تاريخ الإرسال: 14-05-2025 تاريخ القبول:14-07-2025

الجريمة الإلكترونية: مقاربة مفاهيمية قانونية

Cybercrime: a legal conceptual approach

عفاف لعقون*[1]، جميلة فشار[2]

[1]جامعة تامنغست (الجزائر)، lagounafaf@univ-tam.dz

[2]جامعة الجلفة (الجزائر)، djamila.fechar@univ-djelfa.dz

(https://orcid.org/0009-0006-3270-8443)
(https://orcid.org/0009-0008-6674-5204)

الملخص:

جاءت هذه الدراسة تهدف إلى دراسة الجرائم الإلكترونية كنمط جديد في المجال الإجرامي والذي أدى بالعديد من الفقهاء إلى البحث عن مفهوم لها، ولم يقف الأمر حد الفقهاء فانتقل ليشمل الشق التشريعي على الصعيد الدولي وحتى الوطني منه، لهذا أصبح من الضروري البحث في المفهوم الخاص بالجريمة الإلكترونية وكذا خصائصها ودوافع ارتكابها في محاولة لتأطيرها وإيجاد سبل للحد منها.

ومن بين النتائج المتوصل إليها أن هذا التطور الحاصل في مجال تكنولوجيا الاعلام والاتصال ساهم في إحداث ثورة هائلة في مجال المعلوماتية فإذا كانت هذه الثورة التقنية إيجابية في بعض جوانبها كالتعاقد الإلكتروني، والتجارة الإلكترونية، فإنها في جانب آخر خلفت ما يشوبها من السلبيات فبرزت في الساحة الجنائية ما يعرف بالجريمة الالكترونية كتطور جديد وانتقال من الجريمة التقليدية إلى الجريمة الإلكترونية، والذي تعرف العديد من النقائص على الصعيد المفاهيمي والتأطير القانوني.

الكلمات المفتاحية: الجريمة الإلكترونية، تكنولوجيا الإعلام، نظام معلوماتي، جرائم عابرة للحدود.

---

*المؤلف المرسل

Abstract:

This study aimed to study cybercrime as a new type in the criminal field, which led many jurists to search for a concept for it, as well as from a legal perspective at the international and even national levels.Therefore, it has become necessary to research the concept of cybercrime, as well as its characteristics and motives for committing it in an attempt.To frame and limit it.

Among the results reached is that this development in the field of information and communication technology has contributed to a tremendous revolution in the field of informatics.If this technical revolution was positive with the emergence of electronic contracting and electronic commerce, on the other hand, some negatives appear, and what is known as electronic crime has emerged in the criminal arena.As a new development and transition from traditional crime to electronic crime, which has many shortcomings in terms of concept and legal framing.

Keywords: cybercrime, information technology, information system, cross-border crime**.**

مقدمة:

مر الإنسان بعدة مراحل للتطور فكانت المرحلة الأولى معرفة الإنسان للزراعة والمرحلة الثانية معرفته للصناعة، أما المرحلة الثالثة فكانت ثورة معلوماتية، هاته الأخيرة عرفت تطورا رهيبا في ميدان تكنولوجيا الإعلام والاتصال نتيجة التناسق الحاصل بين فرعين هما فرع الحواسيب وفرع الاتصال.

من هنا تدخلت التقنية المعلوماتية في كل جوانب الحياة فتمكنت بما توفره من تسهيلات بربط أجزاء العالم ببعضها البعض متجاوزة بذلك الحدود المكانية والزمانية نتيجة انتشار استخدام الانترنت وتكنولوجيا المعلومات والاتصال، فأصبح العالم يأخذ وصف القرية الصغيرة وأدت هذه التقنيات من خلال مجموعة من التطبيقات إلى التواصل المجتمعي المباشر وتبادل المعلومات وحتى القيام بجملة من التصرفات القانونية عن طريق شبكة الأنترنت كالتعاقد الإلكتروني، الإدارة الإلكترونية دون المرور بالإجراءات التقليدية، وقد وفر ذلك الكثير من الوقت والجهد.

بالرغم من هذه الإيجابيات التي تحسب للتطور التكنولوجي، إلا أن هذا الانتشار المعلوماتي أفرز من السلبيات ما لم يكن في الحسبان إذ أصبحت هذه الوسائل تستعمل لأغراض غير مشروعة فغدت الجريمة ترتكب في نطاق تقني وتكنولوجي متزايدا استخدامها يوما بعد الآخر ليمتد إلى درجة ظهور بعض الأفعال تؤدي إلى الوصول غير المسموح به إلى الأجهزة، وبهذا استغلت هذه التقنية الحديثة لتحقيق مآرب غير مشروعة تصل إلى الإجرام الذي أصبحنا نسمع عنه العديد من المسميات كجريمة الأنترنت، جريمة الكمبيوتر، الجريمة المعلوماتية، وكذا الجريمة الإلكترونية.

وفي محاولة لمواكبة هذا التطور الإجرامي، كان لزوما معرفة الإطار المفاهيمي للجريمة الإلكترونية من جانب فقهي، وجانب تشريعي ومدى مواكبة المشرع الجزائري لهذا التطور في الساحة الجنائية، ومعرفة الدوافع والأسباب التي تؤدي بالمجرم المعلوماتي إلى ارتكابها.

ومن هنا نطرح الإشكالية الآتية:

فما هو المقصود بالجريمة الإلكترونية؟ وماهي الدوافع وراء ارتكاب هذا النوع من الجرائم؟

وعليه جاءت هذه الورقة البحثية تهدف إلى دراسة أحد أهم الجرائم المستحدثة ألا وهي الجريمة الإلكترونية نظرا لخطورتها التي تتعدى الحدود الدولية، ومحاولة تشخيصها ببيان خصائصها والكشف عن مختلف أسباب ارتكابها.

وللإجابة على هذه الإشكالية اقتضت منا جوانب الدراسة الإعتماد على المنهج الوصفي والمنهج التحليلي من خلال عرض المفاهيم الفقهية والقانونية للجريمة الإلكترونية وتحليلها، ودراسة مختلف الأسباب أو الدوافع لارتكاب هذا النوع من الجرائم.

المبحث الأول: حقيقة الجريمة الإلكترونية بين الآراء الفقهية والنصوص القانونية

أدى التطور النوعي في تكنولوجيا الاعلام والاتصال ومختلف الوسائل الإلكترونية والتي أعطت أفراد المجتمع مجالا مفتوحا للاطلاع على المعلومات إلى تغيير كبير في أسلوب حياتهم وتعاملهم بين الناس، كما أثر ذلك بشكل مباشر على حجم ونوع الجريمة، وعلى مشروعية الأفعال بشكل عام ونتج عن ذلك نوع جديد من الجريمة يعرف بالجريمة

الإلكترونية لذا سنعمد من خلال هذا المبحث إلى التطرق إلى الجريمة الإلكترونية من الناحية الفقهية والقانونية (المطلب الأول) وخصائصها (المطلب الثاني)[1].

المطلب الأول: الإطار الفقهي والقانوني للجريمة الإلكترونية

يعد موضوع الجريمة الإلكترونية من المواضيع الحديثة والمتشعبة، ورغم صعوبة إيجاد تعريف جامع مانع لها، إلا أن هذا لم يكن عائقا فحاول العديد من الفقهاء والباحثين من خلال اجتهاداتهم إيجاد تعريف لهذا النوع من الجرائم المستحدثة مما أدى إلى وجود عدة تعريفات للجريمة الإلكترونية وإن كانت قد تباينت تبعا لرؤية كل فئة، فمنهم من عرفها من الجانب الفقهي (الفرع الأول)، والبعض الآخر من الجانب القانوني (الفرع الثاني)، ومن أجل مفهوم شامل لها لابد من التطرق إلى تعريفها من كل هذه الجوانب.

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة الإلكترونية، إذ يطلق عليها البعض منهم الجريمة المعلوماتية، وينهي آخرون إلى تسميتها بجرائم إساءة استخدام تكنولوجيا الاعلام والاتصال ويطلق عليها آخرون مسمى جرائم الكمبيوتر والانترنت، وذلك نسبة للوسائل المقامة بها[2]، وعليه جاء تعريف الجريمة الإلكترونية مستندا إلى موضوع الجريمة في بعض الأحيان وفي أحيان أخرى مستندا إلى وسيلة الجريمة، وفي نقاط أخرى جمع بين الاثنين، وفي أحوال أخرى استند الى الالمام بالمعرفة التقنية.

أ-التعريفات التي استندت إلى موضوع الجريمة

عرف مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية الجريمة الإلكترونية بأنها: "كل فعل غير قانوني أو أخلاقي أو لم يتم التصريح به مرتبط بالمعالجة الالية للبيانات أو بتحويلها".

كما عرفها الأستاذ محمود أحمد عبابنة على أنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجا بطريقة مباشرة وغير مباشرة لتدخل التقنية المعلوماتية"[3].

كما عرفت الجريمة المعلوماتية بأنها غش معلوماتي ينصرف إلى سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها.

وفي ذات السياق عرفت على أنها "جرائم الاعتداء على الأموال المعلوماتية والتي تتمثل في الأدوات المكونة للحاسب وبرامجه ومعداته"[4].

ما من شك أن معيار موضوع الجريمة كأساس للتعريف يعد من أهم المعايير وأكثرها قدرة على تحديد مفهوم الجريمة محل التعريف، على أن لا يغرق في وصف الأفعال التي يعد بارتكابها مجالا للتجريم، إذ قد لا يحيط بها، فإذا سعى إلى الإحاطة بها فإنه سيذهب بالتفصيل إلى محطات لا تستقيم وشكل التعريف والغرض من تحديده، بالإضافة إلى عدم وجود اتفاق لحد الان على الأفعال التي تأخذ وصف الجريمة هذا من جهة، ومن جهة أخرى فإن هذه التعريفات لا تستند في الحقيقة لموضوع الجريمة بالمعنى القانوني الذي هو محل الاعتداء، فهذه التعريفات ركزت على أنماط السلوك الإجرامي وابرزتها متصلة بالموضوع لا بالموضوع ذاته[5].

ب-تعريف الجريمة الإلكترونية استنادا إلى وسيلة الجريمة

يذهب أصحاب هذا الرأي إلى أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر باعتباره وسيلة لارتكاب الجريمة ونقطة التميز بينها وبين الصور التقليدية وحتى الحديثة للجرائم. وبالتالي تعرف على أنها "نشاط اجرامي تستخدم فيه التقنية الإلكترونية المتمثلة في الحاسوب الآلي الرقمي وشبكة الانترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف" كما تعرف بأنها "جرائم الشبكة العالمية التي يستخدم فيها الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب الجريمة، كاستخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب"[6].

فالجريمة الإلكترونية حسب هذا الطرح تعتمد على جهاز الكمبيوتر لقيامها، غير أن الوسيلة لا تأخذ كل هذا الحيز من الاعتبار عند التجريم كون أن أغلب الوسائل متساوية، والتكوين القانوني للجريمة يكون بقيام أركانها ومدى توافرها عند تطبيق نصوص التجريم فضلا على أنه تعريف يوسع من نطاق الجريمة الالكترونية.

ج-تعريف الجرائم الإلكترونية استنادا إلى الجمع بين أساليب ارتكابها وموضوعها

نتيجة قصور التعريفات السابقة جاء هذا المعيار ذو الطابع المزدوج يجمع في تعريف لها -أي الجريمة الإلكترونية- بين الأساليب والموضوع، فالجرائم الإلكترونية وفقا

لهذا التعريف هي "كل سلوك تكون فيه الأنظمة والشبكات المعلوماتية هدفا أو محلا لارتكاب أفعال إجرامية"[7]. وعرفها خبراء مختصون من بلجيكا في معرض ردهم عن استبيان منظمة التعاون الاقتصادي والتنمية حول الغش المعلوماتي سنة 1982 بأنها "كل فعل او امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[8].

رغم أن هذا التعريف حاول الالمام بجوانب الجرائم الإلكترونية من أجل تعريفها وإن كان يبدو أكثر شمولا من التعريفات السابقة إلا أنه الآخر كان عرضة للانتقاد، وهذا شيء طبيعي كون أن الجرائم الالكترونية تتميز بخصوصيتها التي تميزها عن باقي صور الجرائم التقليدية، إضافة إلى حداثتها وتطورها بتطور تقنيات تكنولوجيا الاعلام والاتصال.

د-تعريف الجريمة الإلكترونية استنادا إلى الالمام بالمعرفة التقنية:

هناك اتجاه فقهي آخر لا يهتم بالوسيلة أو موضوع الجريمة الإلكترونية، وإنما يعرفها بوصفها مرتبطة بالمعرفة التقنية باستخدام الحاسب الآلي بمعنى آخر أن أنصار هذا الاتجاه يستندون إلى معيار شخصي يستوجب أن يكون الفاعل ملما بتقنية المعلومات واستخدام الحاسب الآلي من بينهم "ديفيد تومبو" الذي عرف هذا النوع من الجرائم بقوله أنها: "أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[9].

ومن بين التعريفات كذلك نجد تعريف وزارة العدل الامريكية التي تعرف الجريمة الالكترونية بأنها إنتهاك للقانون الجنائي يتطلب المعرفة بتكنولوجيا المعلومات من أجل ارتكابها أو التحقيق فيها أو إجراءاتها الإدارية.

كما عرفها الفقيه STEINSCKJOBERG بأنها: "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه، فهي الجريمة التي يكون العلم بتكنولوجيا الحاسوب لازما لارتكابها"[10].

وما يؤخذ على هذا الاتجاه أنه يضيق على نحو كبير من نطاق الجريمة الإلكترونية لأنه وبحسب رأي المنتقدين له يحصر الجريمة في نطاق معرفة فنية كبيرة لمرتكبها وهذا يمكن وقوعه في حالات ما وليس في جميع الحالات إذ يحدث وأن يرتكب الجاني الجريمة الإلكترونية دون الحاجة إلى قدر كبير من المعرفة والخبرة الفنية، كعملية

اتلاف البيانات المخزنة مثلا فتعتبر من الأفعال غير المشروعة لا تتطلب مهارة وقدر كبير من العلم والمعرفة لارتكابها[11]، كما أن شرط المعرفة التقنية شرط لصيق بشخص الفاعل، غير أن هذه الجرائم يرتكب جزء كبير منها بصفة جماعية تتوزع أدوار مرتكبيها بين التخطيط والتحريض والتنفيذ والمساهمة، قد لا تتوفر لدى بعضهم المعرفة التقنية بالمعلومات، ثم ما هي حدود المعرفة التقنية، وما هو معيار وجودها للقول بقيام الجريمة؟ ثم إن التطور الذي شهدته الوسائل التقنية تهدف نحو تبسيط المعالجة وتبادل المعطيات وتحويل الاجهزة المعقدة الى أجهزة تكاملية سهلة الاستخدام حتى من قبل لا يتقن شيئا في عالم الكمبيوتر، ولم تعد المعرفة العميقة جوهر أساسي ليتمكن شخص من ارسال آلاف رسائل البريد الإلكتروني دفعة واحدة إلى أحد المواقع لتعطيل عملها[12].

وبالبحث عن تعاريف صادرة من الفقه الجزائري فنجد أن هذا الأخير جاء بتعاريف متعددة منها ما يلي: "بأنها الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال". وهناك من يعرفها على أنها: "كل عمل او امتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية والمعنوية، وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها". أو أنها "استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو أحد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع".

من خلال هذه التعاريف تبنى الفقه الجزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام الحاسوب وتتمثل من الناحية المبدئية، في جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية[13].

الفرع الثاني: تعريف الجريمة الإلكترونية من الناحية القانونية

من خلال البحث عن تعريف تشريعي للجريمة الإلكترونية لاحظنا أن المشرع الجزائري قد أغفل عن تنظيم مجال الجريمة الإلكترونية في مرحلة من المراحل، إلا أنه ما فتئ أن تدارك ذلك الفراغ التشريعي من خلال منظومته القانونية وسن قواعد قانونية

لمواجهة هذه الجريمة، وذلك تجلى في القانون رقم 04-15 المتضمن تعديل قانون العقوبات[14]، الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات، ثم تلاه بالقانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما[15]، فكانت البداية بإصداره للقانون 04-15 المتضمن قانون العقوبات والذي خصص فيه القسم السابع مكرر من الباب الأول مكرر لهذه الجريمة تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" وذلك من المادة 394 مكرر إلى المادة 394 مكرر 7، حيث أنه قام باستخدام هذا المصطلح للدلالة على المعلومات والنظام الذي يكمن في جوهره ليبين الاعتداءات الوقعة بموجب هذه الأفعال التي تدخل حيز التجريم والتي يكون النظام المعلوماتي أداة لارتكابها[16].

ونظرا للتقدم المتواصل الذي شهدته وسائل الاعلام والاتصال الحديثة والتي ساعدت على بروز أشكال جديدة من هذه الجرائم، سارع المشرع الجزائري مرة أخرى إلى مواكبة هذه التطورات من أجل مواجهة الجرائم الالكترونية المتولدة عنها وذلك بإصداره لقانون ثان، وهو القانون رقم 09-04 والذي عرف من خلاله هذه الجرائم وذلك بموجب المادة 2 الفقرة أ والتي جاء فيها: "الجرائم المتصلة بتكنولوجيات الاعلام 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 للاتصالات الإلكترونية"[17].

من خلال هذا التعريف نلاحظ بعض المسائل المهمة وهي:

-تبرز أهمية هذا التعريف من الناحية الأولى: أن المشرع الجزائري قد اعتمد في وصفه للجريمة الإلكترونية عدة معايير أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكترونية، وهو الشرط الأولي الذي يلزم تحقيقه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام[18]، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

من الناحية الثانية: حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الإلكترونية في القانون الجزائري[19].

أما بخصوص الملاحظة الثالثة: استعمل المشرع للدلالة على هذا النوع من الجرائم "نظام المعالجة الآلية للمعطيات" وهو تعبير فني تقني يصعب على شاغلي الميدان القانوني إدراك حقيقته بسهولة، ضف إلى أنه تعبير متطور بالتطورات السريعة والمتلاحقة في المجال الرقمي[20].

بالعودة إلى مختلف التعاريف أعلاه سواء الفقهية منها أو التشريعية نجد أن التعبير عن الجريمة الإلكترونية وتحديد مفهومها تغير وتنوع بحسب الزاوية التي ينطلق منها كل تعريف –كما سبق وأن بينا– اذ أن هناك من يعتمد مصطلح الجريمة الالكترونية وهناك من يصطلح عليها بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال وآخر يسميها بجرائم التقنية العالية وآخر يربطها بجهاز الحاسوب أو الكمبيوتر إلى جانب جرائم الانترنت أيضا، وبالرغم من ذهاب الفقه إلى القول بأن جميع المصطلحات السابقة تصب في نفس الاطار وتحمل نفس المدلول، هناك جانب آخر يرى أنه حتى تأخذ الجريمة وصف الجريمة الإلكترونية وجب حدوث اتصال بين جهازين الكترونيين، لأنه لا يمكن ارتكاب جريمة إلكترونية من خلال العمل على جهاز منفرد مهما كان نوع الجرم المرتكب، ذلك لأنه يمكن استخدام الكمبيوتر في الكثير من الجرائم لكن ليس بالضرورة أن يتم تكييفها على أنها جرائم إلكترونية على غرار فعل التزوير في المستندات والوثائق[21].

وعليه يمكن القول بأن الجريمة الإلكترونية في التشريع الجزائري جاءت بشكل موسع تجمع بين عدة معايير من خلال استعمال الأجهزة الإلكترونية كالحاسوب، الهاتف النقال...وغيرها كونها وسائل للاتصال الإلكتروني، ويتحدد موضوعها والقانون الواجب التطبيق عليها بالمساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات ليكون نطاقها في نظام معلوماتي أو يسهل ارتكابها عليه.

المطلب الثاني: خصائص الجريمة الإلكترونية

إذا كان مفهوم الجريمة الإلكترونية والقاضي بأنها ذلك النشاط الإجرامي المتصل باستعمال تقنية الحاسوب وشبكات الاتصال أو ما يعرف بالبيئة الرقمية، يجعل من هذه الجرائم تمتاز بطبيعة خاصة تختلف والمفهوم التقليدي المرتبط بتجريم السلوكيات ذات الطبيعة المادية، والتي تترك أثر ملموسا في العالم الخارجي، ذلك لأن هذا النوع من الجرائم يتخذ من العالم الافتراضي ملجأ له بحيث لا تكاد تظهر فيه السلوكيات الإجرامية، نظرا لما تتميز به هذه الجرائم من خصوصيات تجعل امر اكتشافها صعب للغاية، وهو ما يظهر من خلال خصائصها المميزة لها عن باقي الجرائم التقليدية[22].

الفرع الأول: الجريمة الإلكترونية من الجرائم العابرة للحدود

من المتعارف عليه أنه عندما يكون الفعل أو الامتناع الذي يأتيه الإنسان بواسطة نظام معلوماتي معين اعتداء على حق أو مصلحة بيانات معلوماتية يحميها القانون أو إضرار بالمكونات المنطقية للحاسوب أو بنظم الشبكات المتصلة به ماسا بحدود أكثر من دولة نكون أمام جريمة عابرة للحدود[23]، وبالتالي فإن أهم ما تتميز به الجريمة الإلكترونية أنها جريمة ذات بعد دولي، أي أنها عابرة للحدود، فهي قد تتجاوز الحدود الجغرافية بسبب أن تنفيذها يتم عبر الشبكة المعلوماتية، ومن الأمثلة على هذه الجرائم العابرة للحدود، أنه تمكن أحد الهواة في أوربا من حل شفرة أحد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية)، ومن ثم أصبح المجال أمامه مفتوحا للعبث ببيانات هذا المركز وكذلك عليه الحال في إنتاج الفيروسات[24]، فالطبيعة الدولية لهذه الجرائم تثير في كثير من الأحيان تحديات قانونية إدارية فنية، بالإضافة إلى إشكال الاختصاص القضائي فيما يتعلق بالدولة المختصة بمحاكمة الجاني؟، كما ينتج عنها صعوبات سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية[25].

لذا ظهرت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم، ومحاولة التوفيق بين التشريعات الخاصة التي تعالج هذا النوع من الجرائم، فيجب أن يشمل هذا التعاون التواصل المعلوماتي، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى والوسيلة المثلى لتحقيق كل هذا هو

ابرام الاتفاقيات الدولية[26]، وتجدر الإشارة هنا إلى جهود الانتربول في هذا المجال، من خلال ضباط الارتباطات المنتشرين في كافة الدول عبر العالم، والمكلفين بتوفير قواعد ضخمة من البيانات، يمكن أن تشكل نقطة انطلاق لمكافحة ومجابهة هذه الجرائم[27].

والجدير بالذكر أن المشرع الجزائري قد حقق امتيازا يحسب له حيث نص في القانون 09-04 على بعض القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال هذه الجرائم، كما أنشأ المشرع هيئة وطنية للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته وسن أحكام خاصة بالتعاون والمساعدة القضائية الدولية ناهيك عن القانون 04-15 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات والذي استحدث بموجبه أحكاما خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد 394 مكرر إلى 394 مكرر 7[28].

الفرع الثاني: الجريمة الإلكترونية جريمة خفية

تتسم الجريمة الإلكترونية بالهدوء والخفاء فتنفيذها يحتاج إلى جهد ذهني وتفكير علمي مدروس ولمسة بسيطة لمفاتيح التشغيل الخاصة بجهاز الحاسوب أو أحد ملحقاته، فهي عكس الإجرام التقليدي تماما لا تحدث ضجيجا أو ضوضاء كجريمة القتل أو السرقة مثلا، بل أن فاعلها ينفذها في صمت وسكون تامين كما أنها لا تحتاج أن يبذل جهدا عضليا كالكسر، حيث توصف بالجرائم الناعمة كونها تعتمد على التعامل الدقيق مع الشبكات، كقرصنة الحسابات بهدف الاطلاع على البيانات الشخصية وإرسال الفيروسات المدمرة[29]، وفي المقابل فهي صعبة الاثبات لغياب الآثار المادية المتعارف عليها في مجال الجرائم التقليدية مثل بقع الدم، تكسير،...إلخ فنكون هنا أمام وسائل للإثبات غير كافية، الأمر الذي يستوجب البحث عن أدلة أكثر فعالية وكفاية في الإثبات مثل البصمات الصوتية والبصرية.

الفرع الثالث: صعوبة اكتشاف واثبات الجريمة الإلكترونية

تمتاز الجرائم الإلكترونية بصعوبة الاكتشاف والاثبات فيتعذر في الجرائم الالكترونية اثبات هذا النوع من الجرائم، كونها تحدث في عالم افتراضي يتسم بالديناميكية والحركية السريعة، يصعب معه العثور على الأدلة الرقمية كون الجاني لا يترك خلفه أي

أثر مادي، بل يضع رموز سرية تعيق الوصول لذلك، ولهذا ما يتم اكتشافه من هذه الجرائم يكون بالصدفة أو بعد فوات وقت معتبر على حدوثها، وعليه ما لم يكشف منها أكثر بكثير مما كشف عنه[30]، ضف إلى ذلك أن اكتشافها واثباتها يحيط به الكثير من الصعاب وذلك يرجع لعدة أسباب[31]:

–أن المجني عليه في الجريمة الإلكترونية يحجم عن الإبلاغ عنها نظرا لافتقاره القدرة الفنية التي تمكنه من اكتشف الجريمة، أو خوفا من الاضرار بمصالحه إذا ما أعلن عن تعرضه لاعتداء لاسيما إذا كان الاعتداء واقع على مؤسسات مالية أو مصرفية أو تجارية كبيرة؛

–قدرة الجاني في الجرائم الإلكترونية على تدمير أدلة ادانته في زمن قياسي لا يستغرق أكثر من ثواني معدودة وذلك بتعريض البيانات المخزنة لديه على وسائل ممغنطة إلى مجال مغناطيسي قوي قادر على محوها في طرفة عين، أو بتزويد الحاسب ببرامج من شأنها تدمير وتخزين البيانات في حال استخدامها من طرف شخص غير مرخص له؛

–نقص الخبرة الفنية لدى المحققين يقف عائقا أمام اثبات هذه الجريمة، لأن هذا النوع من الجرائم يتطلب خبرة فنية عالية، وإلماما واسعا باستخدام الحاسوب أو جهاز بإمكانه المعالجة الآلية للمعطيات كأجهزة فك الرموز المقرصنة التي يمكن استعمالها لسرقة الأموال من أجهزة التوزيع الآلي للنقود مثلا أو استعمالها بهدف الدخول الاحتيالي في نظام معلوماتي محمي تقنيا.

الفرع الرابع: الجريمة الإلكترونية تتم بواسطة الأجهزة الالكترونية

من أهم الخصائص التي تتميز بها الجريمة الالكترونية أنها جريمة تتم بواسطة الحاسب الآلي وارتباطه بشبكة الانترنت التي تجعل العالم على اتصال ببعضه البعض مما يسهل الفعل على الجاني، كما أن هذا الاتصال لا مفر منه باعتباره النافذة المفتوحة لمرتكبها، وعليه فإن كل ما تحتاجه هذه الأخيرة هو الكبس على ازرار في لوحة مفاتيح الكمبيوتر والقوة العلمية والذكاء ومهارة التوظيف في سبيل تنفيذها حيث أن الفاعل لا يحتاج إلا لوقت للقيام بالجرم بواسطة الشبكة المعلوماتية الدولية[32].

المبحث الثاني: دوافع ارتكاب الجريمة الإلكترونية

عموما مهما كانت أسباب الظاهرة الإجرامية ومهما اختلف في تفسيرها فلا يمكن أن تنبع الا من انسان، هذ الأخير ينقلها إلى المجتمع بطريقة الاختيار وليس بطريقة الجبر أو الآلية، فلابد أن يكون للإرادة نصيب في ظهور الجريمة، خاصة وأن هناك جرائم ذات خصوصية جلية كالجرائم المعلوماتية والتي تلعب الإرادة فيها دورا كبيرا في ارتكابها، هذه الإرادة تكون أسبابا ودوافع عديدة تساهم في تقويتها[33]، ويعتبر الباعث (الدافع)، الغرض، الغاية، تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا، لأن القاعدة القضائية تقرر أن الباعث ليس عنصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي، وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب فإنها من حيث الدلالة تتمايز وينتج عنها آثار قانونية على درجة كبيرة من الأهمية، وعليه فإن الجريمة تقوم بتحقيق عناصرها وأركانها أيا كان الباعث من ارتكابها وللجريمة الإلكترونية عدة دوافع لارتكابها قد تكون لدوافع شخصية (المطلب الأول) أو لدوافع خارجية (المطلب الثاني)[34].

المطلب الأول: الدوافع الشخصية

يقصد بالدوافع الشخصية تلك العوامل التي تتعلق بشخصية المجرم الإلكتروني والذي تكون دافعا لارتكاب الجريمة الإلكترونية، ويمكن تقسيم الدوافع الشخصية لدى مرتكب الجرائم إلى دوافع مادية (الفرع الأول) وأخرى تتعلق بذهنية المجرم (الفرع الثاني).

الفرع الأول: الرغبة في تحقيق مكاسب مادية

يحدث وأن يواجه رغبة الانسان صعوبات قانونية في تحقيق ثروة مالية وتوفير الحياة الكريمة ما يدفع الجاني إلى القيام بأعمال غير مشروعة من شأنها أن تؤدي به إلى السلوك الإجرامي عن طريق الجريمة الالكترونية المستهدف منها مجتمع أكبر، وذلك لسهولة تنفيذها وتوفير المردودية وقلة خطورتها، وسهولة محو دليلها، باستعمال التقنية الحديثة الغير تقليدية لضمان خفيتها وعدم التشهير، حيث انها تعتبر احد أهم الأسباب الدافعة لتحريك الجاني للقيام بالجريمة الإلكترونية من أجل تحقيق ربح مالي أكبر كما أنه

يقوم بتطوير نفسه ويسعى للاحتراف في المجال الإلكتروني حتى يستطيع تحقيق أعلى المكاسب لسهولة التنفيذ ولتوفير وقت أكبر بدون ترك أثر واضح بالاستعمال غير المشروع للأجهزة المعلوماتية كالحاسوب وأدوات الاتصال الدولية وشبكة الانترنيت[35].

ففي دراسة أشارت إحدى المجلات المتخصصة في الأمن المعلوماتي securite informatique إلى أن الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت إلى أن 43٪ من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال، و23٪ من أجل سرقة المعلومات، وأن 19٪ خاصة بالإتلاف المعلوماتي، و15٪ خاصة بسرقة وقت الآلة، أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية[36].

الفرع الثاني: الدوافع الذهنية

من الأسباب الأساسية التي تدفع المجرم الإلكتروني لارتكابها الرغبة الشديدة في التعلم ومعرفة الأساس التقني لجهاز الحاسوب أو ما يسمى بالهندسة المعلوماتية ومعرفة خفايا وأسس بناء الأنترنت، فقد أشار الأستاذ "ستفن ليفي" في مؤلفه "قراصنة الأنظمة" والمؤلف الثاني "الجنون العظيم للقراصنة" إلى أن أخلاق القراصنة تعتمد على مبدأين أساسين وهما:

-الولوج إلى أنظمة الحاسوب الإلكتروني تمكنك من كيفية تسيير العالم؛

-عملية جمع المعلومات يجب أن تكون غير خاضعة للقيود.

وهناك من القراصنة من يرتكب الجرائم الإلكترونية بهدف الحصول على المعلومات الجديدة في التقنية الرقمية على مستوى الانترنت باستعمال طريقة "الهوية المجهولة" لأكبر وقت ممكن حتى يمكن لهم الاستمرار في التواجد داخل الشبكة[37].

وعليه فمرتكبو الجرائم الإلكترونية ولتعويض احساسهم بالدونية أو شعورهم بجنون العظمة يمتلكهم شعور بالبحث عن القوة يؤدي بهم الى ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة أو لارتكاب فعل الاحتيال الإلكتروني، أو قد ينتاب المحلل أو المبرمج الذي يعتبر مفتاح كل نظام إحساس بالإهمال أو النقص داخل الشركة التي يزاول بها عمله فيندفع تحت تأثير رغبة قوية من أجل اثبات قدراته التقنية لإدارة هذه الشركة إلى

ارتكاب جرائم إلكترونية، ويعتبر هذا الدافع من أكثر الدوافع التي يتم استغلالها من قبل المنظمات الإجرامية حتى يتم استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة[38].

المطلب الثاني: الدوافع الخارجية

من المعلوم أن طبيعة الانسان كمخلوق ضعيف سيكولوجيا، يتأثر في بعض الأحيان بالضغوط الخارجية خاصة في نطاق المنافسة وكذا التجسس والأعمال التجارية[39]، ويستسلم لهذه المؤثرات بارتكابه لبعض الجرائم الإلكترونية، نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، وتتعدد المؤثرات التي تدفع المجرم الإلكتروني الى اقتراف مثل هذا السلوك من بينها دافع الانتقام والتواطؤ على الاضرار برب العمل (الفرع الأول) ودافع الثقة (الفرع الثاني)[40].

الفرع الأول: الرغبة في الانتقام

قد يكون دافع الانتقام من شخص ما أو مؤسسة أو حتى بعض الأنظمة السياسية في بعض الدول من أهم الأسباب التي تشكل لدى الجاني البغض والكره وتولد له الرغبة في الانتقام، فكثير من الأشخاص يتم طردهم من عمل ما بغير سبب وهم يملكون المعلومات اللازمة وخفايا تلك المؤسسة التي طردتهم ما يدفع بالجاني إلى القيام بفعل غير مشروع ليجعل هذه الأخيرة تتكبد الخسائر المالية من جراء ما ألحقته له من ضرر في حياته يحتاج إلى وقت لإصلاحه[41].

ومن أبرز الجرائم التي ارتكبت بدافع الانتقام حادثة شركة "OMEGA" التي تعود وقائعها في أن مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لهذه الشركة من مدينة "DELAWARE" ويدعى "TIMOTHY ALLEN LIOYD" تم اعتقاله في 17 فيفري 1998 بسبب إقدامه على إطلاق قنبلة إلكترونية بعد عزله من منصب عمله، حيث استطاعت تلك القنبلة إلغاء كافة التصاميم وبرامج الإنتاج لإحدى كبرى مصانع التقنية العالمية في "نيوجرسي" والتي تؤثر على نظم تحكم مستخدمة في "NASA" والبحرية الامريكية، ملحقا خسائر بلغت قيمتها 10 ملايين دولار حيث تعتبر هذه الحادثة مثالا حيا على مخاطر جرائم التخريب في بيئة الانترنت[42].

وبالتالي فإن دافع الانتقام يعد من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، فيمكن أن يصل حد أن يصدر التصرف بغرض الانتقام من دولة معادية لدولة أخرى، وذلك عن طريق إما التجسس على المعلومات أو عن طريق زرع الفيروسات أو ارتكاب جرائم السرقة لأصول الأموال أو لمحاولة تشويه صورة هذه الدولة باستخدام الشبكة الدولية الاتصالات[43].

الفرع الثاني: دافع الثقة

تضع بعض الشركات ثقة عمياء في موظفيها مما يؤدي إلى استغلال نقاط الضعف المحتملة لمركز المعالجة في تحقيق مصالحه الخاصة، إذ تعد الألفة بينه وبين الأنشطة التي يزاولها ومركز الثقة الذي يحوزه أفضل سلاح لارتكاب الجرائم الالكترونية يضاف إلى التهاون في تطبيق إجراءات المراقبة وممارسة التفتيش من العوامل الرئيسية التي ساعدت على تضخيم الاعتداءات المالية، فالعديد من الشركات ونتيجة للثقة العمياء التي تحصن بها المسؤولين العاملين لديها عن مراقبتهم، جعلها فريسة سهلة لكثير من ضعاف النفوس الذين استغلوا تلك الثقة التي وضعت فيهم لزيادة أعمالهم الإجرامية[44].

ومن أمثلة ذلك قيام مستشار لدى أحد البنوك الكبرى يسمى " STANLEN RIFKIN" حيث كان يتمتع بثقة كبيرة من طرف هذا البنك حيث سمح له اختصاصه بالولوج والتحكم في مفتاحين إلكترونيين من ثلاثة أساسية للتحكم في التحويلات الالكترونية للنقود من بنك إلى آخر وقد تمكن من الوصول إلى المفتاح الثالث واستطاع أن ينقل 100 مليون دولار إلى حساب بنكي فتح باسمه في سويسرا وبالتالي فالثقة العمياء من قبل الشركة الممنوحة لموظفيها بعدم مراقبتهم قد تجعلها ضحية لهذه الجرائم والتي تكون هي سببها الرئيسي[45].

خاتمة:

وفي الأخير يمكن القول إنّ الجرائم الإلكترونية ظهرت نتيجة للتطور التكنولوجي الذي شهده العالم، فشكلت بذلك نوعا من الجرائم المستحدثة لم يعهدها القانون الجنائي بثوبه التقليدي، فاستبدل المجرم هنا الوسائل التقليدية للجريمة بالوسائل الإلكترونية وشبكة الانترنت، ولم يقتصر الأمر على الأداة فقط بل امتد إلى مسرح الجريمة من واقع ملموس

إلى عالم افتراضي وحتى بشخصيات قد تكون مجهولة، مما زاد الأمر تعقيدا على القائمين بالبحث الجنائي، وما زاد من حدة التعقيد هو التطور الهائل الذي تعرفه الجرائم الإلكترونية فجعل من القوانين عاجزة أمام مواكبة هذا التطور الذي تشهده الجرائم الإلكترونية، خصوصا أمام ازدياد معدلات الاستخدام غير المشروع لخبايا الأنترنت، واختراق الجناة مختلف أرجاء العالم لما يمتاز به هذا النوع من الجرائم من عالمية.

وأمام ما تقدم ذكره توصلت الدراسة إلى مجموعة من النتائج نذكر منها:

-حاولت تشريعات متعددة وآراء فقهية متنوعة تحديد مفهوم واضح للجريمة الإلكترونية يكون جامعا في طياته لمختلف معايير التعريف، إلا أنه لا يوجد تعريف دقيق للجريمة الإلكترونية، وقد يجد هذا الأمر مبرره في التطور التكنولوجي الذي تعرفه البيئة الرقمية؛

-الطبيعة الفنية للجرائم الإلكترونية جعلت كل أطياف المجتمع بصفة عامة في غير منأى عن التعرض لها؛

-خصوصية الجريمة الإلكترونية، جعلت من مرتكبيها لا يحتاجون إلى مستوى علمي كبير إذا كانت هذه الميزة تخدم المجرم الالكتروني، فإنها في الحقيقة تقف عائقا أمام مقدرة سلطات التحقيق في اكتشاف آثار الجريمة؛

-اختلاف أدلة الجرائم التقليدية عن الأدلة في المجال الإلكتروني أدى إلى صعوبة إثبات الجرائم الإلكترونية، خصوصا وأن هذا الدليل خفي ويسهل تدميره، ويعرف في تواجده حيزا دوليا.

وأمام ما تم التوصل إليه يمكن أن نقترح ما يلي:

-ضرورة صياغة نص قانوني خاص يحمل في تفصيلاته الجوانب الموضوعية والاجرائية الخاصة بمكافحة الجريمة الإلكترونية،

-العمل على تدعيم الأجهزة المكلفة بالتحقيق في الجرائم الإلكترونية بآليات وتقنيات تكون مواكبة للتطور الذي تعرفه ساحات الإجرام الإلكتروني مما يضمن مواجهة فعالة لها؛

-تفعيل دور فعاليات المجتمع المدني لنشر التوعية بمخاطر الجريمة الإلكترونية وكيفيات الوقاية منها؛

-عقد دورات تدريبية للكوادر القائمة على سلطة التحري والتحقيق حول الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وإدراج تخصصات جامعية مرتبطة بموضوعات هذه الجرائم وآليات مكافحتها خصوصا على مستوى كليات الحقوق والعلوم السياسية، وتشجيع الابتكارات لمواجهة الهجمات الإلكترونية؛

-تعزيز التعاون الدولي والخبراتي من أجل المكافحة الفعالة للجرائم الإلكترونية.

المراجع

1 – فريد ناشف والطاهر ياكر، "المواجهة الأمنية والجزائية للجرائم الإلكترونية"، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، المجلد 21، العدد 01، 2022، ص62.

2 – محمد نجيب دياب‌لو، الجريمة الإلكترونية وحجية الدليل الرقمي في الاثبات الجنائي، ط1، المركز المغاربي-شرق أدنى للدراسات الاستراتيجية- بريطانيا، 2024، ص 264.

3 – فريد ناشف والطاهر ياكر، المرجع السابق، ص63.

4 – فتيحة خليفي، الجرائم الإلكترونية المرتبطة بشركات المساهمة، أطروحة مقدمة لنيل من أجل نيل شهادة الدكتوراه في قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة عين تموشنت، الجزائر، 2023، 2024، ص84.

5 – سمير شعبان، "الجريمة الإلكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم"، مجلة دراسات وابحاث، المجلد 01، العدد 01، 2009، ص115، 116.

6 – عماد دمان ذبيح وسمية بهلول، "الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الحقوق والعلوم السياسية، مج07، ع01، 2020، ص 139.

7 – فتيحة خليفي، المرجع السابق، ص84.

8 – عبد العزيز بوذراع، خصوصية الجرائم الماسة بأنظمة معالجة المعلومات، رسالة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، الجزائر، 2011، 2012، ص16.

9– نصيرة بوحزمة، التحقيق الجنائي في الجرام الإلكترونية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، الجزائر، 2021، 2022، ص17.

10 – فتيحة خليفي، المرجع السابق، ص82، 83.

11 – نصيرة بوحزمة، المرجع السابق، ص18.

12 – سمير شعبان، المرجع السابق، ص117.

13– راضية عيمور، "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، المجلة الاكاديمية للبحوث القانونية والسياسية، مج 6، العدد الأول، 2022، ص91.

14 – الأمر 66–156 المؤرخ في 08–06–1966 المتضمن قانون العقوبات، الجريدة الرسمية العدد 49، الصادرة في 11–06–1966 المعدل والمتمم بالقانون رقم 24–06، الجريدة الرسمية العدد 30، الصادرة في 30 أبريل 2024.

15 – القانون 09–04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، الصادرة في 16 غشت 2009.

16 – محمد نجيب دياب‌لو، المرجع السابق، ص 48.

17 – فتيحة خليفي، المرجع السابق، ص76، 77.

18 – محمد لمين فتح الله، "الجريمة الإلكترونية مفهومها وخصائصها"، مداخلة ألقيت ضمن فعاليات الملتقى الموسوم ب: الجرائم المتصلة بتكنولوجيات الاعلام والاتصال –الصعوبات والتحديات–، كلية الحقوق، جامعة الجزائر 01، الجزائر، 17 أفريل 2025، ص343.

19 – اسمهان بوضياف، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مج3، ع 11، 2018، ص353.

20 – محمد لمين فتح الله، المرجع السابق، ص343.

21 – عماد دمان ذبيح وسمية بهلول، المرجع السابق، ص142.

22– حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، الجزائر، 2015، 2016، ص27.

23– نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، الجزائر، 2021، 2022، ص27.

24 – المرجع نفسه، ص29.

25 – إسمهان بوضياف، المرجع السابق، ص355.

26 – نصيرة بوحزمة، المرجع السابق، ص30

27 – محمد لمين فتح الله، المرجع السابق، ص344، 345.

28 – نصيرة بوحزمة، المرجع السابق، ص30.

29– فتيحة خليفي، المرجع السابق، ص86، 87.

30– فتيحة حيمر، "تأثير الجريمة الإلكترونية على الأمن في افريقيا"، مجلة أبحاث قانونية وسياسية، المجلد 09، العدد 01، 2024، ص548.

31 – نصيرة بوحزمة، المرجع السابق، ص33 وما يليها.

32 – محمد نجيب ديابلو، المرجع السابق، ص45.

33 – عثمان خرشي، إجراءات سير الدعوى العمومية في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، الجزائر، 2020، 2021، ص40.

34- نصيرة بوحزمة، المرجع السابق، ص79، 80.

35- محمد نجيب دياولو، المرجع السابق، ص46.

36- مداوي سعيد مداوي القحطاني، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية، الأمانة العامة، 2016، ص19. متاح على الموقع: https://www.scpd.gov.kw/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9%20%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9%20%D9%81%D9%8A%20%D8%A7%D9%84%D9%85%D8%AC%D8%AA%D9%85%D8%B9%20%D8%A7%D9%84%D8%AE%D9%84%D9%8A%D8%AC%D9%8A%20%D9%88%D9%83%D9%8A%D9%81%D9%8A%D8%A9%20%D9%85%D9%88%D8%A7%D8%AC%D9%87%D8%AA%D9%87%D8%A7%20-%20%D8%AF%D9%88%D9%84%D8%A9%20%D9%82%D8%B7%D8%B1.pdf تاريخ التصفح 30-04-2025 على الساعة 21:50.

37- نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع الجزائري منها، رسالة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 01، الجزائر، 2016، 2017، ص117، 118.

38- فتيحة خليفي، المرجع السابق، ص92.

39- عثمان خرشي، المرجع السابق، ص42.

40- نصيرة بوحزمة، المرجع السابق، ص85.

41- محمد نجيب دياولو، المرجع السابق، ص45.

42- فتيحة خليفي، المرجع السابق، ص93.

43- نصيرة بوحزمة، المرجع السابق، ص85.

44- صابرين يوسف عبد الله الحياني، جرائم الأموال الناجمة عن استعمال الحاسوب (دراسة مقارنة)، رسالة من متطلبات نيل درجة الماجستير في القانون العام، كلية الحقوق، جامعة النهرين، العراق، 2014، ص18.

45- فتيحة خليفي، المرجع السابق، ص96.