وزارة التعليم العالي والبحث العلمي

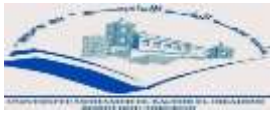
Ministry of High Education and Scientific Research

جامعة محمد البشير الإبراهيمي – برج بوعريريج –

University of Mohamed el Bachir el Ibrahimi-Bba

كلية الحقوق والعلوم السياسية

Faculty of Law and Political Sciences



مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر أكاديمي في الحقوق

تخصص: قانون اعلام الي

الموسومة بـ

خصوصية الجريمة الإلكترونية في التشريع الجزائري

إعداد الطالبان:

– مرابطين علاء الدين

– محمادي مراد

إشراف الدكتور:

– سي حمدي عبد المومن

الاسم واللقب	الرتبة	الصفة
بكيس عبد الحفيظ	أستاذ محاضر .أ.	رئيسا
سي حمدي عبد المومن	أستاذ محاضر .ب.	مشرفا
نجار امين	أستاذ مساعد .أ.	مناقشا

السنة الجامعية 2023/2022


بسم الله الرحمن الرحيم

إهداء

بسم الله والصلاة والسلام على رسول الله محمد و علىآله و صحبه و التابعين إليه بإحسان أما بعد:

فأهدي نتائج سنوات الخمسة الجامعية هذه، إلى من أوصى الله بهما خيرا و جعل طاعتهم مقرونة بعبادته فقال جل وعلا:(۞ وَاعْبُدُوا اللَّهَ وَلَا تُشْرِكُوا بِهِ شَيْئًا ۖوَبِالْوَالِدَيْنِ إِحْسَانًا۞)

(۞وَاخْفِضْ لَهُمَا جَنَاحَ الذُّلِّ مِنَ الرَّحْمَةِ وَقُل رَّبِّ ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيرًا۞) :وقال تعالى

إلى من ربياني صغيرا و شملاني بمعروفهما كبيرا إلى من يستحقون علي أكثر من مجرد إهداء إلى نفسين أحب إلي من نفسي و من كان رضائهما الخير كله نبع الحنان ومصدر العزيمة الذي لا يلين و اللسان الذي لا يكف عن الدعاء رمز المحبة والحنان وعطف والاطمئنان إلى من جعل الله الجنة تحت قدميها، إلى من لا تكفي الكلمات ولا يسع ذكرها السطور، إلى من لا يزال دعاءها يحفظني ويرعاني، إلى رمزي في الوجود و قدوتي في الحياة، إلى من .رمز الإيمان والنقاء أمي الحبيبة أطال الله في عمرها كانت يداه مبسوطتان لتربيتي وتعليمي و لنجاحي و لسعادتي و حمايتي، رمز الاجتهاد و الكفاح و معتمدي في الحياة بعد الله، إلى من علمني العطاء بدون انتظار إلى من أحمل اسمه بكل افتخار أرجو من الله أن يمد في عمرك لترى ثمارا قد حان قطافها بعد طول انتظار و ستبقى كلماتك نجوم أهتدي بها اليوم و في الغد و إلى الأبد أبي العزيز.

إلى من هم أقرب إلي من روحي إلى من شاركوني حضن آلامي وبهم أستمد عزيمتي و إصراري إخوتي و أخواتي الأعزاء.

مرابطين علاء الدين

إهداء

أهدي هذا العمل المتواضع إلى كل من اقترنت طاعتهما بعبادة الله

إلى الوالدين الكريمين أطال الله في عمرهما.

إلى إخوتي وأخواتي وكل عائلتي.

أهدي هذا العمل إلى كل أحبائي وأقاربي وأصدقائي وزملائي في الدراسة والعمل

وإلى كل من ساندني طوال مشواري الدراسي.

محمادي مراد

شكر وتقدير

من لم يشكر الناس، لم يشكر الله عز وجل

الحمد لله حمدا مباركا طبيا على أكرمنا به لإتمام هذه الدراسة التي نرجو أن تنال رضاه؛

أتقدم بجزيل الشكر والامتنان إلى الأستاذ المشرف الذي كان لنا بمثابة المصباح الذي ينير دربا من خلال توجيهاته وتوصياته القيمة خلال مرحلة إنجاز هذا العمل المتواضع؛

نتقدم بجزيل الشكر إلى كل أساتذة القسم الذين لم يبخلوا علينا العلم وأدوا الأمانة على أكمل وجه نرجو من الله عز وجل أن يجازيهم خير الجزاء.

المقدمـــــة

لقد وُجدت الجريمة منذ فجر التاريخ، ولكن تطورت الطرق التي تتعامل بها البشرية معها. في بعض الأحيان يكون انعكاسًا مباشرًا لأولوياتنا، وفي أحيان أخرى يكون مثالاً على دور إنسانيتنا. وبما أن الإنسان دائما في تطور مستمر بفضل الثورة التكنولوجية التي نشهدها، نلاحظ تطور في الجرائم هي الأخرى، وأصبحت هناك جرائم إلكترونية عبر الفضاء الإلكتروني، وتعدت حدود الإقليمي للدولة الواحدة وأصبحت من الجرائم العابرة للقارات، ولذلك تعتبر هذه الجرائم ضربا من ضروب الذكاء الإجرامي.

إن الجرائم الإلكترونية من الجرائم المستحدثة التي تكلف ضحاياها خسائر جسيمة، وهي نتيجة حتمية للتطور العلمي، ولهذا يجب على المشرع تطوير الترسانة القانونية للتصدي لها، فلا يمكن الاعتماد على النصوص التقليدية التي لا تواكب هذه الجرائم.

الجزائر كغيرها من الدول ليست بمنأى عن الجريمة الإلكترونية وتداعياتها، وأمام هذا الوضع الخطير وعدم نجاعة الأساليب التقليدية لمكافحتها، كان لزاما على المشرع الجزائري استحداث أساليب للتحقيق والإثبات في الجرائم الإلكترونية تماشيا مع متطلبات المنظومة الدولية.

أسباب اختيار الموضوع:

هناك أسباب ذاتية وأخرى موضوعية

1. **الأسباب الذاتية:**

- ✓ طبيعة الاختصاص الجامعي فرض علينا اختيار متعلق بالدراسة؛
- ✓ الرغبة الذاتية والميول الشخصي للجرائم التي تتعلق بالفضاء الإلكتروني، كوننا نعيش في عصر الثورة المعلوماتية.

2. **الأسباب الموضوعية:**

- ✓ الانتشار المتنامي للجرائم الإلكترونية في الفترة الأخيرة نظرا للتطور التكنولوجي؛
- ✓ يمثل لموضوع محاولة جادة لفهم خصوصية الجريمة الإلكترونية وما تتميز به خلاف الجريمة التقليدية، خاصة في الجانب الإجرائي سواء من حيث الاختصاص القضائي أو من حيث أساليب التحقيق والإثبات في هذا النوع من الجرائم؛
- ✓ قلة الدراسات التي تناولت الجانب الخاص بالاختصاص القضائي في الجرائم الإلكترونية والقانون الواجب التطبيق عليها.

أهمية الموضوع:

تكمن أهمية الموضوع والمنون بخصوصية الجريمة الإلكترونية كونه من المواضيع التي تتطلب الاهتمام بها في الوقت الراهن كونها:

-الطبيعة الخاصة التي تتمتع بها الجرائم الإلكترونية؛

-إن الجريمة الإلكترونية من الجرائم المستحدثة تعتمد على التقنية الحديثة والذكاء لمرتكبيها؛

-غياب الدليل الإلكترونية أو سهولة إتلافه وهذا ما يصعب إثباتها؛

-قصور التشريعات والقوانين التي تخص الجرائم الإلكترونية سوء على المستوى المحلي أو المستوى الدولي.

أهداف الموضوع:

يسعى الموضوع غلى تحقيق جملة من الأهداف والتي تتمثل في:

1. تقديم مفهوم للجرائم الإلكترونية وسماتها؛
2. تصنيفات الجرائم الإلكترونية؛
3. تبيان الاختصاص القضائي للجرائم الإلكتروني على المستوى الوطني والدولي؛

4. تبيان أساليب التحقيق والإثبات في الجرائم الإلكترونية.

الإشكالية:

إن خصوصية الجريمة الإلكترونية وإجراءات التحقيق وإثبات الجريمة تواجه صعوبات، سواء من ناحية الاختصاص القضائي داخل التراب الوطني أو الجريمة الإلكترونية العابرة للحدود، إن طبيعة هذه الجرائم تثير مشكلات المتعلقة بالتحقيق والإثبات باعتبارها تقع في البيئة الافتراضية ولا تترك أثرا ماديا محسوسا في مسرح الجريمة خلافا للجرائم التقليدية.و على هذا الأساس تتبلور الإشكالية التالية: **ما هي خصوصية الجريمة الإلكترونية في القانون الجزائري؟**

المنهج المتبع:

للإجابة على الإشكالية تم الاعتماد على المنهج الوصفي التحليلي وهذا ما يتناسب مع طبيعة البحث القانونية الذي يهدف إلى تبيان مفهوم الجريمة الإلكترونية وخصائصها، وكذا توضيح تصنيفاتها. بالإضافة إلى التطرق إلى خصوصية الجريمة الإلكترونية من الناحية الإجرائية وتحليل بعض النصوص القانونية التي تتلاءم مع الموضوع.

تقسيم الموضوع:

من أجل الإجابة على الإشكالية تم تقسيم الموضوع إلى فصلين، حيث تناولنا في الفصل الأول والمعنون بخصوصية الجريمة الإلكترونية من الناحية الموضوعية والذي من خلاله تم التطرق إلى مبحثين: المبحث الأول خاص بمفهوم وسمات الجريمة الإلكترونية، أما المبحث الثاني يتطرق إلى تصنيفات الجريمة الإلكترونية.

أما الفصل فهو الآخر تم تقسيمه إلى مبحثين والذي من خلال المبحث الأول تم التطرق إلى المتابعة القضائية في الجريمة الإلكترونية، أما المبحث الثاني فتم تخصيصه للآليات المتخصصة في التحقيق والإثبات في الجرائم الإلكترونية.

الفصل الأول: خصوصية الجريمة الإلكترونية من الناحية الموضوعية

تمهيـــد:

لقد عرفت الجريمة منذ أن خلق الله الإنسان، وهي في تطور مستمر مع تطور الحياة الإنسانية، وتعد من نتاج الحياة الاجتماعية وارتكابها يخل بالنظام الاجتماعي العام.

إن التطور العلمي في العصر الراهن، وبروز الثورة التكنولوجية أدى إلى ظهور نوع جديد من الجرائم التي تعتمد على التقنية الحديثة، تعرف بالجريمة الإلكترونية.

وفي هذا الفصل سنحاول التعرف على الجريمة الإلكترونية وهذا من خلال تقسيمه إلى مبحثين:

المبحث الأول: ماهية الجريمة الإلكترونية

المبحث الثاني: تصنيف الجرائم الإلكترونية

المبحث الأول: ماهية الجريمة الإلكترونية

إن تطور الوسائل المعلوماتية الحديثة أدى ظهور الجريمة الإلكترونية وسهولة ارتكابها، وتأثيرها في مختلف نواحي الحياة. ومن خلال هذا المبحث سيتم التطرق إلى مفهوم الجريمة الإلكترونية في المطلب الأول، وسمات الجريمة الإلكترونية في المطلب الثاني.

المطلب الأول: مفهوم الجريمة الإلكترونية

سيتم التطرق في هذا المطلي إلى تعريف الجريمة الإلكترونية وطبيعتها القانونية.

الفرع الأول: تعريف الجريمة الإلكترونية

قبل التطرق إلى تعريف الجريمة الإلكترونية تعريفا مركبا لا بد من التطرق إلى تعريف كل كلمة على حدى.

أولا: تعريف الجريمة

جاء في لسان العرب الجرم هو التعدي، والجرم: الذنب، والجمع أجرام وجرم، وهو الجريمة وقد جرم بجرم جرما وإجراما، فهو مجرم وجريم[1].

تعرف ابتسام فرام الجريمة على أنها: "فعل أو امتناع ينص عليه نص تشريعي ويعاقب عليه. ويتم التمييز بين ثلاثة أصناف من الجرائم حسب جسامتها المتناقضة: جناية، وجنحة، ومخالفة، وفي مجال التنفيذ نميز: الجريمة المركبة، والجريمة المستمرة، والجريمة الشكلية، والاعتيادية، الفورية والعمدية والدولية...الخ[2].

[1] ابن منظور، **لسان العرب**، ج7، ص605.

[2] أمال بوخنوش، " **مصطلح "الجريمة" في قانون العقوبات الجزائري بين الصيغة والمفهوم _دراسة لغوية_**"، مجلة الحكمة للدراسات الإسلامية، المجلد08، العدد01، 2021، ص33.

وتعرف من الناحية الاجتماعية بأنها: "كل فعل بتعارض مع ما هو نافع للجماعة وما هو عدل في نظرها. وانتهاك العرف السائد مما يستوجب توقيع الجزاء على منتهكيه، وخرق للقواعد والمعايير الأخلاقية للجماعة"[1].

الفرع الثاني: تعريف الإلكترونية

أصلها من كلمة (إلكترون) وهو لفظ أعجمي أقره مجمع اللغة العربية في مصر، وضمته المعاجم الحديثة إليها. ويعرف الإلكترون بأنه: "دقيقة ذات شحنة كهربائية سالبة شحنها هي الجزء الذي لا يتجزأ من الكهربائية"[2].

لقد جاء إلكتروني في نظام التعاملات الإلكترونية السعودي بأنه: "تقنية استعمال وسائل كهربائية، أو كهرومغناطيسية، أو بصرية، أو أي شكل آخر من وسائل التقنية المشابهة"[3].

ثالثا: تعريف الجريمة الإلكترونية

لم يتفق العلماء والباحثين على إعطاء تعريف موحد للجريمة الإلكترونية ومن بين التعاريف المقدمة لها نذكر ما يلي:

[1] سامية عزيز، مازيا عيساوي، "**الجريمة من منظور سوسيولوجي _الأسباب والآثار_**"، مجلة دراسات في سيكولوجية الانحراف، المجلد06، العدد01، 2021، ص129.

[2] عادل بن عبد العزيز بن صالح الرشيد، "**قرائن الجريمة الإلكترونية وأثرها في الإثبات**، دار كنوز إشبيليا للنشر والتوزيع، 2017، ص23.

[3] المرجع نفسه.

ذهب الفقيه (merwe) إلى أن الجريمة الإلكترونية هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية[1].

ويعرفها مكتبة التقنية في الولايات المتحدة الأمريكية أنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[2].

وهناك من عرفها بأنها: "جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، بحيث تطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات[3].

وتوصف الجريمة الإلكترونية بأنها "كل فعل من شأنه القضاء على استخدام التكنولوجيا الحديثة عبر الوسائط الإلكترونية، وتظهر أهميتها عبر شبكة الإنترنت وهذا لصعوبة ضبطها، كونها عابرة للحدود، وتتم بسرعة دون رقابة أي دولة[4].

إن الجريمة الإلكترونية تشمل جميع أنواع الجرائم التي تتم من خلال أو بواسطة الحاسب الآلي منفردا أو متصلا بالإنترنت وذلك[5]:

1. لتوافر مراجع ومؤلفات تسلم بهذا الأمر؛
2. لحصر جميع الجرائم التي تتم بواسطة الكمبيوتر والإنترنت.

---

[1] عبد العالي الديربي، محمد صادق إسماعيل، **الجرائم الإلكترونية دراسة قانونية قضائية مقارنة**، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012، ص40.

[2] محمود مدين، **الجريمة الإلكترونية وتحديات الأمن القومي**، المصرية للنشر والتوزيع، ط2، 2019،ص32.

[3] رفد عيادة الهاشمي، **الإرهاب الإلكتروني**، دار أمجد للنشر والتوزيع، ط1، 2019، ص48.

[4] عبد الصبور عبد القوي علي مصري، **التنظيم القانوني للتجارة الإلكترونية**، مكتبة القانون والاقتصاد، الرياض، 2012، ص92.

[5] غادة نصار، **الإرهاب والجريمة الإلكترونية**، العربي للنشر والتوزيع، ط1، 2017، ص11.

يعرف الفقيهان (mechel &credo) الجريمة الإلكترونية أنها استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته[1].

وبالرجوع إلى التشريع الجزائري فقد أطلق على تسميتها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتم تعريفها وفقا للمادة 02 من القانون 09-04 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"[2].

الفرع الثاني: طبيعة الجريمة الإلكترونية

لقد انقسم الفقه إلى اتجاهين لمعرفة الوضع القانوني للجريمة الإلكترونية، حيث يرى الاتجاه الأول أن المعلومة لها طبيعة من نوع خاص، وذلك انطلاقا من حقيقة مسلم بها هي أن وصف القيمة يضفي على الأشياء المادية وحدها، وبمعنى آخر أن الأشياء التي توصف بالقيم هي الأشياء التي تقبل الاستحواذ عليها، وبمفهوم المخالفة وباعتبار أن المعلومة لها طبيعة معنوية فلا يمكن اعتبارها من قبيل القيم القابلة للاستحواذ عليها إلا في ضوء الحقوق والملكية الفكرية. وأيا كان الأمر فإن الأمر مستقر بصدد وجود خطأ عند الاستيلاء على

[1] عبد العال الديربي، محمد صادق إسماعيل، **الجرائم الإلكترونية دراسة قانونية قضائية مقارنة**، المركز القومي للإصدارات القانونية، ط1، 2012، ص41.

[2] القانون رقم09-04، الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47.

معلومات الغير ولذلك فقد حاول هذا الاتجاه أن يحمي هذه المعلومات بدعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استثنائي[1].

أما الاتجاه الثاني يرى أن المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعامتها المادية، على سند من القول أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، وأنها ترتبط كما يقول الأستاذان " vivant &catala" بمؤلفهما عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال[2].

المطلب الثاني: سمات الجريمة الإلكترونية وأسباب ارتكابها

بعد التعرف والتطرق إلى مفهوم الجريمة الإلكترونية لا بد من التطرق غلى ابرز سماتها ومعرفة الدوافع التي تؤدي إلى ارتكابها.

الفرع الأول: سمات الجريمة الإلكترونية

1. جريمة يصعب اكتشافها: تعتبر الجريمة الإلكترونية التي لا تترك أثر لمتابعتها وملاحظتها بل وقد يستخدم الجاني برامج تقنية من خلالها تعرقل الوصول إليه أو معرفة التقنية للجريمة المرتكبة أيا كان نوعها، وكما أن المجني عليه لا يكتشفها مباشرة ولا يشعر بها إما لضعف قدرته الفنية على ذلك بالمقارنة بمرتكب الجريمة أو للمهارات الفنية التي استخدمها الجاني عند ارتكابه للجريمة، أو لعدم رغبة المجني عليهم بالتبليغ

[1] رمزي حوحو، منيرة بلورغي، "**مواجهة الجريمة المعلوماتية في الجزائر**"، مجلة الحقوق والحريات، العدد02، 2014، ص45.

[2] مخلد إبراهيم الزعبي، "**فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية**" "**دراسة قانونية**""، المجلة العربية للنشر العلمي، العدد73، تشرين الثاني 2021، ص281.

عن وقوع الجريمة حفاظا على السمعة وفقد الثقة فيهم، حيث تلجأ الشركات، المصانع، الجمعيات، المؤسسات، البنوك والجامعات ذات السمعة المرموقة إلى التستر على هذه الجريمة، ويفضلون حلها من خلال موظفي تكنولوجيات المعلومات لديها[1].

2. جريمة يصعب إثباتها: يتصف مرتكبها بالذكاء والفطنة ولهذا يصعب إثباتها ويرجع هذا إلى:

- يتميز الدليل الرقمي بصعوبة محوه أو تحطيمه، إذ حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوي ذلك الدليل ويعتمد على استخدام أجهزة خاصة تقوم بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلا رقميا[2]؛
- إن الطبيعة الفنية للدليل الإلكتروني تمكن من إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله من قبل الجاني، أو التعديل غير المقصود من قبل المحقق أو الخبير المعلوماتي أثناء عملية جمع الدليل؛
- نشاط الجاني لمحو الدليل الإلكتروني قد يعد قرينة لارتكاب الجريمة الإلكترونية حيث إن نسخة من هذا النشاط_فعل الجاني لمحو الدليل_يتم تسجيلها، ويمكن استخلاصها لاحقا لاستخدامها دليل إثبات ضده؛
- امتيازه بالسعة التخزينية العالية، فآلة التصوير الرقمية مثلا يمكن تخزين مئات الصور، وقرص صلب صغير يمكنه تخزين مكتبة كبيرة؛

3. لجوء مرتكبي الجرائم الإلكترونية إلى استخدام وسائل وأساليب حديثة وتميزها بطابعها التقني والفني المعقد.

---

[1] ميرفت محمد حبابية، **مكافحة الجريمة الإلكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني**، دار اليازوري العلمية، عمان، الأردن، 2022، ص45.

[2] محمد مدين، **فن التحقيق والإثبات في الجرائم الإلكترونية**، المصرية للنشر والتوزيع، ط1، 2020.

4. التحديات والصعوبات القانونية التي تعرقل عملية متابعة الجناة التي تنجم عن مشاكل الحدود الأولويات القضائية وذلك نظرا لكون الجرائم الإلكترونية من الجرائم العابرة للحدود القومية[1].
5. الجريمة الإلكترونية جريمة هادئة: إن الجرائم الإلكترونية تختلف عن الجرائم التقليدية كونها جرائم لا تحتاج إلى جهد عضلي مثل جريمة الخطف، القتل، مثلا بل تعتمد على الذكاء التقني والقائم على معرفة تقنية الكمبيوتر. كونها عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أن البعض يشبهها بجرائم العنف وهذا ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكي نظرا لتماثل دوافع المعتدين على نظام الحاسب الآلي مع مرتكبي العنف[2].
6. الجرائم الإلكترونية كثيرة الخسائر: يرجع الاعتماد المتزايد على الحاسب الآلي في إدارة مختلف الأعمال في مختلف نواحي الحياة ضاعف من الخسائر التي تخلفها هذه الاعتداءات الإلكترونية خاصة إذا تعلق الأمر بالقيم المالية إذا تعلق الأمر بالبنوك والمؤسسات المالية ومختلف الشركات على الحاسب الآلي في تسييرها. وحسب تقديرات المكتب الفدرالي للتحقيقات أن الجريمة الإلكترونية تكلف خسائر تقدر بمائة وخمسين ضعف ما تكلفه الجرائم العادية[3].

الفرع الثاني: الأسباب التي تؤدي إلى ارتكاب الجريمة الإلكترونية

هناك عدة دوافع تؤدي إلى ارتكاب الجريمة الإلكترونية نذكر أهمها:

أولا: الدوافع المالية

---

[1] أسمهان بن مالك، "**خصائص الجريمة المعلوماتية وأسباب ارتكابها**"، مجلة البيات للدراسات القانونية والسياسية، المجلد04، العدد01، 2019، ص114-115.

[2] محمد رحموني، "**خصائص الجريمة الإلكترونية ومجالات استخدامها**"، مجلة الحقيقة، العدد41، 2018، ص442.

[3] محمد خليفة، "**خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها**"، دراسات وأبحاث، المجلد01، العدد01، 2009، ص376.

ترتكب الجرائم الإلكترونية بغرض تحقيق أرباح ومكاسب مادية مثل استخدام الإنترنت للإعلان عن صفقات تجارية غير مشروعة مثل صفقات المخدرات والاتجار بالشر ووفقا لبحث المستشار الإعلامي للجمعية المصرية لمكافحة جرائم الإنترنت أن عصابات الإجرام المنظم استغلت التكنولوجيا الحديثة في تيسير شؤون الاتجار في البشر حيث أن الاتجار بالبشر حسبه هو تجارة إلكترونية[1].

ثانيا: الدوافع النمطية

هي تلك العوامل النفسية اللصيقة بالمجرم المعلوماتي تدفعه إلى ارتكاب الجريمة المعلوماتية بهدف الرغبة في إثبات الذات وتحقيق الفوز على تقنية الأنظمة المعلوماتية والرغبة في سحق النظام والتفوق على تعقيد وسائل التقنية وهذا بدون نية آثمة. وهذا ما يظهر من خلال ما يعرف بأنشطة "HACKERS" المتطفلين الداخليين على النظام والمتمثلة في جرائم التواصل مع أنظمة الحاسب تحديدا عن بعد. حيث يظهر المجرم المعلوماتي في هذه الحالة إلى إظهار قدراته وتميزه في المجال الإلكتروني، وإرادتهم في التفوق على كل الأنظمة المعلوماتية المستحدثة، وغالبا ما يتم استدراج هذه الفئة من الشباب واستمالتهم للقيام ببعض الجرائم الإلكترونية[2].

ثالثا: الدوافع السياسية

إن بعض الجرائم العسكرية يكون غرضها سياسي وتقوم بها جهات رسمية مثل الحروب الإلكترونية وهو ما يحصل بين الدول المتقدمة تكنولوجيا[3].

---

[1] مجمع البحوث والدراسات، **الجريمة الإلكترونية في المجتمع الخليجي وككيفية مواجهتها**، مجلس التعاون لدول الخليج العربية، 2016، ص29.

[2] سفيان سوير، **"جرائم المعلوماتية"**، مذكرة شهادة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2011/2010، ص27-28.

[3] مجمع البحوث والدراسات، مرجع سابق، ص30.

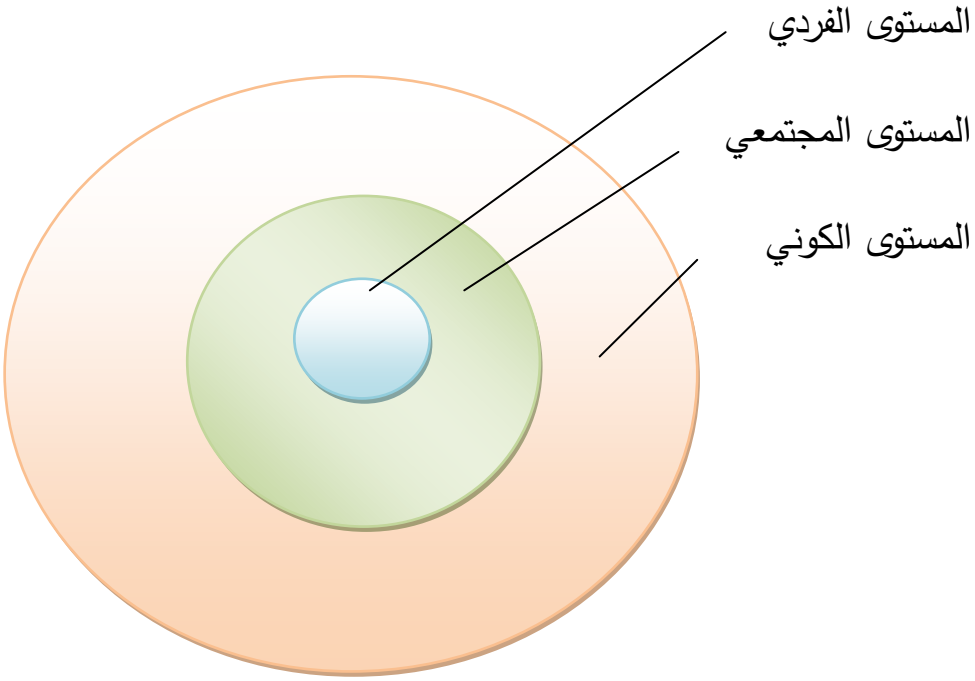
الجدول01: أسباب الجريمة الإلكترونية وفق مستوى التحليل

أسباب الجريمة على المستوى الفردي	أسباب الجريمة على المستوى المجتمعي	أسباب الجريمة على المستوى الكوني
البحث عن التقدير: هي جرائم يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي وحب الظهور في الإعلام	التحضر: يعد التحضر أحد أهم أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى مناطق الحضرية.	التحول للمجتمع الرقمي: في الفضاء الافتراضي، تكونت التفاعلات الافتراضية وحلت محل التفاعل وجها لوجه، وتكونت السلوكيات الافتراضية والشخصية الافتراضية والشخصية الافتراضية والمجتمع المحلي الافتراضي.
الفرصة: لقد وفرت التقنيات الحديثة والإنترنت فرصا غير مسبوقة لانتشار الجريمة الإلكترونية.	البطالة: ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية.	العولمة: إن ظهور الفضاء الإلكتروني يكون ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر أنفسها، والفرص المباشرة للجريمة والتي وفرتها أجهزة الكمبيوتر الآن، فالأشخاص على سبيل المثال، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم.
ضبط الذات المخفض: إن توفر صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك الطائش يعدان عاملين مؤثرين في ارتكاب السلوك الطائش.	الضغوط العامة: تعد الضغوط العامة التي يتعرض لها المجتمع، من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب.	الترابط الكوني: هناك عامل يمكن أن يساهم في دفع مستويات الجريمة هو ظهور الترابط العالمي في سياق تحولات العالم الاقتصادية والديمغرافية.

الضغوط العامة: تلعب العوامل الاجتماعية والاقتصادية دورا هاما في زيادة الجريمة الإلكترونية.	البحث عن الثراء: يلجأ بعض الناس إلى الجريمة الإلكترونية، حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.	انكشاف البنية التحتية المعلوماتية الكونية: حيث تتفاوت البنى التحتية الملعوماتية بدرجة انكشافها إلى الكوارث الطبيعية، والإهمال البشري، وسوء التصرف الإنساني. فمن الصعب ربط التهيدات الإلكترونية بمكان أو زمان، أو جماعة فقد تصدر من هاو أو طفل أو محترف، أو جماعة إرهابية، أو جماعة تنافسية، أو استخبارات أجنبية.
النشاط الروتيني: إن التغيرات في أنشطة الناس الروتينية، من استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك والإيميل والمواقع وغيرها، قد كونت فرصا للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة.	ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية: هناك الكثير من الدول لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها.	

المصدر: عبد السلام محمد المايل، عادل محمد الشربحي، علي قابوسة، "**الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم_الأسباب_سبل المكافحة مع التعرض لحالة ليبيا**"، مجلة آفاق للبحوث والدراسات السياسية، المركز الجامعي إيليزي، العدد04، جوان 2019، ص249-250.

الشكل رقم01: أسباب الجريمة الإلكترونية وفق مستوى التحليل



المبحث الثاني: تصنيف الجريمة الإلكترونية

سيتم تصنيف الجريمة الإلكترونية إلى صنفين المعلومات وسيلة لارتكاب الجرائم الإلكترونية وهذا ما سيتم التطرق إليه في المطلب الأول، والصنف الثاني المعلومات هدفا لارتكاب الجرائم الإلكترونية وهذا من خلال المطلب الثاني.

المطلب الأول: المعلومات وسيلة لارتكاب الجرائم

تشمل الجرائم الإلكترونية في هذا الصنف كل من الجرائم الواقعة على الأشخاص الطبيعية، الجرائم الواقعة على النظم المعلوماتية الأخرى، الجرائم الواقعة على الأسرار.

الفرع الأول: الجرائم الإلكترونية الواقعة على الأشخاص الطبيعية

تشمل ما يلي:

أولا: الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية

تعتبر جرائم الملكية الفكرية والصناعية من الجرائم الاقتصادية الحديثة، ومع ثورة التكنولوجيا أصبح استغلالها في مآرب غير مشروعة، بحيث أصبح جهاز الحاسب الآلي وشبكة الإنترنت وسائل لارتكاب جريمة الملكية الفكرية واتساع رقعة ومجال حقوق الملكية الفكرية وظهور صور جديدة منها، فضلا عن توسع الأنشطة الاقتصادية والتجارية مع ما أفرزته تلك الأنشطة من معاملات، وفي الغالب ترتكز على الملكية الفكرية، هذا ما أدى إلى زيادة معدلات هذه الجرائم وتأثيرها على كافة المجالات[1].

[1] فضيلة عاقلي، "**حماية حقوق الملكية الفكرية والصناعية من الجريمة المعلوماتية**"، مجلة الاقتصاد الصناعي، المجلد7، العدد2، 2017، ص263.

ثانيا: الجريمة الإلكترونية الواقعة على حرمة الحياة الخاصة

يعني بحرمة الحياة الخاصة احترام حياة كل فرد وحفظ أسراره التي لا يجب ان يكشف عنها الآخرون بغير إذنه ويتفرع عن هذه الحرمة بالضرورة الحق في حماية اتصالاته ومراسلاته بما تحتويه من أسرار[1].

من بين أهم المشاكل التي هي بمثابة خطر على الحياة الخاصة في ظل الثورة المعلوماتية نجد[2]:

- إساءة جمع البيانات عن الأشخاص واستخدامها غير الغرض المخصص لها؛

- جرائم القذف والشتم وتشويه السمعة في العالم الافتراضي؛

- التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه؛

- التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بدون إذن صاحبها أو ضاه؛

- الاعتداء على سرية المراسلات باختلاسها أو استخدامها أو إذاعتها من خلال التجسس على الاتصالات والمراسلات عن طريق المراقبة الإلكترونية بالأقمار الصناعية والكاميرات الرقمية والهواتف النقالة وكشفها عبر المواقع الإلكترونية.

[1] عبد الصبور عبد القوي علي مصري، مرجع سابق، ص122.

[2] ابتسام مناع، "**جريمة الاعتداء الإلكتروني على الحياة الخاصة في التشريع الجزائري**"، **مجلة الشريعة والاقتصاد**، المجلد08، العدد01، جوان2019، ص321-323.

الفرع الثاني: الجرائم الإلكترونية الواقعة على النظم المعلوماتية

يعرف النظام المعلوماتي بأنه: "مجموعة برامج وأجهزة تستخدم لإنشاء أو استخراج المعلومات أو إرسالها أو استلامها أو عرضها أو معالجتها أو تخزينها"[1].

عرف المشرع الجزائري النظام المعلوماتي في المدة 2 من القانون رقم 09-04 بأنه أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين[2].

إن الجرائم الإلكترونية تستهدف النظم المعلوماتية وذلك من خلال إعداد برامج خبيثة أو ما يسمى بالفيروسات والتي يتمكن بواسطتها المجرم الإلكتروني من الولوج إلى الأنظمة المعلوماتية التي يتم تخزين البيانات بداخلها. والغاية من استهداف النظم المعلوماتية متعددة ومتنوعة، فلقد يعمد المجرم الإلكتروني إلى إتلاف وتدمير البيانات أو يقوم بتعديلها، أو يكتفي فقط بأخذ نسخ منها أو الاطلاع عليها. كما يمكن زرع برامج تتيح له ربط اتصال مباشر بالجهة المستهدفة بحيث يمكنه اعتراض والتقاط أية بيانات أو التنصت، بصفة عامة يصبح قادر على مراقبة الجهة المستهدفة سواء كانت شخصا طبيعيا أو معنويا[3].

الفرع الثالث: الجريمة الإلكترونية الواقعة على الأسرار

تستعمل هذه الجريمة النظام المعلوماتي للبوح بالأسرار، بمختلف أنواعها عامة أو خاصة بالأفراد والمؤسسات المختلفة. ولها صورتين الجرائم المتعلقة بأسرار الدولة، حيث تتيح شبكة الإنترنت التجسس على الأسرار العسكرية والاقتصادية والاجتماعية لدول أخرى،

---

[1] إبراهيم محمد بن حمود الزنداني، **إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات وأحكامها في القانون اليمني والكويتي والقطري: دراسة شرعية وقانونية مقارنة**، جامعة قطاني، 2019، ض247.

[2] القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق5غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] إسماعيل بن يحي، "**التحقيق الجنائي في الجرائم الإلكترونية**"، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2020-2021، ص26.

والجرائم المتعلقة بالأسرار المهنية، ويكون الغرض من هذه الجريمة سرقة المعلومات من أجل التشهير بشخص أو جماعة أو بيع المعلومات من أجل كسب مادي أو للابتزاز من أجل القيام بعمل أو الامتناع عن القيام بعمل[1].

المطلب الثاني: الجرائم الإلكترونية الواقعة على النظام المعلوماتي

تتمثل في:

الفرع الأول: جريمة الدخول أو البقاء في منظومة معلوماتية

يتعرض النظام المعلوماتي إلى الاختراق من قبل أفراد غير مصرح لهم بالدخول إليه، ويعتبر هذا الدخول غير المصرح به مرحلة سابقة لارتكاب جرائم إلكترونية أخرى مثل السرقة المعلوماتية، التزوير المعلوماتي، الاعتداء على حرمة الحياة الخاصة، ففعل الدخول يقصده بحد ذاته دون أن يهدف إلى ارتكاب جريمة أخرى من ورائه[2].

لم يحدد المشرع الجزائري الوسائل التي تتم بها عملية الدخول، معنى ذلك أن أية وسيلة تقنية تستعمل لغرض الدخول إلى النظام تتحقق بها الجريمة، فمثلا أن يتم الدخول باستخدام الجاني كلمة السر الحقيقية المملوكة للغير بعد الحصول عليها بطريقة غير مشروعة أو باستخدام برنامج أو شيفرة خاصة. ويتم الدخول إلى النظام المعلوماتي بطريقة مباشرة أو غير مباشرة[3].

لقد تم النص على جريمة الدخول إلى النظام الآلي في قانون العقوبات الجزائري في المادة 394 مكرر: "يعاقب بالحبس من ثلاثة (03) أشهر إلى سنة (01) وبغرامة من

---

[1] عائشة نايري، "**الجريمة الإلكترونية في التشريع الجزائري**"، مذكرة ماستر في القانون الإداري، دامعة أحمد دراية أدرار، 2017/2016، ص26-27.

[2] حفيظ بن قربة، "**جريمة الدخول غير المصرح به إلى منظومة معلوماتية في التشريع الجزائري**"، مجلة القانون والعلوم السياسية، المجلد03، العدد02، 2017، ص201.

[3] نسمة بطيحي، "**جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي**"، مجلة الفقه القانوني والسياسي، المجلد01، العدد01، 2019، ص78.

50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.[1]

الفرع الثاني: جريمة المساس بمنظومة معلوماتية

نص المشرع الجزائري في المادة 394 مكرر01 من قانون العقوبات رقم 15/04 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات عن طريق استخدام الغش. سواء كان بالإدخال أو المحو أو التعديل، ولا يشترط المشرع الجزائري اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي، وأفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات قديمة. وهذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثل إدخال فيروسات في البرامج من أجل إتلافها[2].

[1] القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 1966/06/08، المتضمن قانون العقوبات، الجريدة الرسمية الجزائرية، العدد71 بتاريخ 2004/11/10.

[2] عائشة نايري، مرجع سابق، ص29.

خلاصة الفصل:

ومن خلال ما تم التطرق إليه نستنتج أن الجريمة الإلكترونية هي جريمة ذات طابع مادي، وسلوك غير قانوني يرتبط ارتباطا مباشرا بالأجهزة الإلكترونية مثل الحاسب الآلي، وتتمثل أهداف هذه الجريمة في سرقة وقرصنة المعلومات الموجودة في الأجهزة أو تهدف إلى ابتزاز الأشخاص بمعلوماتهم المخزنة على أجهزتهم.

إن الجريمة الإلكترونية تتمتع بالعديد من السمات وتتمثل في أنها جريمة لا يمكن إثباتها، صعوبة الكشف عن مرتكبها، ذات عنف أقل من الجرائم التقليدية، وهي غير مقيدة بزمان ومكان، وسهولة إخفاء آثار الجريمة.

هناك عدة تصنيفات للجريمة الإلكترونية فهناك المعلوماتية وسيلة لارتكاب الجرائم مثل الجرائم الواقعة على الأشخاص الطبيعية، الجرائم الواقعة على النظم المعلوماتية، الجرائم الواقعة على الأسرار، وهناك المعلوماتية هدفا لارتكاب الجريمة وتتمثل في جريمة الدخول أو البقاء في منظومة معلوماتية، جريمة المساس بمنظومة معلوماتية.

الفصل الثاني: خصوصية الجريمة الإلكترونية من الناحية الإجرائية

تمهيـــــــد:

بعد انتشار الجرائم الإلكترونية بشكل متسارع في الآونة الأخيرة، استجوب استحداث الأنظمة والتعليمات والجهات الأمنية المتخصصة في مواجهتها، وهذا ما يؤدي إلى تطوير أساليب الإثبات والتحقيق.

باعتبار الجريمة الإلكترونية من الجرائم المستحدثة وكونها جرائم صعبة الإثبات لعدم وجود آثار مادية يخلفها مرتكبها، هذا ما يؤدي إلى ضرورة البحث عن أدلة أخرى لإثباتها، والحصول على هذه الأدلة يتطلبه منظومة قضائية وقانونية فعالة تتولى مسألة التحقيق والإثبات.

من خلال هذا سيتم تقسيم الفصل إلى مبحثين:

المبحث الأول: المتابعة القضائية في الجريمة الإلكترونية.

المبحث الثاني: الآليات المتخصصة في التحقيق والإثبات في الجرائم الإلكترونية.

المبحث الأول: المتابعة القضائية في الجريمة الإلكترونية

تم تقسيم المبحث إلى مطلبين؛ المطلب الأول للاختصاص القضائي للجرائم الإلكترونية، والمطلب الثاني القضاء الدولي في الجرائم الإلكترونية.

المطلب الأول: الاختصاص القضائي للجرائم الإلكترونية

سنحاول التعرف في هذا المطلب على المبادئ التي تحكم الاختصاص القضائي للجرائم الإلكترونية من خلال الفرع الأول، وموقف لفقه منه في الفرع الثاني، لننتقل إلى موقف المشرع الجزائري من مسألة الاختصاص القضائي.

الفرع الأول: المبادئ التي تحكم الاختصاص القضائي في الجرائم الإلكترونية

يقصد بالاختصاص القضائي هو ما لكل محكمة من المحاكم من سلطة القضاء تبعا لمقرها أو لنوع القضية، وهو نوعي إذا اختص بالموضوع، ومحلي إذا اختص بالمكان[1].

وللاختصاص القضائي مبادئ يقوم عليها:

أولا: مبدأ الإقليمية

يقصد بمبدأ إقليمية القواعد الجزائية هو ذلك المبدأ الذي يعني وجوب تطبيق قانون العقوبات على جميع الجرائم التي تقع داخل النطاق الإقليمي للدولة بغض النظر عن جنسية مرتكبها أي سواء كان وطنيا أو أجنبيا، فينعقد الاختصاص القضائي الجنائي لمحاكم الدولة التي وقعت فيها الجريمة وتطبق قانونها الجنائي على المتهم[2].

---

[1] عبد الرحمن بن خالد بن عثمان السبت، **تمييز العمل التجاري وآثاره دراسة تطبيقية قضائية**، مكتبة القانون والاقتصاد، الرياض، ط1، 2013، ص55.

[2] عبد المجيد إبراهيم عبد الكريم المليقطة، **دور القضاء الجنائي الوطني في مكافحة الجريمة والحد منها لاستتباب الأمن المجتمعي**، شركة دار الأكاديميون للنشر والتوزيع، 2021، ص22.

إن أغلب التشريعات تأخذ بمبدأ إقليمية النص الجنائي للأسباب التالية[1]:

1. يعد مبدأ إقليمية تطبيق النص الجنائي مظهرا من مظاهر ممارسة الدولة لسيادتها على إقليمها، وبالتالي تطبيق قانونها على كل ما يقع عليه من أفعال رأت تجريمها، أيا كان مرتكبها أو المرتكبة عليه، وأيا كانت المصلحة المعتدى عليها وطنية أو أجنبية؛
2. مبدأ إقليمية النص الجنائي يقود إلى تطبيق قانون مكان ارتكاب الجريمة، ويقضي باختصاص المحاكم لجنائية بنظر لدعوى، وهو أنسب مكان لمحاكمة المتهم، حيث به تتوفر أدلة الإثبات، وبه غالبا ما يوجد المتهم؛
3. محاكمة المتهم في المكان الذي ارتكب فيه جريمته، وتوقيع الجزاء عليه في هذا المكان، يرسخ فكرة الردع العام الذي يسعى لتحقيقه الجزاء الجنائي؛
4. من مصلحة المتهم تطبيق قانون البلد الذي ارتكب فيه جريمته، لافتراض علمه بهذا القانون، مما يحقق أغراض مبدأ الشرعية الجنائية، ويحقق العدالة من خلال عدم مفاجئة المتهم بقوانين يجهلها.

ثانيا: المبادئ الأخرى

لم يعد مبدأ إقليمية القانون المعيار الوحيد في كل الجرائم، بل هناك مبادئ أخرى وهي كالتالي:

1. **مبدأ العينية:** يقصد بمبدأ العينية أي تطبيق النص الجنائي على كل جريمة تمس مصلحة أساسية للدولة، وذلك أيا كان مكان ارتكابها وجنسية من ارتكبها. حيث يجعل

[1] عبد المومن بن صغير، "**تطبيق النص الجنائي ين الإقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة**"، مجلة العلوم القانونية والسياسية، المجلد10، العدد03، ديسمبر 2019، ص62-63.

هذا المبدأ الضابط في تحديد سلطان النص الجنائي هو "أهمية المصلحة التي تهدرها الجريمة"، وذلك بغض النظر عن جنسية مرتكب الجريمة والإقليم الذي ارتكبت فيه[1].

2. **مبدأ الشخصية:** ويقصد به أن يطبق القانون على جميع من يحمل جنسية الدولة أينما وجد ولا يطبق على الأجانب ولو كانوا في الدولة، ويطبق المبدأ عادة في المسائل الشخصية والأهلية[2].

3. **مبدأ العالمية:** يقصد به مساءلة ومعاقبة مرتكبي الجرائم الدولية الأشد خطورة أمام القضاء الوطني، كجرائم الإبادة الجماعية والجرائم ضد الإنسانية، بغض النظر عن جنسية مرتكبيها أو حتى المكان الذي ارتكبوا فيه هذه الجرائم. ويمكن أن يعرف بأنه خضوع الشخص الأجنبي الذي يرتكب جريمة في الخارج لقانون عقوبات الدولة التي يتم القبض عليه فيها أو يوجد فوق إقليمها. يقوم على قاعدة مفادها أن لكل دولة ولاية القضاء في أية جريمة أينما تم وقوعها بغض النظر عن مدى مساسها بمصالح هذه الدولة أو عما إذا كان مرتكب الجريمة من جنية هذه الدولة أو من غير جنسيتها[3].

ومن خلال استعراض هذه المبادئ نلاحظ أنه بالإمكان تطبيقها على الجرائم الإلكترونية، لأنه يمكن تفسيرها تفسير موسع، ونلاحظ أن مبدأ الإقليمية هو الأكثر ملائمة لأن في الدولة التي تقع فيها الجريمة توجد مخلفات الجريمة.

---

[1] عبد المجيد **محمود عبد المجيد، المواجهة الجنائية للفساد في ضوء اتفاقية الأمم المتحدة والتشريع المصري ((الجوانب الإجرائية والتعاون الدولي))**، ج3، دار نهضة مصر للنشر، مصر، 2017.

[2] **مجال سريان القانون من حيث المكان**، متاح على الموقع: https://cte.univ-setif2.dz/moodle/mod/book/view.php?id=17514&chapterid=5359

[3] مؤلف جماعي، **التفجيرات النووية الفرنسية في الصحراء الجزائرية**، جامعة أحمد دراية، الجزائر، ط1، 2020، ص192-193.

الفرع الثاني: موقف الفقه من مسألة الاختصاص القضائي في الجرائم الإلكترونية

هناك تنازع فقهي حول الاختصاص القضائي في الجرائم الإلكترونية، وهناك تنازع إيجابي وتنازع سلبي. ففي حالة قيام تنازع إيجابي في الاختصاص بين أكثر من دولة لملاحقة نفس النشاط الإجرامي، أو في حالة الجرائم التي يتوزع فيها السلوك المادي للجريمة في إقليم أكثر من دولة، فهذه الظاهرة تفرض تنازعا في الاختصاص بل وغموضا في تحديد معياره. وإذا كان الأصل أن عناصر الركن المادي للجريمة تكتمل في مكان واحد، أو بالأحرى في نطاق إقليم واحد، إلا أنه في الجرائم الإلكترونية لا يمكن تحديد مكان وقوع الجريمة هل هو مكان وقوع السلوك الإجرامي أم المكان الذي تحققت فيه النتيجة. ولذلك تم إيجاد معايير جديدة لانعقاد الاختصاص القضائي تتجاوز المعايير التقليدية.

ولقد ثار جدل فقهي فيما يخص مسألة تخزين المعلومات أو البيانات المعالجة إلكترونيا خارج إقليم الدولة وهنا ظهر فريقان[1]:

الفريق الأول: يقول أنه من غير المشروع ان تقوم سلطات دولة ما بالتدخل وتفتيش النظم المعلوماتية الموجودة في إقليم دولة أخرى، بهدف كشف وضبط أدلة لإثبات جريمة كانت قد وقعت على أراضيها وذلك استنادا إلى مبدأ الإقليمية.

الفريق الثاني: يرى أنه يمكن السماح بتنفيذ هذه الإجراءات حال توافر ظروف معينة يتم تحديدها كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية.

الفرع الثالث: موقف المشرع الجزائري من مسألة الاختصاص القضائي

قام المشرع الجزائري بتمديد الاختصاص المحلي للمحكمة من خلال القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المتضمن قانون الإجراءات الجزائية ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة

[1] مريم عراب، "**الاختصاص القضائي في الجرائم المعلوماتية**"، حوليات كلية الحقوق والعلوم السياسية، المجلد07، العدد03، 2015، ص282-283.

بأنظمة لمعالجة الآلية للمعطيات. ليأتي بعد ذلك المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ليجسد فعليا بموجب المادة الأولى منه مجال اختصاص بعض المحاكم في إطار الجرائم الماسة بأنظمة المعالجة الآلية[1].

أولا: الاختصاص المحلي لوكيل الجمهورية

لقد نصت المادة 37 من قانون الإجراءات الجزائية على أنه يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، ومحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر. كما يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في الجرائم الإلكترونية[2].

ثانيا: الاختصاص المحلي لقاضي التحقيق

حسب المادة 40 من قانون الإجراءات الجزائية يتحدد اختصاص قاضي التحقيق بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر. كما أنه يجوز تمديد الاختصاص المحلي لقاضي التحقيق عن طريق التنظيم في الجرائم الإلكترونية[3].

حسب المادة 16 من قانون الإجراءات الجزائية فإن يتحدد اختصاص ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة، كما أنه يجوز لهم في حالة الاستعجال أن يباشروا مهمتهم في كافة دائرة اختصاص المجلس

[1] مريم عراب، مرجع سابق،ص284.

[2] الأمر رقم 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.

[3] الأمر رقم 155/66، مرجع سابق.

القضائي الملحقين به، ويجوز لهم أن يباشروا مهمتهم على كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونا، ويجب أن يساعدهم ضابط الشرطة القضائية الذي يمارس وظائفه في المجموعة السكنية المعنية. أما فيما يتعلق بالجرائم الإلكترونية فإن اختصاصهم يمتد إلى كامل الإقليم الوطني، تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع لحالات[1].

ثالثا: الاختصاص المحلي لجهات الحكم

نص المشرع الجزائري من خلال المادة 329 فقرة1 من الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية على أنه: "تختص محليا بالنظر في الجنحة محكمة محل الجريمة، أو محكمة محل إقامة أحد المتهمين أو شركاؤهم أو محل القبض عليهم، ولو كان هذا القبض لسبب آخر".

ولقد نصت الفقرة خمسة من نفس المادة على أنه: "يجوز تمديد الاختصاص المحلي للمحكمة إلى دائر اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود لوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف".

ومنه نلاحظ أن الفقرة الأولى حددت الاختصاص المحلي للمحاكم ذات الاختصاص المحلي الموسع، أما الفقرة الخامسة حددت مجال الاختصاص المحلي الموسع لهذه المحاكم[2].

وقد بدأت الأقطاب القضائية المتخصصة في المادة الجزائية العمل بالفعل في سنة 2008، حيث تم إعطاء إشارة الانطلاق الرسمي للأقطاب الجزائية المتخصصة في كل من

[1] الأمر رقم 155/66، مرجع سابق.

[2] نضيرة بوعزة، "**المحاكم ذات الاختصاص المحلي الموسع كآلية لمكافحة الإجرام الخطير**"، مجلة ميلاف للبحوث والدراسات، المجلد01، العدد01، 2021، ص186.

الجزائر العاصمة يوم 26 فيفري 2008، أما قسنطينة يوم 3 مارس2008، ووهران يوم 05 مارس 2008، أما ورقلة يوم 19 مارس 2008، وهذا تحت إشراف وزير العدل حافظ الأختام[1].

أما بخصوص الجريمة الإلكترونية التي تقع خارج الإقليم الجزائري فقد نص المادة 15 من القانون 09-04 على أنه: "وفضلا عن الاختصاص المنصوص عليه في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجانب وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[2].

المطلب الثاني: القضاء الدولي في الجرائم الإلكترونية

تم تقسيم المطلب إلى فرعين، جاء في الفرع الأول قواعد الاختصاص الدولي في الجرائم الإلكترونية في الاتفاقيات الدولية، أما الفرع الثاني فتم تخصيصه لقواعد الاختصاص القضائي في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

الفرع الأول: قواعد الاختصاص الدولي في الجرائم الإلكترونية في الاتفاقيات الدولية

أولا: اتفاقية بودابست

في حال ارتكاب جريمة إلكترونية عابرة للحدود تثار مشكلة تحديد جهة الاختصاص المعنية بمباشرة إجراءات المتابعة والمحاكمة في مواجهة الجناة، إذا ارتكب أجنبي جريمة إلكترونية يتواجد في إقليم الدولة (أ) يكون الاختصاص في الأصل لمحاكم الدولة (أ) وفقا لمبدأ الإقليمية، إلا انه يرجع الاختصاص لمحاكم الدولة (ب) على أساس مبدأ شخصية القانون الجنائي، وإذا كانت نتائج الجريمة حصلت في الدولة (ج) بحيث تكون مهددة لأمن

[1] محمد بكرارشوش، "**الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري**"، دفاتر السياسة والقانون، العدد 14، جانفي 2016، ص307.

[2] القانون 09-04، مرجع سابق.

وسلامة الدولة (ج) فتدخل في اختصاصها وفقا لمبدأ العينية. وتقتضي المواثيق الدولية أن الاختصاص في الجرائم الإلكترونية يعود إلى الدولة التي ارتكبت فيها الجريمة كليا أو جزئي أو تحققت فيها الجريمة سواء كان ذلك في إقليم الدولة الطرف، أو على متن سفينة تحمل علم الدولة الطرف أو ارتكبت من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأي دولة[1].

ولقد نصت المادة 22 من اتفاقية بودابست على ما يلي:

– يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير اخرى وذلك لإقرار الاختصاص بشأن أي جريمة تنص عليها المواد من 2 غلى 11 من هذه الاتفاقية عندما ترتكب الجريمة: (في إقليمه، على متن إحدى السفن ترفع علم ذلك الطرف، على متن إحدى الطائرات المسجلة بموجب قوانين ذلك الطرف، من جانب أحد مواطنيه، إذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي بمكان ارتكابها، أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأية دولة).

– يجوز لكل طرف الاحتفاظ بالحق في عدم تطبيق، أو التطبيق فقط في حالات أو بشروط معينة قواعد الاختصاص القضائي المنصوص عليها في الفقرات من (ب–د).

– يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإقرار الاختصاص القضائي بشأن الجرائم المشار إليها في المادة (2/24) من هذه الاتفاقية، وفي الحالات التي يكون فيها الجاني المزعوم موجودا في إقليمه، ولا يقوم بتسليمه أو تسليمها لطرف آخر على سند من جنسيته أو جنسيتها، وذلك بعد طلب التسليم.

[1] جمال زين العابدين أمين أحمد، "**الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية "دراسة مقارنة""**، مجلة مستقبل العلوم الاجتماعية، العدد04، يناير 2021، ص87.

– لا تستبعد هذه الاتفاقية أي اختصاص جنائي يمارسه أحد الأطراف وفقا لقانونه الوطني.

– في حالة مطالبة أكثر من طرف من الأطراف بالاختصاص القضائي بشأن جريمة ما تقرها هذه الاتفاقية، يقوم الأطراف المعنيون، متى كان ذلك ملائما بالتشاور بغرض تحديد الاختصاص القضائي الأكثر ملائمة للمحاكمة[1].

الفرع الثاني: قواعد الاختصاص القضائي في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

لقد نصت المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أنه[2]:

1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت:

أ. في إقليم الدولة الطرف.

ب. على متن سفينة تحمل علم الدولة الطرف.

ت. على متن طائرة مسجلة تحت اسم قوانين الدولة الطرف.

ث. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (1) من هذه الاتفاقية في الحالات

[1] جمال زين العابدين أمين أحمد، مرجع سابق، ص87–88.

[2] **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، متاح على الموقع: https://www.courts.gov.ps/userfiles/file/

التي يكون فيها الجاني المزعوم حاضرات في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

3. إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم.

المبحث الثاني: الآليات المتخصصة في التحقيق والإثبات في الجرائم الإلكترونية

سيتم تقسيم هذا المبحث إلى مطلبين، حيث تم تخصيص المطلب الأول إلى الأساليب المتخصصة في التحقيق في الجرائم الإلكترونية، أما المطلب الثاني فهو مخصص للأساليب المتخصصة في الإثبات في الجرائم الإلكترونية.

المطلب الأول: الآليات المتخصصة في التحقيق في الجرائم الإلكترونية

يعرف التحقيق في الجرائم الإلكترونية على أنه عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجريمة الإلكترونية من فاعل لها ودليل إلكتروني لتقديمهم إلى سلطات التحقيق القضائي المتخصصة في هذا النوع من الجرائم لإقامة العدل[1].

إن التحقيق الإلكتروني يتميز بعدد من الخصائص تتمثل في[2]:

1. **السرية:** وهي عدم الاطلاع الغير على مجريات التحقيق وفقا لما نصت عليها المادة 11 من قانون الإجراءات الجزائية؛
2. **التدوين:** تدون جميع إجراءات التحقيق في محاضر ويصادق عليها في محضر رسمي حتى تكون حجة في الإثبات؛
3. **وضع خطة للتحقيق:** بحيث تبدأ مهمة المحق بجمع الاستدلالات، وفي الجريمة الإلكترونية يساعد المحقق في أعمال التحقيق فريق فني مؤهل.

وتم تقسيم هذا المطلب إلى فرعين، الفرع الأول خاص بالأجهزة المكلفة بالتحقيق في الجرائم الإلكترونية، أما الفرع الثاني يتم التطرق إلى الوسائل المستخدمة في التحقيق أما الفرع الثالث فيخص التفتيش في الجرائم الإلكترونية.

---

[1] مصطفى محمد موسى، **التحقيق الجنائي في الجرائم الإلكترونية**، مطابع الشرطة، القاهرة، ط1، 2009، ص169.

[2] عبد القادر فلاح، آيت عبد المالك، "**التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري**"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد4، العدد02، 2019، ص1695.

الفرع الأول: الأجهزة المكلفة بالتحقيق في الجرائم الإلكترونية

تتمثل في:

أولا: جهاز الضبطية القضائية

إن الشرطة القضائية موظفون منحهم القانون صفة الضبطية القضائية وخولهم بموجبها حقوق وفرض واجبات عليهم في إطار البحث عن الجرائم ومرتكبيها وجمع الاستدلالات عنها، يبدأ دورهم بعد وقوع الجريمة وينتهي عند فتح التحقيق القضائي أو إحالة المتهم إلى جهة الحكم[1].

لقد حرص المشرع الجزائري للتصدي للجرائم الإلكترونية حيث قام بتوسيع صلاحيات الضبطية القضائية العادية إلى منح هذه الأخيرة صلاحية حديثة وذلك بإمكانية استعانته بوضع آليات تقنية للكشف بسرعة عن هذه الجرائم وملاحقة مرتكبيها[2].

ثانيا: دور مقدمي الخدمات في التحري والتحقيق في الجرائم الإلكترونية

يعرف مقدمي الخدمات في القانون 09-04 على أنهم:

1. أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.
2. وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها[3].

---

[1] عز الدين عثماني، مرجع سابق، ص53.

[2] نبيل بن عودة، محمد نوار، "**الصلاحيات الحديثة للضبطية القضائية للكشف وملاحظة مرتكبي الجرائم المتعلقة بالتمييز وخطاب الكراهية، "التسرب الإلكتروني نموذجا""**، مجلة الأكاديمية للبحوث في العلوم الاجتماعية، المجلد01، العدد02، 2020، ص328.

[3] القانون 09-04، مرجع سابق.

تتمثل مهام مقدمي الخدمات في التحري والتحقيق في الجرائم الإلكترونية فيما يلي:

أولا: مساعدة السلطات

وفقا للمادة 10 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فإن مزود الخدمات يلتزم بما يلي:

– تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات بمحتوى الاتصالات في حينها، بحيث أنه لمّا كان مزود الخدمة بإمكانه مراقبة ومعرفة جميع الخطوات التي يتبعها المستخدم إذ يتاح له معرفة المواقع التي زارها والمعلومات التي خزنها وكل الاتصالات التي أجراها، ومن ثم فإنه ملزم بتمكين جهات التحقيق من كل المعلومات التي تبحث عنها، وذلك بتجميعها أو تسجيلها.

– وضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من ذات القانون تحت تصرف السلطات المكلفة بالتحريات القضائية.

– الحفاظ على السرية، إذ يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها[1].

ثانيا: حفظ المعطيات المتعلقة بحركة السير

لقد نصت المادة 11 من القانون 09-04 على أن يلتزم مقدمو الخدمات بحفظ:

أ- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ب- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

[1] إلهام بن خليفة، مرجع سابق، ص12.

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه[1].

ثالثا: التزامات خاصة بمقدمي خدمة الإنترنت

حسب المادة 12 من نفس القانون يتعين على مقدمي خدمات الإنترنت على:

أ- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.[2]

الفرع الثاني: الوسائل المستخدمة في التحقيق في الجرائم الإلكترونية

يعتمد المحقق للكشف عن الجرائم الإلكترونية إلى الوسائل التالية:

أولا: الوسائل المادية

تتمثل في الأدوات الفنية التي تستخدم في بنية نظم المعلومات والتي يمكن باستعمالها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها[3]:

[1] القانون 09-04، مرجع سابق.

[2] القانون 09-04، مرجع سابق.

[3] عز الدين عثماني، "**إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية**"، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد04ن جانفي 2018، ص54-55.

- ✓ البروكسي: وسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة؛
- ✓ عناوين IP، البريد الإلكتروني، برامج المحادثة؛
- ✓ برامج التتبع: حيث تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP الذي تمت من خلاله عملية الاختراق، اسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترع، أرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى؛
- ✓ أنظمة كشف الاختراق IDS: تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبة الإلكترونية أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسبة الإلكترونية أو الشبكة؛
- ✓ أدوات تدقيق ومراجعة العمليات الحاسوبية؛
- ✓ أدوات فحص ومراقبة الشبكات: تستخدم في فحص بروتوكول ما وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدواتَ ARP وظيفتها تحديد مكان الحاسبة الإلكترونية فيزيائيا على الشبكة.

ثانيا: الوسائل الإجرائية

تتمثل في[1]:

- ✓ إتباع الأثر: حيث يمكن تقصي الأثر بطرق عدة سواء عن طريق البريد الإلكتروني تم استقباله، أو تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق؛
- ✓ الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته؛

[1] عز الدين عثماني، مرجع سابق، ص55.

- ✓ مراقبة الاتصالات الإلكترونية: إن المشرع الجزائري لم يعرف عملية مراقبة الاتصالات الإلكترونية؛
- ✓ الاستعانة بالذكاء الاصطناعي، وهذا من خلال استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الإلكترونية، وفق برامج صممت خصيصا لهذا الغرض.

الفرع الثالث: التفتيش في الجرائم الإلكترونية

يعرف التفتيش بأنه: "إجراء من إجراءات التحقيق الابتدائي التي تهدف إلى البحث عن الأدلة المادية الجنائية سواء لجناية أو جنحة تتحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقط لإجراءات قانونية محددة"[1].

وهناك من يعرف التفتيش بأنه إجراء من إجراءات التحقيق يقوم به موظف مختص، طبقا للإجراءات المقررة قانوني، في محل يتمتع بحرمته، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها، لإثبات ارتكابها ونسبها إلى المتهم، وقد أحاط إجراء التفتيش نظرا لمساسه بالحريات الخاصة للأفراد بضمانات عديدة[2].

إن التفتيش في الجرائم الإلكترونية يتمتع بمجموعة من السمات تتمثل في[3]:

- ✓ مثله مثل التفتيش بشكل عام، فيه تعرض قانوني لحرية المتهم الشخصية أو لحرمة مسكنه بغير إرادته ورغما عنه، وفيه اعتداء على أسراره وعلى حياته؛
- ✓ من وسائل التحري عن مختلف الأدلة المعنوية والمادية للجريمة، يهدف إلى جمع الأدلة من أجل الكشف عن الحقيقة وضبطها؛

---

[1] عادل عبد الله خميس المعمري، "**التفتيش في الجرائم المعلوماتية**"، مجلة الفكر الشرطي، مركز بحوث الشرطة، الإمارات، المجلد22، العدد86، 2013، ص259.

[2] عوض محمد عوض، **قانون الإجراءات الجنائية**، ج1، مؤسسة الثقافة الجامعية، 1989، ص475.

[3] رضا هميسي، "**تفتيش المنظومات المعلوماتية في القانون الجزائري**"، مجلة العلوم القانونية والسياسية، العدد05، جوان 2012، ص162-163.

- ✓ يعتبر قيدا على حرمة وحصانة الشخص وفيه مساس بحق الشخص في السر، فهو اعتداء على أسراره سواء الموجودة على مستوى نظامه المعلوماتي أو جهاز حاسوبه أو حتى بريده الإلكتروني وفيه مساس لحرمة الشخص في ذاته أو في رسائله؛
- ✓ يسمح التفتيش أو البحث في الشبكات الإلكترونية عن الجرائم الإلكترونية، باستخدام قواعد وأساليب التحقيق الجنائي الفني المعروفة، بتقنيات خاصة، فريدة أو غير مسبوقة؛
- ✓ يتميز التفتيش الإلكتروني بالطابع اللامادي وتجاوزه الحدود الوطنية والفورية وسهولة إتلافه أو مسحه أو تغييره في أوقات قياسية؛
- ✓ التفتيش الإلكتروني عملية معقدة ومتشابكة، فيجب على القائمين بها أن يكونوا على دراية وكفاءة عالية في البحث عن المعلومة، وفي معالجة المعطيات وتحليلها وفك طلاسمها؛
- ✓ فيه مساس بالحياة الخاصة، كونه يتضمن وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وفيه تجميع آني وفوري لهذه الاتصالات، وكذا القيام بعمليات التفتيش والحجز داخل المنظومات المعلوماتية.

إذا كانت الجريمة واقعة على المكونات المادية للكمبيوتر، فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش، أما إذا وقت الجريمة على بيانات الكمبيوتر، هنا تظهر العراقيل على اعتبار أن بإمكان الجاني التخلص من البيانات التي يستهدفها التفتيش عبر إرسالها من خلال نظام معلوماتي من مكان إلى آخر، أو إلى نظام معلوماتي آخر، يستوجب التفتيش عن هذه البيانات الكشف عن الرقم السري للمرور إلى ملفات البيانات، وهذا الرقم السري يعرفه المتهم، ولا يمكن إجباره على البوح به أو الإفصاح عنه[1].

[1] خالد ممدوح إبراهيم، **الإثبات الإلكتروني في المواد الجنائية والمدنية**، دار الفكر الجامعي، الإسكندرية، ط1، 2020، ص121.

لهذا لا يجب أن يكون الإذن بالتفتيش محددا بمكان معين، بل يجب أن يمتد إلى تفتيش أي نظام آلي موجود في مكان آخر بهدف التوصل إلى بيانات يمكن أن تفيد بشكل معقول في كشف الحقيقة، شرط عدم انتهاك سيادة دولة أخرى، وأن يحل قاضي التحقيق محل الشخص صاحب المكان المراد تفتيشه بصورة مؤقتة، ويجب أيضا الإجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات[1].

وتتمثل شروط التفتيش في الجرائم الإلكترونية في:

أولا: الشروط الشكلية وهي كالآتي:[2]

1. **وقت إجراء التفتيش:** عندما يتعلق الأمر بأنظمة المعالجة الآلية للمعطيات فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل من ساعة من ساعات النهار أو الليل وهذا بناء على إذن مسبق من وكيل الجمهورية المختص.
2. **حضور الأشخاص المعنيين أثناء التفتيش:** اشترط المشرع الجزائري تفتيش المنازل في حضور المتهم، وفي حالة إذا ما تعذر عليه الحضور وقت الإجراء، كان على ضابط الشرطة القضائية أن يكلفه بتعيين ممثل له وإذا امتنع عن ذلك أو كان هاربا كان من الواجب أن ينوبه عنه شاهدين غير الموظفين الخاضعين له.
3. **محضر التفتيش** في الجرائم الماسة بالمعطيات الآلية: تسمى محاضر الشرطة القضائية محاضر البحث الابتدائي وتكمن أهميتها في قيمتها الممنوحة لها كوسيلة إثبات على وقوع الجريمة ونسبتها إلى فاعلها من جهة، ومن خطورة الصلاحيات الواسعة الممنوحة بموجبها لضابط الشرطة القضائية.

---

[1] خالد ممدوح إبراهيم، مرجع سابق، ص122.

[2] عز الدين عثماني، "**إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية**"، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد04، جانفي 2018، ص57-58.

ثانيا: الشروط الموضوعية: وتتمثل في[1]:

1. **سبب التفتيش:** ارتكاب الجريمة المعلوماتية بشكل عام.
2. **محل التفتيش:** محل التفتيش بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها على العالم.
3. **السلطة الخاصة بالقيام بالتفتيش:** تتمثل الجهة القضائية التي تم إسنادها مهمة التفتيش في قاضي التحقيق أو النيابة العامة باختلاف التشريعات كسلطة أصلية، أو استثناء في رجال الضبط القضائي. وفي حالة وقوع جريمة من نوع الجنايات أو الجنح ولم يكن قاضي التحقيق المختص موجودا فإن على المسؤول عن التحقيق عندما تقتضي الضرورة إصدار قرار أو إجراء فوري في التحقيق عرض الأمر على أي قاضي في منطقة اختصاص قاضي التحقيق أو أي منطقة قريبة لاتخاذ ما يلزم على أن تعرض الأوراق على قاضي التحقيق المختص في أقرب وقت.

المطلب الثاني: الآليات المتخصصة في الإثبات في الجرائم الإلكترونية

من الوسائل المتخصصة في إثبات الجرائم الإلكترونية تتمثل في المعاينة، الاستجواب، الشهادة، وضبط الأدلة. وهذا ما سنتطرق إليه في هذا المطلب.

الفرع الأول: المعاينة في الجريمة الإلكترونية

يقصد بالمعاينة الفحص الفني الشامل والدقيق لمكان وقوع الجريمة ووصفه وصفا شاملا دقيقا، كما كان عند ما تركه الجاني[2]. يجب أن تتوفر في صفات المحقق الكفاءة العالية والخبرة العملية والمهارة والذكاء.

[1] عز الدين عثماني، مرجع سابق، ص58-59.

[2] محمد نور خالد الدباس، **دليل المحقق في أصول التحقيق**، دار يافا العلمية للنشر والتوزيع، 2023، ص41.

هناك من يرى أن المعاينة في الجريمة المعلوماتية تقل أهمية وهذا يرجع إلى ندرة الآثار المادية في الجريمة الإلكترونية، بالإضافة إلى طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار، فعند تلقي بلاغ عن وقوع إحدى الجرائم الإلكترونية وهذا بعد التأكد من البيانات اللازمة في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته[1].

يجب على قاضي التحقيق قبل الانتقال إلى معاينة مسرح الجريمة المعلوماتي إتباع الخطوات التالية[2]:

- ✓ الدراية المسبقة عن مكان الجريمة، مالك المكان، نوع وعدة أجهزة الحاسب الآلي؛
- ✓ قطع التيار الكهربائي عن موقع المعاينة وهذا من أجل شل فعالية الجاني من لقيام بأي فعل من شأنه التأثير على محو آثار الجريمة؛
- ✓ الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل؛
- ✓ إعداد فريق بحث من المختصين والفنيين.

[1] فاطمة الزهراء بخي، "**إجراءات التحقيق في الجريمة الإلكترونية**"، مذكرة ماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2014/2013، ص86.

[2] ابتسام بغو، "**إجراءات المتابعة الجزائية في الجريمة المعلوماتية**"، مذكرة ماستر في القانون، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي، 2016/2015، ص64.

الفرع الثاني: الاستجواب والخبرة في الجرائم الإلكترونية

أولا: الاستجواب

يعرف الاستجواب بأنه إجراء من إجراءات التحقيق، يثبت المحقق بموجبه من شخصية المتهم، ويناقشه في التهمة المنسوبة إليه، على الوجه المفصل في الأدلة القائمة في الدعوى إثباتا أو نفيا[1].

إن الضوابط المقررة للاستجواب في الجريمة الإلكترونية نفسها المقررة في الجرائم العادية، إلا ان الفرق يتمثل في ضرورة تأهيل السلطة المختصة التي تتولى إجراءات الاستجواب، ذلك أن جهات التحقيق لا بد أن تكون مؤهلة للتحقيق في الجرائم الإلكترونية، حتى يمكن استيعاب واقعة التحقيق والتعامل مع مفردات الجريمة، خاصة وأن المجرم ليس مجرما عادي[2].

ثانيا: الخبرة

إن الخبرة من أهم الإجراءات التي ينبغي الاهتمام بها في إطار التحقيق في الجرائم الإلكترونية، وذلك راجع إلى صعوبة التعامل مع هذا النوع من الجرائم وعدم الدراية بمجالاتها التقنية والفنية.

إن عمليات التحقيق في الجرائم الإلكترونية يستوجب الاستعانة بالخبرات المتعددة والمتنوعة، وهذا بالاعتماد على الخبراء والارتكاز على نوعية الأساليب المستخدمة في الارتكاب (التلاعب بالبيانات، التلاعب في نقل وبث البيانات، التلاعب في البرامج الأساسية أو برامج التطبيقات، تزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة بعد

[1] سامية دايخ، "**ضمانات المتهم أثناء الاستجواب أمام قاضي التحقيق في ظل قانون الإجراءات الجزائية الجزائري**"، مجلة العلوم الإنسانية، المجلد06، العدد01، 2016، ص292.

[2] وهيبة رابح، "**الجريمة المعلوماتية في التشريع الإجرائي الجزائري**"، مجلة الباحث للدراسات الأكاديمية، العدد04، ديسمبر 2014، ص328.

المعالجة). ويتعين على الخبير في الجرائم المرتكبة عبر الإنترنت التنسيق مع المحقق الجنائي في هذه الجريمة، بما في ذلك حصر الأدلة المتوفرة وترتيبها وفاق لأهمية كل دليل أو بيئة أو قرينة، كما يجب على المحقق الجنائي أن يشرح للخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة المقام عنها الدعوى الجنائية ضد المتهم[1].

الفرع الثالث: الشهادة في الجرائم الإلكترونية

يقصد بالشهادة في الجرائم الإلكترونية الشخص الفني صاحب الخبرة العالية في علوم الحاسب الآلي وصاحب التخصص الذي لديه العلم والدراية عن ماذا يدلي بوقائع شهادته، والذي يكون لديه معلومات جوهرية هامة أو لازمة للدخول إلى نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي ذلك للتنقيب عن أدلة الجريمة الإلكترونية[2].

أما الشاهد الإلكتروني يندرج في طوائف عديدة منها[3]:

1. مشغلو الحاسب الآلي: هو الشخص المسؤول عن تشغيل جهاز الحاسب الآلي ومكوناته، يتمتع بالخبرة الكافية ، حيث ينقل البيانات من الوثائق إلى وسائط التخزين التي تجري معالجتها بواسطة الحاسب الآلي؛
2. خبراء البرمجة: يتمثلون في مخططو برامج التطبيقات ومخططو برامج النظم؛
3. المحللون: حيث يقوم المحلل بدراسة البيانات وتحليل النظام، وتقسيمه إلى وحدات واستنتاج العلاقة الوظيفية بين هذه الوحدات؛

[1] وهيبة رابح، المرجع نفسه، ص328-329.

[2] أدهم باسم نمر بغدادي، "**وسائل البحث والتحري عن الجرائم الإلكترونية**"، أطروحة ماجستير في القانون العام، كلية الدراسات العليا في جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص63.

[3] نداء نائل فايز المصري، "**خصوصية الجرائم المعلوماتية**"، أطروحة ماجستير في القانون العام، كلية الدراسات العليا في جامعة النجاح الوطنية ، نابلس، فلسطين، 2017، ص63.

4. مهندسو الصيانة والاتصالات: هم المسؤولون عن أعمال الصيانة المتعلقة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به؛
5. مديرو النظام: هم الذين يوكل إليهم أعمال الإدارة في النظم المعلوماتية.

الفرع الرابع: ضبط الأدلة الإلكترونية

هناك من يعرف الدليل الإلكتروني على أنه: "المعلومات أو البيانات المخزنة في الحاسوب أو المتنقلة عبر شبكات الاتصال، والتي يمكن استخدامها في إثبات أو نفي جريمة ما"[1].

وهناك تعريف آخر للدليل الإلكتروني على أنه: "الشيء أو الوسيلة (مجموعة من النبضات المغناطيسية) المستمد من أحد النظم المعلوماتية أو من أحد الأجهزة الإلكترونية أو شبكات الاتصال، لإثبات حق مدعي به أمام القضاء أو لنفيه"[2].

ولقد عرفت المنظمة العالمية لدليل الكمبيوتر IOCE في 2001 بأنه: "المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة كمبيوتر[3].

ويقصد بضبط الأدلة الإلكترونية وضع اليد على كل ما له علاقة بالجريمة الإلكترونية، مثل ضبط المكونات المعنوية والبرمجيات،ضبط المعطيات التي يرجي تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب معا وما يتصل فيها. والضبط لا يهد من إجراءات التحقيق بل هو الاستدلال الذي يترتب عن التفتيش الذي يعد الأصل في إجراءات

[1] عادل بن عبد العزيز بن صالح الرشيد، **قرائن الجريمة الإلكترونية وأثرها في الإثبات**، دار كنوز إشبيليا للنشر والتوزيع، الرياض، ط1، 2017، ص70.

[2] طارق عفيفي صادق أحمد، **نظرية الحق**، المركز القومي، ط1، 2016، ص309-310.

[3] محمد كمال، **الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلا من القنبلة**، دار كليم للطباعة والنشر، 2022، ص75.

التحقيق. وقد ينصب على مراقبة المحادثات الهاتفية وتسجيلها، وعلى كل ما هو مخزن في أجهزة الحاسوب أو أقراص أو أي دعامة أخرى[1].

[1] فاطيمة فايد، "**التحقيق الجنائي في الجرائم الإلكترونية**"، مذكرة ماستر في قانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، 2021/2020، ص47.

خلاصة الفصل:

إن الجرائم الإلكترونية تتميز بطبيعة خاصة عن الجرائم التقليدية، حيث ظهر هناك تنازع في الاختصاص القضائي بالنسبة للجرائم الإلكترونية سواء على المستوى المحلي أو المستوى الدولي، وهي تخضع لمبدأ الإقليمية تارة، ومبدأ العينية والعالمية والشخصية تارة أخرى. ولهذا نجد العديد من الدول إلى تعزيز تعاونها من أجل مكافحة هذه الجرائم وإبرام اتفاقيات دولية مثل اتفاقية بوداست، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات..

ولقد حدد المشرع الجزائري أساليب متخصصة في التحقيق من إبراز دور الضبطية القضائية ومقدمي الخدمات التحقيق في الجرائم الإلكترونية واستعمال كل الأساليب المادية والإجرائية أثناء عملية التفتيش في مسرح الجريمة الإلكترونية، بالإضافة إلى أساليب الإثبات والتي تتمثل في كل من المعاينة، الشهادة، الخبرة، وضبط الأدلة الإلكترونية.

خاتمـــــة

وبناء على ما سبق نستنتج أن الجريمة الإلكترونية من الجرائم المستحدثة الناعمة، تستخدم الوسائل التقنية في ارتكابها، وهي ذات طبيعة عالمية أي أنها تخترق الحدود الإقليمية للدول. كما أن الجرائم الإلكترونية لا تقتصر على الأفراد والمجموعات بل تمتد إلى مستوى الدول لتشمل التجسس الإلكتروني والسرقة المالية.

نتائج الدراسة:

- تتميز الجريمة الإلكترونية بأنها لا تخضع للرقابة الأمنية وهذا ما أدى إلى انتشارها وتوسعها؛

- الأضرار الجسيمة التي تلحق بالضحية؛

- صعوبة لكشف عنها إلا عن طريق الأساليب المستحدثة؛

- جريمة ناعمة لا تستخدم الجهد العضلي والمالي؛

- سهولة إخفاء الدليل الإلكتروني وإتلافه؛

- تخضع الجريمة الإلكترونية من ناحية الاختصاص القضائي لمبدأ الإقليمية، ومبدأ الشخصية والعينية والعالمية في تطبيق القانون؛

- من الأساليب التي حث عليها المشرع الجزائري في التحقيق والإثبات في الجرائم الإلكترونية: التفتيش الإلكتروني، رصد الدليل الإلكتروني، الشهادة الإلكترونية، الخبرة، المعاينة..إلخ.

- من الأجهزة المكلفة بالتحقيق في الجريمة الإلكترونية في القانون الجزائري: جهاز الضبطية القضائية، مقدمي الخدمات في التحري والتحقيق في الجرائم الإلكترونية.

التوصيات:

- العمل على الاهتمام بالموارد البشرية المختصة في مكافحة الجرائم الإلكترونية؛

- ضرورة توحيد القوانين الوطنية في مجال الاختصاص القضائي لمكافحة الجريمة الإلكترونية، ما تتضمنه الاتفاقيات الدولية في هذا المجال.

- المزيد من التشريعات الجزائرية التي تهتم بالجرائم الإلكترونية.

قائمة المصادر والمراجع

أولا: القوانين

1. الأمر رقم 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.
2. القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 1966/06/08، المتضمن قانون العقوبات، الجريدة الرسمية الجزائرية، العدد71 بتاريخ 2004/11/10..
3. القانون رقم09-04، الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47.

ثانيا: الكتب

1. ابن منظور، **لسان العرب**، ج7.
2. خالد ممدوح إبراهيم، **الإثبات الإلكتروني في المواد الجنائية والمدنية**، دار الفكر الجامعي، الإسكندرية، ط1، 2020.
3. رفد عيادة الهاشمي، **الإرهاب الإلكتروني**، دار أمجد للنشر والتوزيع، ط1، 2019.
4. طارق عفيفي صادق أحمد، **نظرية الحق**، المركز القومي، ط1، 2016.
5. عادل بن عبد العزيز بن صالح الرشيد، "**قرائن الجريمة الإلكترونية وأثرها في الإثبات**، دار كنوز إشبيليا للنشر والتوزيع، 2017.
6. عادل بن عبد العزيز بن صالح الرشيد، **قرائن الجريمة الإلكترونية وأثرها في الإثبات**، دار كنوز إشبيليا للنشر والتوزيع، الرياض، ط1، 2017.
7. عبد الرحمن بن خالد بن عثمان السبت، **تمييز العمل التجاري وآثاره دراسة تطبيقية قضائية**، مكتبة القانون والاقتصاد، الرياض، ط1، 2013.
8. عبد الصبور عبد القوي علي مصري، **التنظيم القانوني للتجارة الإلكترونية**، مكتبة القانون والاقتصاد، الرياض، 2012.

9. عبد العالي الديربي، محمد صادق إسماعيل، **الجرائم الإلكترونية دراسة قانونية قضائية مقارنة**، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012.

10. عبد المجيد إبراهيم عبد الكريم المليقطة، **دور القضاء الجنائي الوطني في مكافحة الجريمة والحد منها لاستتباب الأمن المجتمعي**، شركة دار الأكاديميون للنشر والتوزيع، 2021.

11. عوض محمد عوض، **قانون الإجراءات الجنائية**، ج1، مؤسسة الثقافة الجامعية، 1989.

12. غادة نصار، **الإرهاب والجريمة الإلكترونية**، العربي للنشر والتوزيع، ط1، 2017.

13. مجمع البحوث والدراسات، **الجريمة الإلكترونية في المجتمع الخليجي وككيفية مواجهتها**، مجلس التعاون لدول الخليج العربية، 2016.

14. محمد كمال، **الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلا من القنبلة**، دار كليم للطباعة والنشر، 2022.

15. محمد مدين، **فن التحقيق والإثبات في الجرائم الإلكترونية**، المصرية للنشر والتوزيع، ط1، 2020..

16. محمد نور خالد الدباس، **دليل المحقق في أصول التحقيق**، دار يافا العلمية للنشر والتوزيع، 2023.

17. محمود مدين، **الجريمة الإلكترونية وتحديات الأمن القومي**، المصرية للنشر والتوزيع، ط2، 2019..

18. مصطفى محمد موسى، **التحقيق الجنائي في الجرائم الإلكترونية**، مطابع الشرطة، القاهرة، ط1، 2009.

19. مؤلف جماعي، **التفجيرات النووية الفرنسية في الصحراء الجزائرية**، جامعة أحمد دراية، الجزائر، ط1، 2020.

20. ميرفت محمد حبابية، **مكافحة الجريمة الإلكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني**، دار اليازوري العلمية، عمان، الأردن، 2022.

ثالثا: المقالات

1. ابتسام مناع، "**جريمة الاعتداء الإلكتروني على الحياة الخاصة في التشريع الجزائري**"، **مجلة الشريعة والاقتصاد**، المجلد08، العدد01، جوان2019.

2. أسمهان بن مالك، "**خصائص الجريمة المعلوماتية وأسباب ارتكابها**"، مجلة البيات للدراسات القانونية والسياسية، المجلد04، العدد01، 2019.

3. أمال بوخنوش، " **مصطلح "الجريمة" في قانون العقوبات الجزائري بين الصيغة والمفهوم _دراسة لغوية_**"، مجلة الحكمة للدراسات الإسلامية، المجلد08، العدد01، 2021..

4. جمال زين العابدين أمين أحمد، "**الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية "دراسة مقارنة""**، مجلة مستقبل العلوم الاجتماعية، العدد04، يناير 2021.

5. حفيظ بن قربة، "**جريمة الدخول غير المصرح به إلى منظومة معلوماتية في التشريع الجزائري**"، مجلة القانون والعلوم السياسية، المجلد03، العدد02، 2017.

6. رضا هميسي، "**تفتيش المنظومات المعلوماتية في القانون الجزائري**"، مجلة العلوم القانونية والسياسية، العدد05، جوان 2012.

7. رمزي حوحو، منيرة بلورغي، "**مواجهة الجريمة المعلوماتية في الجزائر**"، مجلة الحقوق والحريات، العدد02، 2014.

8. سامية دايخ، "**ضمانات المتهم أثناء الاستجواب أمام قاضي التحقيق في ظل قانون الإجراءات الجزائية الجزائري**"، مجلة العلوم الإنسانية، المجلد06، العدد01، 2016.

9. سامية عزيز، مازيا عيساوي، "**الجريمة من منظور سوسيولوجي _الأسباب والآثار_**"، مجلة دراسات في سيكولوجية الانحراف، المجلد06، العدد01، 2021.

10. عادل عبد الله خميس المعمري، "**التفتيش في الجرائم المعلوماتية**"، مجلة الفكر الشرطي، مركز بحوث الشرطة، الإمارات، المجلد22، العدد86، 2013.

11. عبد القادر فلاح، آيت عبد المالك، "**التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري**"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد4، العدد02، 2019.

12. عبد المومن بن صغير، "**تطبيق النص الجنائي ين الإقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة**"، مجلة العلوم القانونية والسياسية، المجلد10، العدد03، ديسمبر 2019.

13. عز الدين عثماني، "**إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية**"، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد04ن جانفي 2018.

14. عز الدين عثماني، "**إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية**"، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد04، جانفي 2018.

15. فضيلة عاقلي، "**حماية حقوق الملكية الفكرية والصناعية من الجريمة المعلوماتية**"، مجلة الاقتصاد الصناعي، المجلد7، العدد2، 2017.

16. محمد بكرارشوش، "**الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري**"، دفاتر السياسة والقانون، العدد 14، جانفي 2016.

17. محمد خليفة، "**خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها**"، دراسات وأبحاث، المجلد01، العدد01، 2009.

18. محمد رحموني، "**خصائص الجريمة الإلكترونية ومجالات استخدامها**"، مجلة الحقيقة، العدد41، 2018.

19. مخلد إبراهيم الزعبي، "**فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية" "دراسة قانونية""**، المجلة العربية للنشر العلمي، العدد73، تشرين الثاني 2021.

20. مريم عراب، "**الاختصاص القضائي في الجرائم المعلوماتية**"، حوليات كلية الحقوق والعلوم السياسية، المجلد07، العدد03، 2015.

21. نبيل بن عودة، محمد نوار، "**الصلاحيات الحديثة للضبطية القضائية للكشف وملاحظة مرتكبي الجرائم المتعلقة بالتمييز وخطاب الكراهية، "التسرب الإلكتروني نموذجا""**، مجلة الأكاديمية للبحوث في العلوم الاجتماعية، المجلد01، العدد02، 2020.

22. نسمة بطيحي، "**جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي**"، مجلة الفقه القانوني والسياسي، المجلد01، العدد01، 2019.

23. نضيرة بوعزة، "**المحاكم ذات الاختصاص المحلي الموسع كآلية لمكافحة الإجرام الخطير**"، مجلة ميلاف للبحوث والدراسات، المجلد01، العدد01، 2021.

24. وهيبة رابح، "**الجريمة المعلوماتية في التشريع الإجرائي الجزائري**"، مجلة الباحث للدراسات الأكاديمية، العدد04، ديسمبر 2014.

ثالثا: المذكرات والرسائل الجامعية

1. ابتسام بغو، "**إجراءات المتابعة الجزائية في الجريمة المعلوماتية**"، مذكرة ماستر في القانون، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي، 2016/2015..

2. إبراهيم محمد بن حمود الزنداني، **إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات وأحكامها في القانون اليمني والكويتي والقطري: دراسة شرعية وقانونية مقارنة**، جامعة قطاني، 2019.

3. أدهم باسم نمر بغدادي، "**وسائل البحث والتحري عن الجرائم الإلكترونية**"، أطروحة ماجستير في القانون العام، كلية الدراسات العليا في جامعة النجاح الوطنية، نابلس، فلسطين، 2018.

4. إسماعيل بن يحي، "**التحقيق الجنائي في الجرائم الإلكترونية**"، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2020-2021.

5. سفيان سوير، "**جرائم المعلوماتية**"، مذكرة شهادة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2011/2010.

6. عائشة نايري، "**الجريمة الإلكترونية في التشريع الجزائري**"، مذكرة ماستر في القانون الإداري، دامعة أحمد دراية أدرار، 2017/2016.

7. فاطمة الزهراء بخي، "**إجراءات التحقيق في الجريمة الإلكترونية**"، مذكرة ماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2014/2013.

8. فاطيمة فايد، "**التحقيق الجنائي في الجرائم الإلكترونية**"، مذكرة ماستر في قانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، 2021/2020.

9. نداء نائل فايز المصري، "**خصوصية الجرائم المعلوماتية**"، أطروحة ماجستير في القانون العام، كلية الدراسات العليا في جامعة النجاح الوطنية ، نابلس، فلسطين، 2017.

خامسا: المواقع الإلكترونية

1. **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، متاح على الموقع:
https://www.courts.gov.ps/userfiles/file/
2. **مجال سريان القانون من حيث المكان**، متاح على الموقع: https://cte.univ-setif2.dz/moodle/mod/book/view.php?id=17514&chapterid=5359

فهرس المحتويات

فهرس المحتويات