة ، كهيبة سلام (2020)، الجريمة الالكترونية: بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد 6 / العدد 2، (62 - 91).
- 9 - لبوزيد، محيي، جريدة النصر، العدد 15285، تاريخ النشر: 28 - 04 - 2017.
- 10 - م . مجيد، جريدة الفجر، العدد 5011، تاريخ النشر: 29-03-2017.
- 11 - م . بهاء الدين، جريدة البلاد، العدد 5287 تاريخ النشر: 09-04-2017.
- 12- مراد، عبد الفتاح(2007)، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية، الاسكندرية.
- 13 - محمد الأمين، البشري (2005)، علم ضحايا الجريمة وتطبيقاته في الدول العربية، جامعة نايف العربية للعلوم الأمنية، الرياض.
- 14 - س.عنشر، جريدة الشروق اليومي، العدد 5418، تاريخ النشر: 04-04-2017.
- 15- سعيد سالم، البادي، زايد بن حمد، الجنيبي، يوسف الشيخ يوسف، حمزة، محمود أحمد، العطاء (2016)، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة- نزوى- سلطنة عمان.
- 16- عبد الفتاح بيومي، حجازي(2006)، مكافحة جرائم الانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الاسكندرية.

- المراجع باللغة الأجنبية :

- 1- Dashora, Kamini, (2011), Cyber crime in the society :problèmes and



2- Kamal prevention Journal of Altemative perspectives in the social sciences,3(1). ,MohammadMostufa . Chow hurry, labal Ahmed , Haque,NADIA. Chow hurry ,My dul islam& islam, mohammed Nazrul (2012), Nature of cyber crime and Its impacts on young people : A case from Bangladesh.

3- Little wood , A(2011) , cyber porn and moral panic : an evaluation of press reaction to pornography on the internet, Libray and information recharch, 27(86).

4- Mshana ,J.A.(2008),Cyber cime : An Empirical Study of its impact Social security of Tanzania , International Review of law , Computers and Technology ;3(2).

- المواقع الالكترونية :

1- <http://www.alukh.net/publications-compétitions/0/404>.

2- <http://lljk599.blogspot.com/2014/04/blog-post-6251.html>.



خصائص الفضاء السيبراني المهيئة للسلوك الإجرامي Cyberspace characteristics predisposing to criminal behavior

دليلة جلول

dalila.djelloul@univ-batna.dz

مقدمة:

ساعد مجال الدراسة في علم الإجرام والضحايا عن الكشف عن عوامل الخطورة المرتبطة بالأفعال الإجرامية، ومنها أيضا جاءت الدراسات الوقائية للحد من وقوع الجريمة، من خلال البحث في العوامل المهيئة للفعل الإجرامي، والدوافع الجنائية المحتملة لدى شريحة واسعة من المجرمين. ومع ظهور أنماط مستحدثة للسلوك الإجرامي ضمن الفضاء السيبراني، برزت مجموعة من الدراسات التخصصية في هذا المجال وتحديد الدراسات المتعلقة بسلوك المجرمين في الفضاء السيبراني منها على سبيل المثال التنمر الإلكتروني (Cyberbullying)، وقد عرف بأنه من المظاهر الاجتماعية للجريمة المعلوماتية (Igoneleon Vicent, 2015, 19) وما يميز التنمر الإلكتروني عن التنمر التقليدي شكّل دافعا لدراسة الظاهرة. حيث أشارت نتائج دراسة (Arslan, Savaser, Halett and Balci, 2012) أن 80% من ضحايا التنمر لا يعرفون هوية المتنمر (الشناوي، 2014، ص 4) وهذا بفضل خصائص الجريمة الإلكترونية التي يكون عامل التخفي فيها دافعا قويا للمتنمر (المعتدي عموما)، ومن جانب آخر للإعتداء فإن ضعف التعاطف الوجداني الذي ينبثق من أن المتنمر لا يرى آثار أفعاله على الضحية (الشناوي، 2014، ص 4) ولعل أهم ما يميز الظاهرة أن هناك مشاعر مؤلمة لشخص الضحية ومريحة للآخر (المتنمر) عكس توازن القوة وتساويها في العدوان، غير أنها غير متوازنة في حالة التنمر، ومن هنا تبرز الحاجة الماسة لتدخل الكبار (الصباحين والقضاة، 2013، ص 13). كما أن العالم الافتراضي وما يحتويه من وسائل متعددة صار فضاء رحبا لهذه الممارسات بعيدا عن الرقابة الاجتماعية أو الأمنية، نظرا لما يوفره من حرية متناهية وفرص متاحة باستمرار، مستثمرين مهاراتهم وفتياتهم الخاصة في مجال الأنظمة الرقمية. ففي حين يكون الأفراد منغمسين في تفاعلاتهم الافتراضية وفي علاقاتهم التبادلية لمختلف المنتجات، سواء كانت سلعاً أو خدمات أو معرفة أو خبرات، منهمكين في تسوية مختلف الإجراءات اللازمة لإتمام العمليات التجارية، إذ تهاجمهم على حين غرة، ومن حيث لا يحتسبون، فلن ينتهوا إلا بعد أن يجدوا سلعهم قد افتقدت وتم السطو عليها، دون أن يدركوا الطريقة أو الجهة الفاعلة والمسؤولة عن العملية الإجرامية، مما يجعل هؤلاء الضحايا يقعون في حيرة كبيرة واضطراب شديد يسيطر على نفسيتهم، تستمر أحقاباً زمنية، ويصعب علاجها أو القضاء عليها في فترة قصيرة (قريعة و الجوزي، 2021، ص 661-662).

إن الخصائص المرتبطة بالفضاء السيبراني بقدر ما توفر من تيسير في تفاعلات الحياة اليومية، توفر في الجانب الموازي فرصا كبيرة للمجرمين المعلوماتيين ومقتنصي الفرص لتحقيق أغراضهم الجنائية. ومع حتمية التطور التكنولوجي يقع على عاتق المستخدمين تطوير رصيدهم ومكتسباتهم المعرفية في طبيعة هذا الفضاء وخصائصه.

الإشكالية:

يشير مصطلح الفضاء السيبراني أو الافتراضي إلى عالم بديل بتشكيل في ذاكرة الحواسيب يخلق حالة من التواجد المكتمل، ويعطي أفقا آخر لتطور البشرية، وهو مصطلح ابتكره العالم "جورن لاينر" ويعمل الواقع الافتراضي على نقل الوعي الإنساني إلى بيئة افتراضية



يتم تشكيلها إلكترونيا من خلال تحرر العقل للغوص في تنفيذ الخيال بعيدا عن مكان الجسد، وهو عالم ليس وهميا وليس حقيقيا بدليل حدوثه ومعايشة بيئته، ففيه يتم تنفيذ الأحداث في الواقع المفترض لكن ليس في الحقيقة (قريعة والجوزي، 2021، ص 664). ارتبط الفعل الإجرامي في الفضاء السيبراني بخصائص كثيرة، حيث أن ظرف الزمان والمكان على وجه التحديد جعل المجرم المعلوماتي يطور الكثير من المهارات والأساليب لنشاطه. كما أن التطور التكنولوجي مكن من برمجة الجرائم دون الحاجة لوجود شخص يقوم بذلك، وهناك العديد من جرائم القتل التي نفذت على الأشخاص دون الحاجة للتفاعل وجها لوجه، بل أنه تم تحديدها وتوقيتها مسبقا. تترجم أهداف الجريمة المعلوماتية الكثير من الدوافع التي يبحث المجرم المعلوماتي لتحقيقها، فقد تكون دوافع شخصية مرتبطة بالفضول وتحدي المهارات الذاتية، أو رغبة في الانتقام من شخص معين عن طريق الإبتزاز الإلكتروني أو السب والشتيم، أو التهديد كما قد تكون دوافع أمنية، سياسية أو اقتصادية.

إن ارتباط الإجرام الإلكتروني بالفضاء السيبراني إنطلق من مساحة كبيرة من الحرية وضعف المراقبة على هذا النشاط، ما أثار تساؤلات التالية:

ما هي أهم خصائص الفضاء السيبراني المهيمنة للسلوك الإجرامي المعلوماتي؟
كيف تشجع هذه العوامل على ارتكاب الجريمة المعلوماتية خارج هذه الخصائص؟
ضمن الورقة البحثية تم الاعتماد على المنهج الوصفي، لمعالجة المعلومات وتحليلها للإجابة عن تساؤلات الدراسة، من خلال انتهاز العناصر البحثية التالية:

1. الخصائص المرتبطة بظرفي الزمان والمكان:

المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود. فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد. فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق الحاسوب موجود في دولة معينة يتحقق الفعل الإجرامي في دولة أخرى. تكمن أهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية في أنه لا يوجد هنا مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة. بالإضافة إلى نقص الخبرة لدى الشرطة في وجهات الإدعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع الأدلة عنها للإدانة فيها يشكل عائقا كذلك أمام التعاون في مجال مكافحة ذا النوع من الجرائم (مومني، 2010، ص 52-53).

فالفكرة تتلخص في أن مرتكبي الجرائم يستغلون الثغرات القانونية المتمثلة في:

- 1- صعوبة التوصل إلى اتفاق عالمي حول نوعية الأفعال والأنشطة التي تدخل في نطاق الجرائم المعلوماتية.
 - 2- عدم وجود اتفاق عالمي موحد حول التعريف القانوني للسلوك الإجرامي.
 - 3- غياب التعاون بين الدول فيما يتعلق بتبادل المتهمين في تلك الجرائم وتسليمهم للقضاء (جلبي و أحمد، 2011، ص 220).
- وبالتالي من أجل التصدي للإجرام المعلوماتي لا بد أن تعمل الدول في اتجاهين:
- الأول:** داخلي حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة هذه الجرائم.

الثاني: دولي عن طريق عقد الاتفاقيات الدولية، حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولية من نتائج وآثار هذه الجرائم (مومني، 2010، ص 53).



مفهوم الزمان والمكان في مجال الجريمة المعلوماتية يعتبر من المؤشرات القوية في تحليل طبيعة السلوك الإجرامي، ذلك أن وقوع الجريمة يكون بصورة كبيرة في الفترة الليلية حيث تضعف وتراجع مستويات الرقابة الشعورية للسلوك تحت تأثير تغيرات بيولوجية عصبية، وكذلك مستوى الأكسجين في الدماغ لأن طبيعة الدورة الدموية المغذية للخلايا العصبية تكون غنية بالمواد السامة، ومن هنا تكون عملية التحليل المنطقي ومستويات الإدراك والانتقاء المعرفي أقل كفاءة منها في الفترة الصباحية. لذلك فإن أغلب الممارسين في مجال مكافحة الجريمة المعلوماتية، ينصحون بتجنب التواصل الافتراضي واتخاذ القرارات في مجال التجارة الإلكترونية مثلا أو التوقيع الإلكتروني في الفترة المسائية.

2. الخصائص المرتبطة بآثار الجريمة المعلوماتية:

من أبرز خصائص الجريمة المعلوماتية الغفلية anonymity، وتعني غياب الهوية والاسم المحدد absence of identity، حيث يمكن استخدام أسماء مستعارة وغير حقيقية، فالإنسان يستطيع أن يتفاعل مع آخرين في الفضاء الإلكتروني دون أن يحدد أو يذكر شخصيته الحقيقية، مستخدما أسماء مستعارة، وأماكن غير محددة، وحقائق غير صادقة، وقد يسر الأنترنت تلك الغفلية في هذا المجال.

وساعدت الغفلية الأفراد على ارتكاب أفعال وأنشطة إجرامية مع إخفاء شخصياتهم الحقيقية، لذا يتعذر اكتشاف شخصية القائم بهذا النشاط غير القانوني، فلا تستطيع السلطات المختصة تحديد هوية مرتكب هذا النشاط ومعاقبته. وفي بعض الأحيان، يعتمد المجرم أيضا على عمليات التخفي proxy 70 أثناء التجوال عبر الأنترنت، التي تسمح لمستخدمها بالانطلاق على أي موقع على الشبكة دون أن يتم اكتشاف الشخص الذي زار تلك المواقع. وعلى الرغم من أهمية البروكسيات والهدف الذي صممت من أجله لتأمين الشبكات والمواقع ضد عمليات الاختراق، إلا أنها استغلت استغلالا سيئا، حيث يصعب الوصول إلى الفرد الذي يستخدم تلك التكنولوجيا. كما أن الأمر لم يقف عند هذا الحد، بل يقوم صانعو الفيروسات من خلال استخدام تلك التكنولوجيا بإطلاق فيروساتهم، مما يشكل صعوبة في التوصل لمرتكب هذا الفعل الإجرامي. (جلبي و أحمد، 2011، ص 218).

نظرا للطابع الخاص الذي تتميز به الجريمة المعلوماتية، فإن إثباتها يحيط به كثيرا من الصعوبات، والتي تتمثل في صعوبة إكتشاف هذه الجرائم، لأنها لا تترك أثرا خارجي. فالجرائم المعلوماتية لا عنف فيها، ولا سفك دماء، ولا آثار اقتحام لسرقة الأموال مثلا. وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحواسيب وليس لها أي أثر خارج مرئي.

وهي جريمة هادئة لا تتطلب العنف، ورغم كل ذلك فإن البعض يشبه هذه الجرائم بجرائم العنف "العنف الرقمي" مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية FBI نظرا لثمائل دوافع المعتدين على نظام الحاسوب مع مرتكبي العنف. فإذا تم اكتشاف الجريمة المعلوماتية، فلا يكون إلا بمحض الصدفة، نظرا لعدم وجود أثر كتابي لما يجري خلال تنفيذها من عمليات حيث تم بالنسبة الإلكترونية نقل المعلومات، ولذلك يستطيع المجرم تدمير دليلا لإدانة في أقل من ثانية، إلى جانب إمكانية ارتكابها عبر الوطنية والقارات دون عناء التنقل (العيان، 2004، ص 53-54).

غالبا لا يمكن تحديد حجم الأثر المعنوي الذي تحدثه الجريمة المعلوماتية، ولا حتى الاقتصادي لسبب بسيط وهو غياب التبليغ خوفا من وصمة العار. أما تفسير استغلال هذه الخاصية كدافع لاقتراف الجريمة المعلوماتية، فيرجع لمرحلة مهمة من التفكير الإجرامي وهي لحظة التحضير المسبق للجريمة المعلوماتية قبل المرور إلى الفعل le passage à l'acte criminel، حيث أن المجرم يستغل عوامل ضعف الضحية ويدرسها جيدا ليستغلها كنقاط قوة بالنسبة إليه فيلجأ إلى استخدام حسابات مزورة أو وهمة للإيقاع بضحاياه، كما يسعى إلى التغيرير بهم واستدراجهم قدر المستطاع باستخدام اللغة أو الدعاية الإلكترونية المستندة إلى الخطاب الوجداني، والذي يجعل الرشادة العقلانية القائمة وراء اتخاذ القرارات والتفضيلات السلوكية كما هو الحال في التسويق الإلكتروني في مستوى متدني.



3. الخصائص المرتبطة بطبيعة الفضاء السيبراني:

- يوفر الفضاء السيبراني مجموعة من الظروف التي تميزه عن الفضاء الواقعي، وتتمثل في كل من (عبد الجليل، 2017، ص 76):
 - غياب التفاعل الجسدي، حيث لا يوجد تفاعل جسدي بين الأطراف المتواصلة (الجاني، المجني عليه)، ولا تتطلب طاقة وشجاعة كبيرة في مواجهة الضحايا مثل العنف التقليدي، كما يعتمد على المهارة والكفاءة الذهنية والعقلية وليست الجسدية.
 - سهولة الوصول للضحية وصعوبة دفاعها عن نفسها حيث يمكن الوصول للضحية في أي وقت ليلا ونهارا وفي أي وقت وفي أي مكان، كما يصعب على الضحية تجنب العنف الواقع عليها، أو الدفاع عن نفسها أو القضاء على هجوم المجرم.
 - يتطور الإجرام في الفضاء السيبراني بصفة مستمرة مع تطور الأساليب التكنولوجية الحديثة التي تساعد، على بقاء أثر هذا العنف لوقت طويل، كما أنها سلوكيات مستمرة في معظم أحوالها كما في حالات السب والقذف والتشهير ما لم يتم ضبط الفاعل والتدخل الفني لإنهائها.
 - سهولة حدوثه وسرعة انتشاره، وذلك بسبب سرعة انتشار المعلومات الخبيثة والمكذوبة والشائعات وسهولة الوصول إليها، وغالبا ما تكون غير قابلة للاسترجاع، فبمجرد نشرها على الانترنت لا يستطيع المجرم إيقافها.
 - غياب التفاعل الجسدي، حيث لا يوجد تفاعل جسدي بين الأطراف المتواصلة (المجرم والضحية)، ولا تتطلب طاقة وشجاعة كبيرة في مواجهة الضحايا مثل العنف التقليدي، كما يعتمد على المهارة والكفاءة العقلية وليست الجسدية.
- يشكل الفضاء السيبراني مجالا للتحدي المستمر، حيث يشحذ مستخدميه مهاراتهم التكنولوجية باستمرار، لمواكبة التغيرات السريعة مما يلي احتياجاتهم المعرفية. حيث أن تقدير الذات لديهم يرتبط بمدى القدرة على الإنجاز، والتمكن من استخدام المهارات الجديدة والتمكن من استخدام التطبيقات المستحدثة.

4. الخصائص المرتبطة بمواقع التواصل الاجتماعي:

- تتميز شبكات التواصل الاجتماعي بعدة خصائص تجعلها وسيط مناسب بحدوث وانتشار مظاهر العنف الإلكتروني، ومن هذه الخصائص:
 - 1.4. **الجدّة والدوام:** وذلك لأن تأثيرها والتفاعلات تكون فورية ومتجددة دائما، مع إمكانية التغيير الفوري وتفسير منشوراتها عبر التعليقات وتطويعها لأغراض أخرى.
 - 2.4. **التوازن:** وذلك بين الحرية والخصوصية في التفاعل بين المشتركين، فبقدر ما يستطيع الفرد أن يعبر عن ذاته بحرية تامة دون قيود، وينشر آراءه وأفكاره وتعليقاته يجد قدرا كبيرا من الخصوصية في تفاعلاته مع الآخرين.
 - 3.4. **التفاعلية:** وتعد من أهم خصائص شبكات التواصل الاجتماعي حيث وجود مرسل ومستقبل، وتكون الأدوار قابلة للتبديل بينهما، ووجود تأثير متبادل لكل منهما على الآخر.
 - 4.4. **التكرارية:** بمعنى أنه من السهل نسخ صورة أو تعليق أو مقال أو فيديو ما على الانترنت لموقع آخر بدون تغيير أي من ملامحه.
 - 5.4. **البحث:** وهي قابلية البحث عن أصدقاء ذوي اهتمامات واتجاهات متشابهة وهو ما لا يمكن عمله في الحياة العادية.
- كل مستهلك هم ومنتج: حيث إن أي عضو على شبكات التواصل الاجتماعي يمكنه النشر بمجرد أن يصبح عضوا، ما أن أي مستخدم يمكنه كتابة وتعديل وإزالة أي منشور، وأن يقرر ما إن كان سيسمح بالتعليقات أم لا (عبد الجليل، 2017، ص 77-78).

التواصل والتفاعل الافتراضي عبر مواقع التواصل الاجتماعي، يعتمد على العديد من مهارات التفاعل الاجتماعي الواقعي، غير أن هناك بعضا من الخصوصية والحماية التي توفرها فضاءات التواصل الاجتماعي تجعل الرقابة التي يمارسها الأنا الأعلى على السلوكات



الإجتماعية ضعيفة، ومرد ذلك عدم ووضوح معالم الجريمة المعلوماتية في وسط المستخدمين، وعدم مواكبة النصوص القانونية للتطورات التكنولوجية بما يسهل نفاذ الجرمين من العقوبات لان القوانين لا تنطبق على سلوكياتهم الإجرامية المستحدثة.

5. الخصائص المرتبطة بالجرائم والضحية في الجريمة المعلوماتية :

1.5. الجرم المعلوماتي: الجرم الذي يقترب الجريمة المعلوماتية الذي يطلق عليه الجرم المعلوماتي يتسم بخصائص معينة تميزه عن الجرم الذي يقترب الجرائم التقليدية.

فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها -باعتبارها قاعدة عامة- فغن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الأنترنت. فعلى سبيل المثال فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال تتطلب مهارة وقدرة فنية عالية جدا من قبل مرتكبها.

كذلك فإن الدوافع على ارتكاب الجرم المعلوماتي هذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن دوافع ارتكاب الجرائم من قبل الجرم التقليدي (مومني، 2010، ص58-59).

تتميز الجريمة المعلوماتية بأنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالجهة المحني عليها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المحني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك في إخراج الجريمة المعلوماتية على حيز الوجود قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك يتمثل في مساعدة فنية أو مادية (مومني، 2010، ص58).

الجريمة المعلوماتية نشاط إجرامي منظم وخاضع للتحقيق، وهذا التخطيط لا يكون إلا من خلال أفراد مؤهلين في هذا النوع من النشاط، الذي يعتمد على المعرفة بتقنيات الحاسوب والانترنت، فالجريمة المعلوماتية ليست نشاطا إجراميا عشوائيا، بل يخضع لتخطيط مسبق، ومن ناحية أخرى تعد الجريمة المعلوماتية جريمة منظمة لكونها تعتمد على أساليب تكنولوجية أكثر تعقيدا، وتلك الأساليب تكون أكثر صعوبة في الاكتشاف صعوبة في الاكتشاف من قبل أفراد الأمن (جلي و أحمد، 2011، ص220).

2.5. الضحية في الجريمة المعلوماتية: يلعب الضحية دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.

ويرى البعض أن للمجني عليه دورا مثيرا للريبة في بعض الأحيان، فهو قد يشارك بطريق غير مباشر في ارتكاب الفعل، وذلك بسبب وجوده في ظروف تجعل تعرضه لجريمة المعلوماتية أمرا مرتفعا بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية الذي قد يساعد على ارتكاب الفعل الإجرامي، ويترتب على ذلك نتيجة أخرى تميز الجريمة المعلوماتية هي أن هناك إمكانية للحيلولة دون وقوع هذه الجريمة مقارنة بغيرها من الجرائم، غذ يعتمد ذلك أساسا على تطوير نظم الأمن الخاصة بأنظمة الحاسبات وشبكاتها.



وفي الواقع فإن إحجام المخني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية يبدو أكثر ووضحا في المؤسسات المالية مثل البنوك والمؤسسات الإدخارية، حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها على تضاؤل الثقة فيها من جانب المتعاملين معها. حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه فإن ذلك يؤثر سلبا في السياسة التي يمكن أن توضع لمكافحةها، وقد تم طرح عدة اقتراحات تكفل تعاون المخني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي.

وإلى جانب ذلك فإن المخني عليه يتردد أحيانا في الإبلاغ عن هذه الجرائم خوفا من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي إلى تكرار وقوعها بناء على تقليدها من قبل الآخرين كما أن الإعلان عن هذه الجرائم يؤدي أحيانا إلى الكشف عن مواطن الضعف في برنامج المخني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه (مومني، 2010، ص 54-55).

فقدان الثقة في تعامل السلطات المختصة مع مرتكبي تلك النوعية من الجرائم، وذلك لعدم كفاءة القوانين المعمول بها (جلبي و أحمد، 2011، ص 220).

من خلال تحليل سلوكيات المجرم والضحية والدوافع الجنائية، نجد بأن عامل الاستخدام هو الوعي الحقيقي ولا تنفع الحملات التحسيسية أو غيرها في رفع درجته، بمعنى يجب أن يطرح المستخدم السؤال الهدف والمغزى من استخدامه للإنترنت هل لأغراض طيبة أو إجرامية.

6. عوامل إنتشار الجريمة المعلوماتية:

فضلا عن الخصائص التي توفر بيئة خصبة لارتكاب الجريمة المعلوماتية، هناك عوامل كثيرة تساهم في إنتشارها نذكر منها مجموعة العوامل التالية (محمد فولان، 2010، ص 41):

- لا مركزية الأنظمة المعلوماتية، إذ كلما كثرت أجهزة الحاسوب المتصلة بالشبكة الأم كلما كثرت احتمالات الدخول إلى الشبكة.
- ترابط الأنظمة المعلوماتية في كل المستويات سواء الداخلية منها أو الدولية والخاصة أو العامة فإن ربط الشبكة لتبادل المعلومات يعرضها لخطر الفيروسات والدخول غير الشرعي.
- العراقيل ومحدودية البحث، أين تشكل حدود الدول عرقلة جدية لضمان تحديدها بدقة ومعاقبة مرتكبيها بصرامة فلكل دولة تشريعها الخاص لمواجهة الظاهرة علما أن كثيرا من الدول ما تزال تفتقر إلى تشريع في هذا الميدان، ولذلك تعتبر الجزائر من الدول العربية السبابة في هذا الميدان.
- تحديد هوية ومكان المعتدي، ولا يمكن التغلب على هذه الصعوبة إلا بالدخول لبطاقات التخزين لموردي الإنترنت مع ضمان الحياة الخاصة للأفراد.

- ماهية وطبيعة التطورات المعاصرة في البيئة الإقتصادية العالمية، إن التطورات الهائلة التي حدثت خلال السنوات الأخيرة يمكن إرجاعها إلى عنصرين رئيسيين هما تطور التقنية، وتهيئة البيئة العالمية المناسبة. يتمثل العنصر الأول في مدى التطورات الهائلة في تكنولوجيا المعلومات والاتصالات، في حين يتمثل العنصر الثاني في توفير وإتاحة وتهيئة البيئة لانتقال كافة التغيرات ونفاذها من مكان لآخر بدون مواجهة أية حواجز جغرافية، وهو ما يعرف بعولمة السوق أو الإقتصاد (أمير يوسف، 2008، ص 19).

- صورة المعلومات وتطورات المجتمع المعلوماتي: لقد أصبحت المعلومات في بيئة اليوم ترتبط بمختلف جوانب الحياة وتمثل ركيزة نشاط الإنسان الإقتصادي والإجتماعي والثقافي والسياسي، وتتيح المعرفة بالواقع ومشكلاته وأبعاد هذه المشكلات، بل إنها أصبحت تتيح ميكنة إتخاذ القرارات في كافة المجالات تقريبا، وعلى الرغم من تعدد المصطلحات التي تطلق على ثورة المعلومات، إلا أنه بات هناك



نوع من الإتفاق حول مسمى المجتمع المعلوماتي للتعبير عن التقدم التكنولوجي. وتتمثل المكونات الرئيسية للمجتمع المعلوماتي في ثلاثة مكونات رئيسية، هي الحواسيب والاتصالات، والشبكات والوسائط المتعددة (يوسف، 2008، 20).

- تزايد وعي المجرمين بارتفاع عائد جرائم المعلوماتية، وتدني مخاطرها إذا ما قورنت بأية جريمة أو نشاط إجرامي آخر.
- إحباط وإستياء أفراد الطبقة المتوسطة من المجتمع من الأوضاع والضغوط الإقتصادية المهيمنة - تحت وطأة ما قد يتعرضون له من مشاكل حادة - لاستغلال مراكزهم الوظيفية في إدارة وتشغيل الحاسوب لارتكاب الجرائم باستخدامه (محمد سلامة، 2006، 17).

خاتمة:

إن الاستخدام السوي للتقنيات التكنولوجية يخضع لإرادة الإنسان في توجيه هذا الاستخدام، كما أن وضوح الهدف والغاية هما الضمانان الوحيدان للعوي التكنولوجي، والاستجابة لليقظة التكنولوجية والتربية الإعلامية الموجهة للمستخدمين في هذه الخصوص. وفي ختام الدراسة الوصفية لموضوع الورقة البحثية توصلنا لمجموعة من النتائج، ومجموعة من التوصيات المقترحة.

النتائج:

- 1- التبليغ هو المفتاح الأول للوقاية من انتشار الجريمة المعلوماتية، وتوفير أقصى قدر من الحماية من المجرم المعلوماتي.
- 2- الأثر المعلوماتي يمكن الحصول عليه ولو كان المجرم محترفا ومتمكنا في مجال المعلوماتية، إلا أن كل ما يحدث على فضاء الأنترنت يمكن العثور عليه وغير أن الأمر قد يتطلب مهارات متحدة ومدة زمنية أطول.
- 3- الإعلانات المتخللة لمواقع التواصل الاجتماعية المختلفة، تعتمد على مبادئ الإقناع السيكلوجية المرتكزة على الخطاب الوجداني، لتغيب المنطق التحليلي وفقا لما تنص عليه نظرية الترشيح العقلاني في علم التسويق.
- 4- سهولة التخفي وراء أسماء مستعارة أو استخدام حواسيب عمومية مختلفة لممارسة نشاطه الإجرامي، تدفعه لارتكاب الجرائم بسهولة.
- 5- وجود العديد من المستخدمين الذين لا يتقنون التحكم في التكنولوجيا ما يجعلهم عرضة للتعدي المعلوماتي، ويسهل التغيرير والإيقاع بهم.
- 6- هناك علاقة طردية إيجابية بين التطور التكنولوجي وتطور الجريمة المعلوماتية.

التوصيات:

- 1- تعزيز القيم والروابط الأسرية والاجتماعية داخل الأسرة ومنها إلى مجتمع، مع تفعيل أنشطة اجتماعية تشاركية خاصة لفئة الأطفال والمراهقين من طرف مختلف فعاليات المجتمع المدني.
- 2- تنصيب برامج الحماية الأمنية الموثوقة والأصلية ضمن أجهزة الحواسيب والابتعاد عن برامج التحميل المجاني.
- 3- تهيئة المعلومات الشخصية سواء من المواطنين أنفسهم من خلال التكوين والدراسة، أو من خلال الدورات التكوينية للموظفين في القطاعين العام والخاص.
- 4- عدم الاستهتار أمام الاستخدام العشوائي للأنترنت والحسابات المختلفة لمواقع التواصل الاجتماعي من خلال نشر الصور الخاصة، أو الفيديوهات القصيرة.
- 5- الإبتعاد عن استخدام مواقع التواصل الاجتماعي للتسلية، وتعويضها بأنشطة ومهارات حياتية واقعية كالرياضة أو ممارسة الهوايات المختلفة.
- 6- الرقابة الأسرية والتوعية للأطفال والمراهقين بصورة دورية أو مستمرة، تسمح بالوقاية من خطر التصيد المعلوماتي وتجنب الوقوع في فخ الابتزاز الإلكتروني.



قائمة المراجع:

- إبراهيم، ريهام السيد عبد الجليل (أوت 2017)، دور الجامعة في مواجهة مخاطر العنف الإلكتروني عبر شبكات التواصل الاجتماعي "دراسة تحليلية"، مجلة تطوير الأداء الجامعي، المجلد 05، العدد 02، مصر، ص 1-16.
- العريان، محمد علي (2004)، الجرائم المعلوماتية، د ط، دار الجامعة الجديدة للنشر، مصر.
- جابوري، اسماعيل (ديسمبر 2020)، دور الأمن السيبراني في مواجهة التهديدات الإلكترونية دراسة حالة الجزائر، مجلة تحولات، المجلد 03، العدد 02، الجزائر، ص 65-80.
- جلبي، علي عبد الرزاق و أحمد، هاني خميس (2011)، العولمة والحياة اليومية، ط 1، مكتبة الأنجلو المصرية، مصر.
- فولان، محمد (2010)، الحماية القانونية لتكنولوجيات الإعلام، مجلة المحكمة العليا، العدد الأول 01، قسم الوثائق، المؤسسة الوطنية للاتصال النشر والإشهار وحدة الطباعة، الجزائر.
- سلامة، محمد عبد الله أبوبكر (2006)، جرائم الكمبيوتر والإنترنت، ط 1، منشأة المعارف، مصر. مومني، نخلا عبد القادر (2010)، الجرائم المعلوماتية، ط 1، دار الثقافة للنشر والتوزيع، الأردن.
- يوسف، أمير فرج (2008)، الجرائم المعلوماتية على شبكة الإنترنت، بدون طبعة، دار المطبوعات الجامعية، مصر.
- قريعة، عمر والجوزي، وهيب (2021)، العالم الافتراضي فضاء خصص لممارسة الجريمة الإلكترونية في ميدان التجارة الإلكترونية، مجلة علوم الإنسان والمجتمع، المجلد 10، العدد 02، الجزائر، ص 657-689.
- الشناوي، أمينة إبراهيم (2014)، الكفاءة السيكمترية لمقياس التنمر الإلكتروني (الضحية-المعتدي). pdf
- الصبيح، علي موسى والقضاة، محمد فرحات (2013)، سلوك التنمر عند الأطفال والمراهقين (مفهومه-أسبابه-علاجه)، ط 1، جامعة نايف للعلوم العربية الأمنية، الرياض: السعودية.

Vicente, Igone Leon (2015) : cybervictimization by cyberbullying « children at risk and children as risk ».

تم تصفح الدراسة من الموقع: Addi. ehu.es بتاريخ: 2017/3/12، على الساعة: 14.17



أسباب ودوافع انتشار السلوكات الإجرامية عبر الفايسبوك بين الشباب الجزائري.

Causes of the increased criminal behaviors spread on Facebook among Algerian youth

محمد الأمين بن خيرة

جامعة الجيلالي بونعامة خميس مليانة

مقدمة

تشهد المجتمعات في الوقت الحاضر تغيرات ملحوظة على عديد المستويات، خاصة على مستوى سلوك أفرادها في ظل التطور التكنولوجي، من خلال ظهور العديد من المواقع والشبكات الاجتماعية التي ساعدت في تقريب المسافات واختصار الجهد والوقت، بالإضافة لتوفير العديد من الخدمات بتكلفة أقل، والفايسبوك كفضاء افتراضي يدخل ضمن هذه المواقع، ورغم الجوانب الإيجابية التي يتميز بها الفايسبوك، إلا أنه في المقابل لا يمكن تجاهل الجوانب السلبية التي أصبحت تنشر عبره، سواء ما تمثلت في السياسة الخاصة به والتي لا تلزم المستخدم بتأكيد هويته وهو ما قد يساعد في ظهور حسابات مزيفة تسعى للترويج للسلوكات الإجرامية بين الشباب الجزائري، بالإضافة لفقدان المكانة الاجتماعية للأفراد في مجتمعهم وكذا الإقصاء الممارس عليهم داخل دائرة الحياة الاجتماعية، والذي قد يترجم باللجوء للإجرام والانحراف عبر الفايسبوك من أجل حب فرض النفس، بحيث سنحاول في هذه الورقة العلمية التطرق إلى: أولاً: مفاهيم الدراسة

ثانياً: قراءة لإحصائيات حول الجرائم الإلكترونية الأكثر انتشاراً عبر الفايسبوك.

ثالثاً: أنواع الجرائم الواقعة داخل الفايسبوك.

رابعاً: أسباب ودوافع انتشار السلوكات الإجرامية عبر الفايسبوك بين الشباب الجزائري.

1 . مفاهيم الدراسة:

1.1: الجريمة:

1.1.1. الجريمة لغة: "أصل كلمة جريمة من مجرم أي قطع وكسب، أن الكسب المستهجن والمستحب والمكروه، وفي آخر يراد فيها الحمل على فعل آثم ومن ثم يمكننا إطلاق كلمة جريمة على كل فعل أو سلوك مخالف للحق والعدل المستقيم". (بولمين، 2008، ص 16).

2.1.1. اصطلاحاً: "عرفت الجريمة بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة آتمة يقرر له القانون عقوبة أو تدبيراً احترازياً" (صغير، 2013، ص 7)، و"يعرف رادكليف براون R.Bruwn الجريمة بأنها سلوك يقوم من خلاله المجرم بخرق العادات والقيم والقواعد السائدة في المجتمع، مما يتطلب تطبيق العقوبات الجنائية". (هرزاني، 2005، ص 27).

3.1.1. اجرائياً: الجريمة هي عبارة عن كل فعل أو سلوك يعارض القاعدة الجنائية ويقرر له القانون عقوبة أو تدبير احترازي، أي هي عبارة عن كل فعل ينتج عنه ضرر سواء مادياً كان أم معنوياً وتتوفر فيه أركان الجريمة، وتعريف آخر هي عبارة عن كل سلوك مستهجن وخارج عن الأطر الاجتماعية المتعارف عليها، ينتج عنه ضرر فردي أو جماعي.



2.1. الفايبيوك

1.2.1. اصطلاحا: "هو شبكة تواصل اجتماعي مجانية منتشرة عبر الإنترنت، تسمح للمستخدمين بإنشاء متصفحات أو صفحات شخصية وتحميل الصور والفيديو، وإرسال الرسائل إلى العائلة والملاء بهدف التواصل، وطبقا لبعض الاحصائيات فإن مستخدمى الإنترنت فى الولايات المتحدة الأمريكية -مثلا- ينفقون وقتا على الفايبيوك أكثر من أى مواقع أخرى، ويعد موقع الفايبيوك أكثر مواقع التواصل الاجتماعى انتشارا، حيث يرتاده حوالى مليارى مستخدم حول العالم شهريا". (قمحية، 2017، ص24-25)

2.2.1. اجرائيا: يعتبر الفايبيوك كموقع إجتماعى تفاعلى وإتصالى، يتم من خلاله التواصل بين أفراد المجتمع بطريقة سهلة وغير مكلفة، ويعتبر من بين أهم مواقع التواصل الإجتماعى الأكثر استخداما فى العالم تبعا لعدة مميزات كسهولة الإستعمال وقلة التكلفة، بالإضافة إلى تقريب المسافات واختصار الجهد والوقت، كما يمكن تعريفه على أنه عبارة عن فضاء أو تطبيق عبر الشبكة العنكبوتية يساعد فى إنشاء صفحات شخصية وتبادل المنشورات، ونشر الصور والفيديوهات والنصوص، فهو عبارة عن شبكة إجتماعية يساعد الأفراد على الإتصال والتفاعل فيما بينهم.

3.1. الشباب

1.3.1. اصطلاحا: "تمثل مرحلة الشباب حلقة الوصل بين مرحلة الطفولة ومرحلة إكتمال النضج الجسمى والنفسى والإجتماعى للإنسان، حيث تبدأ بتطورات مرحلة المراهقة والبلوغ وتنتهى بالنضج والإستقرار، وقد تم الإتفاق بين أجهزة رعاية الشباب على تحديد مفهوم الشباب فى إطار مرحلة عمرية معينة، تقع ما بين الخامسة عشر وحتى الخامسة والعشرين لتشمل أفراد المجتمع من الجنسين، وهى المرحلة الزمنية التى يحدث فيها التغيرات الفيسيولوجية والجسمية والنفسية حتى يصل الفرد إلى مرحلة الإستقرار النسبى". (غبارى، 2011، ص 188-189)

2.3.1. إجرائيا: يمكن تعريف مرحلة الشباب على أنها المرحلة التى تتميز ببلوغ الفرد ويصبح واعيا ومدركا لموقعه الإجتماعى، أى يمكن تحديدها من 15 سنة والتى قد تمثل فترة المراهقة إلى 25 سنة، وقد نجد أن المشرع الجزائرى يرجع 18 سنة هو سن البلوغ بالنسبة للرجل، و 19 سنة سن البلوغ بالنسبة للمرأة.

4.1. المكانة الإجتماعية

1.4.1. اصطلاحا: "تعرف على أنها عادة ما تعكس مرتبة الفرد أو قيمته داخل جماعة معينة، أو موقف مؤسسى أو اجتماعى، والجماعة هى التى تقرر هذه المكانة، فإذا امتلك الشخص هذه الصفات أو الخصائص أو الممتلكات التى تقدرها الجماعة، سواء أكان رجلا أو امرأة سيحصل على مرتبة عالية، أما الأشخاص الذين يفتقرون لهذه الخصائص فإن مكانتهم بالطبع متدنية". (العبيدى و ولي، 2009، ص 112).

2.4.1. اجرائيا: ويمكن تعريفها على أنها الموضع والمرتبة التى تمنحها الجماعة للفرد تبعا لعدة متغيرات سواء كان العمل، أى أن الشخص الذى له منصب عال تكون مكانته عالية، أو درجة غنى الشخص، أى كلما كان الشخص ثريا كلما كانت مكانته مرتفعة.



2. قراءة لإحصائيات حول الجرائم الإلكترونية الأكثر انتشارا عبر الفايبروك.

- مصالح شرطة مكافحة الجرائم الإلكترونية تسجل 567 قضية تتعلق بجرائم الإنترنت

"سجلت مصالح المديرية العامة للأمن الوطني، المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خلال الـ 08 أشهر الأولى من السنة الجارية، 567 قضية تتعلق بجرائم الإنترنت، تورط فيها 543 شخصا، حيث تمكنت الفرق المتخصصة في مكافحة الجرائم الإلكترونية للأمن الوطني ومن خلال معالجة كافة المعطيات التقنية والأدلة المادية المرتبطة بالقضايا السالفة الذكر، من معالجة 385 جريمة إلكترونية من أصل 567 قضية مسجلة ومحل متابعة لفك خيوطها، وهذا وفق ما توضحه المعطيات الواردة في الجدول التالي: (المديرية العامة للأمن الوطني، 2016)

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الإنترنت	430	289	365	68%
جرائم الاعتداء على سلامة الأنظمة المعلوماتية	57	31	39	55%
جرائم الإحتيال عبر الإنترنت	25	17	32	68%
جرائم التحريض والتطرف عبر الإنترنت	14	14	31	100%
الجرائم المخلة بالحياة	12	08	22	67%
جرائم بيع السلع المحصورة عبر الإنترنت	06	05	15	84%
جرائم مختلفة (نسخ البرامج دون حق، القرصنة)	23	21	39	92%
المجموع	567	385	543	68%

يمثل الجدول التالي 567 قضية خاصة بجرائم الإنترنت تم تسجيلها من طرف الشرطة الجزائرية، بحيث نجد أن جرائم المساس بالأشخاص عبر الإنترنت كانت في المقدمة بـ 430 قضية، وتليها جرائم الإعتداء على سلامة الأنظمة المعلوماتية بـ 57 قضية، ونجد 25 قضية خاصة بجرائم الإحتيال عبر الإنترنت، و 14 قضية خاصة بجرائم التحريض على التطرف عبر الإنترنت، تليها 12



قضية خاصة بالجرائم المخلة بالحياة، و06 قضايا خاصة بجرائم بيع السلع المحضرة عبر الإنترنت، وأخير 23 قضية خاصة بالجرائم المتنوعة (نسخ البرامج دون حق، القرصنة).

يتبين لنا من خلال معطيات الجدول السابق أن الإجرام الممارس عبر الإنترنت شهد ارتفاعا كبيرا من خلال قضايا متنوعة، فقد يحاول الشخص المجرم الإقدام على سلوك إجرامي عبر الإنترنت ظنا منه أنه محمي من المراقبة الأمنية وكذا المجتمعية، وهذا ما قد نشاهده عبر الفضاء الافتراضي وخاصة الفايسبوك أن بعض الأفراد المنحرفين والمجرمين قد يستغلون خاصية عدم إضهار الهوية الحقيقية من أجل ممارسة سلوكاتهم اللامقبولة اجتماعيا، فالإنترنت ورغم الجوانب الإيجابية التي وفرتها، إلا أننا لا نستطيع إنكار سلبياتها والتي قد نجد أنها أثرت على الأمن القومي للشعوب والدول، خاصة في ظل خطابات الكراهية التي عرفت انتشارا رهيبا في الآونة الأخيرة تبعا للعديد من الإحصائيات والدراسات العلمية.

3. أنواع الجرائم الإلكترونية الواقعة داخل الفايسبوك: تتعدد وتنوع الجرائم الواقعة داخل الفايسبوك، ومن أهم هذه الجرائم نذكر: **1.3. القرصنة الإلكترونية:** "تعني تمكن الفاعل من البرامج والبيانات الالكترونية والحصول عليها دون إرادة مالكها، وقد يشكل فعل القرصنة الإلكترونية أحيانا اعتداء على حق الملكية الفكرية متى توافرت شروط البرنامج أو البيانات لاعتباره داخلا في نطاق حماية حقوق المؤلف الفكرية". (المساعدة، 2005، ص60)

فالفايسبوك كغيره من مواقع التواصل الاجتماعي قد يكون من بين أكثر المواقع تتم فيها ممارسة السلوكات الإجرامية والجرائم الإلكترونية، وخاصة قرصنة المعلومات وحسابات الأشخاص، وقد يكون ذلك بهدف أخذ معلومات وبيانات الأفراد من أجل استخدامها لأغراض إجرامية، دون أن ننسى السرقة العلمية للأفكار وكذا الأعمال العلمية، وهي ظاهرة قد أصبحت منتشرة بكثرة وخاصة في الوسط الجامعي، من خلال أخذ الباحث أو الطالب المعلومة ونسبها لنفسه دون ذكر صاحبها أو مرجعها الأصلي.

2.3. انتحال الشخصيات: "ما زالت عمليات انتحال شخصيات المشاهير تنتشر بقوة في الشبكة العنكبوتية متخذة منها مكانا خصبا للتشويه وترويج الشائعات وكسب المال وتحريف الحقائق عن مسارها" (مبارك فضل الله، 2011، ص21)، وبالرجوع للواقع المعاش من خلال تصفح موقع الفايسبوك قد نجد العديد من الحسابات التي ترجع أسماءها لمشاهير مثلا كلاعي كرة القدم أو المغنيين أو حتى شخصيات سياسية، فأصحاب هذه الحسابات قد يحاولون ترويج سلوكاتهم الإجرامية سواء ما تمثل في زرع الفتن والتحريض على خطابات الكراهية من جهة، وكذا محاولة التستر خلف تلك الأسماء المزيفة حتى لا يكشف أمرهم، وقد تساعدهم تلك الحسابات الوهمية والمزيفة في الترويج للشائعات على غرار الأخبار الكاذبة.

4. أسباب ودوافع الترويج للسلوكات الإجرامية عبر الفايسبوك بين الشباب الجزائري:

1.4. توفر الحرية لدى المستخدم عبر الفايسبوك:

من خلال تتبع الواقع الاجتماعي المعاش قد نجد أن بعض الأشخاص المنحرفين والمجرمين يرون في منصات التواصل الاجتماعي عامة والفايسبوك خاصة على أنه يساعدهم في التعبير عن أفكارهم وآرائهم بحرية وبعيدا عن الضغوط الاجتماعية، "فالمواقع الإلكترونية قد أصبحت مؤثرة بعبارة سب وقذف وتهديد وابتزاز، جرائم إلكترونية ترتكب من خلف منصات التواصل الاجتماعي، بمختلف حساباتها

الالكترونية من فايسبوك وتويتر وانستجرام وسناب شات وواتساب ويوتوب ورسائل نصية، ظنا من بعض مرتكبيها أنها تعبير عن الحريات الشخصية أو التعبيرية، لكنها في الحقيقة تعرض أصحابها للوقوع تحت طائلة قوانين العقوبات والجرائم الإلكترونية والاجراءات الجنائية" (الوردي، 2020، ص12)، فقد نجد أن الواقع الافتراضي وفر خاصية لا توجد في الواقع الحقيقي وهي الهوية المزيفة، أي أن الشخص المجرم أو المنحرف قد يلجأ إلى الجنوح عبر الفايسبوك بهدف عدم معرفته وكشف هويته من طرف الضحايا الممارس



عليهم الفعل الإجرامي، وهنا يتبين لنا أن الفضاءات الافتراضية وفي مقدمتها الفيسبوك قد وفرت جو لهؤلاء المنحرفين من أجل الترويج لأفعالهم الانحرافية والإجرامية بعدا عن الرقابة المجتمعية، وقد نجد أن الفئة الأكثر ترويجا ومشاركة للعديد من الجرائم الإلكترونية تتمثل في الشباب، فقد يمارس الشباب العديد من الأفعال الإجرامية ظنا منهم أنها حرية التعبير، وهو ما شاهدناه في الآونة الأخيرة في الجزائر من خلال النشر والترويج لخطابات الكراهية عبر مواقع التواصل الاجتماعي.

2.4. غياب المراقبة الوالدية:

وقد نجد أن الأسرة التي تعتبر أهم حلقة في المجتمع، المسؤول الأول عن الترويج لخطاب الكراهية من عدمه عبر أبنائها، "...حيث يبدأ الوالدان في زرع أولى البذور التي تكون شخصية الإنسان، فإذا يبدروا المحبة وقبول الآخر واحترامه، وإذا يبدروا الكراهية والعنصرية البغيضة التي تتحكم بعد ذلك في تصرفات الشخص ونظرته لمن حوله" (مسرور. 2019)، وبالرجوع للواقع الاجتماعي المعاش قد نجد أن الأسرة قد ساهمت بقسط كبير في اكتساب أفرادها لسلوكات إجرامية، خاصة في ظل توفير الهواتف الذكية للأبناء منذ الصغر وتودهم عليها، بالإضافة لعدم متابعة المواقع والبرامج التي يقصدها، وهو ما قد يدفع بالشباب إلى الغوص في متاهات هذه التكنولوجيات وخاصة عبر مواقع التواصل الاجتماعي من أجل إبراز أنفسهم أو سب وشتم الآخر، وحتى الترويج لخطابات الكراهية والتشجيع على العنف ونبد الآخر، ومنه يمكن القول أن وظيفة الأسرة تتعدى توفير الحاجات الأساسية الخاصة بالأكل والشرب واللباس إلى الرعاية النفسية والاجتماعية للأبناء، أي قد نجد أن هناك قطيعة بين الآباء والأبناء وهو ما قد يصعب على الأب فهم ابنه وكذا معرفة أهم السلوكات والأفكار التي تحول في خاطره، في ظل ظهور العديد من التكنولوجيات والمواقع الافتراضية، والتي قد يرى الشاب فيها أنها تعتبر كمتنفس حقيقي له بعيدا عن المراقبة الوالدية والمجتمعية.

3.4. البحث عن تحقيق مكانة اجتماعية:

"تعد الهوية بين الواقع والافتراضي بالظاهرة الغير صحية سواء للفرد أو المجتمع، وغالبا ما تكون هذه الإزدواجية سببا رئيسا في حدوث الانعزالية والإنطواء لدى مستخدمي الإنترنت، وذلك لشعور هؤلاء بنوع من الراحة في هذا المجتمع الافتراضي الذي استطاع إشباع بعض الحاجيات التي لم يستطع إشباعها في الواقع، فالمستخدم يتعمد تغيير هويته وشخصيته بالكامل للقيام بأمر لم يكن مسموحا له القيام بها على الواقع كالسب والقذف والتعليقات الخارجة، حيث يعتبر ذلك نوعا من التحرر من تابوهات المجتمع وضغوطاته" (أوسامة، 2018، ص 141)، فقد نجد أن إقصاء الشباب أو تهميشه من طرف أفراد أسرته أو مجتمعه يؤدي به إلى الولوج للفضاء الافتراضي من أجل البحث عن مكانة إجتماعية له، خاصة الأفراد الذين يتم نبذهم واحتقارهم من طرف مجتمعهم، فقد يسعون جاهدين من أجل إثبات مكانتهم وتحقيقها بطرق مشروعة، وإذا وجدوا نوع من عدم التقبل والرفض قد يلجؤون إلى أساليب وطرق غير مشروعة كالسب والشتم عبر الفيسبوك، التشهير بالأشخاص، التهديد ومحاولة قرصنة حسابات الآخرين... إلخ.

4.4. وقت الفراغ: "ويعتبر من بين أسباب انحراف الشباب، فالفراغ داء قاتل للفكر والعقل والطاقت الجسمية، إذ لا بد للنفس من حركة وعمل، فإذا كانت فارغة من ذلك تبتلد الفكر وضعف العقل وحركة النفس، واستولت الوسواس والأفكار الرديئة على القلب" (يوسف أبو زيد، 2017، ص 52)، ففراغ الفرد الدائم قد يجعله يلجأ إلى الانحراف والإجرام ويصبح أكثر قابلية له، والمتتبع للواقع المعاش يرى أن العديد من الشباب ممن لا يعملون، نجدهم طول النهار وهم على الأرصفة وفي محطات الحافلات وحتى أمام المؤسسات التربوية يتعقبون الفتيات ويتحرشون بهم، لهذا فالفراغ قد يشكل دافع لإنحراف الشباب، أو الإجرام عبر الفضاءات الافتراضية من خلال تعلم كيفية قرصنة الحسابات وكذا التهديد وابتزاز الغير.

5.4. الدافع السياسي: "استغلت مواقع التواصل الاجتماعي لخدمة معتقداتها وتوجهاتها السياسية، لما لها من قدرة على التأثير والتغيير، ولما لدى الأفراد والجماعات من عقائد وأفكار سياسية معينة، قد تكون تابعة لدول أو جماعات أو شركات تراها معادية



لها" (بن يعرف، 2019، ص 55)، فقد نجد أن مواقع التواصل الاجتماعي وفي مقدمتها موقع الفايسبوك أصبح فضاء خصبا يتم فيه الترويج للجرائم على اختلاف أنواعها، خاصة تلك المتعلقة بالجانب السياسي، وهو ما نلاحظه في واقعنا الاجتماعي المعاش، ففي الجزائر مثلا كلما اقترب موعد الانتخابات إلا وقد لاحظنا أن الفايسبوك قد أصبح به كم هائل من الصفحات ذات الطابع السياسي، فمنها من قد تسعى للتجريح في أشخاص على حساب آخرين، وأخرى قد تحاول منع الانتخابات، وأخرى قد تسعى للتشويش على المواطنين بمحاولة إقناعهم بضرورة التصويت على شخص معين، ناهيك عن بعض الألفاظ والمسميات التي تم إطلاقها من طرف فئة المقاطعين كـ "الأصبع الأزرق..."، فالفايسبوك قد أصبح له تأثير بالغ في الحياة السياسية، كيف لا وهو الذي قد أسقط العديد من الحكومات والدول خاصة في فترة الربيع العربي.

6.4. الرغبة في الانتقام: "يلجأ البعض إلى ممارسة الإجرام عبر مواقع التواصل الاجتماعي، ويكون ذلك لشعورهم بالظلم وانتابتهم الرغبة بالانتقام من الأشخاص والهيئات" (بن يعرف، 2019، ص 55)، فالانتقام عبر مواقع التواصل الاجتماعي وبالأخص الفايسبوك قد أصبح يعرف منحى تصاعدي، وبالرجوع للواقع الاجتماعي المعاش قد نجد أن بعض الأفراد الذين تم تهميشهم أو حتى وصمهم من طرف أفراد مجتمعهم بصفات بغيضة تبعا لسلوك انحرافي أو إجرامي قاموا به في السابق، قد لا يتقبلوه وهو ما يجعلهم يحبون الانتقام بشتى الطرق، وكما هو معلوم أن الفايسبوك أصبح يوفر خاصية انشاء الحسابات المزيفة عبره دون طلب تأكيد هوية المستخدم، فقد يستغل هؤلاء الأشخاص المنحرفين أو المجرمين أو الذين مورس عليهم الوصم الفرصة بمحاولة الانتقام عبر الفضاء الافتراضي، خاصة إذا كان الشخص المراد الانتقام منه بعيدا أو لا يستطيع الجاني الوصول إليه، فالفايسبوك قد يساعده في الانتقام بشتى الطرق سواء التشهير بنشر الصور الشخصية، السب والقذف، إلصاق عيب بشخص ما... إلخ.

7.4. دوافع المالية (الربح وكسب المال): "وذلك بالرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي، قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقرار جرائمهم من اجل تحقيق المكاسب المالية" (محمد المايل، 2019، ص 249)، أي أن الأفراد الممارسين للإجرام الإلكتروني قد يكون هدفهم الأول كسب مبالغ مالية، سواء ما تمثل في تهديد أفراد بضرورة دفع أموال وإلا يتم التشهير بصورهم والمس بحياتهم الشخصية، وهذا ما قد يمارس على رجال السياسة ورجال الأعمال بالدرجة الأولى، تبعا لمكانتهم الاجتماعية والخوف من فقدانها، بالإضافة للإحتيال على أفراد بسطاء من خلال الترويج لخدمة ربحية معينة عبر مواقع التواصل الاجتماعي، دون أن ننسى سرقة البرامج الإلكترونية والأعمال العلمية ومحاولة إعادة بيعها.

خاتمة:

تعتبر ظاهرة الجريمة قديمة قدم الإنسان، وقد تتطور بتطور الوسائل والأساليب التقنية، وهذا ما يمكن تسميته بالجرائم المستحدثة أو المستجدة، أي هناك جرائم كانت في الماضي وأعادت الظهور في الحاضر ولكن بتطور وتغير أساليب استعمالها، وهناك جرائم أخرى جديدة ظهرت مع التغيرات الاجتماعية الحاصلة داخل النسق الاجتماعي، وكما هو معلوم أن الجرائم الإلكترونية تصنف ضمن الجرائم المستحدثة أو المستجدة، بحيث تنوعت وتعددت هذه الأخيرة تبعا لتنوع وسائل ممارستها، فهي لم تعد تقتصر على من يملك جهاز حاسوب فقط، بل تعدت إلى الهواتف الذكية واللوحات الرقمية وحتى الساعات الذكية، تنشط في فضاء افتراضي يصعب تشخيص مقدار الضرر الناجم عنها، وتبعا لهذه الورقة العلمية قد نجد أنه من أسباب ودوافع نشر السلوكات الإجرامية للشباب عبر الفايسبوك تكون راجعة لحب الظهور تبعا لفقدان المكانة الاجتماعية للأفراد والشباب، وكذا التسهيلات التي أتاحها موقع الفايسبوك بتقصص الشخصيات وإنشاء حسابات وهمية عبره، والرغبة في الانتقام، بالإضافة للدوافع السياسية وكذا غياب الرقابة الوالدية على مثل هذه المواقع، دون أن ننسى رغبة البعض في جني أرباح مالية جراء ممارستهم للإجرام الإلكتروني. ومن بين أهم الإقتراحات التوصيات التي يمكن الوصول إليها مايلي:



- ضرورة القيام بندوات وملتقيات لتحسيس والتوعية بالمخاطر التي قد تنجم عن سوء استخدام مواقع التواصل الاجتماعي عامة والفيسبوك خاصة.
- يجب على الأولياء تشديد الرقابة على الأبناء حول كل ما يتابعونه عبر المواقع الإلكترونية.
- ضرورة توجيه الشباب لأعمال أخرى قد تعود عليهم بالنفع كمطالعة الكتب أو ممارسة الرياضة لتجنب الإجرام والانحراف عبر الفيسبوك.
- يجب تعزيز الرقابة الأمنية على بعض الصفحات والمجموعات الفيسبوكية المضللة.
- يجب سن قوانين وتشريعات بهدف حماية الأشخاص عبر الفيسبوك تبعاً لما أصبح يحدث فيه من إجرام بمختلف أنواعه.

قائمة المراجع:

أ- الكتب:

- 01- العبيدي، محمد جاسم و ولي، باسم محمد. (2009). المدخل إلى علم النفس الاجتماعي. ط1، عمان: دار الثقافة للنشر والتوزيع.
 - 02- غباري، محمد سلامة محمد. (2011). التنمية ورعاية الشباب. د.ط، الإسكندرية: المكتب الجامعي الحديث، مصر 2011.
 - 03- فضل الله، وائل مبارك خضر. (2011). أثر الفيس بوك على المجتمع. ط1، السودان: فهرسة المكتبة الوطنية أثناء النشر.
 - 04- قمحية، حسان أحمد. (2017). الفيسبوك تحت المجهر. ط1، الجزيرة: النخبة للنشر والتوزيع، مصر.
 - 05- هرزاني، نوري ياسين. (2005). الإعلام والجريمة. د.ط، كورديستان: منتدى اقرأ الثقافي.
 - 06- الورد، سعيد. (2020). جرائم السب والقذف عبر وسائل التواصل الاجتماعي والمواقع الإلكترونية. ط1، الرياض: دار الآفاق المغربية للنشر والتوزيع.
 - 07- يوسف أبوزيد، مصطفى. (2017). مشكلات الشباب-فيروس الهجرة غير الشرعية. ط1، بيروت: المكتب العربي للمعارف للنشر.
- ### ب - رسائل وأطروحات دكتوراه:
- 08- أوسامة، عمر. (2018). تكنولوجيا وسائل الإعلام والاتصال والإغتراب الرقمي للطلاب الجامعي. أطروحة دكتوراه، شعبة علوم الإعلام والاتصال، جامعة عبد الحميد ابن باديس مستغانم، الجزائر.
 - 09- بن يعرف، فايزة خليفة أحمد. (2019). المواجهة التشريعية والأمنية للجرائم المتصلة بمواقع التواصل الاجتماعي. رسالة ماجستير، إدارة مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة.
 - 10- بولمين، نجيب. (2008). الجريمة والمسألة السوسولوجية دراسة بأبعادها السوسيوثقافية والقانونية. أطروحة دكتوراه، علم اجتماع التنمية، جامعة منتوري قسنطينة، الجزائر.
 - 11- صغير، يوسف. (2013). الجريمة المرتكبة عبر الإنترنت. رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر.

ج - المجلات العلمية:

- 12- محمد المايل، عبد السلام و محمد الشريحي، عادل و قابوسة، علي. (2019). الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم- الأسباب-سبل المكافحة مع التعرض لحالة ليبيا. مجلة آفاق للبحوث والدراسات. 2(04)، 245-255.

<https://www.asjp.cerist.dz/en/downArticle/665/2/2/125980>

- 13- المساعدة، نائل علي. (2005). أركان الفعل الضار الإلكتروني في القانون الأردني. مجلة دراسات علوم الشريعة والقانون، 32(01). تم الإسترجاع الموقع التالي:

<https://books-library.net/files/books-library.online-12301940Bj8J1.pdf>

د- مواقع إلكترونية:



14- المديرية العامة للأمن الوطني. (2016). مصالح شرطة مكافحة الجرائم الإلكترونية تسجل 567 قضية تتعلق بجرائم الإنترنت. الجزائر، تم الإسترجاع يوم 2022/04/03، من الموقع التالي:

<https://www.algeriepolice.dz>

هـ- الجرائد:

15- مسرور أحمد. (2019). خطاب الكراهية... الأسباب وآليات المواجهة. جريدة الدستور، عمان، تم الاسترجاع من الموقع التالي: <https://www.addustour.com/articles/1118963>

التوصيات

الجرائم الإلكترونية في المجتمع الجزائري

تشخيص الواقع وتحديات الأمن السيبراني



توصيات الملتقى الوطني: الجرائم الالكترونية في المجتمع الجزائري: تشخيص الواقع وتحديات الأمن السيبراني 15 مارس 2022

توصيات عامة:

1. ترقية الملتقى الوطني الى ملتقى دولي بالشراكة مع المؤسسات الأمنية والقضائية.
 2. نشر مداخلات الملتقى الوطني في كتاب جماعي ذو ترقيم دولي
- كما عكفت لجنة التوصيات على حصر وانتقاء توصيات المداخلات العلمية المنتقاة للملتقى الوطني محاور المشاركة بأعادها الثلاث: "البعد القانوني، والبعد الأمني، والبعد السوسيوولوجي" وخلصت الى ما يلي:

البعد القانوني

1. غرس الثقافة الحاسوبية وسط المجتمع، وخاصة لدى رجال الأمن والقانون.
2. تعديل قانون العقوبات لينص على تجريم الجرائم الالكترونية ، او سن قانون مكافحة الجرائم الالكترونية. 3. ضرورة وضع إستراتيجية وطنية لنشر الوعي وثقافة الجرائم الالكترونية لدى مختلف شرائح المجتمع للوقاية من الجرائم الالكترونية .
3. حتمية إنشاء مراكز للسلامة المعلوماتية، والتبليغ الفوري للجرائم المعلوماتية.
4. التعريف بالجرائم الإلكترونية وكيفية التعامل معها، وتوضيح مدى خطورتها، وتعليم آليات مواجهتها وطرق التحقيق والإثبات فيها.
5. حجب المواقع المشبوهة مثل المواقع الجنسية والتي لها آثار مدمرة على الصعيد النفسي والاجتماعي.
6. التكوين " الرسكلة" الجيد للقضاة في مجال المعلوماتية لتأهيلهم لمعالجة القضايا بسهولة .



7. تحديد مجال أولوية تدخل القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال مع القطب الجزائري المالي والاقتصادي في الجرائم المالية والاقتصادية المرتكبة عبر الكمبيوتر.
8. تعديل قانون العقوبات ليشتمل على تجريم الجرائم الالكترونية ، او سن قانون مكافحة الجرائم الالكترونية.
9. تغليظ عقوبة الجرائم الالكترونية ، واعتبار خطورة الجريمة ، بتهديدها للأمن الداخلي والعالمي وحجم الضرر ، من الظروف المشددة للعقوبة التي ترفع مستوى الجريمة لتصبح جنائية.
10. تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة السيبرانية حيث ان التسليم بمبدأ العالمية اضحى ضرورة مجابهة النشاط الاجرامي المعلوماتي بصوره المختلفة بعد استفحال خطره و انتشار آثاره في أكثر من دولة مقابل عجز مبادئ الإقليمية النص الجنائي على التصدي لها .
11. ضرورة إعادة النظر في التشريعات الإجرائية في الجزائر المتعلقة بحماية الحرية الشخصية وحرية الحياة الخاصة من الوسائل الإلكترونية.
12. العمل على انشاء محاكم للقضايا الافتراضية على شبكة الانترنت لتتمكن من التعامل مع هذه الانواع المستحدثة من الجرائم.
13. ضرورة تحيين التنظيمات والتشريعات الخاصة بردع الجرائم السيبرانية وهذا بصفة دورية، مع تشديد العقوبات.

البعد الأمني

1. ردع الجريمة السيبرانية و تحفيز ثقافة وطنية للأمن السيبراني.
2. دورات تكوينية في الأمن السيبراني للطلبة الجامعيين لخلق وعي بالأمن السيبراني بالتنسيق والتعاون مع الجهات الأمنية.
3. تحديث أنظمة الحماية المستخدمة وبرامج مكافحة الفيروسات.
4. التأكد من العناوين الالكترونية التي تتطلب معلومات سرية "كبطاقات الائتمان" كي لا يقع ضحية النصب والاحتيال.
5. تنظيم عمليات توعية وتحسيس لنشر الوعي السيبراني من خلال القيام بملتقيات وأيام دراسية مشتركة مع المؤسسات الامنية قصد تعريف الطالب الجامعي بالجرائم الالكترونية وسبل تفاديها .
6. تطوير قدرات التقنية على شبكة الانترنت، وإنشاء شرطة الانترنت للقبض على مرتكب الجرائم حال دخولهم على الشبكة من خلال التتبع الفني للجهاز او الخط الهاتفي الذي ارتكبت منه الجريمة.
7. العمل على تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم الالكترونية
8. إتخاذ التدابير والإجراءات التي تعتمد على عنصر الأمن السيبراني هي جد ضرورية في الإنتاج، لاسيما ما يخص الشبكات والبرامج والأجهزة الإلكترونية المستخدمة.



9. وضع إستراتيجية سببرانية وطنية واضحة وملزمة، لكل المعنيين بصناعة المعلومات ووسائل الاتصالات، والبنى التحتية، كما لأولئك المعنيين بإستخدامها من موظفي المؤسسات ومختلف شرائح المجتمع المدني.
10. حتمية إنشاء مراكز للسلامة المعلوماتية، لطوارئ الإتصالات مثل عدة الدول الأخرى .
11. تأهيل وتدريب وتكوين الأجهزة القضائية المختصة، و عناصر الأمن للقيام بواجبها على أحسن وجه في مجال ملاحقة ومحكمة المجرمين السببرانيين.
12. تحويل الأمن السببراني إلى جزء من خطط التنمية بإستراتيجية وطنية شاملة يتدخل فيها جميع الأطراف.
13. تنسيق الجهود والاعتماد على الكفاءات و اطلاق مشاريع بحثية باعتبارها جسر للتواصل بين الباحثين والأكاديميين والمهنيين لتعزيز الهياكل الوطنية وتقييم الإنجازات التي تم تحصيلها من طرف الهيئات المدنية او العسكرية المعنية بمكافحة الجريمة السببرانية
14. استحداث هيئة مركزية مختصة في الأمن السببراني ومستقلة عن المؤسسات الأمنية الأخرى، هدفها البت في القضايا الماسة بأمن المؤسسات الكبرى وصياغة إستراتيجيات الأمن السببراني من جهة، والتنسيق بين المؤسسات الأمنية وتكوين إطاراتها في الأمن السببراني من جهة أخرى.

البعد السيبرولوجي

1. -تنصيب برامج الحماية الأمنية الموثوقة والأصلية ضمن أجهزة الحواسيب والابتعاد عن برامج التحميل المجاني.
2. -عدم الاستهتار أمام الاستخدام العشوائي للإنترنت والحسابات المختلفة لمواقع التواصل الاجتماعي من خلال نشر الصور الخاصة، أو الفيديوهات القصيرة والابتعاد عن مواقع التسلية بتعويضها
3. الرقابة الأسرية والتوعية للأطفال والمراهقين بصورة دورية أو مستمرة، تسمح بالوقاية من خطر التصيد المعلوماتي وتجنب الوقوع في فخ الإبتزاز الإلكتروني قيام ملتقيات وندوات والتوعية لسوء استخدام التواصل مع تسديد الرقابة الأنباء
4. يجب سن قوانين وتشريعات بهدف حماية الأشخاص عبر الفايبرسوك تبعاً لما أصبح يحدث فيه من إجرام بمختلف أنواعه مع تعزيز الرقابة الأمنية.
5. -ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية والاقتصادية المترتبة عن الاستخدام السلبي للتكنولوجيا.
6. -ضرورة غرس ثقافة التبليغ لدى المواطنين لأي ممارسة إجرامية قد تعترضهم في البيئة الرقمية.
7. العمل على تحديث التقنيات باستمرار للتمكن من التصدي لهذا النوع من الجرائم.
8. ضرورة خلق فرق أمنية مختصة في مراقبة المضامين الرقمية الموجهة للأفراد و إنشاء مراكز لتبليغ عن الجرائم السببرانية.
9. ضرورة حجب الدولة لأي موقع ترى أنه يسهم في زيادة الانحلال الأخلاقي ويشكل تهديدا لقيمنا الاجتماعية.



10. انشاء مراكز بحوث مشتركة بين جميع التخصصات لدراسة الجرائم السيبرانية ميدانيا و تفعيلها .
11. العمل على توعية افراد المجتمع بجميع شرائحه بمدى خطورة الجرائم السيبرانية مع نشر ثقافة امنية تتماشى مع تطورات الاجهزة التكنولوجية و العالم الافتراضي عن طريق الوسائل الاعلامية وكافة مؤسسات التنشئة الاجتماعية.
12. وضع السلطات والهيئات المختصة، بالتعاون مع منظمات المجتمع المدني، الخطط والبرامج الشاملة، التي من شأنها القضاء على العوامل المؤدية إلى الإجرام أو الظروف المهيئة لمع حل المشاكل والآفات الاجتماعية.
13. تقديم النصح والإرشاد والنصح وذكر الأمور السلبية و المخاطر وهذا التوجيه يكون مباشر ليتعلم الطفل كيف يسلك طريق معين يتناغم مع عمره ومرحلة نموه ومتطلبات حياته اليومية دون انحراف عن القواعد والأعراف الاجتماعية من خلال التربية السليمة ووضع تشريعات توفر الحماية الاجتماعية والآفات الآخرة .
14. -تحقيق احتياجات الفرد داخل البناء الاجتماعي، وفق ما هو مقبول اجتماعيا ومتوافق نفسيا ومضبوط قانونيا، لبناء وعي فردي سليم يؤدي بالضرورة إلى وعي جماعي أو مجتمعي كامل زيادة حملات التوعية في المؤسسات الرسمية غير الرسمية.
15. -ضرورة غرس ثقافة التبليغ لدى المواطنين لأي ممارسة إجرامية قد تعترضهم في البيئة الرقمية مع اتخاذ كافة تدابير الحماية الأمنية.
16. -ضرورة وضع آليات لرصد الظواهر الإجرامية الرقمية وتحليل أثارها على الأمن القومي للدولة وذلك بتنسيق مع الخبراء والمختصين في عديد المجالات بهدف استخلاص استراتيجية دفاعية استباقية نابعة من الميدان وهادفة إلى تحصين الأمن القومي من إي اختلالات قد تمس به. مع تطوير برمجيات آمنة.
17. باعتبار ان الجرائم السيبرانية هي جرائم انتشرت على المستوى العالمي فمن الضروري وجود تعاون فعلي بين مختلف الدول في الحد ومواجهة هذه الجرائم، وهذا ما تم العمل عليه بالفعل في اطار الإعلام الأمني الذي شمل العديد من الخدمات والجوانب في عملية محاربة الجرائم السيبرانية، لذا لا بد التركيز على تطوير وتكثيف أجهزة الإعلام الأمني وتحديث نشاطاته والحرص على التزامن مع التحديثات السريعة التي يعرفها العالم اليوم، في المجال التكنولوجي وبالتالي في مستوى الجرائم السيبرانية التي تزداد خطورة وتعقيد .
18. العمل على توفير وتكوين قدرات بشرية تتميز بالكفاءة والخبرة في المجال التقني والرقمي وتمتلك مهارات خاصة بالفضاء الإلكتروني.
19. -إنشاء تخصصات متعلقة بالجرائم المعلومات والجرائم الإلكترونية ودمجها في مختلف المعاهد والجامعات والاعتماد على احدث الطرق في التدريس والتدريب، وتحسينها بصورة دورية تبعا للتطورات التي تحدث في مجال التقني والمعلوماتي .



20. -ضرورة وضع قوانين خاصة لها القدرة على حماية مستخدمي الأنترنت والمنصات الالكترونية دون التقييد من حريتهم،

وضرورة تطبيق العقوبات المتعلقة بها في ارض الواقع ومحاولة تطوير القوانين وجعلها اكثر صرامة في جرائم الفضاء

السيبراني .

21. -مكافحة الجرائم بكافة أنواعها المستحدثة وغير المستحدثة مسؤولية الجميع، من الفرد إلى الأسرة إلى المجتمع إلى

الدولة، كل له دوره في إصلاح نفسه، وإصلاح أسرته وإصلاح مجتمعه.

22. -يبدو واضحا أن التهميش سبب رئيسي في الدخول في عالم الجريمة، وعليه يكون على عاتق الدولة ضرورة التكفل

بالفئات التي تعاني من القهر النفسي والاجتماعي، خاصة تلك التي تعاني من متاعب مادية، دون أن ننسى الأخلاقية

23. -انتشار الجرائم في المجتمعات المتطورة التي حققت إشباعها المادي، دليل واضح على أن هذه الجرائم تتمكن من النفوس

التي تعاني من فراغ روحي، وبالتالي فتتنمية المعنوي والرضا الداخلي آلية فعالة في مكافحة السلوكيات الإجرامية.

لجنة التوصيات:

د. رقية محمودي، رئيسا، جامعة يحيى فارس المدية.

د. حاج الله مصطفى، رئيس اللجنة العلمية للملتقى. جامعة يحيى فارس المدية

أ. د عمور محمد، جامعة يحيى فارس المدية

د. بن عائشة نبيلة، جامعة يحيى فارس المدية

د. قاسم سعاد، المركز الجامعي أفلو.

د. لكحل صليحة، جامعة تيسمسيلت.

رئيسة الملتقى

د/ رقية محمودي

01	كلمة السيد مدير جامعة يحيى فارس المدية أ.د جعفر بوعروزي
03	كلمة رئيسة الملتقى، د. محمودي رقية
07	تقديم، أ.د معتوق جمال، رئيس الجلسة الافتتاحية للملتقى.
	الجلسة الافتتاحية
11	قراءات في الجريمة السيبرانية أ.د/معتوق جمال، جامعة علي لونيسي البلدية 2.
22	التحديات القانونية لمواجهة الجرائم السيبرانية د. حمالي سمير، نائب رئيس مجلس قضاء المدية
	ضحايا الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في الوسط الطلابي من وجهة
53	نظر الطلبة الجامعيين، دراسة ميدانية على عينة من الطلبة الجامعيين . د. محمودي رقية، ط.د خيزاوي مراد، جامعة يحيى فارس المدية.
	البعد القانوني
83	دور القطب الجزائي في مكافحة الجريمة السيبرانية د/ رمال أمين، جامعة تلمسان
96	الجهود الدولية لمكافحة الجريمة الالكترونية د/ بن عائشة نبيلة، د/ القينعي بن يوسف، جامعة يحيى فارس المدية.
104	إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية د. بوعافية رضا، جامعة برج بوعريريج.
117	مكافحة الجرائم الالكترونية في التشريع الجزائري د. بوخالفة سعاد، جامعة الجزائر 1، كلية الحقوق
127	اللغة الجنائية في الجرائم الالكترونية نمط للتحقيق ووسيلة للإثبات د. حاج الله مصطفى، ط.د جمعة محمد، جامعة يحيى فارس المدية..

- إجراءات البحث والتحري في الجريمة الالكترونية
- 134 د/ ليندة بومحراث
- ط.د عبد النور سعيداني، جامعة الأمير عبد القادر للعلوم الإسلامية.
- 152 جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني
- أ.د/ حفيظ مبارك، ط.د عبد القادر أسماء، جامعة الأمير عبد القادر للعلوم الإسلامية - قسنطينة-
- 160 الإثبات الجنائي بالوسائل المستحدثة للجرائم الإلكترونية (دليل رقمي) نموذجاً
- ط.د سماحي سمية، جامعة طاهري محمد - بشار
- 174 سلطة القاضي الجنائي في تقدير الدليل الرقمي
- ط.د ين حليلة سعاد، جامعة غليزان
- مراقبة الاتصالات الالكترونية في التشريع الجزائري وتأثيرها على الحقوق والحريات
- 180 ط.د/ فاطمة ضيف الله ، جامعة يحيى فارس المدية
- ط.د/ محمد الأبيض، جامعة الجزائر 2
- البعد الامني
- المؤسسة الأمنية ومكافحة الجريمة الإلكترونية:
- 192 أمن ولاية تمنراست بالمرصاد للتهديدات السيبرانية
- د. نجيبة هبهبوب، جامعة سكيكدة
- ط.د شعيب شنيقي، جامعة تامنغست
- 202 دور الأجهزة الأمنية في محاربة الإجرام السيبراني.
- د. عائشة عبد الحميد،
- الجريمة الالكترونية وتهديدها للأمن الاجتماعي في الجزائر
- 214 أ.د/ عبد العزيز ديلمى، جامعة حسيبة بن بوعلی شلف
- ط.د كمال عمتوت، جامعة طاهري محمد- بشار
- 224 دوافع وأسباب ارتكاب الجرائم الإلكترونية في المجتمع الجزائري.
- د. سهيلة بن دادة، جامعة باجي مختار عنابة
- 236 تحديات الأمن السيبراني في مكافحة الجرائم السيبرانية في المجتمع الجزائري
- ط.د صواق عبد القادر، جامعة غرداية.
- الجريمة الالكترونية ودوافع ارتكابها
- 246 د. بن مزيان حنان، د. بومدين إيمان

- جامعة يحيى فارس المدية.
- 257 الآليات المستخورة لمواجهة تحديات الأمن السيبراني في الجزائر
ط.د بوعرعار عادل، جامعة يحيى فارس المدية.
- 268 الاجرام السيبراني
ط.د مكيد نبيل، جامعة يحيى فارس المدية.
- 276 آليات مواجهة المخاطر السيبرانية في المجتمع الجزائري مقارنة بالنظام الدولي.
ط.د لعمر يوي ليلي، ط.د صيلع سعد، المركز الجامعي مرسلبي عبد الله تيبازة.
- البعد الاجتماعي
- المخدرات الرقمية (Les Drogue Numérique) ومدى استيعاب المجتمع
لأضرارها.
- 288 د. بوزيان خير الدين، د. نوار بورزق
جامعة العربي التبسي - تبسة
- المحتوى الرقمي ومدى مساهمته في تفاقم السلوك الإجرامي لدى الأطفال في المجتمع الجزائري
- 300 عرض تحليلي لمحتويات - youtube kids -
د. نبيح أمينة، جامعة الجزائر 03
د. غراز الطاهر، جامعة جيجل.
- دو وسائل التواصل الاجتماعي في انتشار ظاهرة التنمر السيبراني لدى الطلبة الجامعيين -
دراسة تحليلية نظرية
- 312 د. بضيف عادل، د. باشا ياسمين
جامعة يحيى فارس المدية.
- تحليل أبعاد السلوك الإجرامي الرقمي وانعكاساته على المستوى الفردي والمجتمعي.
- 324 أ.د واكلي بديعة، ط.د بوعمامة منال.
جامعة محمد لمين دباغين - سطيف 2
- السلوك الإجرامي الرقمي وانعكاساته على المجتمع الجزائري.
- 332 د. ولد قويل خليفة، ط.د مصايح أمال.
جامعة آكلي محند أولحاج - البويرة
- الجريمة المعلوماتية عبر المنصات الإلكترونية.
- 346 د. معطاوي موسى، ط.د تواتي نعيمة

- جامعة آكلي محمد أولحاج البويرة
- آليات ممارسة جريمة التحريض عبر مواقع التواصل الاجتماعي - فايس بوك أنموذجا
- 359 د. قدوح نور الهدى، جامعة يحيى فارس المدية
- المخدرات الرقمية: ادمان حديث عبر الفضاء الرقمي
- 366 د. رتيمة أسماء، ط.د بخوش شيماء
- جامعة يحيى فارس المدية
- العملة الرقمية و الجرائم السيبرانية :
- 375 الدوافع الفاعلة في الفعل الاجرامي الرقمي-رؤية سوسيولوجية-
- ط.د مرازقية عادل، جامعة يحيى فارس المدية
- قراءة سوسيولوجية للدراسات العربية في مجال مكافحة الجرائم الالكترونية
- 386 د. بن عاشور الزهرة، جامعة علي لونيسي البليدة 2
- د. بأحمد أسامة، جامعة يحيى فارس المدية
- تظاهرات العنف والسلوك الاجرامي الرقمي عبر المنصات الالكترونية بالمجتمع الجزائري
- 403 على ضوء دراسة استطلاعية ميدانية.
- ط.د قطاب نور الدين، ط.د بخيرة أحمد.
- جامعة غليزان
- 416 خصائص الفضاء السيبراني المهينة للسلوك الإجرامي
- ط.د جلول دليلة، جامعة الحاج لخضر باتنة 1.
- أسباب ودوافع انتشار السلوكات الإجرامية عبر الفايسبوك بين الشباب الجزائري.
- 424 ط.د بن خيرة محمد الأمين، جامعة الجيلالي بونعامة خميس مليانة.
- 429 توصيات الملتقى



Yahia Fares University Medea
Faculty of Humanities and Social Sciences
The University's Formative Research Project Team-PRFU
Cybercrimes in the Algerian society, their effects
and how to confront them
Code :I05L02UN260120190001

Virtual National Forum
(via teleconference)



Cybercrime in the Algerian society:

**Diagnosing reality and
cybersecurity challenge**

March 15, 2022

Forum committee:

Honorary President of the Forum: Prof. Jaafar Bouarouri,
Rector of Yahya Fares University Medea
Honorary Director of the Forum: Prof. Moussa Hissam,
Dean of the Faculty of Humanities and Social Sciences
President of the Forum: Dr. Mahmoudi Reguia
Coordination and Supervision: Dr. Djaballah Youssef
Head of the Scientific Committee: Dr. Hadj Allah Mustafa,
Head of the Organizing Committee: Dr. Banaoula Muhammad

Members of the Scientific Committee

Prof. Dr. Mezari Toufik Abdel Samad Yahya Fares University of Medea
Prof. Dr. Djamel Matouk.....Ali Lounisi University, Blida 02
Prof. Dr. Houiti Ahmed University of Algiers 02
Prof. Dr. Souakri taher Ali LounisiUniversity, Blida 02
Lieutenant-Colonel Dekiche AbdelGhani.....National Institute of Criminalistics
and Criminology of the National Gendarmerie
Hamani Samir Vice-president of the judicial council of Meadea
Dekani Nabil Medea council First Assistant Attorney General
Takroust Ali Medea Council Senior Investigating Judge
Prof. Dr. Menadli Mohamed..... Yahya FaresUniversity, Medea
Prof. Dr. Ammour Mohamad Yahya Fares University, Medea
Prof. Dr. Ben Guettaf Mohamad Yahya Fares University, Medea
Prof.Bouhaia Wassila University of Oran 02
Dr.Ledraa Nabila University Center MorsliAbdellah,Tipaza
Prof. Dr. Rami Halim..... University of Blida 02
Prof. Dr. Bibimoune Kalthoum Hadj Lakhdar University Batna
Dr. Amimeur Abd el Kader University of Blida 02
Dr. Kounei Youssef..... Yahya Fares University, Medea
Dr. Mahmoudi Reguia Yahya Fares University, Medea
Dr. Ben Aicha Nabila.....Yahya Fares University, Medea
Dr.Ouldkouil Khalida Akli Mohand Oulhadj University, Bouira
Dr.Mataoui Moussa Akli Mohand Oulhadj University,Bouira
Dr. Ladrem Ahmed Yahya Faris University, Medea
Dr. Retimi Asma Yahya Fares University, Medea
Dr. Kassem Souad Aflou University Center
Dr.Ghoualem Amina Yahya Fares University, Medea
Dr. Belkacem Adel Yahya Fares University, Medea
Dr. Senoussi Hayet Yahya Fares University, Medea
Dr. Lakehal Saliha..... Tissemsilt University Center

Cybercrime in the Algerian society:

Diagnosing reality and



Preamble:

Cybercrime is a new emerging form of crime. It is the product of technological development and digital revolution; it has developed from being computer crimes, information fraud, to being identified as Internet crimes related to the automated processing of data, considering the computer a virtual environment for committing illegal activities such as cyber fraud, hacking, spamming accounts, identity theft, computer viruses and hate crimes, a space where the common denominator is the use of technology and information.

E-crime falls into many categories that vary depending on the methods used, the type of victim, the offender's profile and his operational level (individual, social, global), and difficulty levels. The offenses committed take many forms in cyberspace that guarantees a certain degree of confidentiality on a regional or international scale.

The cybercrime patterns, and the characteristics of the criminal act and the criminal in cyberspace are numerous, emphasizing the gap between the conventional criminal offense in physical reality, and the electronic criminal act in virtual reality. The theoretical approaches analysis also differ to determine the underlying factors to commit the cyber offense from those related to cyberspace "social and criminal learning", "public pressures" and "socio-economic factors", highlighting the correlation between online connectivity and the growing e-criminalization.

Like every other country, Algeria is witnessing an increased growth in cybercrime rates as declared by the security and juridical institutions, which reflects the reality and implications of cybercrime and

its relationship to the digital space that imposes new dimensions and challenges at both the legislative and security levels, to determine the complementary relationship to detect and resolve the digital offense within a digital jurisprudence that align with its specificity by identifying it and defining the with its specificity by identifying it and defining the methods of proof and investigation "the authenticity of digital evidence".

Accordingly, our problem revolves around a realistic diagnosis of cybercrime and the cybersecurity challenges in Algerian society and its repercussions on the individual and society.

Objectives of the conference:

1. Diagnosing the reality of cybercrime in Algerian society.
2. Determining the cybercrime implications and their relationship to cyberspace and its repercussions on the individual and society.
3. Disclosure of new dimensions intertwined with the legislative and security aspect to reveal the circumstances of the digital criminal act.
4. Indication of cybersecurity challenges in fighting cybercrime in Algerian society.

Forum topics

The legal dimension

- Topic 01: Cyber-criminal legislation philosophy.
Topic 02: The reality and challenges of legal legislation in facing cybercrimes.
Topic 03: Legal problems related to investigative and evidentiary methods of digital evidence.

The security dimension:

- Topic 01: The reality of cybercrimes in Algerian society "Measuring cybercrime"
Topic 02: Cyber threats and their impact on societal security.
Topic 03: Cybersecurity challenges in combatting cybercrime.

The sociological dimension

- Topic 01: The transition of crime from the physical reality to the virtual reality.
Topic 02: The cyber-criminal behavior on digital platforms.
Topic 03: Analyzing the dimensions of cyber-criminal behavior and its impact on individuals and society.



Proceedings of the
Virtual National Conference

CYBERCRIME IN ALGERIAN SOCIETY

Diagnosing reality and cybersecurity challenges

March, 15th 2022

legal deposit: July 2022

Preparation and editing:
Dr. Mahmoudi Reguia
Dr. Guedouh Nour El Houda

Cover Design : Fouad Hallouane