الجمهوريــة الجزائريــة الديمقراطيــة الشّعبيــة
وزارة الّتعليــم العــالي والبحث العلــمي
جامعة الشاذلي بن جديد – الطارف –
كلية: الحقوق والعلوم السياسية
قسم: الحقوق

آليات المتابعة الجنائية للجرائم الالكترونية في التشريع الجزائري

مذكّرة تخرّج مقدمة لنيل شهادة ماستر في القانون

من إعداد الطالبتين:

- حريدي نرجس
- فزاع فايزة

إشراف الدكتور:

بوعشة كمال

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
نزار عبدلي	أستاذ تعليم عالي	الشاذلي بن جديد –الطارف–	رئيسا
بوعشة كمال	أستاذ محاضر –أ–	الشاذلي بن جديد –الطارف–	مشرفا ومقررا
بليدي دلال	أستاذ محاضر –أ–	الشاذلي بن جديد –الطارف–	ممتحنا

السنة الجامعية: 2024 / 2025

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): .....نرجس حريدي.....

الحامل لبطاقة التعريف الوطنية رقم: ...110021241000420002.....

الصادرة بتاريخ: ....2025/05/05.....

عن دائرة: .....القالة.....

المسجل بقسم: .....الحقوق.....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

آليات المتابعة الجنائية للجرائم الالكترونية في التشريع الجزائري

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/06./11

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): .....فزاع فايزة.....

الحامل لبطاقة التعريف الوطنية رقم: ...110011230004780000.....

الصادرة بتاريخ: .....2025/05/26.....

عن دائرة: .....الطارف .....

المسجل بقسم: .....الحقوق.....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

آليات المتابعة الجنائية للجرائم الالكترونية في التشريع الجزائري

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/06./11

إمضاء المعني


بسم الله الرحمن الرحيم

شكر وتقدير

نتقدم بخالص الشكر وعظيم الامتنان إلى

الأستاذ المشرف

كمال بوعشة

على ما بذله من جهد، وما قدمه لنا من توجيهات قيمة، وملاحظات بناءة

ومساندته طوال فترة إعداد هذه المذكرة .

فله منا كلّ التقدير والاحترام

الإهداء

إلى من كان سندي بعد الله، إلى رفيق دربي، وشريك حياتي، زوجي الحبيب،

الذي كان لي دعمًا لا ينضب، وظهرًا لا يميل، شكرًا لصبرك، لحبك، ولثقتك التي كانت النور في أصعب اللحظات. لك وحدك، أهدي هذه الثمرة، التي لولاك ما اكتملت.

وإلى روح أبي الطاهرة، الذي غيّبه الموت عن عالمي، لكنه لم يغب لحظة عن قلبي،

إليك يا من علمتني معنى الصبر، والإرادة، والكرامة،

أهدي هذا الإنجاز عرفانًا لذكراك العطرة، ودعاءً بأن يكون هذا العمل صدقة جارية في ميزان حسناتك.

وإلى أمي الحبيبة، نبع العطاء، والدعاء، والحب النقي،

وإلى إخوتي وأخواتي، الذين كانوا عوني وسندي، بدفئهم ودعواتهم،

أهديكم جميعًا هذا العمل المتواضع،

فأنتم من صنعتم نجاحي، وكنتم جزءًا من كل خطوة في هذا الطريق.

حريدي نرجس

الإهداء

إلى من زرع في قلبي حب العلم والمعرفة

إلى من علّمني معنى الثبات والإصرار ...

إلى والديّ العزيزين، اللذين لولاهما لما وصلت إلى ما أنا عليه

إلى أساتذتي الأفاضل

إلى أصدقائي الذين كانوا سندًا لي في كل مراحل هذا المشوار

أهدي ثمرة هذا العمل المتواضع، عربونَ محبةٍ وامتنان

فـزاع فايـزة

مقدمة

مقدمة

يشهد العالم اليوم تحوّلاً جذريًا بفعل الثورة الرقمية والتكنولوجية التي غيّرت نمط حياة الأفراد والمجتمعات، وامتد أثرها ليطال مختلف مناحي الحياة، بما في ذلك المجال الإجرامي. فقد ظهرت إلى الوجود أنماط جديدة من الجرائم، أفرزتها البيئة الإلكترونية، يُطلق عليها اصطلاحًا ''الجرائم الإلكترونية'' أو ''الجرائم السيبرانية''، وهي جرائم تتم عبر الشبكات الرقمية، باستخدام الحواسيب والأنظمة المعلوماتية، وتستهدف الأفراد والمؤسسات والدول على حد سواء.

وتتميّز الجريمة الإلكترونية عن غيرها من الجرائم التقليدية بخصائص معقدة، منها طابعها العابر للحدود، وصعوبة تتبع مرتكبيها، والسرعة الكبيرة في تنفيذها، واعتمادها على وسائل تقنية متطورة، مما يجعل اكتشافها وملاحقتها أكثر صعوبة، ويطرح تحديات جمّة أمام الأجهزة الأمنية والقضائية. وهو ما يفرض على السياسة الجنائية أن تتكيف مع هذه التحولات، وأن تطور آلياتها بما يسمح بمواجهة فعالة لهذا النوع المستحدث من الإجرام.

على الرغم مما تحمله التقنيات الحديثة من تسهيلات وامكانيات هائلة، يسرت على الانسان الوقت والجهد والمال، فان البعض قد اساء استخدامها، وهو ما ادى الى ظهور نمط جديد من الجرائم، وهيا ما يسمى الجرائم الالكترونية والتي تختلف في شكلها ومضمونها ووسائلها عن الجريمة بشكلها التقليدي، ويستمد هذا النوع المستحدث من الاجرام نشاطه من الإمكانيات الهائلة للحاسوب و البرامج وتطور شبكة الانترنت، والتطور الثقافي والعلمي في التعامل مع التكنولوجيا الحديثة بمختلف انواعها، وتتعاظم المخاطر الناتجة عن الجرائم الالكترونية لقدراتها الفائقة على التطور والانتشار وتخطيها للحدود الجغرافية، ماألاحته شبكة الانترنت من انفتاح معلوماتي على العالم باسره.
وتتسم الجريمة الالكترونية بخصائص تجعل من مواجتها امرا بالغ الصعوبة اذ تتعدى الحدود الجغرافية وترتكب في الفضاء الافتراضي، اذ يختفي الجاني وراء حواجز تقنية معقدة ليس من السهل مواكبتها ومجاراتها مما يؤدي ذلك إلى خلق فجوات وثغرات تستغل من طرف مرتكبي هذه الجرائم الذين يطلق عليهم مصطلح المجرمين الالكترونين وهم افراد يمتلكون مهارات تقنية عالية ويستخدمون معرفتهم في التكنولوجيا لتحقيق اهداف غير مشروعة ويتفاوتون في دوافعهم واهدافهم.

كما تتعدد صور الجريمة الالكترونية وتشمل الإختراق غير مشروع للانضمة وسرقة البيانات، الابتزاز الالكتروني، التشهير عبر الشبكات، وقد أدت هذه الجراءم الى خسائر مادية ومعنوية جسيمة مما استدعى ضرورة التصدي لها بفعالية.

وفي مواجهة هذا التحدي ظهرت الحاجة الماسة الى تطوير اليات جنائية فعالة قادرة على الوقايةمن الجرائم الالكترونية تهدف الى كشف هذه الجراءم، تحدي مرتكبيها ،و تقديمهم للعدالة ومنع افلاتهم من العقاب وتشمل هذه الاليات:

- تحديث التشريعات الوطنية لتجريم الافعال الالكترونية الضارة.
- تعزيز قدرات الإجهزة الامنية والقضاءية في مجال التحقيق الرقمي.
- وتطوير التعاون الدولي لملاحقة الجناة الذين ينشطون عبر الحدود.

ومن هنا تبرز لنا اشكالية هذه الدراسة في التساؤل الرئيسي وهو كالتالي:

ما مدى فعالية الاليات الجنائية في متابعة الجريمة الالكترونية ومواجهتها وماهي ابرز الإشكالات التي تعيق هذه الفعالية؟

وكإشكالية فرعية: ماهو دور التعاون الدولي في تعزيز فعالية ملاحقة او مكافحة الجريمة الالكترونية؟

أولاً: أهمية الموضوع

1. الأهمية العلمية:

يكتسي موضوع ''آليات المتابعة الجنائية للجرائم الإلكترونية في التشريع الجزائري'' أهمية علمية بالغة، لكونه يتناول أحد أبرز الإشكالات القانونية المعاصرة، والمتمثلة في مدى فعالية المنظومة القانونية الجزائرية في مواكبة التطور التكنولوجي، ومواجهة الأشكال المستحدثة من الجريمة.

فهو يُسهم في إثراء المكتبة القانونية بدراسة معمقة حول الأسس النظرية والعملية للمتابعة الجنائية في بيئة رقمية تفرض تحديات خاصة على القواعد التقليدية للإثبات، والتحقيق، والمتابعة.

2. الأهمية العملية:

يُعد هذا الموضوع ذا أهمية تطبيقية واضحة، بالنظر إلى تزايد الجرائم المرتكبة عبر الوسائط الإلكترونية، وما تشكله من تهديد حقيقي لأمن الأفراد والمؤسسات، بل والدولة ذاتها.

كما يُسهم في كشف أوجه النقص أو القصور في الإطار التشريعي الجزائري، ويقترح آليات لتعزيز فعالية الأجهزة القضائية والأمنية في التصدي لهذا النوع من الجرائم، خاصة في ظل صعوبة تتبع مرتكبيها، وطبيعتها العابرة للحدود.

ثانيًا: أهداف الدراسة.

تهدف هذه الدراسة إلى:

- تحليل الإطار القانوني المنظم للجرائم الإلكترونية في التشريع الجزائري، لاسيما ما يتعلق بالمتابعة الجنائية.
- بيان الصعوبات القانونية والعملية التي تواجه السلطات القضائية أثناء تتبع هذا النوع من الجرائم.
- تقييم مدى نجاعة النصوص القانونية المعمول بها، ومدى ملاءمتها للتطور التكنولوجي المتسارع.
- مقارنة آليات المتابعة الجنائية في الجزائر مع بعض التجارب الدولية الرائدة، بغرض الاستفادة من الممارسات الفضلى.
- اقتراح توصيات عملية وتشريعية من شأنها تعزيز فعالية مكافحة الجرائم الإلكترونية في الجزائر.

ثالثًا: أسباب اختيار الموضو

1. الأسباب الذاتية:

- ينبع اختيار الموضوع من رغبة شخصية لدى الباحث في التخصص في القانون الجنائي المعاصر، ومتابعة تطوراته الحديثة.
- شغف الباحث بموضوع الجريمة الإلكترونية، وما تطرحه من إشكالات قانونية وفنية مستجدة.
- قناعة الباحث بأهمية التطرق إلى مواضيع حديثة وذات صلة مباشرة بالواقع، بما يخدم المجتمع والعدالة على حد سواء.

2. الأسباب الموضوعية:

• الانتشار المتزايد للجرائم الإلكترونية في الجزائر، وتنوع أشكالها بين جرائم الاحتيال، الابتزاز، التزوير الإلكتروني، واختراق النظم المعلوماتية.

• الطبيعة الخاصة لهذه الجرائم التي تعقّد عملية المتابعة، ما يفرض مراجعة الآليات القانونية المعتمدة حاليًا.

• ضعف الدراسات الأكاديمية المحلية المتخصصة في الجانب الإجرائي لمكافحة الجريمة الإلكترونية، مما يجعل هذه الدراسة إضافة نوعية.

• حاجة المشرّع الجزائري إلى دعم أكاديمي وتوصيات موضوعية تساعد على تطوير المنظومة القانونية بما يواكب التهديدات الرقمية.

رابعا: المنهج المتبع

وصفي تحليلي مع الاستعانة بالمنهج المقارن

.

الفصل الأول:

ماهية الجريمة الالكترونية

المبحث الأول: مفهوم الجريمة الإلكترونية

تعد الجريمة الإلكترونية من الجرائم الخطيرة والمستحدثة، إذ تتزايد أعمال الجريمة الإلكترونية بازدياد مستمر نتيجة التطور في وسائل التكنولوجيا والمعلومات، ومن ثم تلقي بظلال هذا التطور على أمن الأفراد أو الدولة على حد سواء، حيث غالبًا ما تتعرض خصوصية الأفراد أو ملكيتهم الخاصة إلى الخطر نتيجة الاختراق من بعض مخترقي الحاسوب.

أو يكون التعرض على الدولة من خلال الكشف عن مسائل خطيرة تهدد بقاءها، حيث إن الغاية من الاختراق غالبًا ما تكون سيئة النية، ولا مانع من اقترافها حتى وإن كان حسن النية ما دام أن الاختراق غير المشروع قد تحقق. والجريمة الإلكترونية لكي تتحقق لا بد من أن هناك دوافع لاقترافها، تكون ذات دوافع سياسية أو عسكرية، وتارة تكون ذات دافع اقتصادي أو اجتماعي وتارة تكون ذات دافع قانوني. لذا وانطلاقًا من الجريمة الإلكترونية وأهمية معرفتها، نقسم هذا المبحث إلى مطلبين، وهما كالآتي:

المطلب الأول بعنوان تعريف الجريمة الإلكترونية وخصائصها، والمطلب الثاني بعنوان أركان الجريمة الإلكترونية وطبيعتها القانونية[1].

المطلب الأول: تعريف الجريمة الإلكترونية وخصائصها

تمثل الجرائم الإلكترونية أشد أنواع الجرائم التي تُرتكب عن طريق الشبكات الدولية، حيث لم تكن الجريمة الإلكترونية معروفة إلا منذ وقت قريب، مما يشكل أحد أهم التحديات الراهنة التي تواجه الدولة أو الأفراد، وتشكل عائقًا أمام السلطات التنفيذية في الكشف عنها، لا سيما في الدولة التي تعاني من حداثة التقنية، أو تلك التي تعاني من نقص في التشريعات الجزائية التي تجرمها، ومن ثم يستطيع ممتهن تلك الجريمة من ارتكابها عدة مرات بكل يسر وسهولة.

[1]- علي حمزة عسل الخفاجي: الجرائم الناشئة عن اختراق الأمن السيبراني وآليات مكافحتها، دار مصر للنشر والتوزيع، مصر، ط1، 2024–2025، ص13.

ولغرض بيان ما تقدم، علينا أن نعرف مدلول الجريمة الإلكترونية، ولذلك قسمنا هذا المطلب إلى:

- الفرع الأول بعنوان تعريف الجريمة الإلكترونية.
- الفرع الثاني خصائصها.
- الفرع الثالث أسباب ارتكابها[1].

الفرع الأول: تعريف الجريمة الإلكترونية

أولًا: التعريف الفقهي للجريمة الإلكترونية

يذهب البعض إلى تعريف الجريمة الإلكترونية من حيث موضوعها، وهناك من يعرفها من حيث مرتكبها، وهناك من يعرفها مستندًا إلى أداة ارتكابها. وفي التعريف الفقهي للجريمة الإلكترونية سنتطرق إلى كل من تعريفاتها المختلفة، حيث تُعرف الجريمة الإلكترونية بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تُحول عن طريقه[2].

من الملاحظ من التعريف الفقهي أعلاه أنه يستند إلى موضوع الجريمة وصورة السلوك المادي المجرم، ويؤخذ عليه أنه يضيق من مفهوم الجريمة الإلكترونية، حيث إنه يخرج طائفة من الأفعال غير المشروعة يُستخدم فيها الحاسوب كأداة لارتكابها، كاحتيال الإلكتروني. كما أنه اقتصر تعريف الجريمة الإلكترونية على عدة صور للسلوك المادي للجريمة، وقد يؤدي ذلك إلى خروج بعض الأفعال الأخرى التي لم يشملها التعريف من نطاق التجريم مثل: الأفعال التي تستهدف الشبكات والمواقع الإلكترونية بقصد إعاقة الاتصال وانتقال المعلومات، ومنع الوصول للمعلومات، والحرمان من الخدمة الإلكترونية بشكل عام.

أما تعريف الجريمة الإلكترونية استنادًا إلى وسيلة ارتكابها، وهو الحاسوب فهو كالآتي:

[1]- علي حمزة عسل الخفاجي: مرجع سابق، ص13.

[2]- محمد كمال الدسوقي: الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، مصر، ط1، 2021، ص14.

فعل إجرامي يُستخدم الكمبيوتر في ارتكابه كأداة رئيسية. ويُعتبر هذا التعريف منتقدًا، حيث إن تعريف الجريمة الإلكترونية يجب أن يكون تعريفًا يجمع كل العناصر، وليس مقتصرًا على وسيلة تحقيقها[1].

عرفها الفقيه كلاوس تايدومان Klaus Tiedemann بأنها "كافة أشكال السلوك غير المشروع الذي يُرتكب باسم الحاسب الآلي".

ذهب الفقيه ميروي Meruie يعرف الجريمة الإلكترونية بأنها الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، أو هو في اقترافه الحاسب الآلي كأداة رئيسية.

كما عرفها الفقيه روزابلات Rosaplat بأنها: "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقتها."[2]

يرى البعض أن تعريف الجريمة الإلكترونية من طرف كلا من الفقيهين ميروي وروزابلات جاء مقتصرًا على الإحاطة بأوجه الظاهرة الإجرامية، أما تعريف كلاوس تايدومان فيؤخذ عليه أنه بالغ في العمومية والاتساع[3].

أما بالنسبة للتعريف وفقًا لسمات الجاني الشخصية فهي:

الجرائم التي تتطلب اهتمامًا خاصًا بتقنيات الحاسب ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها.

وتُعرف أيضًا بأنها الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني[4].

---

[1]- محمد كمال الدسوقي: مرجع سابق، ص15.

[2]- عبد العالي الديربي: الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، مصر 2012، ص ص 40–41.

[3]- عبد العالي الديربي: مرجع سابق، ص42

[4]- أيمن عبد الله فكري: الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد،المملكة العربية السعودية، ط1، 2014، ص101.

ثانيًا: التعريف القانوني للجريمة الإلكترونية

بالنسبة للتعريف القانوني للجريمة الإلكترونية، فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب أحكام المادة 2 من القانون رقم 09-04[1] على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى تُرتكب أو يُسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

من خلال التعريف أعلاه، نرى بأن المشرع الجزائري تبنى معيار النظام المعلوماتي لتحديد معالم الجريمة، حيث قام بتسميتها بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما قام بتبيانها في قانون العقوبات الجزائري[2] من المادة 394 مكرر 07.

وترك المجال واسعًا لأي جريمة أخرى تُرتكب عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

وبالرجوع إلى الاتفاقية الدولية حول الجرائم المعلوماتية المنعقدة في ببودابست سنة 2001، نجد أن المشرع الجزائري استمد تعريفه من الاتفاقية الدولية سابقة الذكر[3].

ثالثًا: تعريف الجريمة الإلكترونية حسب الخبراء المختصين والمنظمات الدولية الغربية

1- تعريفها حسب الخبراء المختصين:

ذهب خبراء مختصون من بلجيكا إلى أن تعريف الجريمة الإلكترونية هو" أنها كل فعل أو امتناع عمدي ينشأ عن استخدام غير مشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية"[4].

---

[1]- القانون رقم 04-09. الصادر في 5 أغسطس 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.

[2]- القانون رقم 04-15 الصادر في 10 نوفمبر، يعدل ويتمم الأمر رقم 156/66 الصادر في 8 يونيو 1966، متضمن قانون العقوبات، الجريدة الرسمية، العدد 47.

[3]- فتيحة بوهرين: "الجريمة المعلوماتية في التشريع الجزائري"، مجلة الحقوق والعلوم الإنسانية، مج 14، ع 04 ،غرداية 2021، ص55.

[4]- محمد كمال الدسوقي: مرجع سابق، ص15.

عرف خبراء المنظمة الأوروبية للتعاون الاقتصادي: "بأنها كل سلوك غير مشروع أو نافٍ للأخلاق أو غير مسموح به، يرتبط بالمعالجة الآلية للبيانات"[1].

عرف الخبير باركر الجريمة الإلكترونية حيث قال: "إنها كل فعل إجرامي، أياً كانت صلته بتقنية المعلومات، يتكبد المجني عليه نتيجة له خسارة ويحقق الفاعل ربحًا عمديًا"[2].

2- تعريفها حسب المنظمات الدولية العربية:

عرفت منظمة التعاون الاقتصادي والتقنية (D E C D) الجريمة المعلوماتية بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجًا بطريقة غير مباشرة أو مباشرة من تدخل التقنية المعلوماتية"[3].

عرف مكتب التقييم التقني بالولايات المتحدة الأمريكية، حيث يُعرف الجريمة الإلكترونية من خلال تحديد مفهوم جريمة الحاسب الآلي: "بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية، ويتكبد المجني عليه نتيجة لها خسارة، ويحقق الفاعل ربحًا عمديًا"[4].

رابعا: تعريف الجريمة الإلكترونية لدى بعض التشريعات العربية

ترك المشرع المصري مسألة تعريف الجريمة الإلكترونية للفقه، وبالتالي اختلف الفقه في تعريفها.

لكن على عكس المشرع المصري، فإن بعض التشريعات العربية الأخرى قامت بتعريف الجريمة الإلكترونية، مثل المشرع العراقي، حيث قام هذا الأخير بتعريفها من خلال مشروع قانون مكافحة الجرائم المعلوماتية، حيث قام بتعريف الجرائم الإلكترونية بأنها: "كل فعل يُرتكب باستعمال الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات، معاقب عليها وفق أحكام القانون"[5].

---

[1]- عفاف خديري: "الجريمة الإلكترونية والأمن الوطني"، المجلة الجزائرية للدراسات السياسية، جامعة عنابة، 2017، ص199.

[2]- سميرة معاشي: "ماهية الجريمة المعلوماتية"، مجلة المنتدى القانوني، ع7، جامعة بسكرة، 2010، ص277.

[3]- محمد كمال الدسوقي: مرجع سابق، ص15.

[4]- عبد العالي الديربي: مرجع سابق، ص41.

[5]- علي حمزة عسل الخفاجي: مرجع سابق، ص 18.

أما بالنسبة للدولة الفلسطينية، فلم تُعرف كذلك الجريمة الإلكترونية، ولكن أوضحت محكمة النقض الفلسطينية الجريمة الإلكترونية بأنها كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل مشروعًا[1].

عرف المشرع السعودي الجريمة الإلكترونية بأنها "أي فعل يُرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[2].

الفرع الثاني: خصائص الجريمة الالكترونية

أولا: سمات خاصة بالجريمة الالكترونية

تتسم الجريمة الالكترونية بأنها جريمة مستحدثة ومختلفة عن باقي الجرائم التقليدية من حيث محلها ونطاقها ومخاطرها ووسائل ارتكابها والمشكلات الناجمة عنها، فهي تتميز بطبيعة الحال بطبيعة خاصة، وتتميز بعدة خصائص نذكر منها:

1- جريمة ناعمة:

تتطلب الجريمة التقليدية استخدام أدوات العنف أحيانا، كما في جرائم المخدرات والسرقة والسطو المسلح، إلا أن الجرائم الالكترونية تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، فنقل البيانات من كمبيوتر لآخر أو السطو الالكتروني على أرصدة، البنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

2- جريمة صعبة الإثبات:

تتميز الجرائم الالكترونية عن غيرها بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة وغياب الدليل الفيزيقي كالبصمات أو التخريب أو الشواهد المادية، وسهولة محو

[1]- علي حمزة عسل الخفاجي مرجع سابق، ص19.

[2]- ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، دراسة مقارنة، المركز العربي، مصر، 2017، ص 25.

الدليل أو تدميره في زمن متناهٍ القصر. ويضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي وعدم كفاية القوانين القائمة[1].

3- الحاسب الآلي أداة لارتكابها

تُعتبر هذه الخاصية من أهم الخصائص التي تتميز بها الجرائم الالكترونية عن غيرها من الجرائم الأخرى، ذلك لأن شبكة الإنترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة، ولذلك فإن ارتباطها بالحاسب الآلي هو أمر لا مفر منه، باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي، وإن كنا اليوم نُعاصر إمكانية استعمال الهاتف الخلوي[2].

4- سرعة التنفيذ:

لا يتطلب تنفيذ الجريمة الالكترونية وقتا كبيرا، فبضغطة واحدة على لوحة المفاتيح يمكن أن تُنقل الملايين من الدولارات من مكان لآخر. ولكن هذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة[3].

5- جريمة عابرة للحدود

يمكن القول إن من أهم ما يميز الجريمة الالكترونية تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية. فبعد ظهور المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر دول مختلفة. فالقدرة التي تمتلكها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة الالكترونية، وجمع الأموال والمعلومات المستهدفة، والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال قد ميزت الجريمة الالكترونية عن الجريمة التقليدية كثيرا[4].

---

[1]- عبد العالي الديربي: مرجع سابق، ص 56

[2]- غادة نصار، الإرهاب والجريمة الالكترونية، العربي للنشر والتوزيع، ط 1، 2017، ص 35.

[3]- عبد العالي الديربي: مرجع سابق، ص ص 54-55.

[4]- غادة نصار، مرجع سابق، ص 35.

6- الجاذبية:

نظرا لما يتيحه سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها، وتوظيف الكثير منها في تطوير تقنيات وأساليب تُمكن من الدخول إلى الشبكات وسرقة المعلومات وبيعها، أو سرقة البنوك، أو اعتراض العمليات المالية وتحويل مسارها، أو استخدام أرقام البطاقات ...الخ[1].

ثانيا: سمات المجرم الالكتروني

1- المجرم الالكتروني مجرم ذكي

يتمتع بالذكاء المعلوماتي الذي يمكنه من التعديل والتطوير من الأنظمة الأمنية حتى لا يكون من الممكن ملاحقته وتتبع أعماله الإجرامية عبر الشبكات وداخل أجهزة الحاسوب[2].

كما يوصف الإجرام الالكتروني بأنه إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم الالكتروني إنسان على مستوى من الذكاء، بالإضافة إلى أنه مجرم متكيف اجتماعيا، لا يناصب العداء للمجتمع[3].

2- المجرم الالكتروني مجرم مختص

تبين في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر، أي أنهم يتخصصون في هذا النوع من الجرائم دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى[4].

---

[1]- عبد العالي الديربي: مرجع سابق، ص .55

[2]- نور الهدى قادري: الجريمة السيبيرانية وآليات مكافحتها، المجلة الجزائرية للحقوق والعلوم السياسية، المركز الجامعي أحمد بن يحيى، معهد العلوم القانونية، مج 8، ع1، جوان 2023، ص 11.

[3]- عادل يوسف عبد النبي شكري: الجريمة المعلوماتية، أزمة الشرعية الجزائية، الجريمة المعلوماتية، ع 7، جامعة الكوفة، كلية القانون، ص117.

[4]- عماد مفلح الحسبان وآخرون: الجرائم المستحدثة المعلوماتية الإلكترونية السيبيرانية ، ط 1، دار الخليج للنشر والتوزيع، عمان، 2024، ص 98.

مما يعكس أن المجرم الذي يرتكب الإجرام الالكتروني هو مجرم في الغالب متخصص في هذا النوع من الجرائم[1].

3- المجرم الالكتروني مجرم اجتماعي

هو عادة إنسان اجتماعي، قادر على التكيف في بيئته الاجتماعية، بل إن بعضهم يتمتع بثقة كبيرة في مجال عمله[2].

فهو إنسان اجتماعي بطبعه، يمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى، وتطبيقا لذلك فغير من جرائم المعلوماتية تُرتكب بدافع الكبرياء أو بدافع النصب أو الحسد[3].

4- المجرم الالكتروني مجرم عائد إلى الإجرام

يوظف المجرم الالكتروني مهارته في كيفية عمل الحواسيب وتخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات[4].

فيعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وأدت إلى تقديمهم إلى المحاكمة في المرة السابقة، ويؤدي ذلك إلى العودة إلى الإجرام[5].

5- المجرم الالكتروني مجرم محترف

يتمتع بالسلطة اتجاه النظام المعلوماتي، فهو ليس ذلك الشخص المبتدئ الذي يستعصي عليه ارتكاب هذه الجرائم، فهو في غالب الأحيان لديه سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة[6].

---

[1]- عبد العالي الديربي: مرجع سابق، ص 58.

[2]- نهلا عبد القادر المومني: الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان2010، ص 79.

[3]- امينة حمشاشي: ماهية الجريمة المعلوماتية، ماجستير قانون عام، جامعة مصطفى اسطنبولي، معسكر،2009، ص 453.

[4]- يوسف باعدي: طبيعة المجرم في الطبيعة القانونية، مجلة الباحث للدراسات القانونية والقضائية، ع59، اكتوبر 2023، ص40.

[5]- الجريمة الالكترونية: وحجية الدليل الرقمي في الاثبات الجنائي، مركز هردو لدعم التعبير الرقمي، القاهرة 2014، ص19.

[6]- عبد الحميد المليحي: الجريمة الالكترونية مدخل في اطار المفاهيمي، مجلة المنارة للدراسات القانونية والادارية، 2019، 157.

وذلك أنه لا يمكن للشخص العادي في حالات قليلة أن يرتكب جرائم عن طريق الكمبيوتر، فالأمر يقتضي الكثير من الدقة والتخصص في هذا المجال،والتوصل إلى التغلب على العقبات التي أوجدها المتخصصون في حماية المنظومة المعلوماتية[1].

6- المجرم الالكتروني مجرم غير عنيف

إن الجرائم الالكترونية سواء التي تُرتكب بشكل فردي أو ضمن عصابات منظمة هي جرائم غير عنيفة، خصوصا إذا كانت الجريمة المرتكبة هي غاية وليست وسيلة لارتكاب جرائم أخرى[2].

فالمجرم الالكتروني من المجرمين الذين لا يلتجئون إلى العنف بتاتا في تنفيذ جرائمهم، وذلك لأنه ينتمي إلى الحيلة، فهو لا يلجأ إلى العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدر من العناء للقيام به[3].

الفرع الثالث: أسباب ارتكاب الجريمة الالكترونية

هناك العديد من الأسباب التي تؤدي إلى حدوث الجريمة الالكترونية، ومن بين هذه الأسباب نذكر ما يلي:

1- **تحقيق مكاسب مالية:** قد تدفع حاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية ذات أهمية خاصة بمن يطلبها[4].

2- **الدوافع الشخصية:** بحيث يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توفر هذه المؤثرات، فإن الأمر يؤول في النهاية إلى ارتكابه لجريمة معلوماتية[5].

---

[1]- بثينة حبيباتي: الطبيعة الخاصة للجريمة للمعلومة، المجلة العربية في العلوم الانسانية والاجتماعية، مج 12، ع 53، جامعة الجزائر 1، جويلة 2020 ص 610.

[2]- نجم الدين وسامر سمير : الجريمة المنظمة الالكترونية دراسة تحليلية في التشريع الفلسطيني، مجلة الجامعة الاسلامية للدراسات الشرعية والقانونية، مج 29، ع 2، الجامعة الإسلامية بغزة، عمادة البحث العلمي، 2021، ص 97.

[3]- مركز هردو لدعم التعبير الرقمي: مرجع سابق ص 19.

[4]- سعاد طعبة: الجريمة الالكترونية، تفعيل الآليات القانونية من اجل تحقيق العدالة، مجلة الحقوق والعلوم الانسانية، مجلد 15، ع 3، جامعة زيان عاشور بالجلفة، 2022، ص229.

[5]- المرجع نفسه، ص 229.

3- **المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات** وذلك من خلال اختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، فقد تشكل متعة نتيجة كبيرة لمرتكبها وتسلية تغطي أوقات فراغه[1].

4- **الضغوط العامة:** ترجع نظرية الضغوط العامة الانحراف وخرق القانون إلى دافع ناجم عن قوى البناء الاجتماعي أو استجابات نفس اجتماعية للحوادث والظروف التي تعمل كضغوط أو مقلقات، خاصة عندما لا تتاح للأفراد الفرصة لتحقيق أهدافهم المقبولة اجتماعيا[2].

5- **النشاط الروتيني:** يمكن تفسير زيادة ضحايا الجريمة الالكترونية من خلال التغيرات في أنشطة الناس الروتينية في الحياة اليومية، فمع ظهور شبكة الإنترنت قد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية[3].

6- **القصور في برامج التوعية الأمنية** برامج التوعية بأمن المعلومات من أكثر الطرق فعالية في محاربة الجرائم الالكترونية، وهناك نقص شديد جدا في برامج التوعية بأمن المعلومات على مستوى الأفراد والمؤسسات والحكومات، وقد يستغل المجرمون عوامل قلة برامج التوعية بأمن المعلومات في ارتكاب مثل هذه الجرائم[4].

7- **إلحاق الأذى بأشخاص أو جهات:** فبعض المجرمين الذين يقدمون على ارتكاب الجريمة على شبكة المعلومات العالمية وتقنية المعلومات بصورة عامة، يتركز الدافع من ورائها على إلحاق الأذى بأشخاص محددين أو جهات معينة[5].

---

[1]- نهلا عبد القادر المومني: مرجع سابق، ص 91.

[2]- ذياب موسى البداينة: الجرائم الالكترونية المفهوم والاسباب، ورقة علمية بعنوان الجرائر الالكترونية المفهوم والاسباب كلية العلوم الاستراتيجية، عمان، المملكة الاردنية الهاشمية، 2014، ص12.

[3]- لامية طالة: الجريمة الالكترونية بعد جديد لمفهوم الاجرام عبر منصات التواصل الاجتماعي، مجلة الرواق للدرسات الاجتماعية والإنسانية، مج 6، ع2، ص77.

[4]- غادة نصار: مرجع سابق، ص 42.

[5]- عبد العزيز نايف: الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهته، مجمع البحوث والدراسات، اكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان2016، ص 29.

8- **الاستيلاء على المعلومات**: الإقدام على ارتكاب هذا الجرم بواسطة تقنية المعلومات يهدف للحصول على المعلومة ذاتها، والاستيلاء عليها والتصرف فيها، ويتمثل ذلك في الحصول على المعلومة المحفوظة في الحاسب الآلي والمنقولة أو تغييرها أو حذفها أو إلغائها نهائيا من النظام[1].

9- **البطالة**: ترتبط الجريمة الالكترونية شأنها شأن الجريمة التقليدية بالظروف الاقتصادية الصعبة، وترتكز البطالة بين قطاعات كبيرة من الشباب، ولذا فإن الشباب الذين يملكون المعرفة يستثمرون ذلك في النشاط الإجرامي الالكتروني[2].

المطلب الثاني: أركان الجريمة الالكترونية:

تمثل الجريمة الالكترونية إحدى الظواهر الحديثة التي نشأت في ظل تطور التكنولوجيا، والتي تشمل مجموعة من الأفعال الخارجية، وتتميز بأنها لا تقتصر على نطاق جغرافي معين، بل يمكن أن تحدث بين أي طرفين في أي مكان في العالم، ومن أجل أن يُعد هذا الفعل جريمة الكترونية يجب توافر أركان محددة، وهي الركن المادي والمعنوي والشرعي، بحيث نقوم بتقسيم الأركان إلى ثلاثة فروع:

- الفرع الأول: الركن المادي
- الفرع الثاني: الركن المعنوي
- الفرع الثالث: الركن الشرعي.

الفرع الأول: الركن المادي.

يقصد بالركن المادي السلوك الذي يأتيه الجاني أو الامتناع عن إتيانه، والذي من شأنه أن يُحدث ضررا للضحية، فالسلوك الإجرامي في الجريمة الالكترونية يقوم على الفعل المادي والعلاقة السببية[3].

---

[1]- المرجع نفسه، ص 28.

[2]- ذياب موسى البداينة: مرجع سابق، ص 14.

[3]- رقية محمودي ونور الهدى قدوح: الجرائم الالكترونية في المجتمع الجزائري، ط 1، هيئة النشر العلمي، جامعة يحي فارس، المدية 2022، ص 86.

كما أن الركن المادي يمثل النشاط الإيجابي والسلوك المادي المرتبط ببيئة رقمية واتصال هاتفي بالشبكة، ومعرفة هدف هذا النشاط وأسلوبه ونتائجه[1].

فالركن المادي يتكون من ثلاثة عناصر يجب تقسيمها إلى كل عنصر على حدى.

1- السلوك الإجرامي: هو الذي يعبر عن الفعل الذي يقوم به الجاني، والذي يتحصل أن يخضع من تجريمه لقاعدة "لا جريمة ولا عقوبة إلا بنص قانوني"، وهذا ما نصت عليه المادة ثلاثة من قانون الجزاء العماني[2].

فالسلوك الإجرامي في الجريمة الالكترونية يتطلب وجود بيئة رقمية، وجهات كمبيوتر، واتصال بشبكة الإنترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته[3].

2- النتيجة الجرمية: وهي ما يترتب على الفعل الذي أتاه الجاني، فلا يكفي قيام الجانب السلوكي الإجرامي مهما بلغت خطورته، بل لا بد من أن ينتج عن هذا السلوك نتيجة، ففي جريمة القتل لا بد أن ينتج عن سلوك الجاني وفاة المجني عليه[4].

فالنتيجة الإجرامية لها مدلولان، أحدهما المدلول المادي، والآخر المدلول القانوني، فالمدلول المادي يعني الآثار المادية التي تحدثها الجريمة في العالم الخارجي، ويرتب القانون على حصولها عقوبة[5].

3- العلاقة السببية: يجب أن تتحقق علاقة السببية بين سلوك الجاني وبين النتيجة التي تترتب على فعله، أي أن النتيجة الجرمية سببها السلوك الخارجي. ففي جريمة القتل، وفاة المجني عليه

---

[1]- يوسف باعدي: مرجع سابق ص 32.

[2]- محمد وصبرين جابر: "الجريمة الالكترونية ومكافحتها في القانون العماني"، المجلة المصرية للدراسات القانونية والاقتصادية، ع 14، 2020 ص 232.

[3]- عبد الله دعش العجمي: المشكلات العلمية والقانونية للجرائم الالكترونية، رسالة ماجستير قانون عام، جامعة الشرق الأوسط، 2014، ص 27.

[4]- جهاد نزار دغمش: الاشكاليات الموضوعية والاجرائية في النظام القاومني الفلسطيني، في التجربة الالكترونية، مجلة الباحث للدراسات والابحاث القانونية والقضائية، مج 2022، ع 45، ص4.

[5]- فيروز عوض الكريم صالح ميرغني: اجراءات التحري والضبط في الجريمة الالكترونية رسالة دكتوراه قانون عام، جامعة شندي، 2017، ص 87.

بسبب سلوك الجاني الإجرامي. وقد تستطيع تطبيق هذه القواعد العامة المطبقة على الجرائم العادية على الجرائم الإلكترونية فيما يتعلق بعلاقة السببية إذا انطبقت عليها[1].

الفرع الثاني: الركن المعنوي

الركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين الجريمة وشخصية الجاني[2].

وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية وفي القانون الفيدرالي الأمريكي، وأحيانًا أخرى أخذ بالعلم كما هو في قانون مكافحة الاستنساخ الأمريكي[3].

كما أن توافر الركن المعنوي في الجرائم الإلكترونية يعد من الأمور العامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها، لذا بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة وهي جريمة التسرب الغير المشروع[4].

كما أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الإنترنت، مثل جريمة تسريب الوثائق المحمية، من حيث مدى تحديد ما إذا كانت تتطلب قصدًا عامة أم خاصة[5].

فالقصد الجنائي العام يقصد به اتجاه الجاني عند ارتكابه الواقعة الإجرامية مع العلم بعناصرها التي تحقق غرضًا معينًا، أما القصد الجنائي الخاص فيتلاقى مع القصد العام في جميع عناصره ويزيد عليه بتحديد الإرادة الإجرامية[6].

---

[1]- جهاد نزار دغمش: مرجع سابق ص ص 4 5.

[2]- عبد الصبور علي مصري: المحكمة الرقمية والجريمة المعلوماتية ، ط1، مكتبة القانون والاقتصاد، الرياض ، 2012، ص 277.

[3]- مرجع نفسه ص 77.

[4]- عماد مفلح الحسبان وآخرون: مرجع سابق ص 195.

[5]- المرجع نفسه، ص 195.

[6]- صغير يوسف: الجرائم المرتكبة عبر الانترنيت، رسالة ماجستير، قانون دولي للأعمال، جامعة مولود معمري بتزي وزو 2014/2013 ص 70.

الفرع الثالث: الركن الشرعي

يقصد بالركن الشرعي قيام المشرع بتجريم سلوك معين وتحديد العقوبة التي تناسبه من خلال النص على الجريمة في قانون العقوبات، وذلك كله في إطار مبدأ الشرعية الجنائية[1].

كما يقوم الركن الشرعي على وجود نص تشريعي يجرم الفعل ويحدد العقاب المترتب على إتيان الفعل غير المشروع، فلا جريمة ولا عقوبة بغير نص قانوني[2].

وإعمالا لذلك فإنه من غير الممكن بحال الاجتهاد من القاضي الجزائي، فلا يجوز القياس في التجريم، والجرائم الالكترونية حديثة وذات تقنية عالية، ووضع نصوص خاصة بها ليس بالأمر السهل. وعلى الرغم من ذلك، فإن هناك بعض الدول وضعت قوانين لمثل تلك الجرائم، وتعد دولة السويد أول دولة تضع قوانين خاصة لهذه الجرائم، حيث أصدرت في عام 1973 قانون البيانات، وبين عامي 1976 و1985 سنت الولايات المتحدة الأمريكية قانونًا لحماية أنظمة الحاسب الآلي[3].

فتبعتها فرنسا، والتي قامت في عام 1988 بتطوير قوانينها الجنائية لتتوافق مع ما استُحدث من جرائم. أما بعض الدول العربية، فقد قامت بعضها بسن القوانين في هذا المجال، مثل السعودية التي أصدرت في عام 2007 نظام التعاملات الالكترونية ونظام مكافحة الجرائم الالكترونية، والإمارات العربية المتحدة التي أصدرت القانون الاتحادي رقم 2 سنة 2006 بشأن مكافحة جرائم تقنية المعلومات[4].

ونجد أن المشرع الجزائري قد أطلق تسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على الجريمة الالكترونية، وقد عرفها في المادة الثانية من القانون رقم 09-04 المؤرخ في 2009/8/1 بأنها

[1]- رقية محمودي: مرجع سابق، ص 86.

[2]- هدية احمد محمد زعتر: الاشكاليات القانونية للجرائم العابرة للحدود وسبل مواجهتها، مجلة البحوث القانونية والاقتصادية، ع 84، 2023، ص 77.

[3]- جهاد نزار دغمش: مرجع سابق، ص 05.

[4]- المرجع نفسه، ص 06.

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المعددة في قانون العقوبات، وأي جريمة أخرى تُرتكب أو يُسهل ارتكابها عن طريق منظومة معلوماتية ونظام الاتصال الالكتروني[1].

حيث قامت الجزائر بسن قوانين خاصة بالجريمة الالكترونية، وهي متأخرة مقارنة ببعض الدول العربية رغم احتلالها المراتب الأولى عربيًا وإفريقيًا، ومن بين التشريعات نذكر منها قانون العقوبات، حيث قامت الجزائر بتعديل قانون العقوبات بموجب القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004، والذي أُدخل عليه تعديل بتاريخ 20 ديسمبر 2006، ويتضمن قانون العقوبات الجزائري القسم السابع تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 مكرر إلى 394 مكرر 6، والتي تناولت أنواع الجرائم الالكترونية وعقوبتها[2].

الفرع الرابع: الطبيعة القانونية للجريمة الالكترونية

لكل جريمة جنائية طبيعة تميزها عن غيرها من الجرائم، لذا فالجريمة الالكترونية كغيرها من الجرائم لها دلالتها الخاصة المميزة عن غيرها، وتلك الدلالات قد تختلف باختلاف التشريعات التي نصت عليها بوصفها جريمة الكترونية ذات خطر جسيم[3].

فالطبيعة القانونية لاعتبار الجريمة من صنف الجرائم الالكترونية تقتضي اعتبارها جريمة مستقلة تُعالج ضمن أحكام مستقلة من حيث تقدير الجزاء المناسب لها، فإن طبيعتها القانونية لا تقتصر على تكييفها التشريعي، بل يتعدى ذلك إلى نطاق الفقه الجنائي الذي حاول بآرائه المختلفة توظيف الجريمة الالكترونية[4].

[1]- فتيحة بوهرين، مرجع سابق، ص 55.

[2]- فتيحة بوهرين، مرجع سابق، ص 56.

[3]- علي حمزة عسل خفاجي: مرجع سابق، ص 71.

[4]- المرجع نفسه، ص 71.

فالجرائم الالكترونية بطبيعة خاصة كونها ترد على معلومات، وهذه الطبيعة تعود في حقيقتها إلى المعلومات التي يشملها القانون في النهاية من خلال التعدي عليها، في صفة تدل على الجريمة المعلوماتية[1].

كما أن الفقه التقليدي يرى أن الجريمة الالكترونية لها طبيعة من نوع خاص، فهي تتمتع بحماية قانونية لاعتراف الفقه والقضاء بوجود اعتداء، فإن عليه الاستيلاء غير المشروع على معلومات الغير.أما الفقه الحديث، فيرى أن الجريمة الالكترونية عبارة عن مجموعة من القيم المستحدثة[2].

فالجرائم الالكترونية تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، على اعتبار أن معظم هذا النوع من الجرائم يُرتكب ضمن نطاق المعالجة الالكترونية للبيانات، سواء كان في تجميعها أو إدخالها إلى الحاسب المرتبط بشبكة الإنترنت[3].

المبحث الثاني: صور الجرائم الالكترونية

مما لا شك فيه أن الجريمة الالكترونية لها عدة صور، ومن أبرز تلك الصور هو وقوعها على الأشخاص عن طريق اختراق بياناتهم الذاتية، إذ تتمثل تلك الصور في جرائم القذف والتشهير الالكتروني عن طريق تقديم بعض المعلومات والبيانات المغلوطة بحق الأفراد المتضررين، أو عن طريق انتحال شخصية الفرد لغرض مآرب ذاتية، تُستخدم فيها هوية شخصية مزورة لإخفاء شخصية المخترق السيبراني، أو تكون لغرض التجسس والابتزاز الالكتروني من خلال اختراق الشبكات والمواقع للتجسس على الأفراد والتعدي على خصوصياتهم.

بل يتعدى ذلك حتى إلى المساس بممتلكاتهم المالية من خلال القيام ببعض أعمال النصب والاحتيال أو السرقة الالكترونية للأموال المودعة لدى مصرف الائتمان، وكذلك الجرائم الواقعة على النظام الالكتروني والتعدي على البيانات المعلوماتية، والتعدي على كل ما يمكن تخزينه ومعالجته

[1]- محمد بن فردية: الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة دكتوراه، جامعة الجزائر 2015.2016.ص 55

[2]- عيشة خلدون: الطبيعة الخاصة للجريمة الالكترونية وصورها قاعدة بيانات الملخصات العلمية، جامعة زيان عاشور بالجلفة، ص 08.

[3]- محمد حسين مرعي: المواجهة الجنائية للجرائم المستحدثة الماسة بالحياة الخاصة، مجلة الكوفة للعلوم القانونية والسياسية، المج 11، ع 36، جامعة الكوفة ، كلية القانون، 2018، ص415.

وتوليده. وسنتناول كل هذه الصور المتعلقة بجرائم المعلومات حيث سنقسم هذا المبحث إلى ثلاث مطالب حيث:

- المطلب الأول: الجرائم الواقعة على الأشخاص
- المطلب الثاني: الجرائم الواقعة على الأموال
- المطلب الثالث: الجرائم الواقعة على النظام المعلوماتي.

المطلب الأول: الجرائم الواقعة على الأشخاص

الجريمة الالكترونية لها عدة صور عديدة في وقوعها على الأفراد، إذ تكمن هذه الصور في أنماط مختلفة ومتعددة. فتارة تتحقق الجريمة الالكترونية عن طريق الاختراق غير المشروع لغرض تسوية سمعة الفرد عن طريق القذف أو التشهير به، أو قد يكون الاختراق غير المشروع لغرض القيام ببعض الأعمال المخلة بالآداب العامة، وقد يكون الغرض من الاختراق هو التجسس أو الابتزاز الالكتروني لتحقيق مآرب ذاتية، وهي كما يلي[1]:

1- القذف وتشويه سمعة الأفراد:

يعد القذف والتشويه الالكتروني من الجرائم التي لها مردود سلبي وبالغ على حياة الأفراد، فهي من الجرائم الأكثر شيوعًا وتطبيقًا في نطاق تقنية المعلومات المتطورة، حيث يُستخدم هذا الأسلوب للنيل من شرف الغير واعتباره المعنوي من خلال التشهير، إذ يُقصد به "نشر المعلومات المضللة أو الكاذبة عن الأشخاص بقصد التشهير بهم، أو تصميم مواقع خاصة، أو إرسال رسائل الكترونية إلى أشخاص تحتوي على معلومات أو فضائح مالية أو سلوكية مفبركة، مما يُلحق أضرارًا عديدة بحق الأشخاص".

[1]- علي حمزة عسل خفاجي: مرجع سابق، ص 85.

ولهذا، ولأهمية تلك الجريمة وارتباطها بحرمة الأشخاص، عمدت بعض القوانين إلى تجريمها، إذ نلاحظ ذلك في قانون مكافحة الشائعات والجرائم الالكترونية التي رتبت تجريم هذه الأفعال[1].

2- جريمة التهديد:

ويقصد به زرع الخوف في النفس بالضغط على إرادة الإنسان وتخويفه من أضرار ما ستلحقه أو ستلحق أشخاصًا له بهم صلة، ويجب أن يكون التهديد على قدر من الجسامة، المتمثلة بالوعيد بإلحاق الأذى بنفس المجني عليه أو ماله، أو بنفس أو مال الغير. ولا يُشترط أن يتم إلحاق الأذى فعلاً، أي تنفيذ الوعيد، لأنها تشكل جريمة أخرى قائمة بذاتها وتخرج من إطار التهديد إلى التنفيذ الفعلي. وقد يكون التهديد مصحوبًا بالأمر أو الطلب للقيام بفعل أو الامتناع عن فعل، أو بمجرد الانتقام، ولقد أصبحت الإنترنت الوسيلة لارتكاب جرائم التهديد، وهي في حد ذاتها تحتوي على عدة وسائل لإيصال التهديد للمجني عليه، كالبريد الالكتروني أو الويب[2]...

3- جريمة السب عبر الانترنت:

جريمة السب كما تكون باللسان تكون عبر الانترنت، ويكون ذلك بوسائل الكترونية مختلفة كاستخدام احد المواقع الالكترونية واستخدام وسائل التواصل الاجتماعي كالفيسبوك وتويتر ويوتيوب وانستقرام والواتساب وغيرها، لسب الآخرين والتهجم عليهم. كما يتم استخدام البريد الالكتروني بإرسال رسالة إلى الشخص المسبوب وحده أو إرسالها إلى عدة أشخاص.

[1]- علي حمزة عسل الخفاجي: المرجع نفسه، ص 86.

[2]- سورية ديش: انواع الجريمة الالكترونية و إجراءات مكافحتها مجلة الدراسات الإعلامية المركز الديمقراطي العربي ع1 جامعة جيلالي ليابس الجزائر 2018 ص 8.

وبذلك يعظم الأذى ويزداد على كل من وقع عليه السب لانتشاره بين إعداد كبيرة من الناس. والمتتبع لحال الانترنت هذه الأيام، ولا سيما في الساحات ومواقع الحوار والنقاش، يجد جرأة كثير من المشتركين على السب الذي يأنف منه المسلم ويخشى عقوبته[1].

4- جريمة انتحال شخصية:

وهو استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته، ولقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية، وتتم بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيتها للاستفادة منها لارتكاب جرائمه، عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة كالاسم، اللقب، العنوان الشخصي، ... الخ[2].

5- الأعمال المخلة بالآداب والأخلاق العامة:

مما لا شك فيه أن انطلاق عالمية الشبكة الالكترونية قد اثر سلبا على حياة الأفراد من خلال نقل بعض العادات والتقاليد لدى بعض فئات المجتمع الغربي ومحاولة تطبيعها وتكييفها مع المجتمعات التي تحظر مثل تلك الأعمال. وحيث يستغل المجرم الالكتروني احترافيته في مجال الحاسوب الآلي، ليعمد إلى نشر وعرض بعض الصور والأفلام المنافية للعادات والقيم الاجتماعية.

وصفوة القول أن الجرائم المخلة بالآداب العامة عبر الوثائق الالكترونية ما هي إلا صورة من صور الجرائم الالكترونية، حيث تستهدف اقتراف تلك الجريمة في الغالب الأعم الأطفال القصر من خلال إغوائهم على إدمان بعض المشاهد والأفلام غير اللائقة أدبيا واجتماعياً لتحقيق دوافع متعلقة بذات المجرم الالكتروني[3].

---

[1]- صدام حسين ياسين العبيدي جرائم الانترنت و عقوبتها في الشريعة الاسلامية و القوانين الوضعية المركز العربي للنشر و التوزيع مصر 2019 ص 148.

[2]- سورية ديش: مرجع سابق، ص 8.

[3]- علي حمزة عسل الخفاجي: مرجع سابق، ص 88.

المطلب الثاني: الجرائم الواقعة على الأموال:

1- جرائم السطو على أرقام البطاقات الائتمانية

فالبطاقات الائتمانية تعد نقودا الكترونية، والاستيلاء عليها يعد استيلاء على مال الغير، حيث تتم عملية التحويل الالكتروني غير المشروع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمعني عليه، مما يسمح للجاني بالتوغل في نظام المعلومات. وعادة ما يكون هؤلاء من العاملين على إدخال البيانات في دائرة الجهاز[1].

فالاستيلاء على بطاقات الائتمان عبر الانترنت أمر ليس بالصعوبة كما كان إطلاقا، فاللصوص بطاقات الائتمان مثلا يستطيعون الآن سرقة الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت، ومن ثم بيع هذه المعلومات للآخرين[2].

2- التلاعب بالبطاقات المالية:

لقد ظهرت محاولات هذا النوع من الاحتيال بالنقاط والأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود، إلى أن ظهرت الصرافة الآلية Electronic banking و digital cash[3]

أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها، وهو ما يتم عن طريق اختراق بعض المواقع التجارية

[1]- عفاف خذيري: مرجع سابق ، ص 201.

[2]- عبد الصبور عبد القوي علي مصري: مرجع سابق، ص 135.

[3]- رحاب علي عميش: الجريمة المعلوماتية دراسة مقارنة بين القانون الليبي والاماراتي، مجلة علمية محكمة، ع 4، معهد دبي القضائي، 2014، ص 78.

التي يمكن أن تسجل عليها أرقام هذه البطاقات. وفي هذا النوع من الاعتداء لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها[1].

3- جرائم الاستيلاء على النقود الالكترونية

ويمكن تعريف النقود الالكترونية بوضوح أكثر، أنها قيمة نقدية مخزنة ووسيلة الكترونية مدفوعة مقدما وغير مرتبطة بحساب مصرفي، تحظى بقبول من قام بإصدارها وتستعمل كأداة دفع. وتتمثل أهم عناصرها في أن قيمتها النقدية نسخة من بطاقة بلاستيكية او على القرص الصلب للحساب الشخصي للمستهلك[2].

فهي تختلف عن البطاقات الائتمانية، لأن النقود الالكترونية يتم دفعها مسبقا، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية يتم بين طرفين هما العميل والتاجر دون الحاجة إلى تدخل طرف ثالث[3].

4- جريمة غسل الأموال:

هذه الجريمة ترتكب عبر النظام الالكتروني، وهي عملية يقصد بها نقل أموال مستمدة من مصدر غير مشروع بقصد تطهيرها، فعملية التحويل الالكتروني لهذه الأموال يشوبها أي تلاعب، إلا أن صفة المشروعية يرجع إلى مصدر هذه الأموال ذاتها، وتتم عبر الإنترنت عن طريق البنوك، حيث تتم العمليات المصرفية بطريقة الكترونية سريعة[4].

---

[1]- زينب طرقي فهد والعنزي: الجريمة الالكترونية في ميزان الفقه والقضاء، مجلة الدراسات الإسلامية والبحوث الأكاديمية، ع 99، جامعة القاهرة، 2020 ، ص101.

[2]- رحاب علي عميش: مرجع سابق، ص 79.

[3]- عبد الصبور عبد القوي علي مصري: مرجع سابق، ص 138.

[4]- فريجة حسين: الجرائم الالكترونية والانترنيت المعلوماتية، ع 36. المملكة العربية السعودية، 2011، ص 05.

كما أعطت شبكة الإنترنت عدة مميزات لمن يقوم بعملية غسيل الأموال، منها السرعة الشديدة وتخطي الحواجز الحدودية في الدول وتفادي القوانين التي قد تضعها بعض الدول وتعيق نشاطهم، وكذلك تشفير عملياتهم مما يعطيها قدرًا كبيرًا من السرية، وأيضا كان انتشار التجارة الالكترونية عبر شبكة الإنترنت عونا غير معين لهؤلاء القائمين على عمليات غسل الأموال، كالتجارة الالكترونية وانتشارها عبر أنحاء العالم[1].

5- استخدام برامج معدة خصيصًا لتنفيذ الاختلاس:

من بين هذه الوسائل هو تصميم برامج معينة تهدف إلى إجراء عملية التحويل الآلي من حساب إلى آخر، سواء كان ذلك من المصرف نفسه أو من حساب آخر في مصرف آخر، على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج. كما توجد برامج أخرى تقوم بخصم مبالغ من حسابات الفوائد على الودائع المصرفية، مثل الكسور العشرية، حيث يتحول الفارق إلى حساب الجاني، لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة، مما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ[2].

ومن أشهر جرائم سرقة الأموال والتي جرت أحداثها في إمارة دبي بدولة الإمارات العربية المتحدة أواخر عام 255، ما قام به مهندس حسابات آسيوي يبلغ من العمر 21 عامًا. تم نشر وقائع الجريمة في أبريل من عام 2055، حيث قام بالعديد من السرقات المالية لحسابات عملاء في 12 بنكًا محليًا وعالميًا، حيث قام بالاختلاس من الحسابات الشخصية وتحويل تلك الأموال إلى حسابات وهمية قام هو بإنشائها. كما قام أيضًا بشراء العديد من السلع والخدمات عبر شبكة الإنترنت مستخدمًا بيانات بطاقات الائتمان والحسابات الشخصية لعدد كبير من الضحايا[3].

[1]- راضية عيمور: اليات مكافحة الجرائة الالكترونية في التشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، الجزائر العاصمة، 29 مارس 2017، ص36.

[2]- المرجع نفسه، ص35.

[3]- راضية عيمور: المرجع نفسه: ص 35.

المطلب الثالث: الجرائم الواقعة على النظام المعلوماتي:

الجرائم الواقعة على النظام المعلوماتي قد تعد من الجرائم الحديثة التي ظهرت نتيجة لتطورات التكنولوجيا واعتماد المجتمعات بشكل متزايد على الأنظمة المعلوماتية والرقمية، وتتمثل هذه الجرائم في الأفعال غير المشروعة التي تستهدف استخدام أنظمة الحواسب أو الاستعمال الإلكتروني بهدف الإضرار أو الاستفادة غير القانونية. ومن بين هذه الجرائم نذكر ما يلي:

1- التحويل المباشر للأرصدة:

يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور، وأشهرها قيام خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف لقيامه بتحويل 12 مليون دولار لحسابه الخاص في ثلاث دقائق فقط، وعادة ما يتم ذلك عن طريق إدخال معلومات سريعة[1].

فهناك بعض الأنظمة التي تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات كتم ومغناطيسية، حيث إنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفرتها بواسطة جهاز... وإعادة بثها مرة أخرى بعد تحويلها[2].

2- جرائم التعدي على البيانات المعلوماتية:

تشمل الجرائم التي يكون موضوعها البيانات المعلوماتية، أي التي تقع على بيانات مخزنة معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية وجرائم اعتراض بيانات معلوماتية. والبيانات هي كل ما يمكن تخزينه ومعالجته ونقله بواسطة الحاسب الآلي من أرقام وحروف ورموز وما إلى ذلك[3].

[1]- زينب طرقي فهد والعنزي: مرجع سابق، ص 100.

[2]- رحاب علي عميش: مرجع سابق ص 78.

[3]- عماد مفلح الحسبان وآخرون: مرجع سابق، ص 140.

3- جريمة إتلاف المعلومات الإلكترونية:

وذلك بالاعتداء على البرامج والبيانات المخزنة والمتبادلة بين الحواسيب، وتدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي. ويكون الإتلاف العمدي للبرامج والبيانات كمحوها أو تدميرها إلكترونيًا أو تشويهها على نحو يجعلها غير صالحة للاستعمال[1].

4- جرائم الإضرار بالبيانات:

يُعتبر هذا الفرع من الجرائم الإلكترونية من أشدها خطورة وتأثيرًا، وأكثرها حدوثًا وتحقيقًا للخسائر للأفراد والمؤسسات. ويشمل هذا النوع كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة إلكترونية Digital Al Form على الحواسيب الآلية المتصلة بشبكة المعلومات، أو مجرد محاولة الدخول بطريقة غير شرعية عليها[2].

أبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي أثر سلبي عليها، ويقوم بذلك النوع من الأنشطة ما يُطلق عليهم المخترقون ذوو القبعات البيضاء، الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكة المعلومات ومواقع الإنترنت، مستغلين بعض الثغرات في تلك الأنظمة، محترفين بذلك كل ميادين وإجراءات أمن المعلومات التي يقوم بها مديري تلك الأنظمة والشبكة[3].

5- الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي:

قد يتعرض النظام المعلوماتي إلى الاختراق من قبل أفراد غير مصرح لهم بالدخول إليه أو البقاء فيه، بحيث يُعد هذا الفعل مرحلة سابقة وضرورية لارتكاب الجرائم المعلوماتية الأخرى مثل سرقة المعلومات وتوفيرها، أو التجسس المعلوماتي، أو جريمة الاحتيال المعلوماتي[4].

---

[1]- سورية ديش: مرجع سابق، ص 247.

[2]- محمد نصر محمد: المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، ط1 ، مركز الدراسات العربية للنشر والتوزيع، مصر2015، ص 12.

[3]- المرجع نفسه، ص 13.

[4]- الحكيم ومولاي ابراهيم: الجرائم الالكترونية، مجلة الحقوق والعلوم الانسانية، ع 23، جامعة زيان عاشور الجلفة 2015، ص 215.

6- جريمة الاحتيال الإلكتروني:

المجرم الإلكتروني شخص يتميز بالدهاء والقدرة على متابعة ثغرات وسائل وتكنولوجيا المعلومات بطريقة دقيقة، وغالبًا ما يتقن التحدث بعدة لغات. وقد يكون شخصًا حدث له انهيار في أعماله التجارية أو خسر وظيفته في المؤسسة التي كان يعمل بها، وبالتالي يخترق ويحتال على الأنظمة الإلكترونية كنوع من العقاب للمجتمع أو لمكان عمله السابق[1].

7- السرقة من البنوك:

يتم سرقة أموال البنوك بالطريقة المعلوماتية عن طريق اختلال البيانات والمعلومات الشخصية للمجني عليهم، واستخدام شخصية الضحية ليقوم الجاني بعملية السرقة الخفية. كما يؤدي ذلك بالبنك إلى إجراء التحويل البنكي للأموال الإلكترونية أو المادية إلى الجاني، حيث يستخدم الجاني الحاسب الآلي للدخول إلى شبكة الإنترنت والوصول إلى المصارف والبنوك[2].

8- إساءة استعمال الأجهزة أو البرامج المعلوماتية:

تتضح هذه الجرائم في كل من أقدم أو أنشأ أو وزع أو حاز، بغرض الاستخدام، جهازًا أو برنامجًا معلوماتيًا أو أي بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض اختراق أي من الجرائم المنصوص عليها سابقًا[3].

ويتضمن البرنامج المعلوماتي مجموعة من التعليمات والأوامر القابلة للتنفيذ باستخدام الحاسب الآلي، ومعد لإنجاز مهمة ما، أما البرامج المعلوماتية فهي الكيان المعنوي غير المادي من برنامج ومعلومات وما إليها ليكون قادرًا على القيام بوظيفة[4].

---

[1]- شحاتة واحمد ابو زيد: الجريمة المعلوماتية أنواعها ويل مواجهتها، مجلة العلوم القانونية الاقتصادية، مج 65، ع 2، جامعة عين الشمس كلية الحقوق، 2023، ص 40.

[2]- سورية ديش: مرجع سابق، ص243.

[3]- عماد مفلح الحسبان وآخرون: مرجع سابق، ص 140.

[4]- مرجع نفسه، ص 141.

9- جريمة انتحال شخصية المتعامل الشرعي للبيانات:

يُعتبر هذا نوعًا من الجرائم الأكثر حداثة، وذلك نظرًا لسرعة انتشارها، خاصة في الأوساط التجارية التي يتم فيها استخدام هوية شخصية أخرى بطريقة غير شرعية. وهدف الجاني إما الاستفادة من مكانة تلك الهوية أو الهوية القديمة، أو لإخفاء هوية شخصية المجرم لتسهيل ارتكاب جرائم أخرى[1].

[1]- عفاف خديري : مرجع سابق ص 201.

الفصل الثاني:

آليات و إجراءات متابعة الجريمة الالكترونية

المبحث الأول: آليات متابعة الجريمة الإلكترونية

إن تنافي التوجه نحو التحول الرقمي وتبني التكنولوجيات العالمية الحديثة عاد بالكثير من الفائدة على الدول وكذا شعوبها، ولكن في المقابل نشأ عنه شق إجرامي يسعى إلى خلق عالم رقمي يستنزف العديد من الإيجابيات للتكنولوجيا الحديثة الخيّرة، وهو الأمر الذي دفع العديد من الدول والمنظمات والهيئات إلى رفع التحديات لمواكبة التطورات العالمية المتلاحقة، محاولة اعتماد سياسات رامية إلى تطوير استراتيجيات عملها وجعلها تقدمية وإعادة صياغة دورها من أجل توثيق أوامر التعاون والعمل المشترك فيما بينها وتبادل الخبرات بما يساعدها على إيجاد آليات لمكافحة مختلف أنواع الجرائم الإلكترونية التي لم يسلم منها أي ميدان من ميادين الحياة. وسنتطرق في هذا المبحث إلى آليات مؤسساتية لمكافحة الجريمة الإلكترونية المطلب الأول: وإلى آليات مؤسسية دولية لمكافحة الجريمة الإلكترونية المطلب الثاني[1].

المطلب الأول: آليات مؤسساتية الوطنية لمكافحة الجريمة الإلكترونية.

لقد خصصت مختلف التشريعات الوطنية والدولية مؤسسات ومصالح ووحدات من أجل مكافحة الجريمة الإلكترونية، فعلى المستوى الوطني في الجزائر مثلاً، نجد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني، ومركز الوقاية من جرائم الإعلام الآلي، ...الخ.

حيث سنتطرق بالتفصيل في هذا المبحث إلى كل منها على حدى من خلال الفروع[2].

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

بموجب المادة الثالثة عشر من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، نص المشرع الجزائري على إنشاء الهيئة الوطنية

[1]- شنتير خضرة: الآليات القانونية لمكافحة الجريمة الالكترونية لدراسة مقارنة، أطروحة دكتوراه، جامعة احمد دراية بأدرار، 2021/2020، ص 154.

[2]- شنتير خضرة: المرجع نفسه، ص 156.

للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي كانت محط إنذار العديد من وسائل الإعلام التي تحدثت عنها، ولكن بعدها اختفت أخبارها.

إلا أنه في الثامن من شهر أكتوبر سنة 2015، تم إصدار المرسوم الرئاسي رقم 15-261 والذي تم من خلاله تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

وبمقتضى المادة 02 و03 من ذات المرسوم، تعد الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المادية، توضع تحت سلطة رئيس الجمهورية. يُحدد مقر الهيئة بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي[2].

كما تضامنت هذه الهيئة مع وظيفة السلطة الوطنية لأمن المعلومات، إذ تتولى تحديد التدابير التقنية والتشريعية للدفاع والحماية، ومسؤولة أيضًا عن الضوابط والتفتيش على نظم المعلومات المتعلقة بالبنية التحتية الحيوية. ولعل هذا الإنشاء للهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في الجزائر لم يأتِ من العدم، وإنما جاء متماشياً مع التوجه الدولي في هذا الصدد[3].

فقد أنشأت المملكة المتحدة مركز حماية البنية التحتية الوطنيةCPNI، سلطة حكومية تقدم المشورة الأمنية للشركات والمؤسسات، أما في الولايات المتحدة الأمريكية، فتم سن قانون الأمن الإلكتروني، الذي أوجَب على الحكومة وضع معايير محددة وموحدة في مجال الأمن التكنولوجي لتحليل الهجمات الإلكترونية وتطبيق النتائج[4].

[1]- شنتير خضرة: مرجع سابق، ص 157.

[2]- شنتير خضرة: المرجع نفسه، ص 159

[3]- محمد مزوالي: المعالجة التشريعية للجريمة الرقمية في القانون الجزائري، مجلة الحقيقة العدد 43، 2018/2017، جامعة احمد دراية، أدرار، ص 18.

[4]- محمد مزوالي: مرجع نفسه، ص 19.

في الثامن من شهر أكتوبر سنة 2015، تم إصدار المرسوم الرئاسي رقم 261/15، والذي تضمن من خلاله تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

ولأكثر تفاصيل حول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، تم تقسيم هذا الفرع إلى: تشكيل الهيئة أولاً، وإلى مهامها ثانيا.

أولا: تشكيلة الهيئة

حسب المادة الأولى من المرسوم الرئاسي رقم 20-183، فإن هذا المرسوم جاء ليعيد تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فمن خلاله يمكن معرفة تشكيلة الهيئة وكذا طريقة وكيفية سيرها[2].

كما استحدثت هذه الهيئة بموجب القانون 09-04، وبقيت تشكيلتها وتنظيمها وكيفية سيرها لتحدد عن طريق التنظيم، والذي توالت منه التغييرات ابتداء من المرسوم الرئاسي لسنة 2015 ثم سنة 2019، ليأتي المرسوم الرئاسي لسنة 2020 ليعيد تنظيم الهيئة، وعرفها بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة رئيس الجمهورية، ويحدد مقرها في الجزائر العاصمة، ويمكن نقلها إلى أي مكان من التراب الوطني بموجب مرسوم رئاسي[3].

وتتكون الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية، ويقدمان كل منهما نشاطاته. مرسوم رئاسي رقم 20-183 المؤرخ في السابع عشر يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 43، الصادر بتاريخ 18 يوليو 2020، ص 6[4].

---

[1]- شنتير خضرة: مرجع سابق ص 157.

[2]- شنتير خضرة: المرجع نفسه، ص 159

[3]- رضا مهدي: "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"، مجلة إليزا للبحوث والدراسات، مج. 6، ع. 2، 2021، جامعة محمد بوضياف – الجزائر، ص. 120.

[4]- رضا مهدي: مرجع سابق، ص 121

تضم المديرية العامة مديرية للمراقبة الوقائية واليقظة الإلكترونية، ومديرية الإدارة والوسائل، ومصلحة للدراسات والتلخيص، ومصلحة للتعاون واليقظة التكنولوجية. كما يضم مجلس التوجيه مجموعة من الأعضاء، هم: الوزير المكلف بالعدل، الوزير المكلف بالداخلية، الوزير المكلف بالمواصلات السلكية واللاسلكية، المدير العام للأمن الداخلي، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني.

وحسب المادة 05 من المرسوم الرئاسي 172/19 الملغى، فإن مجلس التوجيه كانت تتكون اللجنة المديرة من ممثلي وزارات، وفي ظل المرسوم الرئاسي 15-261 الملغى، كانت تتكون اللجنة المديرية من وزارة وممثل مصالح أخرى، وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، وهو الأمر الإيجابي الذي كان يميز تشكيلتها الإدارية، إضافة إلى أن اللجنة كان يترأسها وزير العدل[1].

ومما سبق نلاحظ أن المشرع الجزائري خطى خطوة إيجابية بسن هذا القانون وتنظيمه، إلا أنه لا يكفي لمواجهة خطورة الجرائم السيبرانية، مما يتطلب مواكبة التطورات التكنولوجية باستمرار[2].

ثانيا: مهام الهيئة

بالنسبة لمهام الهيئة، فقد نصت عليها في البداية المادة 14 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المشار إليها سابقا، كما يلي:

تتولى الهيئة المذكورة، حسب المادة 13 السالفة الذكر، خصوصا المهام الآتية:

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

ب- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

[1]- شنتير خضرة: مرجع سابق ص 162.

[2]- رضا مهدي: المرجع نفسه، ص 121

ج- جمع تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم[1].

ومن خلال اسمها، فإن للهيئة دورين أساسيين يمكن أن تلعبهما في حالة تأسيسها:

1- الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيا الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحايا لها وهم يتصفحون أو يستعملون هذه التكنولوجيات. ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء أو بطاقة ائتمانهم، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية...الخ[2].

2- مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

- مساعدة السلطات القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال.

وبالنسبة للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال بفرنسا، فإن لها مهام أدرجها المرسوم رقم 2405 المؤرخ في 15 ماي 2000، المتضمن إنشاء هذه الهيئة، تتمثل في[3]:

- تنشيط وتنسيق على المستوى الوطني عمليات المكافحة من الفاعلين والمشتركين في ارتكاب الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال.
- القيام بإذن من السلطات القضائية، بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات، كمساعدة لمصالح الشرطة القضائية المتخصصة في تحقيقات بجرائم خاصة ارتكبت

[1]- قانون رقم 09-04 المؤرخ في 25 شعبان 1430هـ، الموافق لـ 16 غشت سنة 2009م، يتعلق القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد 47.

[2]- ضياف اسمهان: "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف – الجزائر، 2018، ص.28.

[3]- ضياف اسمهان: مرجع نفسه، ص 29

أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال، ولكن دون المساس باختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة نص عليها القانون.

- تقديم المساعدة لمصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية، فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة.
- التدخل من تلقاء نفسها، بعد موافقة السلطات القضائية المسبقة (المادة 04، فقرة 02 من القانون 09-04)، في كل مرة تفرضها الظروف، من أجل البحث الميداني في جميع وقائع مرتبطة بتحقيق تقوم به...الخ[1].

كما أن الدور المهم الذي تلعبه الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في تطوير التعاون مع نظيراتها في الدول الأخرى، يجعل من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال همزة وصل مهمة جدا في تطوير تبادل المعلومات والتعاون الدولي، خاصة عندما يتعلق الأمر بتنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية، وكذا التعاون مع المؤسسات والهيئات الوطنية المعنية بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. ومن الأمثلة عن تلك المؤسسات: المركز الوطني للاستعداد للطوارئ الحاسوبية والشبكة التابعة للجهاز القومي لتنظيم الاتصالات، والمركز الفرنسي لمكافحة جرائم تكنولوجيات المعلومات والاتصالات، وفي الولايات المتحدة نجدها كذلك قد وضعت عددا من الوحدات المختصة والأجهزة الخاصة للبحث والتحري في الجريمة الإلكترونية، ...الخ[2].

الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تعزيزا للمنظومة الحقوقية وتكريسا لمبدأ حماية حقوق الإنسان وحفاظا على الحياة الخاصة والكرامة الإنسانية وتجسيدا للمبادئ الدستورية، مثل ما جاء في المادة 47 من التعديل الدستوري الجزائري سنة 2020، ومكافحة للجريمة الإلكترونية، خاصة منها تلك التي تمس المعطيات ذات

[1]- ضياف اسمهان: مرجع نفسه، ص 29

[2]- شنتر خضراء: مرجع سابق، ص. 167.

الطابع الشخصي، ولأجل إعطاء حماية أكثر لتلك المعطيات من الاعتداءات التي قد تقع عليها، قام المشرع الجزائري بإصدار قانون في العاشر من شهر جوان سنة 2018 تضمن 76 مادة بها قواعد قانونية تتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، كما قام بموجب ذات القانون بإنشاء سلطة وطنية لحماية هذه المعطيات[1].

وسنتطرق في هذا الفرع إلى نشأة وتشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وإلى مهامها.

أولا: نشأتها وتشكيلتها

بمقتضى القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، تم إنشاء سلطة وطنية لحماية المعطيات ذات الطابع الشخصي لدى رئيس الجمهورية، مقرها الجزائر العاصمة، تتمتع بالشخصية لمعنوية والاستقلال المادي والإداري.

وحسب المادة 235 من ذات القانون، فإن السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي تتشكل من ثلاثة شخصيات من بينهم:

- الرئيس يتم اختيارهم من قبل رئيس الجمهورية من ذوي الاختصاص في مجال عمل السلطة الوطنية
- وتضم أيضا ثلاثة قضاة يتم اقتراحهم من قبل المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.
- وعضو من كل غرفة من غرفتي البرلمان يتم اختيار كل منهما من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات البرلمانية.
- ممثل واحد من المجلس الوطني لحقوق الإنسان.
- ممثل واحد عن وزير الدفاع الوطني.
- ممثل واحد عن وزير العدل حافظ الأختام.

[1]- شنتر خضراء: مرجع نفسه، ص. 171.

- ممثل واحد عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة.
- عضوين آخرين عن كل من الوزير المكلف بالصحة ووزير العمل والتشغيل والضمان الاجتماعي[1].

ويتم اختيار أعضاء السلطة الوطنية بناء على كفاءاتهم في الميادين القانونية والتقنية في مجال المعطيات ذات الطابع الشخصي، كما يمكن للسلطة الوطنية الاستعانة بأي شخص مؤهل من شأنه مساعدتها في أشغالها. ويتم تعيين رئيس وأعضاء السلطة الوطنية بموجب مرسوم رئاسي لعهدة قابلة للتجديد، وهنا لم يحدد المشرع عدد المرات التي يمكن فيها التجديد، إن كانت مرة واحدة أو عدة مرات.

ذلك أن اكتساب الخبرة يعد عاملا مهما في التسيير الجيد لهذه السلطة، تلك الخبرة التي قد يكتسبها العضو من خلال ممارسته لمهامه داخل السلطة الوطنية، خاصة بالنسبة للقضاة. وهناك نقطة أخرى لابد من الإشارة إليها، وهي مسألة اختيار عضوين من البرلمان الذين يتم اختيارهما من قبل رئيسي غرفتي البرلمان بعد التشاور مع رؤساء المجموعات البرلمانية[2].

ثانيا: مهامها.

أوكل المشرع الجزائري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي عدة مهام مهمة، خاصة أنها تلعب دورا كبيرا في حماية المعطيات ذات الطابع الشخصي، ونذكر منها:

1- تلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي، وتمنح الترخيص عند الاقتضاء إذا تبين لها أن المعالجة المعزم القيام بها تتضمن أخطارا ظاهرة على كل من احترام وحماية الحياة الخاصة والتحريات والحقوق الأساسية للأشخاص.

2- تقوم السلطة الوطنية بإعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، كما تقدم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.

[1]- شنتير خضراء: مرجع سابق، ص. 172.

[2]- شنتر خضراء: مرجع نفسه، ص. 172.

3- تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي[1].

4- تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي، وإعلام أصحابها بمآلها.

5- الأمر بإجراء التغييرات اللازمة من أجل حماية المعطيات ذات الطابع الشخصي المعالجة، والأمر بإغلاق المعطيات أو سحبها أو إتلافها، خاصة إذا كانت غير مطابقة للقانون 18-07.

6- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة على مراعاة مبدأ المعاملة بالمثل[2].

الفرع الثالث: المنظومة الوطنية لأمن الأنظمة المعلوماتية.

تم في العشرين من شهر يناير من السنة الحالية 2020 إصدار مرسوم رئاسي تحت رقم 20-05 لوضع منظومة وطنية لأمن الأنظمة المعلوماتية موضوعة لدى وزارة الدفاع الوطني، والتي تعد المنظومة أداة الدولة وإطارها التطبيقي ووسيلتها لإعداد إستراتيجيتها الوطنية في مجال أمن الأنظمة المعلوماتية. وتشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية على مجلس وطني لأمن الأنظمة المعلوماتية أولاً، ثم لوكالة أمن الأنظمة المعلوماتية ثانيا[3].

أولاً: المجلس الوطني لأمن الأنظمة المعلوماتية.

يعد المجلس الوطني لأمن الأنظمة المعلوماتية أحد العناصر المكونة للمنظومة الوطنية لأمن الأنظمة المعلوماتية، يترأسه وزير الدفاع الوطني أو ممثله، ويتكون المجلس من:

- ممثل عن رئاسة الجمهورية
- ممثل عن الوزير الأول
- الوزير المكلف بالشؤون الخارجية

[1]- شنتر خضراء: مرجعسابق، ص. 173.

[2]- شنتر خضراء: مرجع نفسه، ص. 175.

[3]- شنتر خضراء: المرجع نفسه، ص. 181.

- الوزير المكلف بالشؤون الداخلية
- الوزير المكلف بالعدل
- الوزير المكلف بالمالية
- الوزير المكلف بالطاقة
- الوزير المكلف بالاتصالات
- الوزير المكلف بالتعليم العالي[1]

يتولى المجلس الوطني لأمن الأنظمة المعلوماتية عدة مهام أوضحتها المادة 04 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، وبداية لتلك المهام قيامه بتحديد عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة والبث فيها، كما يقوم بدراسة التقارير المتعلقة بتنفيذ تلك الإستراتيجية والموافقة عليها.

ومن مهامه أيضاً تقرير نشاط الوكالة ودراسة مخطط عملها والموافقة عليه، وللمجلس الوطني لأمن الأنظمة المعلوماتية دور مهم في الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية، نظراً للتطور المخيف الذي وصل إليه المجرم الإلكتروني[2].

ثانياً: وكالة أمن الأنظمة المعلوماتية

هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المادي، مقرها في مدينة الجزائر. تتوفر الوكالة على مركز وطني لعمليات أمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطة المدير العام الذي يسيرها.

كما تدير الوكالة لجنة توجيه مزودة بلجنة علمية. تتكون لجنة التوجيه من ممثلي عدة وزارات ومصالح وسلطات وهيئات، كما يمكنها الاستعانة بأي شخص أو مؤسسة من شأنها أن تساعد في أعمالها[1].

[1]- شنتر خضراء: مرجع سابق، ص. 183.

[2]- شنتر خضراء: المرجع نفسه، ص. 183.

تكلف لجنة التوجيه بعدة مهام نصت عليها المادة 245 من المرسوم الرئاسي رقم 20-05 السالف الذكر. فبحسب هذه المادة تقوم لجنة التوجيه باقتراح عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، ودراسة البرنامج الشفوي والمتعدد السنوات لتنفيذ تلك الإستراتيجية والمصادقة عليه، تقييم نتائج مجموع الأعمال التي قامت بها الوكالة، وتتداول في كل المسائل والبيانات التقديرية للإيرادات والنفقات، وخطط توظيف وتكوين المستخدمين، وكذا مركبات مستخدمي الوكالة. وتقدم لجنة التوجيه موافقتها على النظام الداخلي للوكالة، كما تقوم بتحديد ووضع الطرق والوسائل اللازمة لترقية البحث والتطوير في مجال أمن الأنظمة المعلوماتية[2].

الفرع الرابع: وحدات الأمن الوطني المتخصصة في مكافحة الجريمة الإلكترونية.

مع تزايد الاعتماد على التكنولوجيا، أصبحت الجريمة الإلكترونية تهديدًا حقيقيًا للأمن الوطني، ومن هنا ظهرت أهمية الوحدات الأمنية الوطنية المتخصصة في مكافحة هذا النوع من الجرائم، حيث تعمل على رصدها والتحقيق فيها لحماية الأفراد والمؤسسات من المخاطر الرقمية.

أولًا: الشرطة الوطنية لمكافحة الجريمة الإلكترونية.

تلعب الشرطة دورًا هامًا في مكافحة الجريمة الإلكترونية، وذلك من خلال تعاملها مع الخصائص الجديدة والبيئة المعلوماتية والعاملين والمتعاملين فيها، بالإضافة إلى منع ارتكاب الجرائم والحيلولة دون ارتكابها وتقليل فرص اقترافها على أرواحهم وأموالهم، وذلك بمنع أو اتقاء كل خطر من شأنه أن يسبب ضررًا لهم. يتعاظم دور الشرطة الوقائي يومًا بعد يوم بسبب تعاظم الوظيفة الوقائية للقانون الجنائي على المستوى المحلي والدولي[3].

[1]- شنتر خضراء: مرجع سابق، ص. 184

[2]- شنتر خضراء: المرجع نفسه، ص. 185.

[3]- سعد عاطف عبد المطلب حسين: "دور الشرطة في مكافحة الجرائم المستحدثة وتحقيق الأمن المعلوماتي"، مجلة بحوث كلية الآداب، جامعة المنوفية، ص. 485.

وتنظم دور الشرطة الوقائي التشريعات الوطنية بقوانين ولوائح في مختلف الدول، منها السودان، والكويت، والبحرين، وقطر، والسعودية، والإمارات، ومصر، حيث تأخذ نصوص قوانين هذه الدول بفكرة الخطورة الإجرامية، والغرض من ذلك حماية المجتمع ونظمه[1].

ومن بين الأهداف الإستراتيجية التي تهدف مؤسسة الشرطة القيام بها هي كشف الجريمة، والقبض على مرتكبيها، والوقاية والحد منها، وحماية الحريات، وصون الحقوق، والاستعداد لمواجهة الأزمات والكوارث بفعالية من أجل ضبط الأمن وحفظ النظام العام، وأداء جميع المهام المستمدة للأمن الوطني كما حددها التشريع الوطني، بموارد بشرية متخصصة[2].

ومن الأمثلة على ما قامت به الفصائل لأجل مكافحة الجريمة الإلكترونية، القضية التي عالجتها فرقة مكافحة الجرائم الإلكترونية بالمصلحة الولائية للشرطة القضائية لأمن ولاية عين الدفلى، والمتعلقة بالغش في امتحانات شهادة التعليم المتوسط دورة جوان 2019 بواسطة الوسائل الاجتماعية، حيث أسفرت التحريات التقنية التي باشرتها عناصر الفرقة، وبالتنسيق مع المصلحة المركزية لمكافحة الجرائم الإلكترونية بالمديرية العامة للشرطة القضائية، وبإشراف الهيئات القضائية عن توقيف ثلاثة أشخاص وتقديمهم للعدالة[3].

ثانيًا: الدرك الوطني.

يعد الدرك الوطني من بين قوات الأمن الفاعلة في مكافحة الإجرام عمومًا والجريمة الإلكترونية خصوصًا، وذلك من خلال ما له من إمكانيات بشرية ومادية متخصصة لهذا الغرض. فمكافحة الجريمة الإلكترونية أضحت من بين أولويات الدولة الجزائرية، وذلك في إطار الاستجابة للانشغالات الأمنية المتزايدة والمحافظة على الطمأنينة والأمن العمومي في الفضاء الإلكتروني الوطني. فالبداية الفعلية لمحاربة قيادة الدرك الوطني للجريمة الإلكترونية كانت في سنة 2004، ليتم بعدها إنشاء مركز الوقاية

[1]- سعد عاطف عبد المطلب حسين: المرجع نفسه، ص. 486.

[2]- شنتير خضراء: مرجع سابق، ص. 191.

[3]- شنتير خضراء: المرجع نفسه، ص. 192.

من الجرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، والذي يعد اليوم العصب الذي يسير مهام المكافحة واليقظة وفرض احترام القوانين، في الوقت الذي يُجرى فيه الملايين من المستخدمين عبر صفحة الإنترنت، سواء من الخواص أو المؤسسات في الفضاء الإلكتروني[1].

وبهذا السبب، أكد قائد فصيلة الأبحاث بالدرك الوطني بالعاصمة لقناة الشروق أن قيادة الدرك استحدثت فرقة خاصة أُطلق عليها اسم "داركيو الإنترنت" تابعة لفرقة البحث والتحري، مهمتها منع الجرائم الإلكترونية، وذلك بعد تفشي ظاهرة نشر الصور وابتزاز المواطنين عن طريق شبكة التواصل الاجتماعي، إلى جانب إتلاف المواقع الإلكترونية الخاصة بالمؤسسات الخاصة والحكومية.

وفي سياق الشروع في التصدي لجرائم الفيسبوك ومعاقبة المتورطين، عالجت فصيلة الأبحاث والتحري التابعة للدرك الوطني بالعاصمة أول قضية من نوعها تتعلق بابتزاز المواطنين عن طريق الفيسبوك، حيث تمكنت من الإيقاع بشاب ابتز فتاة عن طريق نشر صورها في وضعيات حرجة بعد رفضها لطلبه الزواج بها مستخدمًا خط الإنترنت اللاسلكي المعروف بالويفي من عند جاره الذي منحه الرقم السري لدخول الإنترنت[2].

لقد عمل مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، منذ سنة إنشائه سنة 2008، على تأمين منظومة المعلومات لخدمة الأمن الوطني العمومي، حيث يهدف ضباط وأعوان الشرطة القضائية المؤهلين في الدرك الوطني إلى تطبيق القوانين، وجمع الأدلة، وتحليل المعطيات وبيانات الجرائم الإلكترونية المرتكبة، والبحث عن مرتكبي الجرائم عمومًا.

وتحديد هوية أصحابها سواء كانوا فرادى أو عصابات، ويعمل المركز على مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها في هذا الخصوص، كما استطاع المركز معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يفوق 500 قضية رقمية خلال سنة 2015، منها 300 جريمة

[1]- شنتير خضراء: مرجع سابق، ص. 200.

[2]- بن بادة عبد الحليم: "إجراءات البحث والتحري عن الجريمة الإلكترونية"، مجلة الحقوق والعلوم الإنسانية، ع 23، م .ج. الثاني، جامعة غرداية، 2015، ص. 81.

تتعلق بمواقع التواصل الاجتماعي "فيسبوك"، و20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات.

وفي خمسة أشهر الأولى من سنة 2019، تم معالجة 1188 قضية بنجاح من مجموع 1515 قضية مسجلة، مع توقيف 1512 متورط. ولأن الأطفال هم من أكثر الفئات العمرية تضررًا من الجريمة الإلكترونية، فقد قامت قيادة الدرك الوطني بمجموعة من البرامج التوعوية بالتنسيق مع وزارة التربية الوطنية، من خلال دروس التوعية في المدارس التي أُجريت فيها تلك البرامج كخطوة أولى نحو زيادة وعي الطلاب بمخاطر الجريمة الإلكترونية وحمايتهم منها[1].

المطلب الثاني: الآليات المؤسساتية الدولية في مكافحة الجريمة الالكترونية

من بين الخصائص التي تتميز بها الجريمة الالكترونية خاصية تعديها لحدود الدولة الواحدة، مما فرض ضرورة إيجاد آليات دولية يستطيع من خلالها مكافحة هذه الجريمة والقبض على مرتكبيها أينما وجدوا. ومن بين تلك الآليات: المنظمة الدولية للشرطة الجنائية "الانتربول" (الفرع الأول)، والتعاون الدولي ومختلف ميكانيزماته التي تعد ضرورية لمواجهة هذه الجريمة (الفرع الثاني).

الفرع الأول: المنظمة الدولية للشرطة الجنائية – الأنتربول.

أولًا: نشأة المنظمة الدولية للشرطة الجنائية.

الأنتربول بالإنجليزية Interpol هي اختصار لكلمة "الشرطة الدولية" بالإنجليزية police International والاسم الكامل لها هو منظمة الشرطة الجنائية الدولية، وباللغة الإنجليزي International Criminal Police Organization. وهي أكبر منظمة شرطة دولية، أنشئت في 1924، مكونة من قوات شرطة لـ 190 دولة، مقرها الرئيس في مدينة ليون الفرنسية، وللمنظمة أربع لغات رسمية هي: العربية، الإنجليزية، الفرنسية، الإسبانية. وهي تعتبر هيئة تتمثل في حكومات اتفقت مع بعضها لتكوين جبهة ضد الجريمة، وكانت هذه الهيئة تسمى في البداية اللجنة الدولية

[1]- شنتير خضراء: مرجع سابق، ص. 201.

للشرطة الجنائية، ثم أصبحت تسمى اللجنة الدولية الثانية للشرطة الجنائية، وتحولت فيما بعد إلى المنظمة الدولية للشرطة الجنائية – الانتربول[1].

فيما يرى البعض أن أصل نشأة منظمة الانتربول يعود إلى عام 1904، بمناسبة الاتفاقية الدولية الخاصة بمكافحة الاتجار الرقيق التي نصت على إنشاء سلطة تُركّز لديها المعلومات الخاصة باستخدام الاتفاقية الدولية الخاصة بمكافحة الاتجار بالرقيق، التي نصت على إنشاء سلطة والتي نص على إنشاء سلطة تركز لديها المعلومات الخاصة بإستخدام النساء والفتيات لفرض الدعارة بالخارج. ولهذه السلطة الحق في أن تخاطب مباشرةً مع الإدارة المتصلة لها في كل الدول الأطراف وتطبيقًا لهذه الاتفاقية، تم إنشاء جهاز دخل أمريكا الجنوبية عام 1905، حيث كانت مهام هذا الجهاز تنسب إلى حد كبير لمهام المنظمة الدولية للشرطة الجنائية[2].

ثانيا: مفهوم منظمة الأنتربول

هي منظمة دولية حكومية ذات طبيعة اجتماعية، أنشئتها مجموعة من الدول للإشراف على وسائل التعاون الدولي الشرطي سنة 1924 تتمتع بالإرادة المستقلة والشخصية القانونية الدولية الوظيفية، وتتكون من أجهزة دائمة. فالأنتربول منظمة فنية متخصصة تهدف إلى تدعيم التعاون الدولي في مجال الشرطة، ودولية لأن العضوية فيها مفتوحة لكل دول العالم التي تقبل الالتزام بما جاء في نظامها الأساسي، كما أنها لا ترتبط بإقليم معين ونشاطاتها تمتد لكل أنحاء العالم[3].

[1]– عائشة عبد الحميد: "النظام القانوني للمنظمة الدولية للشرطة الجنائية الإنتربول ودورها في مجال التعاون القضائي الشرطي"، المجلة الأكاديمية للأبحاث والنشر العلمية، ص. 03.

[2]– غنيم عبد الرحمن علي إبراهيم: "مضمون انضمام دولة فلسطين في المنظمة الدولية للشرطة الجنائية الإنتربول"، مجلة الفقه والقانون، مجلد 75، 2019، ص. 73.

[3]– قسميه محمد: "الوسائل التقنية الدولية للشرطة الجنائية الإنتربول كآلية للتعاون الدولي الشرطي"، جامعة الجزائر، مجلة جامعة محمد بوضياف – الجزائر، مج 34، ع 2، 2020، ص. 126.

كما تُعرف على أنها منظمة تعمل على تمكين أجهزة الشرطة في كافة أنحاء العالم من العمل معا، وذلك لجعل العالم أكثر أمانا، بالإضافة إلى تقديم الدعم الميداني لمواجهة التحديات الإجرامية التي يشهدها القرن الحادي والعشرون[1].

فهي هيئة مستقلة لها كيانها وشخصيتها، تلعب دور الوساطة بين الدول فيما يتعلق بالبحث عن المجرمين وتبادل المعلومات الجنائية، وتهتم أساسا على تنمية كمية المساعدة الجنائية الدولية المتبادلة على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين المعمول بها في مختلف الدول ويروج الإعلان العالمي لحقوق الإنسان، كما تقوم بإعداد وتأطير كل الهيئات القادرة على المساهمة بكل فعالية في الوقاية وقمع مختلف جرائم القانون العام[2].

ثالثا: تكوين المنظمة الدولية للشرطة الجنائية الانتربول

تتكون المنظمة الدولية للشرطة الجنائية من:

الجمعية العامة: تعتبر الجهاز السياسي للمنظمة، فهي أعلى هيئات المنظمة.

اللجنة التنفيذية: هي الجهاز الثاني للمنظمة، وهي المنفذة لقرارات وتوصيات الجمعية العامة ومتابعة تنفيذها، وهي لجنة يترأسها رئيس المنظمة.

الأمانة العامة: تعتبر الجهاز التنفيذي الدائم للمنظمة (الانتربول)، حيث تقوم بدور داخلي متخصص في مكافحة جرائم الحق العام، كما أنها مكلفة بالإشراف على تطبيق قرارات الجمعية العامة واللجنة التنفيذية.

المستشارون: وهم الخبراء المكلفون بدراسة المسائل العلمية، وقد نصت عليهم المادة 24 من دستور المنظمة، حيث إنه يُسمح لمنظمة الأنتربول الاستعانة برأي المستشارين في الأمور العلمية المتعلقة بمكافحة الجريمة المنظمة[3].

[1]- غنيم عبد الرحمان علي إبراهيم: مرجع سابق، ص 75..

[2]- غنيم عبد الرحمان علي إبراهيم: مرجع سابق، ص 126. .

[3]- عائشة عبد الحميد: مرجع سابق، ص. 04..

رابعا: الطبيعة القانونية للمنظمة الدولية للشرطة الجنائية

ذهب الى تحديد الطبيعة القانونية للانتربول إلى اتجاهين: الاتجاه الأول يرى أنها من أشخاص القانون الخاص، أي أنها غير حكومية، وذلك بالاعتبارات التالية: قرارات المجلس الاقتصادي والاجتماعي التابع لهيئة الأمم المتحدة لسنة 1949، الذي اعتبر فيها المنظمة غير حكومية وذات طابع استشاري. بينما الاتجاه الثاني يرى أن المنظمة الدولية الجنائية عبارة عن منظمة دولية حكومية، وبالتالي فهي تتكون من أشخاص القانون الدولي العام، الذي يقوم على عدة عناصر يجب توافرها، وهي الكيان المميز الدائم والإرادة الذاتية[1].

خامسا: مهام منظمة الانتربول

تتمثل مهمتها في تسهيل تبادل المساعدات بين جميع السلطات الأمنية، مما يزيد من قدرة أجهزة الشرطة على التواصل بينها بشكل مأمون في جميع أنحاء العالم، ويتيح إمكانية الاطلاع على البيانات والمعلومات الشرطية في جميع أنحاء العالم. كما تقدم الدعم المعلوماتي في مجالات إجرامية محددة ذات أولوية، وتسعى إلى التبرير المستمر لقدرات الشرطة على منع الجريمة ومكافحتها، وتطوير المعارف والمهارات اللازمة لعمل الشرطة على الصعيد الدولي بشكل فعال[2].

كما تقوم المنظمة باستخدام شبكة اتصالات مؤمنة تغطي كافة أنحاء العالم من أجل القيام بمهمتها في مكافحة الجريمة، حيث تسهل التنقل السريع بين الوسائل الإلكترونية والتي تشمل الوسائل المكتوبة والصور الفوتوغرافية والبصمات. ومن أجل ذلك تم إنشاء مراكز اتصالات إقليمية في طوكيو ونيوزيلندا والنيروبي لتسهيل مرور الرسائل. كما يوجد نوعان من أنظمة الاتصال داخل هذه الشبكة. بخصوص الأول الدول المركزية حيث تُجرى الاتصالات العالمية للشرطة من خلال الجمعية العامة والشرطة التنفيذية بواسطة الأمانة، ويجري مرور كافة الرسائل غير المكانية الوطنية الموجودة في كل من

[1]- حليمة خراز: المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب، الدراسات القانونية المقارنة، مج 1216، ع 2، جامعة حسين بوعلي الشلف، كلية الحقوق والعلوم السياسية، مخبر القانون الخاص، ص 153.

[2]- عبد المنعم أبقال: راهن الأجهزة الأمنية وتحديات الجريمة الإلكترونية. مجلة المنارة للدراسات القانونية والإدارية، ع 12، 2016، ص 154.

داخل الأعضاء، وتعمل هذه المكاتب على تنسيق المعلومات فيما بين أجهزة الشرطة ووكالاتها المختلفة داخل الدولة[1].

كما تعمل المنظمة على تبادل الخبرات والمساعدة التقنية، بما يشمل العناصر الإدارية الفنية والقدرات التقنية لأجهزة العدالة، وكذلك تحليل ونشر البيانات والمعلومات وتنسيق الجهود بين الدول الأعضاء، خاصة في مسألة ملاحقة المجرمين، حيث وضعت الأمانة العامة للانتربول بين يدي الدول الأعضاء مجموعة من الهيئات التقنية والتكنولوجية الحديثة لمكافحة الجريمة وملاحقة المجرمين، أهمها منظومة الاتصالات انتربول 24/7، وقد تمكن المكتب المركزي الوطني للانتربول الجزائر من تحقيق الربط بهذه المنظومة بتاريخ 21 اوت 2003 [2].

سادسا: جهود المنظمة الدولية للشرطة الجنائية الانتربول

تُفسر الجريمة الإلكترونية المرتكبة عبر الإنترنت ضمن الجرائم العابرة للدول، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر، كما وقد يكون الضرر في بلد ثالث في ذات الوقت. ونظرا لهذه الخصوصية، فقد أصبح التعاون الدولي أمرا ضروريا، ويتعين الإشادة بمجهود الانتربول في هذا المجال من خلال ضبط الارتباطات المتواجدة في معظم دول العالم، والمكلفين بتوفير قاعدة ببيانات ضخمة يمكن أن تشكل نقطة انطلاق لمكافحة الجرائم الإلكترونية[3].

وساهمت أيضا منظمة الشرطة الجنائية الدولية "انتربول" في مكافحة الجريمة المنظمة من خلال تزويد الدول الأعضاء بمعلومات مهمة عن المجرمين المطلوبين للعدالة، مركزة اهتمامها على الجريمة المنظمة ذات الصلة بغسيل الأموال، وعقدت هذه المنظمة عدة اجتماعات وندوات حول جريمة

[1]- حليمة خراز: مرجع سابق، ص 159.

[2]- قسيمة محمد: مرجع سابق، ص 127.

[3]- أنيس بن علي العذار: مكافحة الجريمة الإلكترونية، الصعوبات والحلول القضائية. عين 13، وزارة العدل، 2017، ص 414.

المعلوماتية في 19 إلى 20 أبريل 1995، حيث تم اتفاق الدول الأعضاء على اتخاذ قرار يتعلق بمكافحة الجرائم المالية عبر الدول وتعزيز التعاون الدولي[1].

ومن بين الإنجازات التي حققتها الانتربول في ظل مواجهة الجرائم المعلوماتية، تلك العملية التي قامت بها المباحث الفيدرالية الأمريكية بالاشتراك مع الانتربول والمتعلقة بملاحقة الشخص الذي قام بنشر "دودة الحب" عبر الإنترنت في الفلبين، وكذلك العملية التي قامت بها شرطة الانتربول بالاشتراك مع المباحث الفيدرالية وكذلك الشرطة الإنجليزية عام 1998 والتي أحرزت إنجازات كبيرة[2].

سابعا: – دور الانتربول في مكافحة الجريمة الالكترونية

لما كانت الجريمة الالكترونية ذات طابع عالمي يمكن أن تتعدى آثارها عدة دول، فإن ملاحقة مرتكبيها وتقديمهم للمحاكمة وتوقيع العقاب عليهم يتطلب ضرورة التعاون بين الدول للقبض على المتهمين أو لجمع الأدلة أو سماع الشهود أو اللجوء إلى الإنابة القضائية أو تقديم المعلومات التي يمكن أن تساهم في تحقيق ذلك[3].

وهذا ما نصت عليه الاتفاقية الأوروبية لجرائم الانترنت وأكدت عليه، لكونه أصبح يمثل إحدى الضروريات اللازمة لمواجهة هذه الأنشطة الإجرامية المستحدثة على نحو يتكامل مع دور القوانين الوطنية وتجدر الاشارة إلى أنه لم يعد يُنظر إلى ذلك التعاون باعتباره يعيق سيادة حقوق الدول، بقدر ما أصبح يعني التفاهم بين سيادات دول مختلفة ترمي جهودها إلى تشديد وتفعيل حلقات مكافحة الجريمة بوجه عام والجريمة عبر الوطنية بوجه خاص[4].

[1]– رزيقة خرير: واقع مكافحة الجريمة الإلكترونية. كلية العلوم والاتصال، مجلة الحكمة للدراسات الإعلامية والاتصالية، مج 2017، ع 10، مؤسسة كنوز للنشر والتوزيع، الجزائر، 2017، ص 7.

[2]– الطاهر ياكر: مكافحة الجرائم الإلكترونية بين التشريعات الوطنية. مجلة الهدى للدراسة القانونية والسياسية، مج 04، ، ع 04 جامعة الجيلالي بن عمار، خميس مليانة، الجزائر، 2022، ص 15.

[3]– سعد عاطف عبد المطلب حسين: مرجع سابق، ص 530.

[4]– المرجع نفسه: ص ص 530–531.

كما تهدف المنظمة الدولية للشرطة الجنائية إلى دعم أجهزة الشرطة في العالم، وذلك من خلال توفير المعلومات والبيانات التي يمكن تبادلها فيما بين الدول، استنادا إلى قوة اتصال مأمونة، وذلك بفرض تسهيل تبادل وتحليل المعلومات، وهو ما يساهم بشكل كبير في القضاء على الجماعات الإجرامية المنظمة، ويرفع من فاعلية التعاون الأمني بين الدول في هذا المجال[1].

ومثال ذلك عملية نسقها الأنتربول في منطقة آسيا والمحيط الهادي، تسمت بـ first lighte 2015، شاركت به 23 بلدا، تم خلالها اعتقال أكثر من 500 شخص، وإغلاق 15 مركزا للاتصالات. استهدفت هذه العملية أشخاصا قاموا بعملية احتيال ارتكبت بواسطة الهاتف والبريد الالكتروني، قُدّرت قيمتها بملايين الدولارات[2].

وفي سنة 2016 قام الأنتربول والهيئة النيجيرية للجرائم الاقتصادية، بعملية في إطار مشاركة للقضاء على زعيم شبكة إجرام دولية في نيجيريا اسمه مايك، اشترك معه ما لا يقل عن 40 شخصا من نيجيريا وماليزيا وجنوب أفريقيا، قاموا بآلاف عمليات الاحتيال عبر الانترنت، والتي استهدفت مئات الضحايا في جميع أنحاء العالم، مستعملين مختلف مخططات الاحتيال التجارية عبر البريد الالكتروني[3].

اليوروبول والاوروجست آليتين إقليميتين لمكافحة الجرائم الإلكترونية

أولا: اليوروبول

هو جهاز أمني على مستوى الاتحاد الأوروبي، مقره مدينة لاهاي في هولندا، وقد تم تأسيس اليروبول في معاهدة مانستريخيت عام 1992، يكون بمثابة حلقة وصل بين الشرطة الوطنية في مختلف الدول الأعضاء في الاتحاد بهدف تسهيل عملية الملاحقة للجرائم العابرة للحدود[4].

[1]- عائشة عبد الحميد: مرجع سابق، ص 9.

[2]- شنتير خضراء: مرجع سابق، ص 213.

[3]- المرجع نفسه: صفحة 213.

[4]- عبد المنعم أنفال: مرجع سابق، ص 155.

وتقوم وظيفة وكالة تطبيق القانون الأوروبية "اليروبول" بحفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في مجال مكافحة الجرائم الدولية الكبيرة والإرهاب، وهي تعمل بشكل وثيق مع دول الاتحاد الأوروبي ودول من خارج الاتحاد كولايات المتحدة الأمريكية وغيرها. ولا يملك ضباط اليوروبول صلاحيات مباشرة للإيقاف والاعتقال، ولكنهم يقومون بدعم الضباط العاديين بالقيام بجمع المعلومات وتحليلها وتوزيعها، بالإضافة إلى تنسيق المهام المشتركة[1].

ولأجل المكافحة الفعالة للجريمة الإلكترونية، قام اليروبول بإنشاء مراكز ووحدات تابعة له على غرار الفريق العام المعني بالجريمة الإلكترونية السيبرانية European Union Cybercrime Task Force التابع للاتحاد الأوروبي، والذي تم تشكيله سنة 2010 داخل اليوروبول بهدف توظيف منصة لإدارة التحقيق والملاحقات القضائية في مجال الجريمة الإلكترونية، والتطوير، وتحفيز نهج منسق داخل الاتحاد الأوروبي لمكافحة الجرائم الإلكترونية، وجعل الفضاء الإلكتروني مكانًا أمنا لمواطني الاتحاد الأوروبي وممارساته وحكوماته[2].

ثانيًا: الاوروجست

وحدة التعاون القضائي الأوروبي، قدمت الفكرة لأول مرة في اجتماع المجلس الأوروبي في نامبري، فنلندا، في أكتوبر 1999، حيث تأسست على أساس التضامن في تقرير معالجة الجريمة العابرة للحدود من خلال تقرير التعاون بين السلطات القضائية بالاتحاد الأوروبي. وكانت هجمات 11 سبتمبر في الولايات المتحدة الأمريكية المحفز لإضفاء الطابع الرسمي عليها من خلال قرار المجلس الأوروبي عام 2002 بإنشاء **الاوروجست** كوحدة للتنسيق القضائي[3].

فبدأت عملها رسميًا في الفاتح من شهر مارس سنة 2001، وبعد هجمات الحادي عشر من شهر سبتمبر 2001 التي شهدتها الولايات المتحدة الأمريكية، زاد التركيز على مكافحتها للإرهاب، ولم يعد الأمر يُنسب إلى المجال الوطني والإقليمي فقط، بل تعداه ليشمل البعد الدولي، مما دفع المجلس

[1]- عبد المنعم أبقال: مرجع سابق، ص 155.

[2]- المرجع نفسه، ص 155.

[3]- عبد المنعم أبقال: المرجع نفسه، ص 156.

الأوروبي إلى إصدار قرار في الثامن والعشرين من شهر فبراير سنة 2002. مهمتها، كما جاء في المادة 85 من معاهدة لشبونة، دعم وتطوير التنسيق والتعاون بين السلطات الوطنية المؤسسة على التحقيق في الجرائم الخطيرة التي تمس دولة أو أكثر من الدول الأعضاء أو مقاومتها على أساس مشترك[1].

وتتجلى مهمتها أيضًا في ملاحقة المجرمين فيما يتعلق بالإجرام الخطير العابر للحدود الوطنية، والذي يؤثر على دولتين أو أكثر من الدول الأعضاء في الاتحاد الأوروبي. وتعمل اليوروجيست على مكافحة جرائم الإرهاب، والاتجار الدولي بالمخدرات، وغسل الأموال، والجرائم الإلكترونية، والمنظمات الإجرامية، وتقدم المساعدة في أنواع أخرى من الجرائم بطلب إحدى الدول الأعضاء المساعدة في التحقيقات والملاحقة القضائية[2].

ولليوروبول دور فعال في مكافحة الجرائم الإلكترونية، حيث يقوم بتسهيل التحقيقات المرتبطة بوقائع بث أو امتلاك محتويات إباحية عبر الإنترنت بين الدول الأوروبية، ونجد الإشارة إلى ملفات التحليل الغنية بالمعلومات المبلّغة من قبل سلطة التحقيق التابعة للدول الأطراف في الاتحاد الأوروبي، والتي تمثل وسيلة هامة في عمل المحققين وفي مكافحتهم للشبكات الإجرامية، ومن أمثلتها ملف تحليل الدعارة عبر الإنترنت[3].

أما **الاوروجست** فتتمثل دوره في تحسيس، وتنسيق، والتعاون بين السلطات القضائية للدول الأطراف، وتبادل المعطيات بين الدول الأعضاء في الاتجاه الأوروبي، وكذا التحفظ عنها، كما يمكنه أن يطلب من الوكلاء العاملين ذوي الاختصاص الوطني إجراء تحقيقات أو ملاحقات أو التبليغ عن الجرائم إلى سلطات المحكمة للدول الأطراف[4].

الفرع الثاني: التعاون الدولي ودوره في مكافحة الجريمة الإلكترونية

[1]- شنتير خضرة: مرجع سابق، ص 250

[2]- المرجع نفسه: ص 156.

[3]- سعد عاطف عبد المطلب حسين: مرجع سابق، ص 536.

[4]- سعد عاطف عبد المطلب حسين: مرجع سابق، ص 537.

أولًا: مفهوم التعاون الدولي

التعاون يعني العون المتبادل، أي تبادل المساعدة والعون لتحقيق هدف معين، وقد دعا الإسلام إلى التعاون ونص عليه كمبدأ عام عند كل الجماعات الإنسانية، فهم يتعاونون فيما بينهم لتحقيق أهداف أو خدمات أو حل مشكلة مشتركة لتحسين أحوالهم المختلفة، حيث خلق الله سبحانه وتعالى الحياة وهي متواصلة الأطراف متماسكة الشؤون، يسمى الناس فيها سد جوانب العجز والنقص في ذاتهم، وكثيرًا ما يلجأ الأفراد إلى الاستعانة بآخرين من أجل قضاء حوائجهم، لأن الإنسان بطبعه لا يستطيع العيش بمفرده[1].

وهذا المعنى العام للتعاون هو الذي حث عليه القرآن الكريم في قوله تعالى: "وتعاونوا على البر والتقوى ولا تعاونوا على الإثم والعدوان واتقوا الله إن الله شديد العقاب"، وحث عليه النبي صلى الله عليه وسلم في قوله: "والله في عون العبد ما كان العبد في عون أخيه"، وقوله: "المسلم أخو المسلم لا يظلمه ولا يسلمه"[2].

ثانيًا: أسس التعاون الأمني الدولي في مكافحة الجرائم الإلكترونية

- التعاون العلمي لبحث ظاهرة جرائم الإنترنت
- التنسيق بين المؤسسات الأمنية بآلياتها المختلفة في الساحات الأمنية الإقليمية والدولية
- تحديد سبل التعاون في مجال التدريب والتعاون التقني
- إعداد مدونة دولية تتضمن توحيد المعايير والأركان القانونية
- وضع استراتيجيات وقائية قادرة على خلق مناخ ملائمة لأعمال المكافحة[3]

ثالثا: أهم صور التعاون الدولي:

[1]- عادل عبد العالي إبراهيم خراشي: آليات التعاون الدولي في مكافحة الجرائم المعلوماتية والسبل التغلب عليها. دار الجامعة الجديدة للنشر، خلية الشريعة والقانون بالقاهرة، 2015، ص 180.

[2]- عادل عبد العالي إبراهيم خراشي: مرجع نفسه: ص 181.

[3]- عادل عبد العالي إبراهيم خراشي: مرجع سابق، ص 192–193.

تتميز الجريمة الإلكترونية بالعالمية وبكونها عابرة للحدود، فإن مكافحتها تتحقق بتعاون دولي، وقد أسس الأنتربول عدة مراكز للاتصالات الإقليمية في كل من طوكيو، نيوزيلندا، نيروبي، أذربيجان، بيونس آيرس، لتسهيل مرور الرسائل المختلفة، بالإضافة إلى قيام المجلس الأوروبي في لوكسمبورغ عام 1991 بإنشاء الشرطة الأوروبية لملاحقة الحياة في الجرائم العابرة للحدود، ومنها الجرائم المتعلقة بالإنترنت[1].

بالإضافة إلى القيام ببعض العمليات الشرطية والأمنية المشتركة، وذلك من خلال تفشي الجرائم الإلكترونية وتحقيق الأدلة الرقمية وضبطها، والقيام بعملية تنسيق عابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكة الاتصال بحثًا عما قد تحتويه من أدلة وبراهين على ارتكاب الجريمة الإلكترونية، كلها أمور تستدعي القيام ببعض العمليات الشرطية والأمنية المشتركة[2].

رابعا: مظاهر التعاون الدولي في مكافحة الجريمة الإلكترونية

تنظيم الدورات التدريبية للعاملين فيها، وهي تهدف لتقريب وجهات التطور وتوفير المفاهيم بين المشاركين في مكافحة الجريمة الإلكترونية في الدول المختلفة، من خلال تبادل الخبرات وطرح موضوعات ومشكلات للتدارس المشترك، والتعرف على أحدث التطورات في مجال الجريمة الإلكترونية وأساليب مكافحتها[3].

كذلك نصت عليه الاتفاقية الأوروبية ببيودابست في المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة، وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر،

[1]- ثامر علي النويران: الجرائم الالكترونية الحد منها تجربة الأردن، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC كلية العلوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية السعودية ، المملكة العربية السعودية، الرياض، 2015، ص 178.

[2]- عادل عبد العالي ابراهيم خراشي: مرجع سابق، ص 194.

[3]- الهادي خضراوي: تجربة الجزائر في مكافحة الجريمة الالكترونية، المؤتمر الدولي الأول في مكافحة الجريمة المعلوماتية ICACC جامعة الإمام محمد بن سعود الإسلامية السعودية ، المملكة العربية السعودية، الرياض، 2015، ص 169.

الذي ينوي الطرف الطالب مساعدته أن يقدم طلبًا للمساعدة بغرض التفتيش والدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها[1].

خامسا:الصعوبات التي تعيق التعاون الدولي في مكافحة الجريمة الإلكترونية

أ- التجريم المزدوج في تسليم المجرمين:

هذا الشرط في نظام تسليم المجرمين عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، لاسيما وأن معظم الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبات أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تطبق على الجرائم المتعلقة بشبكة الإنترنت، الأمر الذي يعيق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين ويحول دون جمع الأدلة ومحاكمة مرتكب الجرائم المتعلقة بالإنترنت[2].

ب- تنوع واختلاف النظم القانونية الإجرائية:

من بين تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحدي والتحقيق والمحاكمة التي تثبت فائدتها وفعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى، أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية والتسليم المراقب والعمليات المنتشرة، وغيرها من الإجراءات الشبيهة. فإذا اعتُبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى[3].

[1]- جمال محمد خلفان محمد النقبي واخرون: التعاون الوطني والدولي في الجرائم الالكترونية المشكلات والحلول، مجلة المعهد العالي للدراسات النوعية، مج 3، ع 16 ، 2023، ص 5480.

[2]- محمد صفاء الدين علي شرشر: الجهود الدولية والتشريعية لمكافحة جرائم الانترنيت، مجلة البحوث القانونية والاقتصادية، مج 54، ع 03، اكتوبر 2021، ص 587.

[3]- وائل محمد عبد الرحمان نصرات: الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها، المؤتمر الدولي في مكافحة الجرائم المعلوماتية ICACC، كلية العلوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية السعودية ، المملكة العربية السعودية، الرياض، 2015، ص 177

وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة السلطات في إنفاذ القانون في الدول الأخرى على استخدام ما تعتبره هي أداة فعالة[1].

ج- مشكلة الاختصاص في الجرائم المتعلقة بالجريمة الإلكترونية:

يقصد بالاختصاص السلطة التي يقررها القانون في أن ينظر في دعاوى من نوع معين حدده المشرع، والأصل أن يُنسب هذا الاختصاص إلى القضاء الحاكم بأن يعود موضوعه لتحمله سلطة الفصل في الدعاوى. اختلاف التشريعات والنظم القانونية قد ينجم عنه تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت، التي تتميز بكونها عابرة للحدود[2].

يظهر تنازع الاختصاص القضائي في تقديم الدعوى عن ذات الجريمة وعدة جرائم مرتبطة من جهتين من جهات التحقيق والحكم، كلٌ يجهد في إثبات اختصاصه، وهو ما يسمى بتنازع الاختصاص الإيجابي، أو أن تتنصل كلا الجهتين من النظر على أساس عدم الاختصاص، وهو ما يسمى بتنازع الاختصاص السلبي[3].

د- عدم وجود قنوات اتصال.

إن من أهم الأهداف الموجودة في التعاون الدولي في مجال الجريمة والمجرمين هو الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لازمًا أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع أدلة معينة أو معلومات مهمة. فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العلمية التي غالبًا ما تكون مفيدة في التحري لجرائم معينة ولمجرمين معنيين، وبالتالي تتقدم الفائدة من هذا التعاون[4].

سادسا: حل الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة الإلكترونية.

- حل العقبة المتعلقة بالمساعدة القضائية الدولية

[1]- وائل محمد عبد الرحمان نصرات :مرجع سابق، ص 177..

[2]- محمد صفاء الدين علي شرشر: مرجع سابق ص 577.

[3]- المرجع نفسه، ص 577.

[4]- البركة الطيبي: إشكالية الإثبات في الجرائم الالكترونية، مجلة أفاق علمية ، مج 11، ع 1، جامعة أدرار 2019، ص 279.

- حل عقبة تنوع واختلاف النظم القانونية الإجرائية
- حل عقبة عدم وجود قنوات اتصال
- حل عقبة الاختصاص في الجرائم الإلكترونية[1]

سابعا: التعاون الدولي في مجال تسليم المجرمين:

يعد مبدأ تسليم المجرمين وسيلة من وسائل التعاون الدولي، فهو يُعد من أقدم الوسائل وأكثرها فعالية في تحقيق مردود إيجابي، ليكمن في اراد المجرم السيبيراني من الدولة المطلوب منها التسليم. إذ يُقصد به قيام دولة ما بتسليم شخص موجود على إقليمها إلى دولة أخرى (الدولة طالبة التسليم) بناءً على طلبها، بغرض محاكمته عن جريمة نسب إليه ارتكبها، أو لتنفيذ حكم صدر ضده من محاكمها[2].

فالجرائم الالكترونية تهدد استقرار التعاملات الإلكترونية وأمن المعلومات، لذا فإن الاتفاق على تبادل تسليم المجرمين بين الدول حول هذه الجرائم يُعد ضرورة مُلحة، وهذا ما نصت عليه اتفاقية بودابست في المادة 54 منها، حيث أكدت هذه المادة على ضرورة أن تلتزم الأطراف المتعاقدة بإدراج هذه الجرائم بوصفها جرائم تستوجب تسليم المجرمين[3].

ثامنا: التعاون الدولي في مجال التدريب:

ويقصد بتدريب رجال العدالة هي تلك العملية التي يُحظى بها وتصمم لها البرامج، وتُبادل فيها الجهود والأموال لتوفير السلوك للعاملين في أجهزة العدالة، سواء كانوا من القضاء أو من رجال السلطة القائمين على تنفيذ القانون أو من الموظفين المتعاونين مع تلك الأجهزة كخبراء أو غيرهم. حيث تهدف هذه العملية إلى تطوير سلوكهم ورفع مستوى مهاراتهم واتجاهاتهم بما يكفل حسن إنجاز العمل القانوني والقضائي والتنفيذي[4].

---

[1]- وائل محمد عبد الرحمان نصرات :مرجع سابق، ص 174.

[2]- علي حمزة عسل الخفاجي، مرجع سابق ص 185.

[3]- الهادي خضراوي: مرجع سابق، ص 168.

[4]- علي حمزة عسل الخفاجي، مرجع سابق ص 191.

تاسعا: أهمية التعاون الدولي ودوره في مكافحة الجريمة الإلكترونية:

تتضح أهمية التعاون الدولي من خلال تبني قضية متطورة لإجراءات التحريات والتحقيقات في مجال مكافحة الجريمة الإلكترونية باستخدام التكنولوجيا الحديثة، مثل انتقال الدوائر التلفزيونية، واستعمال أساليب خاصة بالتحري والمراقبة، واستخدام قنوات الاتصال والتنسيق الأمني والقضائي بين حماة القضاء المختصين عن طريق الأقمار الصناعية والشبكة الإلكترونية لتبادل المعلومات سريعًا. وانتقال القاضي إلى الدولة المعينة للتحقيق واتخاذ ما يراه من إجراءات، ليس فقط في مرحلة التحقيق الابتدائي بل وفي المرحلة العامة أيضًا[1].

المبحث الثاني: إجراءات متابعة الجريمة الإلكترونية.

نظرًا للطبيعة الخاصة التي تتمتع بها الجريمة الإلكترونية، كونها جريمة حديثة النشأة وتتمتع بخصوصية من حيث مرتكبها والوسائل المستعملة في ارتكابها والمحل الذي تقع عليه، فقد أمسى من الضروري إيجاد إجراءات حديثة وفعالة في البحث والتحري ومتابعة الجريمة الإلكترونية. حيث إن الوسائل القديمة والتقليدية بالرغم من أنها لا زالت عاجزة في شكلها الحالي عن مواكبة سرعة تطور وسائل الإجرام الإلكتروني ودقته، إلا أنها لا تزال تُستعمل، ولكن لن نقول إنها ناجعة ما لم يتم تدعيم جهات البحث والتحري بأدوات ووسائل جديدة تكون متوافقة مع طبيعة تلك الجريمة. ولذلك، قمنا بتقسيم دراستنا في هذا المبحث إلى مطلبين، حيث سنتحدث في المطلب الأول عن الإجراءات التقليدية للحصول على الدليل المعلوماتي، وفي المطلب الثاني سنتحدث عن الإجراءات الحديثة للحصول على الدليل المعلوماتي[2].

[1]- جمال محمد خلفان محمد النقبي واخرون: مرجع سابق، ص 5472.

[2]- بن بادة عبد الحليم: مرجع سابق، ص 77.

المطلب الأول: الإجراءات التقليدية للحصول على الدليل المعلوماتي.

من المعلوم أن الأنظمة الإجرائية لمختلف الدول تحتوي على مجموعة من الأساليب والوسائل التقليدية التي تلجأ إليها سلطات البحث والتحري للكشف عن مختلف الجرائم مثل الخبرة والتفتيش، حيث تعتبر تلك الوسائل من الأساليب العامة والتقليدية المستعملة في التحقيق في أي جريمة كانت.

ونظرًا لاختلاف الجريمة الإلكترونية عن غيرها من الجرائم، فإنه أصبح من الضروري إعادة تحيين تلك الوسائل التقليدية بما يتوافق مع الطبيعة الخاصة للجريمة المعلوماتية حتى تتمكن من إنتاج دليل يُعتمد عليه قضائيا[1].

الفرع الأول: التفتيش

يذهب أغلب فقهاء القانون الجنائي إلى القول بأن التفتيش هو أحد إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة خاصة، وذلك وفقًا للضمانات والقيود القانونية المقررة[2].

كما يُعرف أيضًا أن التفتيش هو إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يُعتبر من أهم إجراءات التحقيق لأنه غالبًا ما يُصفر عن أدلة مادية تؤيد نسبة الجريمة للمتهم[3].

أولًا: مدى قابلية مكونات وشبكة الحاسوب للتفتيش

تتكون نظم الحاسوب من مكونات مادية ومكونات منطقية:

1- تفتيش مكونات الحاسوب المادية:

الواقع أن تفتيش المكونات المادية للحاسوب بحثًا عن شيء يتصل بجريمة إلكترونية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها بدأ يدخل في نطاق التفتيش طالما تم وفقًا للإجراءات القانونية

---

[1]- المرجع نفسه، ص 78.

[2]- بن بادة عبد الحليم: مرجع سابق، ص78.

[3]- بوعنّاد فاطمة زهرة: مكافحة الجريمة الإلكترونية في التشريع الجزائري. مجلة الندوة للدراسة القانونية، ع. الأول لعام 2014، جامعة الجيلالي اليابس، سيدي بلعباس، ص 05

المقررة، بمعنى أن حكم تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، سواء من الأماكن العامة أو الأماكن الخاصة.

2- مدى خضوع مكونات الحاسوب المعنوية للتفتيش.

لقد ثار خلاف تشريعي وفقهي بشأن مدى جواز تفتيش المكونات المعنوية للحاسوب تمهيدًا لضبط الأدلة الإلكترونية.

فذهب الرأي الأول إلى جواز التفتيش لنظم الحاسوب لتشمل المكونات المادية وغير المادية، وعلى النقيض من ذلك، هناك رأي آخر يرى أنه إذا كانت الغاية من التفتيش هي كشف الحقيقة، فإن هذا المفهوم المادي لا ينطبق على الجرائم الإلكترونية. وقد جرّم المشرع الجزائري أفعال المساس بأنظمة المعالجة الآلية للمعطيات[1].

3- مدى خضوع شبكة الحاسوب للتفتيش عن بعد:

إن التطور الحاصل والظاهر في شبكة المعلومات وما نتج عنه من تواصل بين مختلف أقطار العالم لدرجة جعلت الكرة الأرضية قرية واحدة، كان له تداعيات سلبية، حيث استغل مجرمو الإنترنت تلك الإيجابية وحولوها إلى نقطة قوة في مجال جرائمهم. حيث أضفوا على الجريمة الإلكترونية صفة العبور للحدود، إذ صارت الجريمة تُرتكب في بلد، وتظهر نتيجتها في بلد آخر، وتُرتكب وسائلها في بلد ثالث. كل ذلك جعل سلطات البحث والتحري في حيرة من أمرهم، خاصة فيما يتعلق بالتفتيش، ولذا ظهرت فكرة التفتيش عن بعد. وللتوضيح أكثر سنتطرق إلى احتمالين[2]:

أ- الاحتمال الأول: في حالة اتصال حاسوب المتهم بحاسوب شخص آخر غير متهم داخل الدولة

ذهبت مختلف التشريعات المقارنة إلى الاعتراف بحق سلطات البحث والتحري في تمديد اختصاصها في التفتيش إلى حواسيب الأشخاص غير المتهمين، وذلك وفق الضوابط التالية:

[1]- بوعنّاد فاطمة زهرة: مرجع سابق، ص 05.

[2]- بن بادة عبد الحليم: مرجع سابق، ص80.

- إذا كان ذلك ضروريًا لكشف الحقيقة بشأن الجريمة محل البحث.
- إذا وجدت مخاطر تتعلق بضياع بعض الأدلة، نظرًا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث[1].

وقد أجاز المشرع الجزائري، بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التفتيش إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، فيجوز تمديد التفتيش بعد إعلام السلطات القضائية المختصة مسبقًا بذلك[2].

ب- الاحتمال الثاني: اتصال حاسوب آخر موجود خارج الدولة

ذهب الفقه إلى أن التفتيش الإلكتروني العابر للحدود يجب أن يتم وفق الاتفاقيات الثنائية بين الدول من أجل السماح بذلك، ولا يجوز القيام بالتفتيش العابر للحدود في غياب تلك الاتفاقيات أو على الأقل الحصول على إذن من الدولة الأخرى[3].

كما أن لجوء مرتكبي الجرائم المعلوماتية إلى نقل وتخزين المعلومات والبيانات في منظومة معلوماتية تتواجد خارج الإقليم تهربًا من إجراءات التفتيش، خلق تحديًا جديًا للسلطات القائمة بالتحقيق في البحث عن الأدلة، لأن تمديد التفتيش إلى إقليم دولة أخرى دون موافقتها يصطدم بمبدأ احترام سيادة الدولة.

وهو ما أثار خلافًا بين الفقهاء. غير أنه، خلافًا لذلك، جاءت المادة 32 من اتفاقية بودابست باستثناءات على هذا المبدأ، بإجازة التمديد دون الشروط الآتية (وجود اتفاقية أو ترخيص)، وذلك في حالتين هما:

[1]- مرجع نفسه ، ص 81.

[2]- بوعنّاد فاطمة زهرة: مرجع سابق، ص 5.

[3]- بن بادة عبد الحليم: مرجع سابق، ص81.

- الدخول على بيانات حاسوب مخزنة علنًا من مصدر مفتوح، بغض النظر عن تواجد البيانات جغرافيًا.
- حالة الدخول على بيانات حاسوب مخزنة موجودة في طرف آخر، أو أن يتلقاها عن طريق نظام حاسوب في إقليمه، وذلك في حالة حصول ذلك الطرف على الموافقة القانونية والطوعية من الشخص الذي له السلطة القانونية في الكشف عن البيانات من خلال نظم الحاسوب[1].

ما نراه من الاستثناء الثاني هو أن موافقة الشخص الذي له سلطة الكشف عن البيانات المطلوبة يُغني عن ضرورة وجود اتفاقية بين البلدين أو طلب الإذن من الدولة المتواجدة على إقليمها تلك البيانات.

غير أن المشرع الجزائري قيّد الحصول على المعلومات والبيانات التي تم نقلها خارج الجزائر بأن يكون بمساعدة السلطات الأجنبية المختصة، بحيث نصت المادة 55 من القانون 09-04 على أنه إذا تبين مسبقًا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقًا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقًا للاتفاقيات الدولية[2].

[1]- عبد القادر عميمر: اليات اثبات الجريمة المعلوماتية في التشريع الجزائري دراسة مقارنة، اطروحة دكتوراه، جامعة الجزائر1، الجزائر، 2019-2020، ص ص 297.298.

إتفاقية بودابست بشأن الجرائم المعلوماتية :هي أول معاهدة دولية تهدف إلى مكافحة الجرائم التي ترتكب عبر الإنترنت و ذلك من خلال:

-تنسيق التشريعات الجنائية بين الدول.

-تحسين إجراءات التحقيق و التعاون الدولي.

-توفر أطر قانونية لملاحقة مرتكبي الجرائم الإلكترونية.

الهيئة المصدرة:مجلس أوروبا (council Europe) هو الجهة التي أعدت و أصدرت الاتفاقية بالتعاون مع دول غير أوروبية مثل الولايات المتحدة و كندا أو اليابان.

سنة الإصدار :تم توقيع الإتفاقية في بودابست ؛هنغاريا بتاريخ 2001/11/23 و دخلت حيز التنفيذ في 2004/07/01

[2]- عبد القادر عميمر: مرجع سابق، ص 298.

ثانيًا: الشروط التقليدية لعملية التفتيش

نظرًا لخطورة التفتيش على حقوق الأفراد وحرياتهم وحرمة حياتهم الخاصة، فقد أحاطته التشريعات المقارنة ومن بينها التشريع الجزائري بجملة من الشروط والضوابط الموضوعية والشكلية التي يترتب على مخالفتها بطلان هذا الإجراء والآثار المترتبة عنه، ويوضح الشروط فيما يلي:

1- الشروط الموضوعية للتفتيش:

تتمثل الشروط الموضوعية للتفتيش حسب غالبية الفقهاء في ثلاثة شروط وهي السبب، المحل، الجهة المختصة بالتفتيش.

أ- وجود سبب للتفتيش:

من المتفق عليه بين الفقهاء أن سبب التفتيش هو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث[1].

فالسعي إلى التفتيش لا يكون منطقيًا إلا في حالة وقوع جريمة، سواء كانت جنحة أو جناية. ولا يكفي وقوع جريمة أن يكون وحده سببًا للقيام بالتفتيش، بل يجب أن تتوفر دلائل كافية تدعو للاعتقاد أن المشتبه فيه هو من قام بارتكاب هذه الجريمة أو ساهم في ارتكابها[2].

وبناء عليه، وتطبيقًا على الجرائم المعلوماتية، فلابد ليكون التفتيش مشروعًا أن نكون:

- بصدد جريمة معلوماتية واقعة بالفعل سواء كانت جنحة أو جناية.
- لابد من اتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة المعلوماتية أو المشاركة في ارتكابها.
- لابد من توفر أمارات قوية أو قرائن على وجود أجهزة أو أدلة معلوماتية تفيد في كشف الحقيقة لدى المتهم[3].

[1]- عبد القادر عميمر: مرجع سابق، ص 289.

[2]- المرجع نفسه، ص 289.

[3]- عادل بن عبد الله خميس المعمري، مرجع سابق، ص 13.

ب- وقوع الجريمة:

إن وقوع الجريمة شرط أساسي لإصدار الأمر بالتفتيش في الجرائم التقليدية، لأن مجرد الشك أو ورود معلومات إلى السلطات المختصة بإمكانات وقوع جريمة لا يعطيها الحق في إصدار الأمر بالتفتيش[1].

أما في جرائم المعلوماتية، فإن إضافة إلى هذا الشرط، يجب أن تكون الجريمة المرتكبة من نوع الجرائم المعلوماتية، فلا يمكن استغلال إذن بالتفتيش الخاص بجريمة من الجرائم التقليدية للبحث بواسطتها عن جريمة معلوماتية دون إذن خاص بذلك[2].

ج- أن تكون الجريمة جنحة أو جناية:

يشترط أن تكون الجريمة الجاري التفتيش بشأنها جنحة أو جناية، لأن المخالفة لا تستدعي إهدار حرمة الشخص أو مسكنه نظرًا لعدم خطورة الأفعال التي تشكلها المخالفة.

د- توافر دلائل كافية لنسبة الوقائع للمشتبه فيه في ارتكاب الجريمة او المشاركة في ارتكابها:

إن التفتيش لا يمكن أن يُؤذن به من طرف قاضي التحقيق إلا إذا توفرت لديه دلائل قوية ومتماسكة تفيد تورط المشتبه فيه في ارتكاب الجريمة أو المشاركة في ارتكابها، لأن مجرد وقوع جريمة.

هـ- وجود قرائن قوية على وجود محل الجريمة:

يشترط القانون لإجراء التفتيش أن توجد إشارات ودلائل كافية ترجّح ارتكاب الجريمة، فلا يجوز انتهاك حرمة الأشخاص وخصوصياتهم إذا لم يتوفر هذا الشرط.

2- الشروط الشكلية للتفتيش

[1]- عبد القادر عميمر: مرجع سابق، ص 289.

[2]- عبد القادر عميمر: مرجع سابق، ص 289.

أ- الإذن بالتفتيش:

بالرجوع إلى أحكام المواد 44 وما بعدها من ق إ ج ج، نرى أن الإذن بالتفتيش أمر لازم في جميع الأحوال سواء في حالة التلبس أو في غير أحوال التلبس، والسلطة المختصة بإصداره هي النيابة العامة ممثلة في شخص وكيل الجمهورية وقاضي التحقيق. وحددت المادة 44، الفقرة 13 من نفس القانون، البيانات التي يجب أن يتضمنها الإذن بالتفتيش تحت طائلة البطلان، وتتمثل هذه البيانات في تحديد موضوع الجريمة، عنوان المسكن المعني، على أن يتم الاستظهار بهذا الإذن قبل الشروع في التفتيش[1].

ب- القيام بالتفتيش من طرف السلطة المختصة:

يأخذ التفتيش في المنظومة المعلوماتية منحنيين، فإما أن يكون عملًا من أعمال التحقيق تقوم به السلطات القضائية المختصة، وإما أن يكون من أعمال الاستدلال الذي يقوم به ضباط الشرطة القضائية بأمر من السلطة المختصة أو تقوم به السلطات المختصة بالتحقيق، والتي يُقصد بها وكيل الجمهورية، قاضي التحقيق، وقاضي الحكم، وهذا ما يُستشف من المادة الخامسة من القانون 09-04[2] التي تضمنت عبارة "يجوز للسلطات المختصة وكذا ضباط الشرطة القضائية."

إلا أنه، ونظرًا لخصوصية الجريمة المعلوماتية والمهارات التي تتطلبها عملية التفتيش فيها، فقد أجاز المشرع الجزائري، بناء على الفقرة الأخيرة من المادة 5 من القانون 09-04، للسلطات المكلفة بالتفتيش تسخير كل من له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[3].

---

[1]- عبد القادر عميمر: مرجع سابق، ص 290.

[2]- المادة الخامسة من القانون 09-04 على انه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية في الحالات المنصوص عليها في المادة 04 أعلاه، الدخول إلى التفتيش ولو عن بعد إلى:

- المنظومة المعلوماتية او جزء منها وكذا المعطيات المخزنة فيها منظومة ترين معلوماتية

[3]- عبد القادر عميمر: مرجع سابق، ص 292.

ثالثا: آثار التفتيش

التفتيش هو إجراء من إجراءات التحقيق يمس الحرية الشخصية وحرمة الأماكن كما سبق توضيحه، وهو بذلك يهدف إلى الحصول على أدلة الجريمة، سواء كانت الأدلة معلوماتية في الجرائم المعلوماتية. ويترتب على التفتيش أثر مباشر وهو ضبط الأدلة المعلوماتية، حيث:

1- ضبط الأدلة:

يقصد بالضبط هو وضع اليد على الأدوات والأسلحة والأوراق الخاصة بالجريمة والتي لها دور في كشف الوقائع. أما الضبط في مجال المعلومات، فهو وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية أو المعلومات المتصلة بالجريمة المعلوماتية التي وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبها.ويُوجد نقد لهذا التعريف، لأن وضع اليد لا يكون فقط على الدعائم المادية المخزنة فيها المعلومات، لسبب واحد، وهو أن المعلومات قد تكون أحيانًا داخل الشبكة، أي عندما تكون في طريقها إلى محل إرسالها، ويكون ذلك عند مراقبة الاتصالات الإلكترونية[1].

والنتيجة الأساسية لإجراء التفتيش هو الضبط في محل الجريمة المعلوماتية، سواء كان هذا المحل جهاز الحاسوب أو الشبكة أو المراسلات البريدية الإلكترونية، فالضبط هو الأثر المترتب على الجريمة[2].

الفرع الثاني: المعاينة.

عرف جانب من الفقه المعاينة بأنها: "رؤية بالغة لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة". والأصل في المعاينة أنها إجراء من إجراءات التحقيق[3].

وينبغي التعامل مع مسرح الجريمة الإلكترونية على أنه مسرحان، وهما:

أولا: مسرح تقليدي

[1]- عادل بن عبد الله خميس المعمري، مرجع سابق، ص 14

[2]- عادل بن عبد الله خميس المعمري، مرجع نفسه، ص 15.

[3]- بوعنّاد فاطمة زهرة: مرجع سابق، ص 4.

يتمثل هذا المسرح من الجريمة المعلوماتية في الوسائل الموجودة والملموسة في المكان الذي ارتكبت فيه الجريمة، مثل أجهزة الإعلام الآلي، أقراص التخزين، الصور، البصمات.وبالتالي، فهذا المسرح لا يختلف عن المسرح في الجريمة التقليدية[1].

ويُعرف كذلك على أنه يقع خارج بيئة الحاسوب والإنترنت، ويتكون من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية يترك فيها الجاني آثاره كبصمات أو وسائل تخزين رقمية[2].

ثانيا: مسرح افتراضي

هذا المسرح هو الذي يصنع الفرق والخصوصية بين الجريمة المعلوماتية وباقي الجرائم، كونه يتجلى فيه فنيات وتقنيات ارتكاب الجريمة المعلوماتية، ومن خلاله يمكن الحكم على وسائل البحث والتحري التقليدية فيما إذا كانت تنجح في الكشف عن مثل تلك الجرائم. ويتمثل هذا المسرح في داخل الحاسوب، من خلال المكونات الرقمية، أي يتواجد فيه وفي مختلف مكوناته كالذاكرة والأقراص الصلبة، ولا يمكن أن يتعامل مع هذا المسرح إلا شخص خبير ذو دراية واسعة بفنيات وتقنيات الحاسب الآلي[3].

ويُعرف أيضا على أنه "يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة القرص الصلب الموجودة داخله".

ومن الإجراءات التي يتم اتباعها عند إجراء المعاينة ما يلي:

- القيام بتصوير جهاز الحاسوب الآلي وما قد يتصل به من أجهزة ترفيه ومحتويات.
- عدم التسرع في نقل أي مادة معلوماتية، للتيقن من عدم وجود أي مجالات مغناطيسية في العالم الخارجي.
- القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية.

[1]- بن بادة عبد الحليم: مرجع سابق، ص 79.

[2]- بوعنّاد فاطمة زهرة: مرجع سابق، ص 4.

[3]- بن بادة عبد الحليم: مرجع سابق، ص 79.

- ربط أقراص الكمبيوتر التي قد تحمل أدلة مع جهاز يمنع الكتابة عليه، مما يتيح للمحققين قراءة بياناتها من دون تغييرها[1].

الفرع الثالث: الضبط

يختلف الضبط في الجريمة الإلكترونية عن الضبط في غيرها من الجرائم من حيث المحل، وذلك بسبب أن الأول يرد على أشياء ذات طبيعة معنوية، كالمراسلات والاتصالات الإلكترونية، أما الثاني فيرد على أشياء مادية.

وتجدر الإشارة إلى أن الضبط قد يرد على عناصر معلوماتية منفصلة، مثل الأسطوانات الممغنطة، وهنا لا تثور أي مشكلة قانونية عند القيام بالضبط. لكن الصعوبة تثار عندما يلزم ضبط النظام كله أو الشبكة، وكل ذلك لأنها تحتوي على عناصر لا يمكن فصلها، ومع ذلك يتعين ضبطها لأنها تتضمن عناصر مهمة للإثبات.

أما بالنسبة للمكونات المادية للحاسب، فلا يثير ضبطها أي مشكلات، فيمكن ضبط الوحدات المعلوماتية الآتية:

وحدة المداخلات، بما تشمله من مفردات، كلوحة المفاتيح، نظام الفأرة، نظام القلم الضوئي. وحدة المخرجات، وما تشمل عليه من وسائل كالشاشة، الطابعة، الرسم والمصفرات الفيلمية. والمعروف أن ما يتم ضبطه من بيانات إلكترونية يتعين تحريره وتأمينه فنيًا، خاصة أمام غياب الثقافة المعلوماتية عن المحقق الجنائي، مما يجعل تلك الأدلة عرضة للإتلاف أو الإفساد[2].

أولا: قواعد الضبط

1- قواعد ضبط الأدلة: سوف نتحدث في هذا الجزء عن قواعد الضبط، سواء كانت قواعد قانونية أم قواعد فنية، والتي تضمن الحفاظ على الدليل المعلوماتي من التلف أو التغيير، حيث:

أ. ضبط المكونات المادية للحاسوب:

[1]- بوعنّاد فاطمة زهرة: مرجع سابق، ص 4.

[2]- بوعنّاد فاطمة زهرة: مرجع نفسه، ص 4.

إن الهدف هو وضع اليد على الأدلة التي تفيد في كشف الحقيقة، ولهذا لا توجد مشكلة في تطبيق القواعد التقليدية المتبقية في ضبط الأدلة المادية. تتكون مكونات الحاسوب المادية من الحاوية التي تحمل الدوائر الإلكترونية وذاكرته، لوحة المفاتيح، الفأرة، الشاشة، جهاز الطابعة، جهاز السكانر، وغيرها من الملحقات. وإذا ما رجعنا إلى قانون أصول المحاكمات العراقي، نرى أنه قد تطرق إلى ضبط الأدلة الناجمة عن التفتيش في عدد من نصوص هذا القانون. وقد عالج هذا النقص عدد من التشريعات، ومنها قانون الإجراءات الجنائية القطري، بقوله: "لمأموري الضبط القضائي أن يصنعوا الأقدام على الأماكن التي بها آثار أو أشياء تفيد في كشف الحقيقة وإن لم يُقيموا حرصًا عليها، ويجب عليهم إخطار النيابة العامة بذلك، وإذا ما رأت ضرورة لذلك أن ترفع الأمر خلال ثلاث أيام إلى قاضي محكمة الجناح المختصة لإقراره، وإلا اعتُبر الإجراء كأنه لم يكن. ولكل من شأنه أن يتظلم للقاضي من الأمر الذي أصدره بتأييد القرار أو إلغائه".

ب. ضبط الأدلة المعلوماتية

أثار ضبط الأدلة المعلوماتية خلافًا كبيرًا بين فقهاء القانون الجنائي، وانقسم إلى رأيين، وهما:

الرأي الأول: يرى أصحاب هذا الرأي، ومعظمهم من الفقهاء الألمان، أنه لا يمكن تصور ضبط البيانات المعلوماتية ووضع اليد عليها لأنها ليست ذات مظهر مادي محسوس، لذلك لا يمكن ضبطها بسبب طبيعتها غير المحسوسة. ويستند أنصار هذا الرأي إلى المادة 94 من قانون الإجراءات الألماني[1].

الرأي الثاني: يرى أصحاب هذا الرأي أنه لا يوجد ما يمنع من أن يرد الضبط على البيانات المعلوماتية، فالفقه الجنائي في بعض الدول يعطي الإمكانيات لسلطات التحقيق بالقيام بأي شيء يكون لازمًا وضروريًا لجمع وحماية الدليل، ومنهم القانون اليوناني والكندي[2].

المطلب الثاني: الإجراءات الحديثة للحصول على الدليل الرقمي.

[1]- عادل بن عبد الله خميس المعمري، مرجع سابق، ص 15

[2]- عادل بن عبد الله خميس المعمري، مرجع نفسه، ص16.

أدت التطورات التكنولوجية إلى ظهور إجراءات حديثة للحصول على الدليل المعلوماتي، تعتمد على استخدام التقنيات الرقمية، وقواعد البيانات الإلكترونية، وأساليب البحث الذكي. وتعد هذه الإجراءات خطوة نحو تشريع الوصول إلى المعلومات بدقة وموثوقية لدعم البحث العلمي وصناعة القرار.

الفرع الاول: التسرب

1- تعريفه

عرفه المشرع من خلال المادة 65 مكرر 12 من قانون الإجراءات الجزائية، بأنه قيام ضباط أو أعوان الشرطة القضائية، تحت مسؤولية ضباط الشرطة القضائية المكلفين بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بأنها مهمة، سواء كانوا فاعلين، أو شركاء، أو مخفيين. وبذلك، فالتسرب هو إجراء أو تفتيش يسمح لضباط الشرطة القضائية بالتوغل داخل جماعة إجرامية[1].

ويمكن افتراض عملية التسرب في مجال الجريمة المعلوماتية من خلال قيام ضابط أو عون الشرطة القضائية بالتوغل والدخول إلى العالم الافتراضي، وذلك باختراقه لمواقع معينة، وفتح ثغرات إلكترونية فيها، أو الشراكة في محادثات غرف الدردشة، أو حلقات الاتصال المباشر مع المشتبه فيهم، وظهور معظم ذلك كفاعل معهم أو مشارك، مستخدمًا أسماء وصفات وهمية من أجل الإيقاع بهم

ومن المعلوم، فإن التسرب يخضع لعدة شروط، وفي حالة تجاوزها أو مخالفتها تكون العملية باطلة[2].

2- شروط صحة التسرب:

[1]- نور المجدوب: الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، مجلد 06، ع 3، المركز الجامعي ، مغنية الجزائر، 2023، ص 199.

[2]- بن بادة عبد الحليم: مرجع سابق، ص 85.

صدور إذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، كما يجب أن يكون الإذن مكتوبًا ومسببًا، ويُذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة، كما يُحدد مدة عملية التسرب التي لا يمكن أن تتجاوز ثمانية أشهر، غير أنه يمكن أن تتجدد[1].

كما لا يجوز إظهار الهوية الحقيقية لضباط وأعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات[2].

ويعاقب كل من يكشف هوية الضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات، وبغرامة من 50,000 إلى 200,000 دينار جزائري. وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب أو جرح على أحد هؤلاء الأشخاص أو أزواجهم أو أصولهم المباشرين، تكون العقوبة من خمس سنوات إلى عشر سنوات، وبغرامة من 200,000 دينار إلى 500,000 دينار[3].

إذ يتوجب أن يكون إجراء التسرب محددًا بفترة زمنية، غير أنه إذا تقرر وقف العملية أو انقضت المهلة المحددة في الرخصة دون تمديدها، فيمكن للعون المتسرب مواصلة النشاطات للوقت الضروري الكافي لتوقيف عملية المراقبة في ظروف آمنة، دون أن يكون مسؤولًا جنائيًا، على أن لا يتجاوز ذلك أربعة أشهر[4].

الفرع الثاني: اعتراض المراسلات

[1]- بوعنّاد فاطمة زهرة: مرجع نفسه، ص 06.

[2]- وردة شرف الدين: مشروعية اساليب التحري في مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والحريات، جامعة محمد خيضر، بسكرة ص 11.

[3]- وردة شرف الدين: مرجع سابق، ص 116.

[4]- نوال مجدوب: مرجع سابق، ص 201.

1. تعريفها.

يعرفها البعض بأنها عملية مراقبة سرية للمراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة لجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب الجريمة[1].

وقد استحدث المشرع الجزائري لهذا الأمر عن طريق قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بمراقبة الاتصالات الإلكترونية، غير أنه حدد الحالات التي يُسمح فيها باللجوء إلى المراقبة الإلكترونية، كالأفعال الموصوفة بجرائم الإرهاب والتخريب، أو الجرائم الماسة بأمن الدولة، أو في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو مؤسسات الدولة، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2].

كما جاء في المادة ثلاثة من القانون 09-04 أنه مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن للنيابة العامة حماية النظام العام ومستلزمات التحريات أو التحقيقات القضائية الجارية، وفق القواعد المنصوص عليها في قانون الإجراءات الجزائية، أن تضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتسجيل محتواها في حينه، أو القيام بإجراء التفتيش والحجز داخل منظومة معلوماتية[3].

2. خصائص اعتراض المراسلات:

اعتراض المراسلات هو إجراء يتم دون رضا أو علم صاحب الشأن، فلو كان صاحب الشأن عالمًا بالإجراءات المطبقة عليه لانعدمت بذلك خاصية الاعتراض. هكذا، عند وضع الخط الهاتفي تحت المراقبة لا يمكننا القول بأننا أمام إجراء علني، ولهذا فهو سري[4].

3. الشروط والضمانات المقررة لاعتراض المراسلات:

[1]- وردة شرف الدين: مرجع سابق، ص07.

[2]- بوعنّاد فاطمة زهرة: مرجع نفسه، ص 08.

[3]- بن بادة عبد الحليم: مرجع سابق، ص 85.

[4]- رقية محمودي ونور الهدى قدور: مرجع سابق ص 144.

ترخيص السلطة القضائية ومراقبتها للعملية التنفيذية، فطبقًا للمادة خمسة مكرر من قانون الإجراءات الجزائية قابلة، لا يمكن لضبط الشرطة القضائية اللجوء إلى اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبق من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية وحدها المختصة بإصدار هذا الإذن، وهو يُعد ضمانًا لمشروعية هذا الإجراء[1].

ضابط الشرطة القضائية مقيدة أثناء قيامها بالعمليات المحددة في المادة 65 مكرر بالحفاظ على السرية المهنية، حرصا على نجاحها من جهة، وخوفا من فشلها من جهة أخرى. يجب أن يتضمن الإذن المذكور كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها، كتحديد رقم الهاتف واسم المشترك، وتسليم الإذن مكتوبًا بمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق من نفس الشروط الشكلية او الزمنية[2].

الفرع الثاني: الشهادة في الجريمة الالكترونية

أولًا: مفهومها

الشهادة لا تختلف في مدلولها عن تلك المتعلقة بالجريمة الإلكترونية، إذ يبقى أمر سماع الشهود متروكًا لفطنة المحقق ومرتبطًا بظروف التحقيق وما تسفر عنه. والأصل أن يطلب الخصوم من يرون من الشهود، وللمحقق أن يدعو الشهادة الذي يقدّر أن لشهادته أهمية، وله أن يسمع من يتقدم من تلقاء نفسه[3].

كما أن الشاهد في الجريمة العادية أو التقليدية يختلف عن الشاهد في جرائم المعلوماتية، وهو ما اصطلح عليه بالشاهد المعلوماتي، كون هذا الأخير ينبغي أن يكون ذو خبرة وكفاءة وتأهيل في

[1]- سعيد ابن نعيم: اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة الماجيستير، قانون عام، جامعة لخضر باتنة، 2012-2013، ص 181.

[2]- وردة شرف الدين: الجوانب الموضوعية والإجرائية لمكافحة الجرائم المعلوماتية في التشريع الجزائري، مجلة المنارة للبحوث والدراسات القانونية والسياسية، ع 3 ، جامعة محمد خيضر بسكرة، ديسمبر 2017، ص 44.

[3]- مليكة ابو ديار: الإثبات الجنائي في الجرائم الالكترونية، المجلة الالكترونية للأبحاث القانونية، كلية الحقوق ب مكناس، ع 2، 2018، ص 106.

مجال معين متعلق بالبرمجيات والتقنيات المرتبطة بمجال الحاسوب، حيث تمكنه خبرته من استخراج الأدلة أو الكشف عنها[1].

أ. المقصود بالشاهد المعلوماتي

يقصد بالشاهد في الجريمة المعلوماتية، هو الشخص صاحب الخبرة والمتخصص في تقنية المعلومات، والذي يمكنه الدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب ذلك، لذلك يُطلق عليه الشاهد المعلوماتيTémoin d'informatique تمييزًا له عن الشاهد التقليدي[2].

ب. التزام الشاهد بالإعلام في الجريمة المعلوماتية:

ويقصد به أنه إذا كان الشاهد حائزًا لمعلومات جوهرية لازمة لاختراق نظام المعالجة الآلية للبيانات بحثًا عن أدلة جوهرية تتطلبها مصلحة التحقيق، فإنه يكون مطالبًا بأن يُعلم سلطات التحقيق على سبيل الإلزام، وإلا تعرض للعقوبات المقررة لجريمة الامتناع عن الشهادة[3].

2- شروط قبول الشهادة كأداة إثبات في الجريمة الإلكترونية:

- يجب أن تكون الشهادة بمثابة دليل يقيني، تستوجب أن تقرب نحو الحقيقة الواقعة قدر المستطاع، وأن تبتعد عن الظنون والتخمينات.

- يتعيّن مناقشة الشاهد كدليل على الجريمة الإلكترونية تطبيقًا لمبدأ المواجهة، فإذا كانت الشهادة تُعد دليل إثبات قائمًا في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم[4].

---

[1]- وهيبة رابح: الجريمة المعلوماتية في التشريع الجزائري، مجلة الباحث للدراسات الأكاديمية جامعية عبد الحميد بن باديس مستغانم، ع 4، 2014، ص 329.

[2]- محمد بن فردية: الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة دكتوراه، جامعة الجزائر، كلية الحقوق، 2015-2016، ص 152.

[3]- محمد بن فردية: مرجع سابق، ص 153.

[4]- ناصر ال ثنيان: إثبات الجريمة الالكترونية، دراسة تأصيلية تطبيقية، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية الرياض، ص92.

3- دور الشهادة في إثبات الجريمة الإلكترونية:

تدل الشهادة على واقعة ذات أهمية، فهي تدل على وقوع الجريمة ونسبتها إلى المتهم في الأثر الجزائي. والشهادة يقدمها رأي يدلي به الشاهد، وهو شخص خارج عن أطراف الخصومة ولديه معلومات تفيد في الكشف عن الحقيقة المتصلة بتحديد الأفعال المرتكزة وجسامة الجريمة، وبالتالي نسبتها إلى فاعلها، ومن هنا فتزيد القناعات وليس الشائعات من قبل الشهادة[1].

الفرع الثالث: الخبرة التقنية

1. مفهومها

الخبرة هي الوسيلة التي من خلالها تستطيع سلطة التحقيق أو المحكمة التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلًا مستقلًا عن الدليل القولي أو المادي، وإنما هي تقييم لهذا الدليل. فهي في مجملها تقرير صادر عن الخبير في أمر من الأمور المتعلقة بالجريمة[2].

وتعرف أيضا بانتا إجراء يتعلق بموضوع يتطلب الإلمام بالمعلومات فنية لما كان استخلاص الدليل الرقمي منه، آو هي الاستشارة الفنية التي يستعين بها المحقق آو القاضي في مجال الواثبات، لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدة فنية أو أدارية[3].

2. القواعد الأساسية التي يجب أن يلتزم بها الخبير:

هناك قواعد عامة يجب مراعاتها لضمان نجاح التحري حول جرائم الحاسب الآلي، والتي لا يمكن اكتشافها:

---

[1]- مرجع نفسه، ص 100.

[2]- مراد فلاك: آليات الحصول على الأدلة الرقمية كوسائل اثبات في الجرائم الالكترونية، مجلة الفكر القانوني والسياسي، ع 5، مسيلة 2019، ص 2013.

[3]- حسام احمد كيلالي علي: الدليل الرقمي والمعيقات إثبات الجريمة الالكترونية، مجلة البحوث الفقهية والقانونية، مج 47، ع 47، كلية الشريعة والقانون، بدمنهاور، أكتوبر 2024، ص 722.

- ضرورة مراعاة تعاملات سلطات الضبط أو التحري مع خبراء الحاسب الآلي العاملين في المؤسسة المتضررة.
- مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإلكتروني وغير ذلك.
- ضرورة العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها وبرامجها اللينة[1].

3. الأحكام العامة للخبرة التقنية:

نظم المشرع الجزائري الميدان الجزئي في المواد 143 إلى 156 ق.إ.ج فيما يتعلق بمرحلة التحقيق الابتدائي، وفيما يتعلق بمرحلة المحاكمة فقط، نصت المادة 219 من ق.إ.ج على إتباع الأحكام المنصوص عليها في المواد السابقة الذكر. أما المشرع الفرنسي فقد تناول تنظيم مسألة الخبرة في المواد من 156 إلى 169 من ق.إ.ج[2].

4. مكانة الخبرة كدليل إثبات:

عندما ينهي الخبير المهمة المسندة إليه، يقوم بتحرير عرض عن أعماله المنجزة، وكذا رأيه، كل هذا يشتمل في تقريره، ويجب أن يكون تقرير الخبير واضحًا متضمنًا لكافة المسائل المطلوبة منه، وهذا لتمكين القاضي والخصوم من مناقشة كل ما جاء فيه. وقد نصت المادة 153 من ق.إ.ج الجزائرية على تقرير الخبرة، وجاء فيها: يحرر الخبراء لدى إنجاز أعمال الخبرة تقريرًا يجب أن يشمل على وصف ما قاموا به من أعمال ونتائجها[3].

5. مجالات الخبرة في الجريمة الإلكترونية:

هناك العديد من الأنماط المختلفة والمتنوعة من العمليات الإلكترونية، والتي ترتبط ارتباطًا وثيقًا باستعمال الرسائل الإلكترونية. فعلى سبيل المثال نجدها في الأعمال المصرفية، في التجارة الإلكترونية،

[1]- فيروز عوض عبد الكريم مرغني: مرجع سابق، ص 108.
[2]- محمد بن فردية: مرجع سابق، ص 336.
[3]- محمد بن فردية: مرجع سابق، ص 338.

حيث إنه من المتوقع أن تتنوع الجرائم طبقًا لتنوع الوسائل التي يتم استخدامها من خلال استهداف تلك العمليات، فعلى سبيل المثال نجد عمليات تزوير المستندات المدخلة في أنظمة المعالجة[1].

6. الضوابط الخاصة بالخبرة:

- خضوع الخبرة للرقابة القضائية.
- إنجاز الخبير لأعمال الخبرة بنفسه.
- إيداع تقرير الخبرة التقنية[2].

7. أهمية الخبرة القضائية في الإثبات الجنائي:

تتجلى أهمية الخبرة القضائية في كونها تدير نظر القاضي وتعينه في الوصول إلى الحقيقة، فالقاضي شخص مختص في القانون، فلا يمكن الإلمام بكل الفنون والعلوم لكثرتها، وهذا ما يدفعه للاستعانة بأهل الفن والاختصاص كالأطباء والمهندسين الذين بإمكانهم إفادة القاضي وتوضيح الرؤية له[3].

الفرع الرابع: المراقبة الإلكترونية

1- مفهومها:

يقصد بالمراقبة الإلكترونية بوجه عام تعمد الإنصات والتسجيل على المحادثات الخاصة، أما المحادثات العامة فلا قيد على مراقبتها وتسجيلها سواء علم أصحابها بذلك أم لم يعلموا، لأن ذلك لا يمس بحرمتهم وخصوصياتهم ما دامت هذه المحادثة عامة[4].

هذا الإجراء تم استحداثه بموجب المادة 03 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وأجاز تبعًا لمستلزمات التحريات

[1]- نبيهة قنفود: البرة التقنية مجال اثبات الجريمة الالكترونية، جامعة عبد القادر للعلوم الاسلامية، مجلد 36، ع 2، جامعة الامير عبد القادر للعلوم الاسلامية، 2022، ص 410.

[2]- المرجع نفسه، ص 413.

[3]- عبد القدر عميمر: مرجع سابق، ص 247.

[4]- المرجع نفسه، ص 275.

والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم أو اللجوء إلى وضع الترتيبات التقنية لمراقبة الاتصالات التكنولوجية وتجميع وتسجيل محتواها[1].

2- مضمون قرار الوضع تحت المراقبة:

إجراء الوضع تحت المراقبة الإلكترونية هو حرمان المتهم أو المحكوم عليه من التغيب عن محل إقامته أو أي مكان آخر يعنيه، ويتم الأمر الصادر عن النيابة العامة أو المحكمة المختصة بحسب الأحوال، ويُنفذ عن طريق وسائل إلكترونية تسمح بالمراقبة عن بعد أو تلزم الخاضع لها بحمل جهاز إرسال إلكتروني مدمج طوال فترة الوضع تحت الرقابة[2].

3- إجراءات قرار الوضع تحت المراقبة:

وفقًا للمادة 369 من المرسوم بقانون اتحادي رقم 17 لسنة 2018، فإنه للمحكمة عند الحكم بالحبس لمدة لا تزيد عن سنتين أن تأمر في الحكم بتنفيذ العقوبة المحكوم بها بنظام الوضع تحت المراقبة الإلكترونية، إذا رأت من ظروف المحكوم عليه أو سنة ما يبعث على الاعتقاد بأنه لن يعود إلى ارتكاب جريمة أخرى جديدة، وبأن له محل إقامة ثابتًا ومعلومًا في الدولة[3].

4- الجهة المختصة بفرض المراقبة الإلكترونية:

وفقًا لقانون الإجراءات الجزائية الجزائري وبعد تعديله بموجب الأمر 15-02، يختص قاضي التحقيق باتخاذ قرار بوضع المحكوم عليه تحت المراقبة الإلكترونية، وهذا ما يُستشف من نص المادة 125 مكرر المادة 01 الفقرة 03، تنص على: يمكن لقاضي التحقيق أن يأمر باتخاذ ترتيبات من أجل المراقبة الإلكترونية للتحقق من مدى التزام المتهم بالتدابير المذكورة[4].

5- حالات اللجوء إلى المراقبة الإلكترونية للاتصالات:

---

[1]- بن بادة عبد الحليم: مرجع سابق، ص 86.

[2]- حسين وعبير حمدي: أحكام المراقبة الالكترونية ، مجلة القانون والأعمال، ع93، جامعة الحسن الأول: كلية العلوم القانونية والاقتصادية والاجتماعية، 2023، ص 84.

[3]- حسين وعبير حمدي: ص 81.

[4]- عبد الهادي درار:السوار الالكتروني ومساسه بالحياة الخاصة للمتهم بمنظور الأمر 02-15 مجلة اليزة للبحوث والدراسات، ع 2، المركز الجامعي الجزائر2017، ص84.

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو المؤسسات الدولة أو الاقتصادية الوطني في إطار تنفيذ الطلبات المساعدة القضائية الدولية المتبادلة[1].

[1]- رقية محمودي: مرجع سابق، ص 147.

خـــاتمـة

في ختام هذه الدراسة حول "الآليات الجنائية لمتابعة الجريمة الإلكترونية"، يتضح أن الجريمة الإلكترونية تمثل تحديا متناميًا للأنظمة القانونية الوطنية والدولية، نظرا لطبيعتها المعقدة، وعدم تقيدها بالحدود الجغرافية، واستخدامها لتقنيات متطورة يصعب أحيانا تتبعها بالوسائل التقليدية.مما لا شك فيه أن التطور الهائل في تكنولوجيا المعلومات والاتصالات قد ساهم في تحقيق نقلة نوعية في حياة الأفراد والمجتمعات، إلا أنه في المقابل أفرز صورا جديدة من الإجرام عابرة للحدود، من أبرزها الجريمة الإلكترونية، التي أضحت تمثل تحديا حقيقيا للمنظومات القانونية الوطنية والدولية، سواء من حيث التعريف، أو الإثبات، أو المتابعة، أو حتى التعاون الدولي في مكافحتها.

وقد بيّنت هذه الدراسة أن الآليات الجنائية التقليدية أصبحت عاجزة عن الإحاطة الشاملة بهذا النوع من الجرائم، بسبب خصوصياته التقنية والبنيوية، مما يفرض على المشرّع والسلطات العدلية والأمنية إعادة النظر في المنظور الكلاسيكي للعدالة الجنائية، وتبنّي مقاربات حديثة وفعّالة ترتكز على التخصص والتنسيق وسرعة الاستجابة، في ظل احترام الضمانات الدستورية وحقوق الإنسان.

كما أبرزت الدراسة أن التحدي لا يكمن فقط في النص القانوني، بل أيضا في البنية المؤسساتية والتقنية، وهو ما يدعو إلى إصلاح شمولي يراعي التحولات الرقمية المتسارعة ويُعد العدّة القانونية والتقنية والموارد البشرية المؤهلة لمواجهتها.

- **النتائج الرئيسية:**

1. تُعاني التشريعات الوطنية من نقص في الشمول والوضوح فيما يتعلق بتجريم بعض الأفعال الإلكترونية الحديثة.
2. ضعف التكوين والتخصص لدى أجهزة الضبط القضائي والقضاء في التعامل مع الجرائم الإلكترونية.
3. غياب التنسيق الفعّال بين الجهات المتدخلة في مكافحة هذا النوع من الجرائم.
4. محدودية التعاون الدولي، بسبب التباين التشريعي واختلاف المعايير القانونية بين الدول.

5. وجود إشكاليات في الإثبات الجنائي الرقمي، من حيث حجية الدليل الرقمي، طرق جمعه، ومعالجته قانونياً.
6. الحاجة إلى إعادة تأهيل البنية القانونية والمؤسساتية بما يتماشى مع واقع الجريمة الإلكترونية.

➢ **أهم التوصيات:**

1. إصلاح المنظومة التشريعية بإصدار قانون خاص بمكافحة الجريمة الإلكترونية، يتضمن تعريفاً دقيقاً للجرائم والمفاهيم التقنية.
2. إنشاء وحدات قضائية وأمنية متخصصة ومزودة بالإمكانيات التقنية والبشرية الكافية لمتابعة هذه الجرائم بفعالية.
3. تعزيز التعاون القضائي والأمني الدولي، والانخراط الفعّال في الاتفاقيات ذات الصلة، خاصة اتفاقية بودابست.
4. تقنين وسائل الإثبات الرقمي وإضفاء حجية قانونية على الدليل الرقمي بما ينسجم مع المبادئ القانونية العامة.
5. تبني مقاربة وقائية تقوم على التحسيس، وتعميم الثقافة الرقمية القانونية، واستباق الجريمة بدل الاقتصار على مواجهتها بعد وقوعها.
6. إنشاء هيئة وطنية تنسيقية مستقلة تُعنى بمكافحة الجريمة الإلكترونية، وتضمن التكامل بين مختلف الفاعلين.

إنّ التصدي للجريمة الإلكترونية لا يمكن أن يتحقق بمجرد تطوير التشريعات، بل يتطلب بناء منظومة عدالة رقمية شاملة، ترتكز على الفعالية، والشفافية، والمرونة، وتتكامل فيها الأدوار بين القضاء، والشرطة، والهيئات التقنية، بما يضمن حماية المجتمع الرقمي وضمان سيادة القانون في العالم الافتراضي.

قائمة المصادر والمراجع

أولا النصوص القانونية

1. القانون رقم 04-09. الصادر في 5 أغسطس 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.

2. القانون رقم 04-15 الصادر في 10 نوفمبر، يعدل ويتمم الأمر رقم 156/66 الصادر في 8 يونيو 1966، متضمن قانون العقوبات، الجريدة الرسمية، العدد 47.

3. قانون رقم 09-04 المؤرخ في 25 شعبان 1430هـ، الموافق لـ 16 غشت سنة 2009م، يتعلق القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد 47.

ثانيا: اتفاقيات

1- إتفاقية بودابست بشأن الجرائم المعلوماتية :هي أول معاهدة دولية تهدف إلى مكافحة الجرائم التي ترتكب عبر الإنترنت.

ثالثا: الكتب القانونية

1. أيمن عبد الله فكري: الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد،المملكة العربية السعودية، ط1، 2014

2. الجريمة الالكترونية: وحجية الدليل الرقمي في الاثبات الجنائي، مركز هردو لدعم التعبير الرقمي، القاهرة 2014

3. ذياب موسى البداينة: الجرائم الالكترونية المفهوم والاسباب، ورقة علمية بعنوان الجرائر الالكترونية المفهوم والاسباب كلية العلوم الاستراتيجية، عمان، المملكة الاردنية الهاشمية، 2014

4. رقية محمودي ونور الهدى قدوح: الجرائم الالكترونية في المجتمع الجزائري، ط 1، هيئة النشر العلمي، جامعة يحي فارس، المدية 2022

5. صدام حسين ياسين العبيدي جرائم الانترنت و عقوبتها في الشريعة الاسلامية و القوانين الوضعية المركز العربي للنشر و التوزيع مصر 2019

6. ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، دراسة مقارنة، المركز العربي، مصر، 2017

7. عادل عبد العالي إبراهيم خراشي: آليات التعاون الدولي في مكافحة الجرائم المعلوماتية والسبل التغلب عليها. دار الجامعة الجديدة للنشر، خلية الشريعة والقانون بالقاهرة، 2015.

8. عبد الصبور علي مصري: المحكمة الرقمية والجريمة المعلوماتية، ط1، مكتبة القانون والاقتصاد، الرياض، 2012

9. عبد العالي الديربي: الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، مصر 2012

10. عبد العزيز نايف: الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهته، مجمع البحوث والدراسات، اكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان2016.

11. علي حمزة عسل الخفاجي: الجرائم الناشئة عن اختراق الأمن السيبراني وآليات مكافحتها، دار مصر للنشر والتوزيع، مصر، ط1، 2024–2025،

12. عماد مفلح الحسبان وآخرون: الجرائم المستحدثة المعلوماتية الإلكترونية السيبيرانية ، ط 1، دار الخليج للنشر والتوزيع، عمان، 2024

13. غادة نصار، الإرهاب والجريمة الالكترونية، العربي للنشر والتوزيع، ط 1، 2017

14. فريجة حسين: الجرائم الالكترونية والانترنيت المعلوماتية، ع 36. المملكة العربية السعودية، 2011

15. محمد كمال الدسوقي: الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، مصر، ط1، 2021

16. محمد نصر محمد: المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، ط1 ، مركز الدراسات العربية للنشر والتوزيع، مصر2015

17. نهلا عبد القادر المومني: الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان2010.

رابعا : المقالات

1. احمد كيلالي علي: الدليل الرقمي والمعيقات إثبات الجريمة الالكترونية، مجلة البحوث الفقهية والقانونية، مج 47، ع 47، كلية الشريعة والقانون، بدمنهاور، أكتوبر 2024

2. أنيس بن علي العذار: مكافحة الجريمة الإلكترونية، الصعوبات والحلول القضائية. عين 13، وزارة العدل، 2017

3. بثينة حبيباتي: الطبيعة الخاصة للجريمة للمعلومة، المجلة العربية في العلوم الانسانية والاجتماعية، مج 12، ع 53، جامعة الجزائر 1، جويلة 2020

4. البركة الطيبي: إشكالية الإثبات في الجرائم الالكترونية، مجلة أفاق علمية ، مج 11، ع 1، جامعة أدرار 2019

5. بن بادة عبد الحليم: "إجراءات البحث والتحري عن الجريمة الإلكترونية"، مجلة الحقوق والعلوم الإنسانية، ع 23، م .ج. الثاني، جامعة غرداية، 201

6. بوعنّاد فاطمة زهرة: مكافحة الجريمة الإلكترونية في التشريع الجزائري. مجلة الندوة للدراسة القانونية، ع. الأول لعام 2014، جامعة الجيلالي اليابس، سيدي بلعباس.

7. ثامر علي النويران: الجرائم الالكترونية الحد منها تجربة الأردن، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC كلية العلوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية السعودية ، المملكة العربية السعودية، الرياض، 2015، ص 178.

8. جمال محمد خلفان محمد النقبي واخرون: التعاون الوطني والدولي في الجرائم الالكترونية المشكلات والحلول، مجلة المعهد العالي للدراسات النوعية، مج 3، ع 16 ، 2023.

9. جهاد نزار دغمش: الاشكاليات الموضوعية والاجرائية في النظام القاومني الفلسطيني، في التجربة الالكترونية، مجلة الباحث للدراسات والابحاث القانونية والقضائية، مج 2022، ع 45، ص4.

10. حسام مراد فلاك: آليات الحصول على الأدلة الرقمية كوسائل اثبات في الجرائم الالكترونية، مجلة الفكر القانوني والسياسي، ع 5، مسيلة

11. حسين وعبير حمدي: أحكام المراقبة الالكترونية ، مجلة القانون والأعمال، ع93، جامعة الحسن الأول: كلية العلوم القانونية والاقتصادية والاجتماعية، 2023

12. الحكيم ومولاي ابراهيم: الجرائم الالكترونية، مجلة الحقوق والعلوم الانسانية، ع 23، جامعة زيان عاشور الجلفة 2015

13. حليمة خراز: المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب، الدراسات القانونية المقارنة، مج 1216، ع 2، جامعة حسين بوعلي الشلف، كلية الحقوق والعلوم السياسية، مخبر القانون الخاص

14. راضية عيمور: اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، الجزائر العاصمة، 29 مارس 2017

15. رحاب علي عميش: الجريمة المعلوماتية دراسة مقارنة بين القانون الليبي والاماراتي، مجلة علمية محكمة، ع 4، معهد دبي القضائي، 2014

16. رزيقة خرير: واقع مكافحة الجريمة الإلكترونية. كلية العلوم والاتصال، مجلة الحكمة للدراسات الإعلامية والاتصالية، مج 2017، ع 10، مؤسسة كنوز للنشر والتوزيع، الجزائر، 2017.

17. رضا مهدي: "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"، مجلة إليزا للبحوث والدراسات، مج. 6، ع. 2، 2021، جامعة محمد بوضياف – الجزائر

18. زينب طرقي فهد والعنزي: الجريمة الالكترونية في ميزان الفقه والقضاء، مجلة الدراسات الإسلامية والبحوث الأكاديمية، ع 99، جامعة القاهرة، 2020

19. سعاد طعبة: الجريمة الالكترونية، تفعيل الآليات القانونية من اجل تحقيق العدالة، مجلة الحقوق والعلوم الانسانية، مجلد 15، ع 3، جامعة زيان عاشور بالجلفة، 2022

20. سعاد طعبة: الجريمة الالكترونية، تفعيل الآليات القانونية من اجل تحقيق العدالة، مجلة الحقوق والعلوم الانسانية، مجلد 15، ع 3، جامعة زيان عاشور بالجلفة، 2022

21. سعد عاطف عبد المطلب حسين: "دور الشرطة في مكافحة الجرائم المستحدثة وتحقيق الأمن المعلوماتي"، مجلة بحوث كلية الآداب، جامعة المنوفية

22. سميرة معاشي: "ماهية الجريمة المعلوماتية"، مجلة المنتدى القانوني، ع7، جامعة بسكرة، 2010

23. سورية ديش: انواع الجريمة الالكترونية و إجراءات مكافحتها مجلة الدراسات الإعلامية المركز الديمقراطي العربي ع1 جامعة جيلالي ليابس الجزائر 2018

24. شحاتة واحمد ابو زيد: الجريمة المعلوماتية أنواعها ويل مواجهتها، مجلة العلوم القانونية الاقتصادية، مج 65، ع 2، جامعة عين الشمس كلية الحقوق، 2023

25. شحاتة واحمد ابو زيد: الجريمة المعلوماتية أنواعها ويل مواجهتها، مجلة العلوم القانونية الاقتصادية، مج 65، ع 2، جامعة عين الشمس كلية الحقوق، 2023

26. ضياف اسمهان: "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف – الجزائر، 2018

27. الطاهر ياكر: مكافحة الجرائم الإلكترونية بين التشريعات الوطنية. مجلة الهدى للدراسة القانونية والسياسية، مج 04، ، ع 04 جامعة الجيلالي بن عمار، خميس مليانة، الجزائر.

28. عادل يوسف عبد النبي شكري: الجريمة المعلوماتية، أزمة الشرعية الجزائية، الجريمة المعلوماتية، ع 7، جامعة الكوفة، كلية القانون

29. عائشة عبد الحميد: "النظام القانوني للمنظمة الدولية للشرطة الجنائية الإنتربول ودورها في مجال التعاون القضائي الشرطي"، المجلة الأكاديمية للأبحاث والنشر العلمية.

30. عبد الحميد المليحي: الجريمة الالكترونية مدخل في اطار المفاهيمي، مجلة المنارة للدراسات القانونية والادارية، 2019، 157.

31. عبد المنعم أبقال: راهن الأجهزة الأمنية وتحديات الجريمة الإلكترونية. مجلة المنارة للدراسات القانونية والإدارية، ع 12، 2016

32. عبد الهادي درار:السوار الالكتروني ومساسه بالحياة الخاصة للمتهم بمنظور الأمر 02-15 مجلة اليزة للبحوث والدراسات، ع 2، المركز الجامعي الجزائر2017

33. عفاف خديري: "الجريمة الإلكترونية والأمن الوطني"، المجلة الجزائرية للدراسات السياسية، جامعة عنابة، 2017

34. عيشة خلدون: الطبيعة الخاصة للجريمة الالكترونية وصورها قاعدة بيانات الملخصات العلمية، جامعة زيان عاشور بالجلفة

35. غنيم عبد الرحمن علي إبراهيم: "مضمون انضمام دولة فلسطين في المنظمة الدولية للشرطة الجنائية الإنتربول"، مجلة الفقه والقانون، مجلد 75، 2019، ص. 73.

36. فتيحة بوهرين: "الجريمة المعلوماتية في التشريع الجزائري"، مجلة الحقوق والعلوم الإنسانية، مج 14، ع 04 ،غرداية 2021

37. قسميه محمد: "الوسائل التقنية الدولية للشرطة الجنائية الإنتربول كآلية للتعاون الدولي الشرطي"، جامعة الجزائر، مجلة جامعة محمد بوضياف

38. لامية طالة: الجريمة الالكترونية بعد جديد لمفهوم الاجرام عبر منصات التواصل الاجتماعي، مجلة الرواق للدرسات الاجتماعية والإنسانية، مج 6، ع2

39. محمد حسين مرعي: المواجهة الجنائية للجرائم المستحدثة الماسة بالحياة الخاصة، مجلة الكوفة للعلوم القانونية والسياسية، المج 11، ع 36، جامعة الكوفة ، كلية القانون، 2018

40. محمد صفاء الدين علي شرشر: الجهود الدولية والتشريعية لمكافحة جرائم الانترنيت، مجلة البحوث القانونية والاقتصادية، مج 54، ع 03، اكتوبر 2021

41. محمد مزوالي: المعالجة التشريعية للجريمة الرقمية في القانون الجزائري، مجلة الحقيقة العدد 43، 2018/2017، جامعة احمد دراية، أدرار

42. محمد وصبرين جابر: "الجريمة الالكترونية ومكافحتها في القانون العماني"، المجلة المصرية للدراسات القانونية والاقتصادية، ع 14، 2020

43. مليكة ابو ديار: الإثبات الجنائي في الجرائم الالكترونية، المجلة الالكترونية للأبحاث القانونية، كلية الحقوق ب مكناس، ع 2، 2018

44. نبيهة قنفود: البرة التقنية مجال اثبات الجريمة الالكترونية، جامعة عبد القادر للعلوم الاسلامية، مجلد 36، ع 2، جامعة الامير عبد القادر للعلوم الاسلامية، 2022.

45. نجم الدين وسامر سمير : الجريمة المنظمة الالكترونية دراسة تحليلية في التشريع الفلسطيني، مجلة الجامعة الإسلامية للدراسات الشرعية والقانونية، مج 29، ع 2، الجامعة الإسلامية بغزة، عمادة البحث العلمي، 2021

46. نور المجدوب: الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، مجلد 06، ع 3، المركز الجامعي ، مغنية الجزائر، 2023.

47. نور الهدى قادري: الجريمة السيبيرانية وآليات مكافحتها، المجلة الجزائرية للحقوق والعلوم السياسية، المركز الجامعي أحمد بن يحي، معهد العلوم القانونية، مج 8، ع1، جوان 2023

48. الهادي خضراوي: تجربة الجزائر في مكافحة الجريمة الالكترونية، المؤتمر الدولي الأول في مكافحة الجريمة المعلوماتية ICACC جامعة الإمام محمد بن سعود الإسلامية السعودية ، المملكة العربية السعودية، الرياض، 2015

49. هدية احمد محمد زعتر: الاشكاليات القانونية للجرائم العابرة للحدود وسبل مواجهتها، مجلة البحوث القانونية والاقتصادية، ع 84، 2023

50. وائل محمد عبد الرحمان نصرات: الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها، المؤتمر الدولي في مكافحة الجرائم المعلوماتية ICACC، كلية العلوم الحاسب والمعلومات جامعة الإمام محمد بن سعود الإسلامية السعودية ، المملكة العربية السعودية، الرياض، 2015

51. وردة شرف الدين: الجوانب الموضوعية والإجرائية لمكافحة الجرائم المعلوماتية في التشريع الجزائري، مجلة المنارة للبحوث والدراسات القانونية والسياسية، ع 3 ، جامعة محمد خيضر بسكرة، ديسمبر 2017

52. وردة شرف الدين: مشروعية اساليب التحري في مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والحريات، جامعة محمد خيضر، بسكرة.

53. وهيبة رابح: الجريمة المعلوماتية في التشريع الجزائري، مجلة الباحث للدراسات الأكاديمية جامعية عبد الحميد بن باديس مستغانم، ع 4، 2014

54. يوسف باعدي: طبيعة المجرم في الطبيعة القانونية، مجلة الباحث للدراسات القانونية والقضائية، ع59، اكتوبر 2023

خامسا: الرسائل و المذكرات

1. سعيد ابن نعيم: اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة الماجيستير، قانون عام، جامعة لخضر باتنة، 2012-2013

2. شنتير خضرة: الآليات القانونية لمكافحة الجريمة الالكترونية لدراسة مقارنة، أطروحة دكتوراه، جامعة احمد دراية بأدرار، 2021/2020

3. صغير يوسف: الجرائم المرتكبة عبر الانترنيت، رسالة ماجستير، قانون دولي للأعمال، جامعة مولود معمري بتزي وزو 2014/2013.

4. عبد القادر عميمر: اليات اثبات الجريمة المعلوماتية في التشريع الجزائري دراسة مقارنة، اطروحة دكتوراه، جامعة الجزائر1، الجزائر، 2019-2020

5. عبد الله دعش العجمي: المشكلات العلمية والقانونية للجرائم الالكترونية، رسالة ماجستير قانون عام، جامعة الشرق الأوسط، 2014

6. فيروز عوض الكريم صالح ميرغني: اجراءات التحري والضبط في الجريمة الالكترونية رسالة دكتوراه قانون عام، جامعة شندي، 2017 87.

7. محمد بن فردية: الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة دكتوراه، جامعة الجزائر 2015.2016.

8. محمد بن فردية: الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة دكتوراه، جامعة الجزائر، كلية الحقوق، 2015-2016

9. ناصر ال ثنيان: إثبات الجريمة الالكترونية، دراسة تأصيلية تطبيقية، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية الرياض.

الفهرس

ملخص

تتناول هذه المذكرة موضوعًا ذا أهمية بالغة وراهنية كبيرة، وهو" :آليات المتابعة الجنائية للجرائم الإلكترونية في التشريع الجزائري."

ففي ظل الانتشار السريع لتكنولوجيات الإعلام والاتصال، ظهرت أشكال جديدة من الجرائم العابرة للحدود، تتسم بتعقيدها التقني وصعوبة تحديد مرتكبيها.

وتهدف هذه الدراسة إلى تحليل الإطار القانوني والمؤسسي المعتمد في الجزائر لمكافحة هذا النوع من الجرائم، من خلال فحص الآليات والإجراءات الجنائية التي تستخدمها السلطات القضائية وأجهزة إنفاذ القانون في كشف الجرائم الإلكترونية والتحقيق فيها ومتابعتها قضائيًا، كما تسعى الدراسة إلى تحديد مواطن القوة والقصور في المنظومة الحالية، ومدى قدرتها على مواجهة التحديات التقنية والقانونية التي تفرضها هذه الظاهرة.

وقد اعتمدت الدراسة على منهجية متعددة الأبعاد، شملت التحليل القانوني للنصوص، والمقارنة ببعض التجارب الدولية المختارة، إضافة إلى المقاربة الوصفية لتقييم الواقع العملي.

وأظهرت النتائج وجود تطور جزئي في الإطار التشريعي الجزائري، حيث تم إدراج بعض صور الجرائم الإلكترونية ضمن قانون العقوبات وقانون رقم 05-20 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، غير أن هذه الإجراءات لا تزال غير كافية لتشكيل منظومة شاملة ومتكاملة قادرة على مواكبة المتطلبات الرقمية والقانونية الحديثة.

وقد خلصت الدراسة إلى جملة من التوصيات، من بينها:

- تحديث التشريع الوطني بما يتلاءم مع التطورات التكنولوجية.
- تعزيز قدرات أعوان الضبط القضائي والقضاة في المجال التقني.
- تفعيل التعاون القضائي والتقني الدولي.
- إنشاء هيئة وطنية متخصصة في مكافحة الجريمة الإلكترونية وتنسيق الجهود بين الجهات المعنية.

Abstract

This dissertation addresses a highly topical and increasingly important issue, namely:
“Criminal Prosecution Mechanisms for Cybercrimes in Algerian Legislation.” In light of the rapid proliferation of information and communication technologies, new forms of cross-border crime have emerged, characterized by their technical complexity and the difficulty of identifying perpetrators.

The objective of this study is to analyze the legal and institutional framework adopted in Algeria to combat such crimes, by examining the criminal procedures and mechanisms used by judicial authorities and law enforcement agencies in detecting, investigating, and prosecuting cybercrimes. The research also seeks to identify the strengths and shortcomings of the existing system in addressing the technical and legal challenges posed by cybercriminal activity.

This study adopts a multidisciplinary methodology, including analytical review of legal texts, comparative analysis of selected international practices, and a descriptive approach to assess the current practical realities.

The findings reveal a partial legislative evolution in Algeria, as some forms of cybercrime have been incorporated into the Penal Code and Law No. 20-05 on the prevention and fight against crimes related to information and communication technologies. However, these measures remain insufficient to form a comprehensive and coherent system capable of responding to today’s digital and legal demands.

The study concludes with several recommendations, including:
- Updating national legislation to align with the evolving digital landscape,
- Enhancing the technical capacity of judicial police officers and magistrates,
- Strengthening international judicial and technical cooperation,
- And establishing a national specialized body to combat cybercrime and coordinate actions among relevant stakeholders.