

## الجريمة الإلكترونية وسبل مواجهتها في الجزائر Cybercrime and ways to combat it in Algeria

عبد الكريم زنتوت<sup>(1)</sup>

<sup>(1)</sup> جامعة الجزائر 2 (الجزائر)

zentoutkarim@gmail.com

تاريخ النشر:

2025/04/01

تاريخ القبول:

2025/03/15

تاريخ الارسال:

2025/01/20

### الملخص:

تعد الجريمة الإلكترونية من الجرائم التي ظهرت نتيجة الاستغلال السيئ للوسائل التكنولوجية الحديثة، كما أنها تختلف عن الجرائم التقليدية في طبيعتها وخصائصها وأنواعها ودوافعها والوسائل المستعملة في ارتكابها، بالإضافة إلى خصوصية مرتكبي هذه الجريمة، الأمر الذي يجبرنا إلى معالجة هذه الظاهرة لا سيما من خلال الوقوف على مختلف القوانين المكرسة لمواجهتها في الجزائر، والبحث عن أهم الحلول للتصدي لها.  
الكلمات المفتاحية: جريمة إلكترونية، سبل، مواجهة.

### Abstract:

Cybercrime is one of the phenomena that has arisen as a result of the delinquent use of modern technological means, and it differs from traditional crimes in terms of nature, characteristics, types, motives and means used, in more characteristics of the perpetrators of these crimes, which prompted us to try to explore this phenomenon by examining the various laws devoted to dealing with it in Algeria, the search for the most important solutions to deal with it.

**Key words:** cybercrime, means, confrontation.

## مقدمة:

يشهد العالم المعاصر حالياً ثورة هائلة في مجال تكنولوجيات المعلومات والاتصال بمختلف وسائلها الحديثة، أدى إلى تطورات كبيرة في خدمات الإنترنت وتزايد أعداد ونسب مستخدميها وأصبح الإتصال سهل بين الأفراد والمؤسسات والدول من خلال إستخدام أجهزة الحاسب الشخصي والمحمول والهواتف الخلوية، ولقد ظهر نمط جديد من الإعلام يعتمد على النشر من خلال المواقع الإلكترونية على الإنترنت، وأصبح الإعلام الإلكتروني هو أحد الوسائل الأساسية التي يعتمد عليها حالياً الأفراد في قضاء العديد من الحاجيات الضرورية، لكن لهذه الوسائل والتكنولوجيا بطبيعتها لها إيجابيات وسلبيات، كل هذا زاد من تطورها من خلال ظهور ما يسمى بالعملة الإعلامية والإتصالية التي أصبحت من بين معالمها هي إختصار العالم في قرية صغيرة يصبح كل الأفراد بإستطاعتهم الولوج في عالمها والعيش فيها رغم بعدهم عنها، وكل هذه الوسائل التكنولوجية والشبكات المعلوماتية التي فرضتها ظاهرة العملة تتحكم فيها القوى العظمى وتتصرف وتسيطر عليها وتبث كل ما هو منافي للقيم والعادات والتقاليد التي تتميز بها الدول العربية والإسلامية.

ومن بين الإيجابيات التي تتميز بها هذه التكنولوجيات الحديثة أنها يستطيع الفرد أن يلاحظ كل ما يحيط به في العالم من معلومات وأخبار وغيرها كما تساعده على قضاء الحاجيات الضرورية وتزويده بمختلف العلوم والمعارف، غير أنها إذا خرجت عن عملها الإيجابي فتستغل في غير محلها، وتصبح نقمة على الأفراد والأسر والمجتمعات، من خلال الإستغلال غير العقلاني لهذه التكنولوجيات الحديثة من خلال الوسائل التكنولوجية والمعلوماتية المتطورة في إرتكاب العديد من الجرائم الإلكترونية المتصلة بشبكات الإنترنت ضد الأفراد والأسر والمجتمعات، ومن بين هذه الجرائم الإلكترونية هي: تبييض الأموال عبر الوسائط التكنولوجية الحديثة، نشر الصور الإباحية، إستغلال القصر والفتيات تحت التهديد، تحطيم قاعدة المعطيات للأشخاص والدول والمؤسسات، التشهير وغيرها من الجرائم التي تدخل ضمن خانة الجرائم الإلكترونية، وأن وجود الجرائم الإلكترونية (المعلوماتية) يتوجب على كافة المهتمين بالشأن الأمني والقانوني إلى خلق إطار قانوني يقوم على تصنيفها وتقسيمها وضبطها، وفرض العقوبات الردعية اللازمة لحماية الأفراد والمجتمعات من تأثيرها وحماية كل النشاطات بمختلف أشكالها التي تستخدم شبكات الانترنت.

تهدف هذه الدراسة إلى تسليط الضوء على ظاهرة الجريمة الإلكترونية دراسة نظرية وكذا المعالجة القانونية لها وفق قانون العقوبات الجزائري، وفي هذا الإطار يمكن للمشروع الجزائري أن يحدد طبيعة الأحكام القضائية التي تحد من إنتشار وتطور هذه الظاهرة الدخيلة على المجتمع الجزائري المرتبطة أساسا بتطور مختلف الوسائل التكنولوجية الحديثة والتغلب عليها.

ومن هذا المنطلق يمكننا طرح الإشكالية الآتية:

ما هي الجريمة الإلكترونية؟ وما هي سبل مواجهتها في الجزائر حسب أحكام قانون العقوبات الجزائري؟

لمعالجة هذه الإشكالية سيتم إتباع المنهج التحليلي وتقسيم الدراسة إلى مبحثين:

- المبحث الأول: السياق النظري والمفاهيمي للجريمة الإلكترونية.

- المبحث الثاني: العقوبات المقررة على مرتكب الجريمة الإلكترونية.

المبحث الأول: السياق النظري والمفاهيمي للجريمة الإلكترونية.

المطلب الأول: مفاهيم:

توجد العديد من المفاهيم حول الجريمة الإلكترونية وذلك وفق كل حقل من الحقول العلمية والمعرفية نتطرق إلى البعض منها من خلال هذا المطلب.

الفرع الأول: مفهوم الجريمة:

توجد العديد من التعاريف للجريمة وتعرف من الناحية السوسيولوجية: سلوك سيء غير مرغوب فيه من الناحية الإجتماعية، إذ أن هناك أنماط من السلوك المضادة للنظام الإجتماعي والأخلاقي، ليس من الضروري أن تدخل ضمن نطاق الجريمة كجرائم اللباقات البيضاء، التي هي شكل من أشكال السلوك المنحرف التي يمارسها كبار الأعمال فهي من وجهة النظر الإجتماعية تعتبر إنحرافا، بينما لا تشكل من الناحية القانونية جرائم.<sup>1</sup>

من خلال هذا التعريف السابق نستطيع أن نعرف الجريمة وفق النظرة السوسيولوجية " هي عبارة عن ظاهرة إجتماعية موجودة في المجتمع، أي بمعنى آخر أنها وجدت بوجود المجتمعات الإنسانية وهي عبارة عن أفعال يقوم بها الأفراد نتيجة العلاقات

<sup>1</sup>. طلعت إبراهيم لطفي، دراسات في علم الإجتماع الجنائي، ط1، دار غريب، القاهرة، 2008، ص 17

الإنسانية المتداخلة فيما بينهما وطبيعة المصالح المرتبطة بهذه العلاقات، ولهذا تنتج عنها سلوكات تكون غير سوية".

#### الفرع الثاني: تعريف المعلوماتية:

فهو مشتق من كلمة المعلومات (Information)، وهي الكلمة التي شاع إستعمالها منذ الخمسينيات في العديد من التخصصات ومهام شتى مما جعل لها في الإستخدام المدرج كثير من المفاهيم.<sup>1</sup>

المعلومات في اللغة الإنجليزية والألمانية والروسية تعني كلمة (Information) اللاتينية الدالة حسب الأصل على شيء للإبلاغ والتوضيح، أو على عملية (Process) الإبلاغ أو النقل أو التوصيل هو نفس ما يعنيه لفظ «Xinxi» المقابل لها في اللغة الصينية.<sup>2</sup>

#### الفرع الثالث: تعريف جرائم الحاسب الآلي:

هي عبارة عن السلوكات التي تعتبر اعتداء على الأجهزة الإلكترونية سواء في العناصر المادية المتمثلة في الإدخال والإخراج أو العناصر المعنوية وتتمثل في المعلومات التي تم تخزينها في الجهاز الآلي.

#### الفرع الرابع: تعريف جريمة الإنترنت:

سلوك غير شرعي على المواقع الإلكترونية بهدف توقيفه أو إتلاف أو تغيير والولوج غير الشرعي للمسائل غير المسموح الولوج إليها، وأستعمال عناوين مزيفة للولوج إلى منظومة المعلومات، واختراق الشبكات وتحميل الفيروسات أو إرسال الرسائل بكل أشكالها عبر البريد الإلكتروني كمثال على ذلك التي يضرب كرامة الإنسان أو من أجل تعميم مواد استهلاكية معينة أو سلوكات غير صالحة (مشروعة).

#### - الفرع الخامس: تعريف الجريمة الإلكترونية:

تشكل الجريمة الإلكترونية من عنصرين هما الجريمة (crime) والإلكترونية (cyber) ويستعمل مصطلح الإلكترونية لتصوير معلومة تعتبر جزء من الحاسب أو عصر المعلوماتية، فالجريمة فهي عبارة عن سلوكات وأفعال سيئة معاقب عليها في القانون

<sup>1</sup> عزة محمود خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي: دراسة مقارنة في

القانون المدني والشرعية الإسلامية، رسالة ماجستير، قانون وشرعية، القاهرة، 1994، ص 18.

<sup>2</sup> سوير سفيان، جرائم المعلوماتية، رسالة ماجستير، العلوم الجنائية والإجرام، كلية الحقوق والعلوم

السياسية، تلمسان، 2011، ص 09.

الجنائي، والجريمة الإلكترونية هي "تجاوزات التي ترتكب ضد الأشخاص أو الجماعات من الأفراد بهدف الجريمة، بمعنى تشويه سمعة الضحية أو ضرر مادي أو نفسي للضحية مباشرة أو غير مباشرة باستعمال الوسائط شبكات الاتصالات مثل شبكة الإنترنت"<sup>1</sup> من التعاريف السابقة يمكن أن نقول أن الجريمة الإلكترونية هي جريمة حديثة ترتكب من طرف الأفراد والعصابات ضد الأشخاص والمجتمع والمؤسسات الحكومية نتيجة الاستخدام السيئ للوسائل التكنولوجية الحديثة.

### المطلب الثاني: الخصائص والمميزات التي تتصف بها الجريمة الإلكترونية:

تتميز الجريمة الإلكترونية بمجموعة من الخصائص والمميزات وهي كالآتي:

#### الفرع الأول: الجريمة الإلكترونية خفية ومستترة

أن الجريمة الإلكترونية "بأنها في الغالب خفية ومستترة، لأن ضحية هذه الجريمة لا يلاحظها رغم أنها قد ترتكب في حالة وجوده بالشبكة العنكبوتية، الجاني يتميز بمؤهلات فنية تجعله قادر على تنفيذ جريمته بدقة كبيرة، كنقل الفيروسات، والإعتداء على الأموال والمعلومات الخاصة أو تسريبها والتجسس على المكالمات الهاتفية والتي تتم عن طريق الوسائط الافتراضية وغيرها من السلوكات المضادة للمجتمع"<sup>2</sup>.

#### الفرع الثاني: الجرائم الإلكترونية تتعدى الحدود الوطنية:

تعتبر أنها من الجرائم التي لا يعتد بالحدود الجغرافية للبلدان ولا بين القارات، فمن خلال تطور شبكات الاتصالات بين بلدان العالم وبين القارات أستطاع ربط عدد معتبر من وسائل الكمبيوتر عبر العديد من بلدان العالم بهذه الشبكة العنكبوتية، حيث يكون المجرم في بلد والضحية في بلد آخر، وهكذا فالجرائم المعلوماتية ترتكب في الغالب عبر حدود دولية كثيرة.

وخلاصة القول أن الجريمة الإلكترونية تعتبر عابرة للحدود بمعنى أنها ترتكبها العصابات الإجرامية في تنفيذ العمليات الإجرامية خارج الحدود الجغرافية للبلدان التي تنتمي إليها هذه العصابات.

<sup>1</sup>. البدانية دياب موسى، "الجرائم الإلكترونية: المفهوم والأسباب"، ورقة مقدمة للملتقى العلمي حول

الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، 2-09/03/2014 بعمان، ص 03.

<sup>2</sup>. الكعبي محمد عبيد، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، دط، دار النهضة

العربية، القاهرة، 2009، ص 31.

لا توجد هناك في الوقت الحاضر عوائق تقف حاجزا أمام توصيل المعلومات والبيانات بين الأجهزة الآلية المنتشرة في مختلف بلدان العالم عبر الشبكة المعلوماتية فيمكن في بضع دقائق إرسال عدد كبير من المعلومات بين جهاز وآخر يبعد عنه آلاف الكيلومترات، كما يمكن أن يرتكب الجرم من مجرم من بلد معين على ضحية من بلد آخر. في وقت قصير جدا مسجلة خسائر كبيرة لا سيما مع الدور الكبير الذي تقدمه الشبكة العنكبوتية، خاصة في إختصاص التجارة الإلكترونية والإعتماد الكبير على البنوك.<sup>1</sup>

### الفرع الثالث: الجريمة الإلكترونية من الجرائم الناعمة:

إن الجريمة الكلاسيكية تحتاج إلى بدل جهد عضلي قوي لإرتكابها كالقتل والإعتداء على الأموال والممتلكات وغيرها من الجرائم، فالجرائم الإلكترونية لا تحتاج أدنى جهد عضلي بل تعتمد على بدل جهد أساسه الدراسة الذهنية والجهد العقلي والعلمي المدروس القائم عن معرفة التقنيات المتطورة للكمبيوتر.

### الفرع الرابع: الجرائم الإلكترونية صعبة الإثبات:

في كثير من الأحيان يصعب العثور على عامل مادي للجريمة المعلوماتية ولعل العامل في ذلك يعود إلى إستعمال المجرم أجهزة فنية وتقنية على قدر كبير من التعقد في الغالب، كما يتمثل السلوك المشكل للركن المادي فيها بشغل سريع لا يتطلب حتى ثوان بالإضافة على ذلك سهولة مسح الدليل والتلاعب به في الزمن الذي لا تحتاج فيه هذه الجرائم إلى الدليل المادي الكلاسيكي.<sup>2</sup>

من خلال الخصائص والمميزات السابقة التي تميزت بها الجريمة الإلكترونية أن أغلبها هي خصائص ومميزات الجريمة المنظمة، وبمعنى آخر أنها تعتبر جريمة منظمة تعمل على تكوينها جماعات وعصابات إجرامية تهدد بها الأفراد والدول.

### المطلب الثالث: تصنيف مرتكبو الجرائم الإلكترونية:

يصنف المجرمين الذين يقومون بالجرائم الإلكترونية كالآتي:

<sup>1</sup>. قورة نائلة عادل محمد فريد، جرائم الحاسب الإقتصادية: دراسة نظرية تطبيقية، دط، دار النهضة العربية، القاهرة، 2003، ص 49.

<sup>2</sup>. سالم محمد علي وهجيج حسون، الجريمة الإلكترونية، مجلة بابل للعلوم الإنسانية، جامعة بابل كلية الحقوق، العراق، العدد 2، 2004، ص 92.

## الفرع الأول: المثلثين (المراهقين)

في الغالب يعتبرون أشخاص غير مدربين أو لديه مهارة، وهم فئة الشباب الذين تتجاوز سنهم ما بين 13-26 سنة والذين لديهم هدف يصلون إلى الإعتراف الاجتماعي، وهم الذين يريدون أن يكونون في واجهة الضوء في أجهزة الإعلام، وتتصف أفعالهم بأنها تدفع إلى الخراب عالميا ولكنها لا توجد على المستوى الشخصي، مثل الحرمان الكثير من مواقع هامة في نشاط المعاملات التجارية الإلكترونية في شهر فبراير عام 2000 والتي عملت على تحقيق أضرار كبيرة لهذه الشركات وفي أغلب الأحيان كما يعمل على مهاجمة المثلثيون أنظمة المعطيات بفيروسات طوروها من خلال الإنتاج المعرفي لهم، وخطرهم الفعلي على شخص لا يستطيع أن يذكر وغالبا ما يتوقعون في سن 26 سنة عندما يصبحون يفهمون نتائج أعمالهم.

## الفرع الثاني: الجشع- المدفع (المجرمون المهنين):

وهذا النوع من مجرمي الإنترنت خطير، وهذه الفئة عادة ما تكون عديمة الضمير وهم على إستعداد لارتكاب أي نوع من الجرائم طالما أنها تجلب لهم المال حيث بدأوا في إنتاج المواد الإباحية وغالبا ما تسمى السبيرية للمواد الإباحية والتي تشمل الإباحية القانونية وغير القانونية على شبكة الإنترنت، أنهم عادة ما يكونوا أذكيا جدا ومنظمون ويعرفون كيفية الهروب من وكالات إنقاذ القانون ومجرمو الإنترنت هؤلاء يرتكبون الجرائم الخطيرة، وخاصة في جرائم إباحية الأطفال والقمار الإلكتروني وهذه تشكل تهديدا خطيرا للمجتمع.

## الفرع الثالث: الافتراضي-الإرهابيون:

هم مجموعة من الأحداث والأكثر خطورة، والدفع الأساسي لهم ليس المال فقط ولكن أيضا لديهم قضية ما والتي يدافعون عنها، وعادة ما ينغمسون في إرسال رسائل التهديد وتدمير البيانات المخزنة في الغالب في نظم المعلومات الحكومية لمجرد أن يسجلوا وجهة نظرهم، ويمكن مقارنة تهديد الإرهاب الإلكتروني بتهديدات السلاح النووي، والبيكتريولوجية أو الكيمائية، هذه المسألة المرتبطة بالهمم هي أنهم لا يعملون داخل حدود الدولة، بل يمكن أن يعلموا من أي مكان في العالم، وهذا يجعل من الصعب اقتناصهم.<sup>1</sup>

<sup>1</sup>. البداينة دياب موسى، "الجرائم الإلكترونية: المفهوم والأسباب"، المرجع السابق، ص 24-25.

يمكن لنا أن نقول الجريمة الإلكترونية التي يقومون بها الإرهابيون الذين يرتكبون أعمالهم باستخدام الوسائل التكنولوجية الحديثة، أو عن طريق تنفيذ نشاطاتهم عبر الأوساط الافتراضية لضرب أهدافهم معينة والمتمثلة سواء في الأفراد أو الدول، كما يمكن أن تكون جرائمهم تنفذ في أي مكان إقليمي جغرافي في العالم.

### المطلب الثالث: أنواع الجرائم الإلكترونية:

يمكن حصرها في الأنواع التالية وهي كالآتي:

#### الفرع الأول: تعديل البرنامج المعلوماتي:

ويتم البرنامج المعلوماتي عن طريق التلاعب فيه بغرض إختلاس المال عن طريق البرامج المعلوماتية، كما حدث عندما قام أحد المبرمجين بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بوسيلته الخاصة حيث قام بإضافة 10 سنتم بمصاريف إدارة الحسابات الداخلية على كل عشرة دولارات وقام بقيد المصاريف الزائدة في حساب خاص به أسماه Zzwick وتمكن من الحصول على مئات الدولارات كل شهر، وقد تم إكتشاف هذه الجريمة بالمصادفة فأراد البنك بمناسبة تأسيس شركة جديدة للدعاية والإعلان أن يكافئ أول وآخر عميل له وفق للترتيب الأبجدي وحينئذ أكتشف عدم وجود ما يدعى Zzwick .

#### الفرع الثاني: جريمة الإعتداء على البيانات الموجودة في النظام المعلوماتي:

ويتم الإعتداء على المعلومات المدرجة بالنظام المعلوماتي بوسيلتين:

- الوسيلة الأولى: التلاعب في المعلومات: يتم من خلال إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي لكي يحصل من خلال هذا الإدخال عن غرضه الإجرامي.
- الوسيلة الثانية: إتلاف المعلومات: ويتم إتلاف المعلومات عن طريق إستبدالها أو محوها من على النظام وقد حدث ذلك حينما قام شخص بإختلاس 61.000 دولار، وهي عبارة عن مبالغ مرسلة من شركات التأمين إلى إحدى المراكز الجامعية حيث قام المحللون بمحو كل الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز وجعلها غير قابلة للتحصيل.

#### الفرع الثالث: جريمة التلاعب على البرنامج المعلوماتي:

ويتم التلاعب في البرنامج المعلوماتي عن طريق زرع برنامج فرعي غير مسموح به في البرنامج الأصلي ويسمح من خلاله الدخول إلى العناصر الأساسية للبرنامج الأصلي، كما حدث في فرنسا عندما قام تشكيل عصابي مكون من عدة أفراد يعملون في إحدى الشركات

بالإستلاء على مبالغ مالية من أرصدة وحسابات العملاء، وذلك خلال إستغلال النظام المعلوماتي للشركة.<sup>1</sup>

نستنتج من خلال هذه الفئة من المجرمين أن أغلب جرائمهم تتم الإعتداء على البرامج المعلوماتية التي تكون ضمن الأجهزة سواء التابعة للمؤسسات العمومية أو الخواص.

#### الفرع الرابع: جرائم السب والقذف عبر الإنترنت:

وهي الجرائم التي ترتكب ضد الأفراد بإستعمال النظام الإلكتروني عن طريق الشبكة العنكبوتية المادة 297 من القانون العقوبات الجزائري السب ب" يعتبر السب كل كلام سيء أو مصطلح يحتوي على تحقير أو قدحا لا يركز على إسناد ظاهرة".

يمكن أن نعرف القذف بأنه" هو إسناد وصمة محددة تتطلب عقاب من تنسب إليه أو التندر إسنادا عموديا يفيد نسبة الأمر إلى الفرد على أن يحتوي ذلك إسناد ظاهرة معنية إلية"

فالفارق بين السب والقذف يتعلق بإسناد وصمة محددة إلى شخص في حين أن السب لا يتعلق بذلك.<sup>2</sup>

إن جرمي السب والقذف عن طريق الوسائط الافتراضية ضد الأشخاص من بين الجرائم التي انتشرت بكثرة مؤخرا نظرا للإستغلال السيء للوسائل التكنولوجية الحديثة.

#### الفرع الخامس: الدخول إلى المواقع المعادية:

مصطلح المواقع المعادية هو مصطلح جديد ظهر استعماله بعد التطور التكنولوجي الذي نستخدمه حاليا ومنتجي تلك المواقع المضادة، قد أستغلوا تلك التطور التكنولوجي لخدمة حياتهم الشخصية في طرح أفكارهم الشخصية الكاذبة والمواقع المضادة قد يتم أنشاؤها لتحقيق أغراض معينة منها الإساءة إلى الدين الإسلامي الذي يعتبر دين التسامح والتعايش الديني بين الأفراد، والهدف الآخر والإيذاء إلى دولة معينة أو إلى تصرف سياسي معين،

<sup>1</sup> شريهان ممدوح حسن، الجريمة الإلكترونية وسبل مواجهتها على المستويين الوطني والمحلي، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية، عمان، العدد 21، 2020، صص 12-13.

<sup>2</sup> فريحة حسين، الجرائم الإلكترونية والأنترنت، المجلة المعلوماتية، دار المنظومة السعودية، السعودية، العدد 36، أكتوبر 2011، صص 06-07.

ويقف بذلك في الغالب معارضي النظام القائم والدين يحالون نشر الأخبار الفاسدة، والتي تؤدي إلى الفتنة والفرقة بين أفراد الشعب أو الإساءة إلى فرد معين بما يعبر عن وضعية دينية أو سياسية أو وطنية وغيرها من الأهداف التي ترمي للإساءة إلى شخصية أو فرد أو شخصية إعتبارية أو حزب أو عائلة أو غير ذلك.

#### الفرع السادس: جريمة القرصنة:

تواجه شبكة الإنترنت ما يسمى "بالقرصنة" من قبل بعض الجماعات التي تؤمن بالحرية المطلقة في الرأي والتعبير والإستخدام أيضا، وهي جماعات تستطيع أن تدخل عبر طرق خاصة تخترق أجهزة الحاسوب، الأرقام السرية للأشخاص وإلى بريدهم الإلكتروني، ما يؤدي إلى معرفة أسرار الناس وخصوصيات أعمارهم وحياتهم الشخصية، وهذه أيضا مسألة هامة أثارت أخلاقيات الإلتزام في إستخدام الإنترنت.<sup>1</sup>

#### الفرع السابع: قيادة الجماعات الإرهابية:

من بين دوافع الجرائم المعلوماتية التي طهرت بشكل كبير في الوقت الحاضر هي الأسباب الإرهابية، نظرا لسهولة إستعمال مختلف التقنيات المتطورة الحديثة وخدمتها للجماعات الإرهابية بواسطة تسهيل الإتصال والتواصل بين مختلف العناصر القيادية وأعضائها وإرسال الأفكار الإيديولوجية والآراء وتلقي الأوامر وإيصال الأخبار والتعليمات والبرقيات الأخرى التي تساهم في إرتكاب السلوكات الإرهابية.<sup>2</sup>

كما أستغلت مواقع التواصل الاجتماعي في غير محلها وذلك لتمير بعض الأفكار الجهادية والخطابات مثل "تويتر" كانت أداة إيجابية في يد المنظمات الإرهابية واستخدموه كأداة للحصول على معلومات حول ما تم تحضيره لهم من طرف السلطات الأمنية، ووسائل التواصل الاجتماعي الجديدة يمكن أن يستغل من طرف الإرهابيين.<sup>3</sup>

<sup>1</sup>. المصري مهران زهير، الخداع بإستعمال الأنترنت، مجلة المعلوماتية، العدد 72، فيفري 2012، تاريخ التصفح 2023/04/24، [www.infomag.newesy](http://www.infomag.newesy).

<sup>2</sup>. القحطاني عبد الله بن حسين آل حجرا، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية: دراسة تطبيقية على المحققين في هيئة التحقيق والإدعاء العام بمدينة الرياض، مذكرة لنيل شهادة ماجستير، القانون وأصول المحاكمات الجزائية، قسم العلوم الشرطية كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، العربية السعودية، 2014، ص 37.

<sup>3</sup> Paul levinson, New Media, international édition, New York, P167.

نظرا للتطور التكنولوجي الذي يشهده العالم جعل المنظمات الإرهابية تستغله استغلال مفرط في تنفيذ أهداف معينة تتمثل في تنفيذ أعمال إرهابية كاستهداف المؤسسات الحكومية والمتمثلة أساسا في المنشآت البترولية والغازية في بعض الدول، اختطاف السياح والأجانب وطلب الدية، نشر منشورات تحريضية لبعض الدول من أجل خلق نوع من التمرد بها، ونشر بعض الخطابات والرسائل محاولة منهم زعزعة الاستقرار الأمني والاجتماعي بالعديد من الدول ومن تم تصبح هذه الدول سهلة الدخول إليها نتيجة الفوضى التي انتشرت فيها جراء هذه الرسائل والخطابات المحرصة لتنفيذ عمليات إرهابية والحصول على معلومات دقيقة عليها لاستغلالها في عمليات إجرامية أخرى.

ومن هنا نعطي مقارنة بين الجرائم التقليدية والجرائم الإلكترونية، وكيف تدرجت من الإطار الكلاسيكي (التقليدي) إلى الإطار الافتراضي المعاصر حسب الجدول الآتي:

| الجرائم الإلكترونية                                     | الجرائم الكلاسيكية (التقليدية) |
|---------------------------------------------------------|--------------------------------|
| القرصنة على شبكة الإنترنت، الحرمان من الخدمة، الفيروسات | السطو                          |
| أنظمة الدفع عن بعد على الشبكة                           | غسل الأموال                    |
| تصفح المواقع الإباحية، واستغلال الأطفال جنسيا على النت  | جرائم الأطفال الجنسية          |
| جرائم الملكية الفكرية، جرائم انتحال الهوية.             | السرقه                         |
| الإحتيال على الشبكة، الإحتيال بالمزاد الإلكتروني...     | الإحتيال                       |

من خلال هذا الجدول يمكن أن نفصل بين أنواع الجرائم التقليدية والجرائم الإلكترونية وذلك من خلال التطور التاريخي للجريمة، ويعود هذا إلى مجموعة من العوامل المرتبطة بتطور المجتمعات الإنسانية من حيث استخدام الوسائل التكنولوجية الحديثة في مختلف أنماط حياتهم اليومية، وبمعنى آخر إن الجريمة الإلكترونية تطورت بظهور فكرة العولمة الاتصالية المرتبطة أساسا بالإستخدام المتزايد لهذه الوسائل مما جعلها تستغل في غير محلها، من خلال ارتكاب أغلب الجرائم الإلكترونية التي تمس الحياة الشخصية

للأفراد والمؤسسات والمنشآت الحكومية وغيرها من الجرائم المرتبطة بهذه الوسائل التكنولوجية.

#### المطلب الرابع: أسباب ارتكاب الجريمة الإلكترونية:

لا تختلف دوافع الجريمة الإلكترونية عن الجرائم الأخرى الموجودة وهي كالتالي:

##### الفرع الأول: الدوافع الشخصية (الذاتية):

فتنقسم لدى مرتكبي الجرائم المعلوماتية إلى دوافع مادية (يعتبر من أهم دوافع ارتكاب الجرائم المعلوماتية بما فيه من تحقيق الربح والثراء والكسب المادي بأعلى المكاسب وأقل مجهود دون أن يترك المجرم أثر وراءه).<sup>1</sup>

\*الأسباب السيكلوجية: تعتبر من العوامل الشخصية" وتنتج من شخص له خلل سيكولوجي أو أمراض نفسية تنعكس على العمل الفردي مما تدفعه للنشاط الإجرامي عن طريق الوسائل التكنولوجية الحديثة"

##### الفرع الثاني: الأسباب الخارجية :

يسعى المجرم المعلوماتي في بعض السلوكات غير السوية لا لكسب المال ولا للمتعة والتسلية، ومن أهم هذه العوامل فيما يلي:

##### الفرع الثالث: سبب يتعلق بالتعاون والتواطؤ :

يعني هذا الدافع أنه كثير التكرار في ارتكاب الجرائم المعلوماتية حيث قد تدفع الحاجة إلى بعض مسؤولي الدول أو المنشآت الإستراتيجية والأمنية إلى الاتصال بأفراد يشغلون أماكن حساسة في إحدى الدول الكبرى أو المنشآت ذات الطابع الإستراتيجي والأمني الأخرى وذلك بهدف الإطلاع على بعض المعلومات الحساسة والتقنيات التكنولوجية والعلمية المتوفرة لديها للاستفادة منها والتي قد يصل في بعض الأحيان إلى زرع جواسيس في تلك الأماكن مع استخدام عدة أساليب منها منح الرشوة أو استخدام وسائل الإقناع والإغراء المرتبط بالتهديد حتى يتحصل عليها.

##### الفرع الرابع: دافع الانتقام:

يعتبر هذا السبب من أخطر الأسباب التي تمكن المجرم من ارتكاب الجريمة المعلوماتية (الإلكترونية)، ونجدها في غالب الأمر تعود إلى أسباب متعلقة بالحياة المهنية لشخص والذي

<sup>1</sup> - الحمود وضاح محمود الحمود، والمحالي شأت مفضي، جرائم الإنترنت، التعرض للإنحراف والآداب العامة،

الحض على الفجور، جرائم الإستغلال الجنسي للأطفال، دار المنار، عمان، 2005، ص 30

يملك معلومات كبيرة على المؤسسة أو الشركة التي تشتغل فيها كالحرمان من أحد الحقوق كالترقية في الدرجة أو الطرد من الوظيفة ينشأ لديه نوع من الإحباط ومن ثم يتولد لديه الانتقام من رب العمل أو مسؤول المؤسسة أو من أحد الزملاء في العمل.

#### الفرع الخامس: الأسباب السياسية والعسكرية:

أن التطور العلمي والتقني أستطاع أن يعتمد بشكل كامل تقريبا على أجهزة الحاسوب، وبذلك حيث أصبح اختراق الأنظمة من أجل الحصول على معلومات سياسية وأمنية و بيانات إقتصادية موضوع أكثر أهمية.

#### الفرع السادس: السبب القومي الوطني:

في هذه الحالة يستطيع الهاكرز بالإعتداء على مواقع المعادية لدولة معينة ليس لها نفس القيم والعادات للمجتمع الذي ينتهي إليه بهتديم أو تبديل هذه المواقع، مما ينتج إلى المنع من أي تهديد إيديولوجية وسلوك أفراد ذلك المجتمع الذي ينتهي إليه.<sup>1</sup>

تعتبر هذه الدوافع هي نفسها دوافع الجريمة بكل أشكالها بما فيها الجريمة الإلكترونية التي تختلف عن الجريمة التقليدية من حيث خصائصها وطبيعتها والدوافع التي تدفع لارتكابها، حيث تختلف حسب طبيعة المجتمع وحسب الزمان والمكان.

#### المطلب الخامس: وسائل مكافحة الجريمة الإلكترونية

توجد العديد من الوسائل لمكافحة الجريمة الإلكترونية نذكر منها:

1/لتمكين أجهزة العدالة الجنائية من أداء دورها في المكافحة الفعالة للجريمة الإلكترونية على المستويين الدولي والإقليمي تتطلب تشريعات مرتبطة بتطور أنواع الجرائم الإلكترونية الحديثة وإرتباطها مع التشريعات الداخلية الوطنية والقواعد والقوانين المقارنة.

2/ العمل التدريب والتأهيل الجيد للعاملين في مجال جمع الأدلة الرقمية والمتمثلة في التقنيين والمهندسين.

<sup>1</sup> - مولاي أحمد ، صعوبات تطبيق الإدارة الإلكترونية بالجزائر : الجريمة الإلكترونية نموذجا، المؤتمر العالمي الأول للإدارة الإلكترونية ، مركز المدينة للوسائط المتعددة، ليبيا، 2010، ص 249.

3/ ضرورة الإستخدام الأمثل للوسائل الإلكترونية المرتبطة بالتكنولوجيا والمتمثلة في نظم الحواسب الآلية والإتصالات وذلك للحد من مخاطر ارتكاب الجريمة الإلكترونية وذلك باتباع كافة وسائل التوعية.

4/ العمل على رصد تحركات وتهديدات والمخاطر الناتجة عن الجرائم الإلكترونية والتبليغ المبكر عن وجود تجاوزات في هذا الشأن وذلك من خلال تزويدها بالوسائل المتطورة في مجال التكنولوجيا، وهذا يتطلب كفاءة عالية من الأجهزة التقنية.

تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية.

5/ ضرورة تدريب وتأهيل المختصين التابعين لجهاز العدالة الجنائية على كيفية وطريقة العمل على جمع الأدلة الرقمية لمركبي الجرائم الإلكترونية.

كل هذه الوسائل من شأنها تساعد كل الذين ينشطون في هذا الإطار لمكافحة الجريمة الإلكترونية ومتابعة مجرمي هذا النوع من الإجرام نتيجة الإستغلال السيئ لهذه الوسائل وخاصة في ظل التطور الكبير الذي شاهده المجتمع المعاصر وما ينجر عنه من سلوكات سيئة وإنحرافية.

### المبحث الثاني: العقوبات المقررة على مرتكب الجريمة الإلكترونية:

#### المطلب الأول: العقوبات السالبة للحرية:

نتناول من خلال هذا العنصر العقوبات السالبة للحرية التي جاءت ضمن القسم السابع المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات من قانون العقوبات الجزائري وهي كالتالي:

كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة والآلية للمعطيات أو يحاول ذلك، يقرر المشرع معاقبته من ثلاثة (03) أشهر إلى سنة (01)، كما تصبح العقوبة مضاعفة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وذلك يعاقب ب ستة (6) أشهر إلى سنتين(2)

حسب ما تنص عليه المادة 394 مكرر2 من قانون العقوبات الجزائري يعاقب كل شخص من أستطاع أن يدخل بطريق الغش في معلومات في نظام المعالجة الآلية أو حذف

أو غير عن طريق الغش في المعلومات التي يتضمنها بعقوبة ستة(6) أشهر إلى ثلاث(3) سنوات.<sup>1</sup>

كما تناول المشرع من خلال نصوص المواد ما يسمى باعتراض أنظمة المعالجة الآلية للمعطيات، وهو قيام الشخص متعمدا باعتراض الاتصالات والدخول الغير مشروع لأنظمة المعالجة الآلية للمعطيات، ونلاحظ نص المادة 394 مكرر 2 قد نص على عقوبة مرتكب جريمة التعامل في معطيات بطريقة غير مشروعة

وحسب ما تناول قانون العقوبات من خلال المادة 394 مكرر 1 التي تنص على عقوبة الحبس من شهرين (2) إلى ثلاث(3) سنوات كل من يعمل عمدا وعن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معلومات مخزنة أو معالجة أو إرسال عن طريق أرضية معلوماتية يمكن أن يرتكب بها السلوكات المجرمة المتضمنة في القسم بالإضافة إلى حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعلومات المتحصل عليها من إحدى الجرائم الذي تطرق إليها في هذا القسم.

تضاعف العقوبة المنصوص عليها في هذا القسم إذا كانت الجريمة أستهدف الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق العقوبات أشد.

يعاقب بالعقوبات المقررة للجريمة ذاتها كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان التحضير مجسدا للعقل أو عدة أفعال.

وطبقا لنص المادة 394 مكرر 5، فقد أقر المشرع الجزائري بأن الشريك للفاعل الأصلي بالجريمة الإلكترونية، عن طريق الشراكة أو الاتفاق، يعاقب بنفس عقوبة الفاعل الأصلي للجريمة، وفي اعتقادنا، يعود سبب تجريم المشاركة في هذه الجريمة بنفس عقوبة الفاعل الأصلي لطبيعة الجريمة ذاتها، كونها ترتكب غالبا من قبل مجموعة من الأشخاص لا شخص واحد.

<sup>1</sup> - قانون العقوبات، رئاسة الجمهورية الجزائرية، الأمانة العامة للحكومة، 2009، ص 113 المادة 394

من خلال ارتكاب الجريمة الإلكترونية المنصوص عليها في هذا القسم يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا بجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أرتكب بعلم مالكيها.

جاء نص المادة 394 مكرر6 بالعقوبات التكميلية مع الإحتفاظ بحقوق الغير حسن النية، بمصادرة الوسائل المستخدمة في الجريمة وغلق المواقع محل الجريمة، وهنا يمكننا القول أن العقوبات التكميلية غير كافية في نظرنا لردع مرتكب الجريمة، فالمشرع العقابي لم ينص هنا على المنع لمدة معينة من ممارسة الحقوق المدنية والسياسية، أو المنع لمدة معينة من ممارسة مهنة أو وظيفة لها علاقة بارتكاب الجريمة مثلا.. يعاقب على الشروع في ارتكاب الجنب المنصوص عليها في القسم بالعقوبة المقررة للجنة ذاتها.

#### المطلب الثاني: العقوبات المالية ( الغرامات المالية):

نتناول في هذا العنصر أهم العقوبات المقررة على مرتكب الجريمة المتعلقة بالمساس بالمعالجة الآلية للمعطيات.

يعاقب كل من يلج أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعلومات أو يحاول ذلك، تتضاعف العقوبة إذا ترتب على ذلك بإزالة أو تبديل لمعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تدمير نظام إشتغال المنظومة بغرامة من 50.000 دج إلى 150.000 دج وذلك وفق قانون العقوبات الجزائري في مادته 394 مكرر .

أصدر المشرع الجزائري في قانون العقوبات غرامة والتي تقدر 1.000.000 دج إلى 5.000.000 دج على كل من يقوم عمدا وعن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معلومات مخزنة أو معالجة أو إرسالية عن طريق منظومة معلوماتية يمكن أن يرتكب بها الجرائم المتضمنة في هذا القسم بالإضافة إلى الحصول أو تسريب أو نشر أو إستخدام لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في قانون العقوبات الجزائري.

مما سبق يمكن القول أنه إذا كانت ثورة المعلومات ساعدت المجتمعات البشرية على عولمة المعلومات، كما أنها تعمل على تسهيل كثير من الخدمات والأعمال وتمكننا من مسيرة التطورات والأخبار السائدة في العالم من خلال استغلال الواسع للوسائل التكنولوجية التي تساعد على أداء هذه المهمة إلا أنها عندما تكثر استغلالها السيئ وفي غير محلها تجعل الفرد يرتكب العديد من الجرائم بإستخدام هذه الوسائل التكنولوجية، ونجد منها بناء ونشر برامج فيروسات الحاسب الآلي والدخول غير المشروع للمواقع الإلكترونية بالإضافة إلى أنظمة المعالجة الآلية للمعطيات، وإتلاف البرامج وتزوير المسندات..... وغيرها من الجرائم التي تدخل في نطاق الجرائم المعلوماتية المعاصرة.

من أجل الحد من هذه الجرائم المعاصرة يتطلب من المشرع الجزائري مواجهتها من خلال تطبيق مجموعة من القواعد القانونية المكرسة في قانون العقوبات، وتعتبر الجرائم الإلكترونية من بين الجرائم الحديثة التي تتطلب إجتهد المحققين ورجال القانون في الكشف عن مثل هذه الأمراض الاجتماعية التي نخرت أجساد المجتمعات البشرية والأمر الحضري، بالإضافة إلى نشر الوعي بين أفراد المجتمع بمخاطر التعامل مع المواقع الإباحية على شبكة الإنترنت للأطفال عبر الهواتف الذكية ، ومن أجل ذلك وجب التنسيق بين العديد من المهتمين بهذا الشأن للحد من هذه الظاهرة الدخيلة على المجتمعات العربية والاسلامية، ومن خلال هذه الدراسة قد توصلنا إلى مجموعة من النتائج كالآتي:

#### أ- النتائج:

- تعتبر الجريمة الإلكترونية بأنها عابرة للحدود الوطنية بمعنى أنها عالمية.
- إن العصر الحديث يتميز بتطور الجرائم من التقليدية إلى الجرائم الحديثة وذلك من خلال التحول من الواقع المادي إلى الواقع الافتراضي الرقمي.
- الجرائم الإلكترونية هي جرائم تتطور بسرعة هائلة وهذا مرتبط بمدى الإستخدام الواسع للشبكات العنكبوتية مما يؤدي إلى الاستغلال السيئ بها.
- الجريمة الإلكترونية هي جريمة انتهاك وتعدي على حرمة الأفراد والمجتمع والأمن والاقتصاد.
- الجرائم الإلكترونية تتطور من يوم لأخر مرتبط بمدى تطور وسائل التكنولوجيا الحديثة كالهواتف الذكية، والإستخدام الواسع لها.

- إن الجريمة الإلكترونية تعتبر طريقة سهلة للتعدي على حرمان الأفراد.

#### ب- التوصيات:

- ضرورة التنسيق بين الجهات المكلفة بإعداد الخطط الأمنية لمواجهة الجريمة الإلكترونية.
- إعداد تكوين ورسكلة التقنيين والمهندسين على متخلف التقنيات والطرق لمواجهة الجرائم المعلوماتية المنتشرة في المجتمع.
- المراقبة المستمرة للشبكات العنكبوتية وما تبتها من أفلام إباحية وفاضحة.
- ضرورة إجراء حملات تحسيسية حول مخاطر الاستخدام العشوائي للوسائل التكنولوجية الحديثة.
- مراقبة الأطفال عند استخدام الشبكة العنكبوتية وكل ما يشاهدونه من برامج متعددة بهذه الشبكة التي تضر بأخلاقهم وسلوكياتهم.
- ضرورة المتابعة اليومية للأطفال وخاصة الإناث من خلال التواصل عبر مواقع التواصل الاجتماعي والعلاقات التي تربطهم مع أشخاص عبر هذه الوسائط الافتراضية لحمايتهم من التحرش والإستغلال الجنسي.

#### - قائمة المصادر والمراجع:

أولا/ قائمة المصادر:

- القوانين:

1- الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، الذي يتضمن قانون العقوبات المعدل والمتمم، قانون العقوبات ، 2012.

ثانيا / قائمة المراجع:

أ- الكتب:

- 1- إبراهيم لطفي طلعت، دراسات في علم الاجتماع الجنائي، ط1، دار غريب، القاهرة، 2008.
- 2 - عادل محمد فريد نائلة، جرائم الحاسب الإقتصادية: دراسة نظرية تطبيقية، دار النهضة العربية، القاهرة، 2003.
- 3 - محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، 2009.
- 4 - وضاح محمود الحمود الحمود، مفضي المحالي نشأت، جرائم الأنترنت- التعرض للانحراف- والأداب العامة- الحز على الفجور- جرائم الاستغلال الجنسي للأطفال، دار المنار، عمان، 2005.

1- سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير ، العلوم الجنائية والإجرام، كلية الحقوق والعلوم السياسية، تلمسان الجرائ، 2001.

2- عبد الله بن حسين آل حجاراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية: دراسة تطبيقية على المحققين في هيئة التحقيق والإدعاء العام بمدينة الرياض، مذكرة ماجستير ، قانون وأصول المحاكمات الجزائية، قسم العلوم الشرطية كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، العربية السعودية، 2014.

3- محمود خليل عزة، مشكلات المسؤولية المدنية في مواجهة الحاسب الآلي: دراسة مقارنة في القانون المدني والشرعية الإسلامية، مذكرة ماجستير ، قانون وشرعية، القاهرة، 1994.

#### ج- المقالات في المجالات:

1- محمد علي سالم وحسون هجيج، " الجريمة الإلكترونية" مجلة بابل للعلوم الإنسانية، كلية الحقوق جامعة بابل، العراق، العدد 02، 2004.

2- حسين فريحة، "الجرائم الإلكترونية والأنترنت"، المجلة المعلوماتية، دار المنظومة السعودية، السعودية، العدد 36، 2011.

3 - ممدوح حسن شريهان، " الجريمة الإلكترونية وسبل مواجهتها على المستويين الوطني والمحلي" ، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية، عمان، العدد 21، 2020.

#### د- المقالات في الملتقيات والندوات:

1- أحمد مولاي، " صعوبات تطبيق الإدارة الإلكترونية بالجزائر: الجريمة الإلكترونية نموذجا"، المؤتمر العالمي الأول للإدارة الإلكترونية، مركز المدينة للوسائط المتعددة، سنة 2010 بدولة ليبيا.

2- دياب موسى البدانية، "الجرائم الإلكترونية: المفهوم والأسباب"، ملتقى علي حول الجرائم المستحدثة في ظل المتغيرات والتحوليات الإقليمية والدولية، 02-03/09/2014 بدولة عمان.

#### هـ- المقالات على مواقع الانترنت:

1- مهران زهير المصري، "الخداع باستعمال الأنترنت"، المجلة المعلوماتية، العدد 72، تاريخ التصفح

[www.infomag.newesy](http://www.infomag.newesy) 2023/04/24