جامعة عمار ثليجي الأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة بعنوان

الآليات الإجرائية في مكافحة الجريمة المعلوماتية

مذكرة تخرج لنيل شهادة الماستر في الحقوق

تخصص: القانون الجنائي والعلوم الجنائية

من إعـداد الطلبة:

– تونســي أحميدة

– مسعودي بدر الدين

تحــت إشــراف الأســـتاذ:

د – بلحسن حسام الدين لحسن

لجنة المناقشة :

الاسم واللقب	الرتبة	الصفة
د– التجاني عبد القهار	أستاذ محاضر –ب–	رئيسا
د– بلحسن حسام الدين لحسن	أستاذ محاضر –ب–	مشرفا ومقررا
د– لكحل عائشة	أستاذ محاضر –ب–	عضوا مناقشا

السنة الجامعية 2025/2024

كلمة شكر

بسم الله الرحمن الرحيم والحمد لله رب العالمين

"محمد" وعلى آله وصحبه أجمعين

سبحان الله الذي وهبنا نعمة العقل، سبحان الذي يستحق الشكر

على نعمته وحده لا شريك له، سبحان الذي جعل لنا العلم نور

وهدانا سبيل الرشاد

أما بعد :

أتقدم بالشكر والتقدير عرفانا بالجميل إلى

الدكتور * بلحسن حسام الدين لحسن * على تقبله الإشراف على هذا العمل.

كما أتقدم بتشكراتي الخالصة

إلى كل من أمد لنا يد المساعدة من قريب وبعيد.

وشكرا جزيلا.

إهداء

إلى من اضاءت دربي بدعوات الخير

إلى من حتى وإن وصفتها فلا أوفيها حقها إلى من كان صدرها

الأمان الدائم لي وابتسامتها الدنيا التي أعيش لها إلى من

صوتها كان التفاؤل نفسه إليها اقول أحبك. إليك انت كل شيء

إليك أقول أنت أنا. – أمي الغالية

إلى أبي العزيز الذي أفنى عمره في تربيتنا ورعايتنا

أطال الله في عمرهما

الى زوجتي وأبنائي حفظهم الله

إلى من أعمل لهم في قلبي أرقى وأنبل الإحساس إخوتي

وأخواتي حفظهم الله

إلى جميع العائلة والأصدقاء

الذي وسعهم قلبي ولم يسعهم قلمي. إلى كل هؤلاء أهدي ثمرة

جهدي المتواضع.

تونسي أحميدة

اهداء

بسم الله الرحمان الرحيم

"وقل اعملوا فسيرى الله عملكم ورسوله والمؤمنون"

الى روح أبي الغالي رحمه الله وأسكنه فسيح جناته

إلى هدية الرحمان منال الحب والحنان إلى التي علمتني الأصول والإحترام إلى أمي الغالية.

إلى كل أفراد العائلة كبيرا وصغيرا وأسأل الله أن يحفظهم

إلى كل أخوتي وأخواتي

إلى كل الزملاء والزميلات

إلى كل الذين يسعهم قلبي ولم تسعهم صفحتي.

مسعودي بدر الدين


المقدمة

لقد غيّر التطور التكنولوجي العميق الذي شهده العالم خلال العقود الأخيرة من معالم الحياة الإنسانية في مختلف جوانبها، حيث باتت تكنولوجيا المعلومات والاتصال تلعب دورًا محوريًا في الأنشطة الإدارية، الاقتصادية، التعليمية، وحتى الأمنية. وقد أدّى هذا التحول إلى ولادة ما يُعرف بـ"المجتمع الرقمي" الذي أتاح للأفراد والمؤسسات والدول فرصًا غير مسبوقة للتواصل وتبادل البيانات، ولكنّه في ذات الوقت كشف عن مخاطر جديدة تمثلت أساسًا في ظهور نوع جديد من الإجرام هو "الإجرام المعلوماتي" أو "الجريمة السيبرانية."

إن الجريمة المعلوماتية لم تعد مجرد تهديد محتمل، بل أصبحت واقعًا ملموسًا تتسارع وتيرته يومًا بعد يوم، وهي تختلف عن الجرائم التقليدية في عدة جوانب، لعل أبرزها: الطابع غير المادي للوسيلة والنتيجة، غموض هوية الجاني، اتساع الرقعة الجغرافية للجريمة، وصعوبة تتبع الأدلة، بل وأحيانًا انعدام الإقليمية وامتداد الأثر العابر للحدود. ومما يزيد الأمر تعقيدًا أن مرتكبي هذه الجرائم غالبًا ما يمتلكون مهارات تقنية عالية تمكنهم من تنفيذ أفعالهم الإجرامية عن بُعد، وبوسائل يصعب كشفها وتتبعها.

وأمام هذا الواقع المتغيّر، أصبحت الدول ملزمة بإعادة صياغة مناهجها التشريعية والقضائية، ووضع أنظمة قانونية وأمنية تستجيب للخصوصيات المستحدثة للجريمة المعلوماتية، سواء على مستوى التجريم والعقاب أو على صعيد التحريات والإجراءات القضائية .وفي هذا الإطار، لم تكن الجزائر بمنأى عن هذه المتغيرات، حيث عمد المشرع الجزائري، بدايةً من سنة 2004، إلى سنّ جملة من الأحكام القانونية تهدف إلى تنظيم مجال مكافحة الجريمة المعلوماتية، من خلال إدراج نصوص جزائية في قانون العقوبات ، وفرض آليات إجرائية خاصة تتلاءم مع خصوصية هذا النوع من الجرائم.

ورغم هذه الخطوات التشريعية، لا تزال الجريمة المعلوماتية في الجزائر تمثل تحديًا حقيقيًا لأجهزة إنفاذ القانون، سواء على مستوى الوقاية أو المكافحة، حيث إن الطبيعة التقنية المعقدة للجريمة تتطلب أدوات متخصصة في التتبع والتحقيق، كما تتطلب كفاءة بشرية

مدرّبة، وتشريعات مرنة قادرة على التكيف مع التحديثات المتسارعة التي يعرفها الفضاء السيبراني. ويزداد الوضع تعقيدًا في ظل ضعف التعاون الدولي التقني والجنائي، وضبابية مفاهيم السيادة الرقمية والأدلة الإلكترونية المقبولة، ومن خلال ما سبق نطرح التساؤل الرئيسي للدراسة :

ما مدى كفاءة وفعالية الآليات الإجرائية التي أقرها التشريع الجزائري في التصدي للجريمة المعلوماتية؟

وبناءا على التساؤل الرئيسي للدراسة نطرح التساؤلات الفرعية التالية :

- ما المقصود بالجريمة المعلوماتية وما هي خصائصها في القانون الجزائري؟

- ما هي الآليات القانونية والإجرائية التي اعتمدها المشرّع الجزائري لمكافحة الجريمة المعلوماتية؟

-ما مدى فعالية هذه الآليات في الكشف عن مرتكبي الجريمة المعلوماتية ومتابعتهم قضائيًا؟

تنبع أهمية هذه الدراسة من الأهمية المتزايدة لموضوع الجريمة المعلوماتية، الذي بات يشكل تهديدًا حقيقيًا لأمن الأفراد والمؤسسات والدول على حد سواء، خاصة مع التوسع المتسارع في استخدام تكنولوجيا المعلومات والاتصالات في مختلف مناحي الحياة. وتزداد أهمية الدراسة في السياق الجزائري نظرًا لحداثة النصوص التشريعية التي تُعالج هذا النوع من الجرائم، مما يفرض ضرورة تحليل وتقييم الآليات القانونية والإجرائية المعتمدة لمكافحتها، والتأكد من مدى فعاليتها في التصدي لهذا النمط الجديد من الإجرام الذي يتجاوز في كثير من الأحيان الحدود الجغرافية التقليدية. كما تسهم هذه الدراسة في دعم المشرّع والجهات الأمنية والقضائية بمقترحات قد تساعد في تحسين الأداء التشريعي والمؤسساتي لمواجهة هذه التحديات التقنية المعقدة، وهو ما يُكسب الدراسة بعدًا علميًا وعمليًا في آن واحد.

و أما أهداف الدراسة تتمثل في :

- التعرف على مفهوم الجريمة المعلوماتية وخصائصها القانونية والتقنية.
- تحليل الإطار التشريعي الجزائري المنظم لمكافحة الجريمة المعلوماتية.
- دراسة الآليات الإجرائية التي تعتمدها السلطات المختصة في التصدي لهذا النوع من الجرائم.
- إبراز التحديات والصعوبات التي تواجه تطبيق النصوص القانونية في هذا المجال.

و أسباب إختيارنا لدراسة هذا الموضوع , أولها أسباب ذاتية تتمثل في :

- الاهتمام الشخصي بالجرائم المستحدثة في البيئة الرقمية.
- الرغبة في التعمق في الجوانب القانونية والإجرائية للجريمة المعلوماتية.
- تطلع الباحث إلى المساهمة العلمية في موضوع معاصر وذي أبعاد تقنية وقانونية.
- توافر خلفية أكاديمية مرتبطة بالقانون الجنائي والتشريع الجزائري.

و ثانيًا الأسباب الموضوعية و تتمثل في :

- تزايد معدلات الجريمة المعلوماتية في الجزائر والعالم بشكل ملحوظ.
- قلة الدراسات القانونية المتخصصة التي تعالج الجانب الإجرائي في مكافحة هذه الجريمة.
- الحاجة الماسة لتقييم مدى فعالية التشريعات الجزائرية في مواكبة التطورات التكنولوجية.

و إعتمدنا في هذا البحث على المنهج الوصفي التحليلي، وذلك من خلال تحليل النصوص القانونية والتنظيمية ذات الصلة بمكافحة الجريمة المعلوماتية في التشريع الجزائري، بهدف الوقوف على الآليات الإجرائية التي أقرها المشرّع ومدى فعاليتها في مواجهة هذه الظاهرة المتنامية. كما يستند إلى المنهج المقارن، عند الضرورة، لمقارنة بعض الجوانب الإجرائية مع

التشريعات العربية أو الأجنبية ذات التجربة الرائدة في هذا المجال، من أجل إبراز أوجه القصور أو القوة في النموذج الجزائري. ويساعد هذا الجمع بين المنهجين على تقديم رؤية شاملة ومتكاملة للجوانب النظرية والتطبيقية للموضوع محل الدراسة.

-الدراسات السابقة :

الدراسة الأولى :دراسة عبد الله بن سعيد الشهراني بعنوان *"الجريمة الإلكترونية في النظام السعودي: دراسة تحليلية مقارنة"*، تخصص قانون، جامعة نايف العربية للعلوم الأمنية، 2017، والتي سعت إلى تحليل البنية القانونية لمكافحة الجريمة المعلوماتية في السعودية، وركّزت على بيان أوجه النقص في النصوص، واعتمدت المنهج التحليلي المقارن، وتوصّلت إلى ضرورة تطوير التشريعات بما يتماشى مع المستجدات الرقمية.

الدراسة الثانية : دراسة كريمة بوكرط بعنوان *"مكافحة الجريمة الإلكترونية في التشريع الجزائري والمقارن "*تخصص قانون جنائي، جامعة الجزائر 1، 2019، والتي تناولت الإطار القانوني والتنظيمي للجريمة المعلوماتية في الجزائر مقارنة ببعض التشريعات الأجنبية، وطرحت إشكالية مدى كفاية التشريع الجزائري في الحد من هذه الجرائم، معتمدة على المنهج الوصفي التحليلي، وانتهت إلى توصيات أبرزها ضرورة تحديث الترسانة القانونية ومواكبة الاتفاقيات الدولية.

الدراسة الثالثة : دراسة سمية عكاشة بعنوان *"التحقيق الجنائي في الجرائم المعلوماتية "*، تخصص علوم جنائية، جامعة باتنة، 2020، وركزت هذه الدراسة على آليات جمع الأدلة الرقمية والتحديات المرتبطة بها، وبيّنت أهمية التكوين التقني لأعوان الضبطية القضائية، واعتمدت المنهج الوصفي، وخلصت إلى أن نجاح ملاحقة هذا النوع من الجرائم مرتبط بشكل مباشر بامتلاك الإمكانيات التكنولوجية والقانونية المناسبة.


الفصل التمهيدي

المبحث الأول : ماهية الجريمة المعلوماتية .

الجرائم المعلوماتية هي من الجرائم الحديثة نسبيا، والتي ظهرت بظهور تكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات، وهي بلا جدال جرائم ضربت بقوة وتنامت بسرعة فائقة في ضل الانفتاح العالمي وارتباط الأسواق العالمية ببعضها البعض، فأصبحت تشكل خطرا يهدد الأفراد في ممتلكاتهم وخصوصياتهم[1]، والمؤسسات في كيانها المادي والاقتصادي، ونظرا لجسامة أخطار هذه الجرائم وفداحة خسائرها وسرعة انتشارها من جهة وحداثتها النسبية من جهة أخرى وهذا ما سنحاول التطرق إليه في هذا المبحث من خلال تقسيمه إلى مطلبين المطلب الأول تحت عنوان تعريف الجريمة المعلوماتية والمطلب الثاني بعنوان "صور الجريمة المعلوماتية".

المطلب الأول: تعريف الجريمة المعلوماتية

تعتبر الجرائم المعلوماتية من الأنماط المستحدثة التي رافقت التطور التكنولوجي الحديث، فهي لم تحظ بعد بالاستقرار على النحو الذي حظيت به نظيرتها من الجرائم التقليدية، الأمر الذي أدى الى وجود اختلافات جوهرية بين شرائح القانون بصفة عامة والقانون الجنائي بصفة خاصة، سواء من حيث المصطلحات المستخدمة للتعبير عنها، أو من حيث التعريفات التي وضعت لها. [2]

مع دخول الحاسوب والانترنت إلى مجتمعاتنا وفي كافة جوانب حياتنا بدأ يظهر نوع جديد من الجرائم تسمى الجرائم المعلوماتية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم والتوعية حولها، حيث سنقوم بتعريفها قانونيا وفقهيا.

---

[1]– بن زرط أسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، ميدان الحقوق والعلوم السياسية، تخصص قانون جنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم 2018–2019، ص 02.

[2]– نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت،2005 بدون صفحة.

الفرع الأول: التعريف الفقهي.

لقد أعطى الفقهاء والدارسون عددا ليس قليلا من التعريفات تتميز وتتباين تبعا لموضع العالم المنتمي إليه وتبعا لمعيار التعريف ذاته، وقد اجتهدنا في جمع غالبية التعريفات التي وضعت في هذا الحقل، فمن التعريفات التي تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك محل التجريم ، تعريف الأستاذ ROSENBALT بأنه نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو هي كما عرفها الفقيه سولارز وهي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات.[1]

أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة فان أصحابها ينطلقون من أن الجرائم المعلوماتية تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة، ومن هذه التعريفات تعريف الأستاذ جون فورستر فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية ويعرفها ادمان بأنها كل أشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب ونشير أيضا إلى أن جانبا من الفقه والمؤسسات ذات العلاقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل فتعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية أي جريمة لفاعلها معرفة فنية بالحسابات تمكن من ارتكابها، كما عرفها الأستاذ دافيد تومسن أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي.[2]

يعرف الفقيه الفرنسي (Mass) جريمة الكمبيوتر بأنها " الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد

[1]– هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة 1992، ص 120.

[2]– هشام محمد فريد رستم ، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة 2000، ص 20.

الأموال استخدم لهذا التعري[1]ف معيارين هما الوسيلة، وتحقيق الربح المستمد من معيار محل الجريمة المتمثل في المال.

ويعرفها الفقيهان الفرنسيان (Vivant و Le Stant)بأنها مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب، هذا التعريف مستند من بين معيارية على احتمال جدارة الفعل بالعقاب وهو معيار غير منضبط ولا يستقيم مع تعريف قانوني وان كان يصلح هذا التعريف في نطاق علوم الاجتماع وغيرها.

ذهب الفقيه (Merwe) إلى أن الجريمة المعلوماتية هي: "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الاجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية".

الفرع الثاني : التعريف القانوني

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02 الفقرة القانون أ- **من** رقم 04-09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بالقول بأن "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية، فإنه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب المتعلقة بالجريمة هذه فنعرفها بأنها "كل السلوكات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها أو محلا لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الإلكترونية".

[1]- براهيمي سهام، مذكرة لنيل إجازة المدرسة العليا للقضاء الجزائر، 2004-2005 ص07.

المطلب الثاني: صور الجريمة المعلوماتية

حسب يصنف الفقهاء والدارسون جرائم الكومبيوتر والانترنت ضمن فئات متعددة، تختلف الأساس والمعيار الذي يستند إليه التقسيم المعني، فبعضهم يقسمها إلى جرائم ترتكب على نظام الحاسوب وأخرى ترتكب بواسطته وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، وكذا تعدد الحق المعتدي عليه، فتوزع جرائم الحاسوب وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الحياة الخاصة، ومن الملاحظ أن هذه التقسيمات لم تراعي خصائص هذه الجريمة وموضوعها، والحق المعتدي عليه لدى وضعها الأساس أو معيار التقسيم. [1]

الفرع الأول: الجرائم الواقعة على الكومبيوتر

الجرائم الواقعة على الكمبيوتر تنصب بدخول المواقع أو الأجهزة بطريقة غير مشروعة أو بطريقة مشروعة كما لو تمت الجريمة من قبل موظف مختص أو إتلاف البيانات أو سرقها أو نسخها أو تبديلها أو نشر فيروس يؤدي إلى ما ذكر، وقد تتعدد أسماء وأشكال الجرائم التي تستهدف الكمبيوتر ولكن كلها تدور في حلقة واحدة، فهذه الجرائم قد تتغير أساليب وطرق ارتكابها مع التطور التكنولوجي.[2]

[1]– عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر الطور الثاني ميدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير ، تخصص إدارة تحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح ورقلة 2018–2019 ص04.

[2]– بلعيد منصورية، النظام الإجرائي للجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، ميدان الحقوق والعلوم السياسية، تخصص قانون قضائي، جامعة عبد الحميد بن باديس 2019–2020، ص ص 27.28.

أولا: الدخول والبقاء غير المصرح به لنظام المعالجة الآلية:

حسب نص المادة 394مكرر عاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50000 دج إلى دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو 100.000 دج أو يحاول ذلك.

وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة. وإذا ترتب عن الأفعال المذكورة أعلاء تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000دج.[1]

تكون الجريمة في صورتها البسيطة إذا كانت مجرد دخول وبقاء غير مشروع، وإما إذا توافرت ظروف معينة ينتج فيها عن الدخول والبقاء غير المشروع تغيير في المعطيات فتحقق الصورة المشددة.

1- فعل الدخول : أي الاطلاع على المعلومات التي تمت معالجتها دون التصريح والدخول قد يكون مباشرا أو غير مباشرا بالنسبة للدخول المباشر فله عدة صور حيث أن الجاني يمكنه الاستيلاء على المعلومات المخزنة بعده طرق سواء بطبعها أو استخدام شاشة النظام أو قراءة ما هو مكتوب أو استخدام ما هو مكبر الصوت.

أما الولوج غير المباشر يكون عن طريق إمكانيات حديثة يتم من خلالها الولوج والاستفسار من المراكز المعلوماتية عن بعد، فتكون المعلومات مهددة بالالتقاط والتسجيل غير المشروع

[1]- المادة 394 مكرر من القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الامر 66-156 المتضمن قانون العقوبات الجزائري.

في أي لحظة، كالقيام مثلا بتوصيل نظام معلوماتي بالنهاية الطرفية ومعرفة كلمة السر أو الشفرة المناسبة.[1]

2- فعل البقاء : يعتبر البقاء جريمة إذا تم طباعة نسخة من المعلومات في الوقت الذي له فيه بالرؤية فحسب، كما نجده أيضا في الخدمات المفتوحة للجمهور مثل: الخدمات التلفزيونية التي يمكن للمجرم من خلال طرق غير مشروعة الحصول على الخدمات دون مقابل، أو زيادة مدة استفادته من الخدمة، ألا أنه قد يجتمع فعلا الدخول والبقاء غير المشروعين معا، وذلك في حالة ما إذا لم يكن من حق الجاني الدخول إلى النظام.

يعتبر قانون العقوبات الجزائري من القوانين العربية السباقة إلى هذا الموضوع حيث خطى المشرع هذه الخطوة بالمبادرة إلى تقدير قانون العقوبات بمقتضى القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 بإدراج القسم السابع بمحتوى المادة 394 مكرر إلى 394 مكرر 7، ويبدو أن المشرع لم يكتف بذلك بل قطع أشواطا أخرى في اتجاه فرض حماية جنائية على حياة الافراد الخاصة.

ثانيا: جريمة التلاعب بمعطيات الحاسب الآلي

نص عليها المشرع الجزائري في المادة 394 مكرر 1 على أنه "يعاقب بالحبس من سنة أشهر (6) أشهر إلى ثلاث (3) سنوات وبغرامة مالية من 500.000 دج إلى 400.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها .[2]

[1]- عميور خديجة، قواعد اختصاص ألقطاب الجزائية للنظر في جرائم الفساد، مجلة دراسات في الوظيفة العامة، العدد 02 جامعة جيجل 2014. ، ص 28

[2]- المادة 394 مكرر 1 من قانون العقوبات الجزائري.

جريمة التلاعب الثانية التي ينص عليها قانون العقوبات الجزائري بعد جريمة الدخول والبقاء غير المصرح بها ، أما قانون العقوبات الفرنسي فينص عليها بعد جريمة إعاقة وإفساد أنظمة المعالجة نظرا للتشابه الكبير بينهما وبين جريمة التلاعب بالمعطيات بحيث يصعب في الكثير من الأحيان التمييز بينهما وذلك لأن الأفعال التي تتضمنها جريمة التلاعب تؤدي الأخرى إلى إعاقة النظام وإفساده، وقد اكتفى المشرع الجزائري نتيجة إفساد النظام كظرف مشدد فقط لجريمة الدخول واستبعادها كجريمة قائم بذاتها والنشاط الإجرامي في هذه الجريمة يتمثل في أفعال الإدخال والتعديل، ويكفي توافر أحدهما لقيام الجريمة لا يشترط اجتماعها حتى يتوافر النشاط الإجرامي فيها ، ومن ثم يقام الركن المادي للجريمة لكن القاسم المشترك في هذه الأفعال جميعها هو انطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل.[1]

الفرع الثاني: الجرائم الواقعة على الأشخاص

إن للحياة الشخصية خصوصية و حرمة لا يجوز لأي شخص أن يقتحمها، ومثال ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الخاصة بشخص ما، أو تسجيل مكالمات أو فيديو أو مراقبته.

أولا: جرائم القذف والسب وتشويه السمعة.

تعد جرائم السب والقذف الأكثر شيوعا في نطاق الشبكة، حيث يستعمل الجاني حسب القواعد العامة جرائم القذف والسب عبارات رديئة تمس شرف المجني عليه، بل إن إرادته اتجهت لذلك بالذات، وبالتطور أصبحت الإنترنت إحدى هذه الوسائل إذ لم نقل أكثرها رواجا

[1]– ابتسام موهوب، جرائم المساس بأنظمة المعالجة الآلية لمعطيات للتشريع الجزائري ، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي 2014–2015 ص 15

فعادة ترسل عبارات السب والقذف عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب ما يؤدي بكل من يدخل هذا الموقع مشاهدتها أو الاستماع إليها، ويتحقق بذلك ركن العلنية الذي تطلبه الكثير من التشريعات في السب العلني[1]، وإذا لم يطلع عليها أحد فإنه يمكن تطبيق مواد السب أو القذف غير العلني ، وهذا مانصت عليه المادة 144 مكرر 3" يعاقب بغرامة من 10.000دج الى 500.000 دج، كل من اساء الى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان عن طريق الكتابة أو الرسم أو التصريح أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية ".[2]

ثانيا: جرائم الاعتداء على حركة الحياة الخاصة

تعتبر جرائم الاعتداء على حرمة الحياة الخاصة من الجرائم القديمة التي عرفتها المجتمعات الإنسانية القديمة ولكنها سرعان ما تطورت نظرا للتقدم التكنولوجي الذي لعب دور في سرعة وسهولة انتشار الأخبار والصور الذي من شأنه أن يمثل تهديدا لخصوصية الأشخاص وسهولة الاعتداء على حرمة حياتهم الخاصة ومن هنا كانت الحاجة إلى وجود حماية قانونية صارمة تساهم في الحد من هذه الجرائم وهذا نصت عليها المادة 303 مكرر" يعاقب بالحبس من سنة (6) أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك[3]:

1-بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

[1]- سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماجستير ، كلية الحقوق والعلوم السياسية، جامعة خيضر بسكرة 2014 ص 26.

[2]- المادة 144 مكرر من قانون العقوبات.

[3]- المادة 303 مكرر من قانون العقوبات.

2 –بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه."

المبحث الثاني : خصائص وأركان الجريمة المعلوماتية .

مع تطور وسائل التكنولوجيا والاعتماد المتزايد على الفضاء الرقمي في مختلف مجالات الحياة، برزت أنماط جديدة من الجرائم لم تكن مألوفة في السابق، من أبرزها الجريمة المعلوماتية، التي باتت تشكل تهديدًا حقيقيًا لأمن الأفراد والدول والمؤسسات على حد سواء. وتتميز هذه الجرائم بخصائص فريدة تختلف عن الجرائم التقليدية من حيث الفاعل، والوسيلة، والمكان، والزمان، وحتى من حيث الأدلة الجنائية وطبيعة التحقيق.

ويهدف هذا المبحث إلى تسليط الضوء على الخصائص الجوهرية التي تميز الجريمة المعلوماتية عن غيرها من الجرائم، من حيث الطابع اللا مادي، والانتشار السريع، والطبيعة العابرة للحدود، وغيرها من السمات الخاصة. كما يتناول المبحث الأركان الأساسية التي يقوم عليها هذا النوع من الجرائم، وهي الركن القانوني، والركن المادي، والركن المعنوي، وهي أركان لا بد من توفرها معًا لقيام المسؤولية الجنائية في إطار هذا النمط المستحدث من الجرائم.[1]

المطلب الأول: خصائص الجريمة المعلوماتية.

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواحي، سواء كان هذا التميز في السمات العامة لها أو في الباعث على تنفيذها أو في طريقة هذا التنفيذ ومن أهم خصائصها:

[1]- - خضري حمز ، عشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجازئري، مجلة الدراسات القانونية والسياسية، العدد 02 المجلد 6 جامعة محمد بوضياف، المسيلة جوان 2020. ص42

الفرع الأول : صعوبة اكتشاف الجريمة المعلوماتية:

تتسم الجرائم الناشئة عن استخدام الانترنت بأنها خفية ومستترة في أغلبها ، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الجزائر.

كما أن وسيلة تنفيذها تتميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى الأحجام عن التبليغ عنها في حالة اكتشافها لخشية المجني عليهم فقدان عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة تقل عن الثانية. [1]

تتميز الجريمة المعلوماتية بصعوبة اكتشافها واذا اكتشفت فان ذلك يكون بمحضي الصدفة عادة ، ويمكن رد الاسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية لعده امور قيام الجاني بارتكاب هذه الجريمة في دول وقارة أخرى وقدرته على إخفاء دليل الإدانة في وقت قياسي يشكل عاملا اضافيا في صعوبة اكتشاف هذه الجرائم يلعب المجني عليه دور رئيسيا في صعوبة وقوع الجريمة المعلوماتية ويظهر ذلك في عدة جوانب منها تحرص أكثر الجهات التي تتعرض انظمتها المعلوماتية للانتهاك على عدم الكشف عن ما تعرضت له وتكتفي عاده باتخاذ اجراءات اداريه داخليه دون الابلاغ عنها السلطات المختصة تجنبا للتشهير بها وهز الثقة في كفايتها الى جانب ذلك فأن المجني عليه يتردد احيانا في الابلاغ عن هذه الجرائم.

[1]– عمار حشمان، ن المرجع السابق، ص 10.

ولعل أبرز مثال على احجام المجني عليه عن الابلاغ يظهر في المؤسسات المالية خوفا من التشهير بها وزعزعه ثقة العملاء بها.[1]

الفرع الثاني: صعوبة إثبات الجريمة المعلوماتية.

فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلبها لاكتشافها والبحث عنها ، وتستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي ضد هذه الظاهرة، حيث لم تعد القوانين التقليدية قادرة على مواجهة تطور الجريمة المعلوماتية في ظل السرعة الهائلة للتطورات التكنولوجية[2].

الفرع الثالث: أسلوب ارتكاب الجريمة المعلوماتية.

الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها ، وطريقتها ، فإذا كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر كما هو الحال في جريمة السرقة،2 وتحتاج كذلك إلى وجود شبكة المعلومات الدولية الانترنت مع وجود مجرم يوظف خبرته التوجه النظري والإطار المنهجي للدراسة أو اختراق خصوصيات الغير للتغرير وقدراته على التعامل معالشبكة للقيام بجرائم مختلفة كالتجسس بالقاصرين كل ذلك دون الحاجة لسفك الدماء.

[1]– لصغير جميل عبد الباقي، القانون الجنائي والتكنولوجية الحديثة، ط1 دار النهضة العربية، القاهرة 1992، ص 17.

[2]– نهلة عبد القادر مومني، الجرائم المعلوماتية، ط2 دار الثقافة للنشر والتوزيع ب س ن، صص 57.58.

الفرع الرابع: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص .

تتميز الجريمة المعلوماتية عادة أنها تتم بتعاون أكثر من شخص على ارتكابها للإضرار بالجهة المجني عليها، وغالبا ما يشترك في إخراج الجريمة المعلوماتية إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت، يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.[1]

تتسم الجريمة المعلوماتية بأنها يتم تنفيذها من عدة اشخاص حيث يكون هناك شخص متخصص في التقنيات المعلوماتية يقوم بالجانب التقني من المشروع الاجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطيه عملية الاحتيال والتحويل الأرباح إليه والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون بفعل سلبي من خلال صمت من يعلم بهذه الجريمة لتسهيل تنفيذها وقد يكون بفعل ايجابي من خلال المساعدة أي كان نوعها.[2]

المطلب الثاني: أركان الجريمة المعلوماتية

تتشكل الجريمة المعلوماتية من الاركان الثلاثة المعروفة للجريمة الكلاسيكية، غير ان الأولى تتميز بخصوصيات تجعلها تختلف نوعا ما عن الجريمة الثانية، وهذا ما سنبينه من خلال هذا المبحث بتفصيل الاركان الثلاثة لهذه الجريمة والمتمثلة في الركن الشرعي للجريمة المعلوماتية الفرع الأول، والركن المادي لها (الفرع الثاني، وأخيرا الركن المعنوي لقيامها (الفرع الثالث).

[1]– عمار حشمان، المرجع السابق، ص 11.

[2]– عفيفي عفيفي كامل، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية، ط1، دار الكتب القانونية، القاهرة 2002 ص13

الفرع الأول: الركن الشرعي للجريمة المعلوماتية

انطلاقا من مبدأ الشرعية وفقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على: "لا جريمة ولا عقوبة أو تدابير امن بغير قانون حرم القانون رقم 04-15 بعض صور الجريمة المعلوماتية ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات [1]" من الفصل الثالث المعنون" الجنايات والجنح ضد الأموال من الباب الثاني المتعلق بالجنايات والجنح ضد الأفراد وذلك في المواد من 394 مكرر إلى 394 مكرر 08 من قانون العقوبات المعدل والمتمم. في حين جاء القانون 09-04[2] متضمنا للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية، من خلال وضع ترتيبات تقنية المراقبة الاتصالات الالكترونية وتسجيل وتجميع محتواها في حينها والقيام بإجراءات التفتيش داخل المنظومة المعلوماتية، ولجوء المشرع الى تقنين او النص على مثل هذه الجرائم وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء إلى القياس،[3] بمعنى عدم جواز لجوء القاضي الجنائي الى قياس فعل لم يرد نص على تحريمه على فعل ورد نص بتحريمه، فيقرر القاضي الجنائي للأول عقوبة الثاني بسبب التشابه بين التشابه بين الفعلين .

[1]- حمز خضري، عشاش ،حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، العدد 02، المجلد 6، جامعة محمد بوضياف المسيلة، جوان 2020 ص 173.

[2]- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 47، بتاريخ 16 أوت 2009.

[3]- أحمد خليفة الملط الجرائم المعلوماتية دار الفكر الجامعي للنشر والتوزيع، مصر 2006، ص10.

الفرع الثاني: الركن المادي للجريمة المعلوماتية

يعتبر الركن المادي للجريمة هو المظهر الخارجي لها وكيانها المادي الظاهر، وهو الماديات المحسوسة في العالم الخارجي كما حددتها نصوص التجريم، فالقاعدة أنه "لا" جريمة دون ركن مادي" أو "لا" جريمة فعل[1]"، إلا أن الركن المادي للجريمة المعلوماتية يختلف نوعا ما عن الجرائم التقليدية كون انه يقوم على صور في فعل الاعتداء والمتمثلة في:

أولا: الدخول او البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك.

نصت المادة 394 مكرر في قانون العقوبات على أن الدخول أو الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك يشكل فعلا إجراميا ولهذا الفعل حسب المادة المذكورة صورتين كالتالي:

1- الصورة البسيطة يتمثل النشاط الاجرامي في هذه الصورة في الافعال الآتية: أ فعل الدخول يتحقق فعل الدخول بمجرد الوصول الى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبه لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات.

ب – البقاء : معنى البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام، أو بتجاوز المدة المسموح له بالبقاء فيها، أو عدم الانسحاب فورا وقطع وجوده في نظام البيانات أو يطبع معلومات حين يسمح له بالرؤية فقط.

[1]– عبد الرحمان خلفي محاضرات في القانون الجنائي العام، دار الهدى للطباعة والنشر والتوزيع الجزائر، دون طبعة ص101.

2- الصورة المشددة

نصت المادة 394 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين أما محو أو تحويل المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب نظام اشتغال المنظومة. [1]

ثانيا : ادخال المعطيات بطريق الغش

يقصد بفعل الادخال حسب المادة 394 مكرر 01 من قانون العقوبات اضافة معطيات جديدة الى نظام المعالجة الآلية او التعديل من معلومات داخله كان يتضمنه مسبقا فغير فيها، ومثال ذلك حالة الاستخدام التعسفي البطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير [2].

الفرع الثالث: الركن المعنوي للجريمة المعلوماتية

يتخذ الركن المعنوي في اغلب الجرائم بصفة عامة صورة القصد الجنائي، والذي يتحقق بتوافر إرادة بعمل غير شرعي لدى الجاني مع علمه بأن القانون يجرمه، ونفس الأمر ينطبق على الجريمة المعلوماتية التي يقوم ركنها المعنوي على توافر الارادة الجرمية لدى الفاعل، وهذا ما يظهر من خلال استعمال المشرع الجزائي لعبارة "الغش" و "العمد" "الاعداد الجريمة" في المواد 394 مكرر و 394 مكرر 1 و 394 مكرر 2 وفي الخير 394 مكرر 5 من قانون العقوبات، وهذا ان دل فإنما يدل على ان الجريمة المعلوماتية جريمة عمدية بامتياز ولا يفترض فيها عنصر الخطأ هذا ويختلف الركن المعنوي في الجرائم المعلوماتية من جريمة

[1]- حمز خضري، حمزة عشاش المرجع السابق، ص 174.

[2]- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع الجزائر 2007 ص121.

إلى أخرى فجريمة الدخول غير المصرح به الى نظام الحاسب الآلي تتطلب قصدا جنائيا يتمثل في علم الجاني بعناصر الركن المادي للجريمة، أي العلم بأن الولوج إلى داخل النظام بشكل غير مصرح بعد جريمة باعتبار حماية المشرع محل الحق وهو الحاسب الآلي لما يتضمنه من برامج ومعلومات.[1]

وفي جريمة الاحتيال الالكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي القيام مسؤولية الجاني والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام والخاص، فالمحرم يعلم بأنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع. [2]

[1]– حمز خضري وعشاش ،حمزة المرجع السابق، ص 175.

[2]– عبد العزيز أحمد ، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي والعلوم الجنائية كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي سعيدة 2021–2022 ص 19.

الفصل الأول
القواعد الاجرائية لمكافحة الجريمة المعلوماتية

تمهيد :

مع تزايد الاعتماد على تكنولوجيا المعلومات والاتصالات في شتى مجالات الحياة اليومية، برزت تحديات قانونية وأمنية جديدة، تمثلت في ظهور نمط جديد من الجرائم يُعرف بـ "الجريمة المعلوماتية"، والتي باتت تُشكل تهديدًا خطيرًا للأمن العام،الاقتصادي والاجتماعي، نظراً لطبيعتها غير التقليدية وارتباطها بالبيئة الرقمية. وقد أصبحت هذه الجرائم تأخذ أشكالاً متعددة، كاختراق الأنظمة الإلكترونية، والتجسس الرقمي، والاحتيال عبر الإنترنت، وسرقة الهوية، والتشهير، وانتهاك الخصوصية، وغيرها من الأفعال التي تنفذ عبر أدوات تكنولوجية معقدة، ما يجعل اكتشافها وملاحقة مرتكبيها أكثر تعقيداً من الجرائم التقليدية.

ونظراً لهذه الخصوصية، أصبح من الضروري وضع قواعد إجرائية قانونية متخصصة لمكافحة هذا النوع من الإجرام، تضمن فعالية الكشف عن الجريمة، وتحقيق الدقة في جمع الأدلة الرقمية، مع مراعاة احترام حقوق الأفراد وخصوصيتهم.

وفي هذا الإطار، عمل المشرع الجزائري على استحداث منظومة قانونية تتماشى مع خصوصية الجريمة المعلوماتية، من خلال القانون رقم 09/04 [1]المؤرخ في 5 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والقانون رقم 04/18 المؤرخ في 10 ماي 2018،[2] الذي أدرج مفهوماً جديداً للجريمة المعلوماتية، محدداً إياها على أنها كل فعل يمس بأنظمة المعالجة الآلية للمعطيات أو يرتكب باستخدام وسائل إلكترونية.

[1]–القانون رقم 04–09 المؤرخ في 5 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الجريدة الرسمية للجمهورية الجزائرية العدد 46 الصادرة بتاريخ 05 أوت 2009.
النصوص العقابية. الجريدة الرسمية للجمهورية الجزائرية، العدد 27، الصادرة بتاريخ 16 ماي 2018.

[2]– القانون رقم 18–04 المؤرخ في 10 ماي 2018 يتضمن تعديل قانون العقوبات، بإدراج الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ضمن النصوص العقابية. الجريدة الرسمية للجمهورية الجزائرية، العدد 27 ،الصادرة بتاريخ 2018. ماي 16

المبحث الأول : التفتيش كإجراء تقليدي لضبط الدليل الرقمي

يناط بالتفتيش البحث عن الوسيلة التي استخدمت في ارتكاب الجريمة أو لها علاقة بمرتكبها، غير أنه وباعتبار أن المعلوماتية تتضمن كيانات مادية، وأخرى معنوية فإنه كان لزاما أن يكون هناك نوعين من التفتيش نشير إليهما كالتالي [1]:

تفتيش الكيانات المادية، ويشمل كل الكيانات المادية ذات الطابع المادي الملموس، والمرتبطة بالجريمة مع مراعاة جملة من الضوابط، و المتمثلة في:

– تحديد المكان الذي توجد به الكيانات المادية أو الأجهزة.

– تبيان ما إذا كان المكان عام أو خاص، باعتبار أن تفتيش الأماكن الخاصة كالمنازل من شأنه المساس بخصوصية الأشخاص.

–التمييز بين ما إذا كانت مكونات الكمبيوتر المراد تفتيشها منعزلة عن غيرها من أجهزة الكمبيوتر، أو متصلة بمكان آخر.[2]

تفتيش المعدات المعنوية، إذ اختلف الفقه القانوني حول إمكانية خضوع المعدات المعنوية وغير المادية للتفتيش، و تم الخروج برأي راجح مفاده إمكانية خضوع الكيانات المعنوية للتفتيش، و يبقى من الضروري أن ينص المشرع صراحة على جوازية تفتيش المكونات المعنوية للحاسوب ومن ثم و من أجل دراسة إجراء التفتيش كإجراء تقليدي للكشف عن الجريمة المعلوماتية، تجدر الإشارة إلى أنواع التفتيش المطلب الأول، بالإضافة إلى الوقوف على الضبط كإجراء يتبع التفتيش(المطلب الثاني).

[1]–رحيمة نمديلي، خصوصية الجريمة اللإكترونية في القانون الج ازئري و القوانين المقارنة، كتاب أعمال المؤتمر الدولي الرابع عشر : الجرائم الإلكترونية، مركز جيل البحث العلمي طرابلس ، لبنان ، 24 مارس 2017 ، ص60

[2]- بثينة حبيباتي الطبيعة الخاصة للجريمة المعلوماتية ، دراسات مجلة وأبحاث، مجلد جامعة زيان عاشور، الجلفة، الجزائر، مجلد 12 عدد 03 جويلية 2020 ، ص284

المطلب الأول: أنواع التفتيش

يُعدّ التفتيش أحد أهم الإجراءات التحقيقية التي تلجأ إليها السلطات القضائية للكشف عن الجرائم وجمع الأدلة، لما له من أثر حاسم في الوصول إلى الحقيقة. وتزداد أهمية هذا الإجراء في ظل الجرائم الإلكترونية،[1] بالنظر إلى طبيعتها الخاصة وما تطرحه من تحديات تقنية وقانونية في آن واحد. ونظرًا لما قد ينطوي عليه التفتيش من مساس مباشر بحرمة الحياة الخاصة للأفراد وحقهم في الخصوصية، فقد حرصت غالبية التشريعات الإجرائية على تقييده بضوابط دقيقة تضمن مشروعيته وتمنع التعسف في استعماله.[2]

تنقسم هذه الضوابط إلى نوعين رئيسيين: ضوابط موضوعية تتعلق بأسباب وشروط التفتيش من حيث المضمون الفرع الأول، وأخرى شكلية أو إجرائية تتعلق بكيفية تنفيذه وفقًا للقانون (الفرع الثاني).

الفرع الأول : الشروط الموضوعية للتفتيش الإلكتروني

حتى يكون التفتيش متوافقًا مع القانون لا بدّ من تحقق ثلاثة عناصر أساسية تمثل الشروط الموضوعية له، وهي: وجود سبب مشروع للتفتيش (أولاً)، تحديد محل التفتيش بوضوح (ثانيًا)، وتوفر الصفة القانونية لدى الجهة القائمة به (ثالثا).

[1]– زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، سنة 2011 ص53.–

[2]- محمد زروقي، إجراءات التفتيش في الجرائم الإلكترونية ، المجلة الجزائرية للقانون والعلوم السياسية، العدد 2، 2020، ص. 44

أولاً : سبب التفتيش

يمثل "السبب" أحد الشروط الجوهرية لمشروعية إجراء التفتيش، ويُقصد به توفر دلائل جدية على وقوع جريمة ما تستدعي التدخل للتحقيق وجمع الأدلة. ولا يُعتدّ بالتفتيش متى تم دون وجود مبرر قانوني كافٍ، إذ يُعد حينها إجراءً باطلاً ومخالفًا لأحكام القانون. [1]

وتكتسب هذه القاعدة أهمية خاصة في نطاق الجرائم الإلكترونية، إذ يجب أن يتوافر ما يلي:

- **وقوع جريمة إلكترونية** : لا يجوز إجراء التفتيش ما لم يكن هناك نشاط إجرامي مثبت، يتخذ وصف الجناية أو الجنحة، إذ تُستبعد المخالفات لعدم خطورتها القانونية أو المجتمعية.

- **وجود اتهام موجه لشخص معين** : يجب أن يكون التفتيش موجها ضد شخص يُشتبه في مساهمته في الجريمة، سواء كفاعل أصلي أو كشريك. وإذا عجز قاضي التحقيق عن تحديد المتهم، فقد يُغلق الملف لعدم كفاية الأدلة.[2]
- وجود قرائن قوية : لا يكفي وقوع الجريمة فقط، بل يجب توافر دلائل وقرائن قوية تشير إلى إمكانية وجود أدلة مادية أو رقمية في المكان المراد تفتيشه، مثل أجهزة إلكترونية أو وسائط تخزين أو مستندات رقمية.

ثانياً: محل التفتيش

يقصد بمحل التفتيش في البيئة الرقمية كل ما يتعلق بالنظام المعلوماتي المستخدم من قبل المشتبه فيه، ويشمل ذلك مكونات الحاسب الآلي (الفيزيائية والبرمجية) وكذا شبكات الاتصال المرتبطة به، بالإضافة إلى الحسابات السحابية أو قواعد البيانات المرتبطة بالشخص محل التحقيق.

[1]–محمد صغير، "شرح قانون الإجراءات الجزائية"، دار هومة، الجزائر، 1988، ص. 52.

[2]- أحمد جمال، التحقيق في الجرائم الإلكترونية"، دار الفكر الجامعي، الإسكندرية 2017-2018، ص. 49

ويكتسي تحديد محل التفتيش أهمية خاصة في الجرائم الإلكترونية، نظرًا لاتساع المجال الرقمي وصعوبة حصره مايتطب دقة في تحديد الموقع المراد تفتيشه لتفادي التوسع غير المشروع في انتهاك الخصوصيات. [1]

ثالثاً: الجهة المختصة بالتفتيش

نظرًا لما قد ينطوي عليه إجراء التفتيش من مساس مباشر بالحقوق والحريات، فقد أناط القانون هذه السلطة بجهات تحقيق محددة، كقاضي التحقيق أو وكيل الجمهورية. غير أن مقتضيات الواقع العملي في الجرائم الإلكترونية، واعتبارات السرعة ، دفعت المشرّع إلى منح صلاحيات التفتيش أيضًا لأعوان الضبط القضائي تحت إشراف السلطة القضائية المختصة.[2]

وقد أجاز المشرع الجزائري لقاضي التحقيق أن يُنيب الضبطية القضائية في إجراء التفتيش، بل وأجاز له الاستعانة بخبراء في المجال المعلوماتي، لضمان فاعلية التفتيش وحسن استخلاص الدليل الرقمي دون الإضرار بسلامته أو حجيته القانونية . [3]

الفرع الثاني : الشروط الشكلية والإجرائية للتفتيش

إلى جانب الشروط الموضوعية، أوجب القانون مجموعة من الشروط الشكلية والإجرائية لضمان نزاهة التفتيش، وتفادي أي تعسف قد يُفقده مشروعيته القانونية. وتتمثل هذه الشروط فيما يلي:

[1]– سلمى عفيفي، "الضوابط القانونية للتفتيش الإلكتروني"، رسالة ماجستير ، جامعة الجزائر 1، ص. 237

[2]- المادة 49 من قانون الإجراءات الجزائية الجزائري

[3]– خليفة عبد القادر، التحقيق الجنائي في الجريمة المعلوماتية"، مجلة القانون والتكنولوجيا، ماي 2020، ص. 33

أولاً : احترام التوقيت القانوني للتفتيش

تنص القوانين الإجرائية في الغالب على أن يُجرى التفتيش خلال ساعات النهار فقط، أي بين الساعة الخامسة صباحًا والثامنة مساءً، وذلك كضمانة لحماية حرمة المساكن ومنع انتهاك الحياة الخاصة ليلاً[1] .ومع ذلك، فقد قرر المشرع استثناءً على هذه القاعدة في حال الجرائم الإلكترونية، حيث أجاز التفتيش في أي وقت، نظرًا لطبيعة هذه الجرائم التي قد تُرتكب أو تُمحى أدلتها في أي لحظة دون سابق إنذار.[2]

ثانياً : شرط الإذن القضائي المسبق

أحد أهم الضمانات التي تكسب التفتيش المشروعية هو صدوره بإذن كتابي من وكيل الجمهورية أو قاضي التحقيق، خاصة في الجرائم الإلكترونية التي تمس بشكل مباشر خصوصية الأفراد وبياناتهم الحساسة. ويأتي هذا الشرط لضمان رقابة القضاء على مثل هذه الإجراءات وتفادي تعسف السلطة التنفيذية في مداهمة الفضاء الرقمي للأفراد دون مبرر قانوني كافٍ.

ثالثاً: حضور المتهم أثناء التفتيش

كقاعدة عامة، يجب إجراء التفتيش بحضور المتهم أو من ينوب عنه، ويُعدّ هذا الشرط من ضمانات نزاهة الإجراءات، حيث يُمكّن المتهم من متابعة ما يجري وحماية ممتلكاته من أي عبث أو تلف. غير أن هذا المبدأ يشهد استثناءً في جرائم المعلوميات، حيث أجاز المشرع الجزائري للضبطية القضائية إجراء التفتيش دون اشتراط حضور المتهم أو الشهود، وهو ما يعكس مرونة القانون في مواكبة الطبيعة الخاصة لهذه الجرائم.

[1]- قانون الإجراءات الجزائية الجزائري، المادة 44.
[2]- القانون رقم 66/155 المؤرخ في 8 جوان 1966، المعدل والمتمم

وفي جميع الأحوال، يُعدّ محضر التفتيش وثيقة رسمية تثبت ما جرى أثناء العملية، ويتعيّن أن يتضمن بدقة جميع الخطوات المتخذة والمضبوطات التي تم العثور عليها، مع الإشارة إلى الأشخاص الحاضرين. ورغم غياب نصوص خاصة بمحاضر التفتيش الإلكتروني، إلا أنه يُرجع في ذلك إلى القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية. [1]

ومن الفروق الجوهرية بين التفتيش التقليدي والإلكتروني أن القائم بهذا الأخير ينبغي أن يكون ضابطًا ذا كفاءة تقنية عالية أو على الأقل يُرافقه خبير تقني مختص، لضمان الفعالية

في التعامل مع المعطيات الرقمية دون الإضرار بها، مما يعكس التداخل بين القانون والتكنولوجيا في ميدان العدالة الجنائية الحديثة.

المطلب الثاني: ضبط الأدلة في الجريمة الإلكترونية

يُعد ضبط الأدلة من الإجراءات الجوهرية في مسار التحقيق الجنائي، وهو الامتداد الطبيعي لعملية التفتيش، حيث يتم وضع اليد فعليًا على الأشياء أو البيانات المرتبطة بارتكاب الجريمة. ويكتسي الضبط أهمية خاصة في مجال الجريمة الإلكترونية، نظراً لطبيعة الأدلة الرقمية التي تختلف عن الأدلة التقليدية من حيث الشكل والمكان وطبيعة التخزين والإتاحة. وتتجلى هذه الأهمية في كون الدليل الرقمي، إذا تم ضبطه وفقاً للضوابط القانونية والتقنية، يشكّل عنصراً حاسماً في إثبات الجريمة وتعقب مرتكبها.[2]

وسوف نقسم هذا المطلب إلى فرعين، نتناول في الفرع الأول مفهوم وطبيعة الأشياء محل الضبط في الجريمة الإلكترونية، ونتناول في الفرع الثاني الإجراءات القانونية لضبط البيانات الرقمية وفقاً للتشريع الجزائري.

[1]– محمد صغير، مرجع سابق، ص52.

[2]- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر (أساليب وتغرات) ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر ، سنة 2010، ص153

الفرع الأول: طبيعة الأشياء محل الضبط في الجريمة الإلكترونية

في الجرائم التقليدية، غالبًا ما تكون الأشياء المضبوطة ذات طبيعة مادية محسوسة، مثل السلاح المستخدم في القتل أو الأداة المستعملة في السرقة. أما في الجرائم الإلكترونية، فإن نطاق الأشياء التي يمكن ضبطها أوسع وأكثر تعقيداً، إذ تشمل كلاً من الأدوات المادية والبيانات غير المادية. [1]

أولا: الأشياء المادية القابلة للضبط

تشمل هذه الفئة كافة المعدات والأجهزة التي استعملت في تنفيذ الجريمة أو التي تحتوي على بيانات رقمية مرتبطة بها. ومن أمثلتها :

- أجهزة الحاسب الآلي المكتبي أو المحمول.
- الأقراص الصلبة الداخلية والخارجية.
- مفاتيح التخزين المحمولة.(USB)
- القواعد الاجرائية لمكافحة الجريمة المعلوماتية
- الطابعات، الماسحات الضوئية، وأجهزة الفاكس[2].
- أجهزة المودم والراوتر والهواتف الذكية.
- بطاقات الائتمان والبطاقات الممغنطة الأخرى.

تمثل هذه العناصر أدوات مادية يُمكن مصادرتها ووضعها في أحرار مادية مغلقة بعد جردها، تماما كما هو الشأن في الضبط التقليدي، مع ضرورة اتخاذ الاحتياطات لمنع التلاعب بالبيانات المخزنة فيها ، كاستخدام أختام إلكترونية أو برمجيات تحقق من سلامة الملفات.

[1] – جميل عبد الباقي الصغير، االنترنيت والقانون الجنائي، االحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية ، القاهرة، سنة 2001 ، ص74

[2]- الغافري عبد الحق، "التحقيق" في الجرائم المعلوماتية"، دار الخلدونية، الجزائر، 2009، ص. 32.

ثانيًا: المضبوطات غير المادية (البيانات الرقمية)

تشكل البيانات الرقمية جوهر الأدلة في الجرائم الإلكترونية، وهي تختلف عن الادلة المادية في انها :

- غير ملموسة.
- قابلة للنسخ بسهولة.
- قد تكون موزعة على خوادم متعددة أو تخزين سحابي
- تحتاج إلى أدوات تقنية لاستخراجها وتفسيرها.

وتشمل هذه المضبوطات الرقمية:[1]

- الملفات المحفوظة على الحاسوب (مستندات ،صور، مقاطع صوت وفيديو .)
- البريد الإلكتروني والمراسلات الإلكترونية.
- سجلات الدخول والخروج من الأنظمة.
- قواعد البيانات.
- محتوى الحسابات على منصات التواصل الاجتماعي.

وبسبب طبيعتها غير المادية، تتطلب هذه الأدلة تعاملا خاصا من حيث الضبط والحفظ والمعالجة، وهو ما ينقله بنا إلى الإجراءات القانونية التي تحكم هذه المسائل.

الفرع الثاني: الضوابط القانونية والإجرائية لضبط البيانات الرقمية

نظراً للطبيعة الحساسة والمعقدة للبيانات الرقمية، أولى المشرع الجزائري أهمية بالغة لضمان قانونية الضبط وسلامة الأدلة المجمعة، وهو ما يتجلى في أحكام القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[1]- الحلبي، علي عبد القادر، شرح قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، 2011، ص. 169.

أولًا: الحجز الجزئي للبيانات

تنص **المادة 6** من القانون السالف الذكر على أنه:

"عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها ، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار ".[1]

وهذا ما يعني أن الضبط في هذا السياق لا يعني دائمًا مصادرة الجهاز كله، بل يمكن أن يقتصر على نسخ البيانات محل الاهتمام إلى وسائط تخزين إلكترونية مخصصة، شريطة أن تكون قابلة للحجز والتقديم كدليل أمام المحكمة.

ثانيًا : ضمان سلامة البيانات الرقمية

يشترط القانون على السلطة القائمة بالتفتيش والحجز أن تضمن سلامة المعطيات الرقمية، وأن لا تؤثر العملية على البيانات الأصلية، وذلك حفاظاً على مصداقية الدليل. ولهذا الغرض، يتم اللجوء غالباً إلى أدوات متخصصة في استخراج البيانات دون تعديلها، مع استعمال تقنيات "البصمة الرقمية" لضمان أن البيانات المضبوطة لم تتعرض لأي تغيير.

ثالثًا: الحماية من الاطلاع غير المشروع

في الحالات التي يتعذر فيها الحجز لأسباب تقنية، كأن تكون البيانات مخزنة على خوادم في الخارج أو يصعب الوصول إليها، يوجب القانون اتخاذ تدابير وقائية تمنع الوصول غير المشروع إلى هذه البيانات أو نسخها، من خلال استخدام تقنيات الحجب أو التشفير أو القفل الرقمي.

[1]- مال، عبد الحميد، التحقيق الجنائي في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2015، ص46.

وفي حالة ما إذا كان محتوى البيانات يشكل جريمة في ذاته، يجوز للسلطة التي تباشر التحقيق اتخاذ الإجراءات الضرورية لمنع الاطلاع على هذا المحتوى من أي طرف غير مختص، حماية للمعطيات وحفاظاً على الأمن العام.

رابعا : قيد استعمال البيانات المضبوطة

ينص القانون صراحة على أنه لا يجوز استعمال المعطيات التي تم ضبطها خلال التفتيش لأي غرض خارج نطاق التحري أو التحقيق أو العمل القضائي، وإلا فإن من قام بذلك يعرض نفسه للمساءلة الجنائية. ويأتي هذا القيد تأكيدًا لمبدأ سرية المعلومات، وضماناً لحقوق الأفراد في حماية بياناتهم الخاصة. [1]

المبحث الثاني: الإجراءات المستحدثة للكشف عن الجريمة المعلوماتية

استحدث المشرع قواعد إجرائية جديدة أكثر راهنية ومردودية تساعد الجهات المكلفة بالبحث والتحري عن الجريمة الإلكترونية والوصول إلى الدليل الرقمي و المتمثلة في كل من التسرب الإلكتروني (المطلب الأول)،

وكذلك اعتراض المراسلات والمراقبة الإلكترونية المطلب الثاني، ناهيك عن الإجراءات المرتبطة بالمعطيات (المطلب الثالث).

المطلب الأول: التسرب الإلكتروني

تعد الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات من الجرائم التي خصها المشرع الجزائري بأحكام خاصة، لا سيما في ما يتعلق بإجراءات التحقيق فيها. ومن بين هذه الإجراءات التي أتاحها المشرع هو إجراء التسرب[2]"، الذي يعتبر من أبرز الوسائل

[1]– آمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الثانية ، دار هومه للطباعة والنشر والتوزيع، الجزائر ، سنة 2007 ، ص72

[2]- جمال، عبد الحميد، المرجع السابق، ص. 48

المستخدمة للكشف عن الجريمة المعلوماتية، والذي تم تنظيمه بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية (66/156 المؤرخ في 10 نوفمبر (2004). حيث يُعرف التسرب كإجراء يهدف إلى توغل ضباط الشرطة القضائية ضمن دائرة الأشخاص المشتبه في ارتكابهم الجرائم المعلوماتية، وذلك من خلال إيهامهم بأنهم شركاء في الجريمة أو أنهم جزء من المخطط الإجرامي.[1]

ويُعتبر التسرب من الإجراءات الاستثنائية التي تستهدف القضاء على الجرائم المنظمة أو المعقدة، مثل الجرائم الإلكترونية، والتي يصعب اكتشافها بالطرق التقليدية. وفي هذا السياق، تبرز خطورة التسرب كون المتسرب يتعرض لمخاطر كبيرة من حيث الأمن الشخصي، إلا أن المشرع الجزائري، من أجل حماية المتسرب وعائلته، نص على ضمانات تضمن سرية هويته في جميع مراحل الإجراء.[2]

كما أشار المشرع إلى أن التسرب يعتبر شكلاً من أشكال الاختراق" الذي يتم استخدامه في إطار مكافحة الجرائم، وقد تم تنظيمه بشكل خاص في القانون رقم 06/01 المؤرخ في 20 فبراير 2006، والمتعلق بالوقاية من الفساد، حيث أجاز اللجوء إلى أساليب تحري خاصة، مثل التسليم المراقب والترصد الإلكتروني، في التحقيق في الجرائم المتصلة بالفساد.[3]

وقد حدد المشرع الجزائري مجموعة من الضوابط الموضوعية والإجرائية التي يتعين مراعاتها عند اللجوء إلى التسرب، وتتمثل في العناصر التالية:

[3]– مادة 65 مكرر 12. قانون الإجراءات الجزائية رقم 66/156 المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية،–

[2]- وردة جوان ، إجراءات التحري في الجرائم الإلكترونية، الطبعة الثانية 2017، صفحة 543.

[3]- القانون رقم 01/06 المتعلق بالوقاية من الفساد ومكافحته المؤرخ في 20 فبراير 2006، الجريدة الرسمية.

الفرع الأول: الشروط الموضوعية لإجراء التسرب

يستوجب إجراء التسرب وجود شروط موضوعية محددة، وتتمثل في العنصرين التاليين:

أولاً: عنصر التسبيب

يعد عنصر التسبيب من الضمانات الأساسية التي تبرر إجراء التسرب، ويجب أن يُبيِّن بوضوح الأسباب التي دفعت وكيل الجمهورية لإصدار الإذن بالتسرب. وذلك لضمان أن الإجراء يتم بناءً على مبررات قانونية صحيحة، وتجنب أي تعسف أو تجاوزات قد تحدث.[1]

إذا تم الإجراء بدون تسبيب ،واضح، فإن ذلك يؤدي إلى بطلان الإذن وجميع الإجراءات المرتبطة به.

ثانياً: تحديد نوع الجريمة

يجب تحديد نوع الجريمة التي تبرر اتخاذ إجراء التسرب، وهي جرائم يتم تصنيفها على أنها خطيرة وفقا للمادة 65 مكرر 05 من قانون الإجراءات الجزائية، التي حددت قائمة معينة من الجرائم التي يجوز التحقيق فيها باستخدام هذه الوسيلة الاستثنائية وتقتصر هذه الجرائم على حالات يكون فيها الجاني متورطا في جرائم إلكترونية معقدة أو منظمات إجرامية يصعب مراقبتها باستخدام الطرق التقليدية. [2]

الفرع الثاني : الشروط الإجرائية لإجراء التسرب

لا يتوقف الأمر عند الشروط الموضوعية فحسب، بل يتطلب الأمر أيضًا توافر شروط إجرائية محددة تضمن صحة وشرعية استخدام هذا الإجراء، وتتمثل في النقاط التالية:

[1]–محمد نجيمي، الجرائم الإلكترونية في التشريع الجزائري، دار النشر القانونية2011.ص 452

أولاً: الإذن القضائي

يعد الحصول على الإذن القضائي من أولى المتطلبات الضرورية لإجراء التسرب. حيث لا يجوز لضابط الشرطة القضائية الشروع في أي عملية تسرب دون الحصول على إذن مسبق من وكيل الجمهورية، والذي يعتبر المسؤول الأول عن إدارة تحقيقات الضبطية القضائية. كما يشترط أن يكون الإذن كتابيًا، وليس شفهيًا، ويجب أن يتضمن جميع البيانات المتعلقة بالجريمة المتورط فيها الشخص المستهدف، فضلاً عن تحديد الشخص المكلف بالإشراف على العملية.[1]

ثانياً: تحديد مدة التسرب

من الشروط الأساسية الأخرى هي تحديد مدة زمنية لإجراء التسرب، حيث يجب أن يكون لهذه العملية مدة محددة لا تتجاوز أربعة أشهر. وإذا اقتضت الضرورة تمديد هذه المدة، يجب الحصول على إذن جديد من الجهة القضائية المختصة. وعند انقضاء المدة المقررة دون التوصل إلى النتائج المطلوبة، يجوز للعون المتسرب مواصلة العملية في إطار معين من الأمان، دون أن يتحمل مسؤولية قانونية عن ذلك.[2]

وتجدر الإشارة إلى أنه في ظل قانون مكافحة التمييز وخطاب الكراهية رقم 05/20 المؤرخ في 28 أبريل 2020 ، أتاح المشرع الجزائري توسيع نطاق استخدام إجراءات التسرب لتشمل الكشف عن الجرائم المرتبطة بالتمييز وخطاب الكراهية، مما يبرز التكيف التشريعي مع التحديات المستمرة في مجال مكافحة الجرائم الإلكترونية .

[1]- مال الحلبي، التحقيقات الجنائية وضبط الأدلة، دار الكتاب القانوني، 2011ص169

[2]- سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم القانونية، جامعة الحاج لخضر باتنة، سنة دراسية 2102/2013.ص31

المطلب الثاني : اعتراض المراسلات والمراقبة الإلكترونية والكشف عن الجريمة المعلوماتية عن طريق المعطيات.

يعد الاعتراض على المراسلات والمراقبة الإلكترونية من أهم الأدوات الحديثة في التحقيقات الجنائية المتعلقة بالجرائم المعلوماتية، حيث توفر وسائل فعالة لكشف الأنشطة غير القانونية التي تتم عبر الأنظمة المعلوماتية مع التطور السريع لتكنولوجيا المعلومات والاتصالات، أصبح من الضروري أن تتوافر تشريعات تسمح للسلطات المختصة باستخدام تقنيات المراقبة لاعتراض المراسلات الإلكترونية التي قد تتضمن أدلة على جرائم معينة. إن استخدام هذه

الأدوات يشكل تحديًا قانونيًا وأخلاقيًا، حيث يجب موازنة مصلحة التحقيق في الجرائم مع احترام حقوق الأفراد وحمايتهم من التعدي على خصوصياتهم. [1]

من خلال هذا المطلب، سنستعرض الوسائل القانونية والتقنية المتاحة للاعتراض على المراسلات الإلكترونية ومراقبة الاتصالات الرقمية كأداة للكشف عن الجريمة المعلوماتية. كما سنتناول الجوانب القانونية المرتبطة بهذه الإجراءات، بما في ذلك الضوابط التي تضمن احترام الحقوق الأساسية للأفراد، وكيفية استخدام المعطيات الرقمية المكتسبة من خلال هذه الوسائل في التحقيقات القضائية.

الفرع الأول: اعتراض المراسلات والمراقبة الإلكترونية

إن دراسة عملية اعتراض المراسلات كآلية للكشف عن الجريمة المعلوماتية تتطلب بالضرورة تحديد مفهوم اعتراض المراسلات والمراقبة الإلكترونية (أوات، بالإضافة إلى الوقوف على المراسلات التي يمكن أن تكون محلا لإجراء الاعتراض (ثانيا)، مع تحديد

[2] – المادة 26 من القانون قانون الوقاية من التمييز وخطاب الكراهية رقم 05/20 المؤرخ في 28 أبريل 2020، الجريدة الرسمية.

الشروط الموضوعية والشكلية المتطلبة قانونا من أجل تبني عملية اعتراض المراسلات (ثالثا).

أولا : مفهوم عملية اعتراض المراسلات يناط باعتراض المراسلات تلك العملية التي تسمح بمراقبة سرية المراسلات السلكية و اللاسلكية في إطار البحث والتحري عن الجريمة، وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في إرتكاب الجريمة. [1]

وعرفت المادة 65 مكرر 05 عملية مراقبة المراسلات على أنها " اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية و اللاسلكية ". و لم تشر المادة المذكورة أعلاه لطبيعة هذه المراسلات مما يفتح المجال للمراسلات المكتوبة مهما كان شكلها (كتابة ، رموز أشكال (صور) ويستوي أن تكون ورقية أو رقمية، وسواء كانت بالفاكس أو تيلغرام أو لاسلكية مثل البريد الالكتروني ، و الهاتف النقال (03/2000، المؤرخ في 05 أوت (2000) ، استنادا إلى المفاهيم الواردة في المادة 02 من القانون رقم 04/09.

وعلى ذلك فإن عملية الاعتراض أو المراقبة تتم عن طريق ترتيبات تقنية سرية، يتم وضعها دون موافقة الأشخاص المعنيين المشتبه فيهم ، بغرض التنصت والتقاط وتثبيت وتسجل البيانات المرسلة أو المحادثات التي أجراها المشتبه في أماكن عامة أو خاصة، من أجل استعمالها كدليل لمواجهته.

[1]–عباس أبو شامة عبد المحمود، عولمة الجريمة االقتصادية، جامعة نايف العربية للعلوم أألمنية، الرياض،سنة 2007 ص14

[2]– أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة للطباعة والنشر، الجزائر،2006ص80

كما تعد المراسلات عبر البريد الإلكتروني مجالا خصبا للربط والاتصال الإلكتروني بين الأشخاص في مختلف أنحاء العالم وبوقت قياسي، ومن ثم يمكن إخضاعها لعلمية الاعتراض والمراقبة للكشف عن الجرائم الإلكترونية.

ثانيا : الشروط المطلوبة في المراسلات محل الاعتراض

يشترط في المراسلات التي يمكن أن تكون محلا لإجراء الاعتراض أو المراقبة أن تتسم بالسرية والخصوصية، ولاشك أن ذلك لا يتحقق إلا في ظل توافر عنصرين . هما :

– فحوى الرسالة والتي تنصب على معلومات أو أفكار سرية و شخصية.

– تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون المراسلة[1].

مع الإشارة أن المشرع الجزائري لم يتبنى إجراء مراقبة الاتصالات الإلكترونية كإجراء للتحقيق القضائي، و كذلك التحري بموجب القانون رقم 09/04 ، بل أعطى تصريح للجهات القضائية باستعمال الاعتراض بهدف الوقاية من بعض الجرائم التي تشكل خطرا على أمن الدولة.

وإتماما لهذا الهدف تم استحداث الهيئة الوطنية الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والتي أوكل لها القانون مهمة تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها مع السلطات القضائية، وذلك من خلال المادة 13 من القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها.

[1]–زيبحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى الجزائر، 2011ص153

[2]– صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،2003 ص247

وبالتالي هي عبارة عن هيئة أو سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي ومقرها بالجزائر العاصمة، تم تحديد تشكيلتها وعملها بموجب المرسوم الرئاسي رقم . 261/15.

ثالثا : الشروط القانونية لاعتراض المراسلات

تبقى عملية الاعتراض أو مراقبة المراسلات مرهونة على توافر الشرط التالية :

توافر إذن مكتوب من الجهات القضائية المختصة، أي من طرف وكيل الجمهورية بمرحلة التحقيق الابتدائي، أو من طرف قاضي التحقيق بمرحلة التحقيق القضائي تحت طائلة بطلان الإجراء القضائي، ولاشك أن اشتراط الإذن هو إجراء حتمي من منطلق أسلوب اعتراض المراسلات السلكية واللاسلكية يتم دون علم المعنيين، لأنه ورغم نجاعته في الكشف عن الجرائم المعلوماتية، إلا أنه يشكل اعتداء على سرية المراسلات والاتصالات، ومساس بحرمة الحياة الخاصة التي كفلها الدستور (442/20، المؤرخ في 30 ديسمبر 2020)،[1] ويشترط أن يتضمن الإذن طبيعة الجريمة التي تبرر الإجراء، مع ضرورة أن تكون من الجرائم التي يجوز منح الإذن فيها، بالإضافة إلى تحديد المراسلات المراد اعتراضها وتسجيلها وتحديد الأماكن المقصودة، سواء كانت أماكن عامة أو خاصة تحديد مدة مع الاعتراض والتي لا تتجاوز 04 أشهر قابلة للتجديد.

التسبيب، أي تبيان دواعي اللجوء إلى الاعتراض ومراقبة المراسلات، و تبيان مدى جدية تلك الدواعي ودورها إظهار الجريمة والجناة.

تحديد الجرائم محل الاعتراض والمراقبة والتي يتوجب أن لا تخرج عن ما هو مقرر قانونا، مع مراعاة سرية الإجراءات وكتمان السر المهني.

[1]– حاجب هيام الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء الجزائر ، 2005_2006. ،ص24

الفرع الثاني: الكشف عن الجريمة المعلوماتية عن طريق المعطيات

تلعب المعطيات دورًا هامًا في الكشف عن الجريمة المعلوماتية، ويتم الاستفادة منها إما عن طريق الحفظ والإفشاء العاجلان (أولا)، أو عن طريق تجميعها بوقتها الفعلي (ثانيا). [1]

أولا: الحفظ والإفشاء العاجلان للمعطيات الإلكترونية

يُعد الحفظ والإفشاء العاجلان من الإجراءات المستحدثة التي تهدف إلى الكشف عن الجريمة المعلوماتية والوصول إلى الأدلة الرقمية اللازمة لإثبات الجريمة. وتعتبر هذه الإجراءات ضرورية في ظل تزايد استخدام التكنولوجيا الحديثة في ارتكاب الجرائم، خاصة الجرائم الإلكترونية التي يصعب كشفها بالطرق التقليدية. ولذلك، عمد المشرع الجزائري إلى تنظيم هذه الإجراءات في المادة 10 من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .[2] وتنص هذه المادة على إمكانية اللجوء إلىإجراءات الحفظ والإفشاء العاجلين للمعطيات الإلكترونية التي يتم تبادلها عبر شبكات الإنترنت، بهدف ضمان استمرارية التحقيقات في الجرائم الإلكترونية وضمان حماية الأدلة الرقمية من الضياع أو التلاعب.

وفي هذا السياق، يقوم مقدمو خدمات الإنترنت بالحفظ عبر الأرشيف، الذي يُعتبر بمثابة حفظ إلكتروني للمعطيات والبيانات على الخوادم أو قواعد البيانات الخاصة بمقدمي الخدمة. ويتم ذلك بهدف حماية المعطيات التي كانت موجودة في شكل مخزن، وذلك للحفاظ على مصداقيتها وحالتها الأصلية دون تلاعب أو تغيير، بحيث تظل صالحة للاستخدام في الإجراءات القضائية. من المهم أن يتم تنفيذ هذه العملية وفق نماذج معترف بها قانونيًا ووفق معايير فنية محددة تضمن سلامة البيانات أثناء الحفظ.

[1] – طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر 1 ، كلية الحقوق، 2011، 2012ص192

[2]- لقانون رقم 04/09 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها.

1- المعطيات محل التحفظ

حددت المادة 11 من القانون 04 / 09 بدقة المعطيات التي يجب على مقدمي خدمات الإنترنت ،تحفيظها، وذلك بناءً على طلب من السلطات القضائية المختصة. هذه المعطيات تشمل : [1]

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة : وتتمثل في الهوية الرقمية للمستخدم مثل اسم المستخدم، عنوان البريد الإلكتروني، أو رقم الهاتف المحمول المستخدم للتواصل عبر الإنترنت.
- المعطيات المتعلقة بالتجهيزات المستعملة بالاتصال : مثل الرقم التسلسلي للأجهزة المتصلة بالإنترنت، نوع الجهاز المستعمل، وطرق تشغيله. هذا يشمل الحواسيب،

الهواتف الذكية، الأجهزة اللوحية، وأي أجهزة إلكترونية أخرى تستخدم في عملية الاتصال.

- المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم : تشمل أرقام الهواتف أو العناوين البريدية الإلكترونية للمرسلين والمستقبلين. ويعد هذا النوع من المعطيات أساسيًا في التحقيقات المتعلقة بالجرائم الإلكترونية التي تستخدم وسائل الاتصال الحديثة.[2]

- الخصائص التقنية : مثل نوع الاتصال الإنترنت السلكي أو اللاسلكي)، سرعة الاتصال، تاريخ ووقت الاتصال، ومدة الاتصال، وهي تفاصيل مهمة في التحقيقات التي تتعلق بالجرائم الرقمية.

[1]- نائلة عادل محمد فريد قورة – جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية – منشورات الحاتي الحقوقية 2005 ص 90

[2]- عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر و الأنترنت في القانون العربي النموذجي، دار الفكر الجامعي الإسكندرية 2006ص64

– المعطيات المتعلقة بالخدمات التكميلية : كالمعلومات المستعملة ومقدمي الخدمات، مثل المواقع التي تم زيارتها أو الخدمات التي تم الوصول إليها عبر الإنترنت، بما في ذلك تفاصيل حول عمليات شراء أو معاملات إلكترونية.

2– الضوابط الواجب مراعاتها خلال عملية حفظ المعطيات

نظرًا لأن عملية حفظ المعطيات تمس حق الأفراد في الخصوصية، فقد وضع المشرع الجزائري مجموعة من الضوابط التي يتوجب على مقدمي خدمات الإنترنت التقيد بها لضمان احترام حقوق الأفراد وحماية بياناتهم أبرز هذه الضوابط تشمل: [1]

– احترام المدة الزمنية المقررة لعملية الحفظ حدد المشرع الجزائري في المادة 11 من القانون 04/ 09مدة سنة واحدة فقط كفترة زمنية يجب خلالها حفظ المعطيات. تبدأ هذه المدة من تاريخ التسجيل أو التبادل الرقمي للمعلومات، وفي حال انقضائها، يتوجب على مزود الخدمة اتخاذ تدابير قانونية وفنية لسحب المعطيات المخزنة وإغلاق إمكانية الوصول إليها.[2]

– مراعاة سرية عملية التحفظ : يتوجب على مقدمي خدمات الإنترنت الحفاظ على سرية جميع الإجراءات المتعلقة بالحفظ، وذلك طوال الفترة المحددة يشمل ذلك اتخاذ تدابير فنية مثل تشفير البيانات أو تخزينها في بيئات آمنة لمنع الوصول غير المصرح به، بحيث تكون المعلومات محمية من التلاعب أو الفقدان .

– حماية البيانات الشخصية : تتم عملية التحفظ وفق معايير تضمن الحد الأدنى من التعرض للمعلومات الشخصية للمستخدمين. ويجب على مقدمي الخدمة ضمان أن العملية تتماشى مع قواعد حماية البيانات الشخصية وحمايتها من أي تسريب قد يضر

[1]–د. محمد امين الشوابكة، جرائم الحاسوب و الانترنت (الجريمة المعلوماتية) ، دار الثقافة ط1 . 2009.ص85

[2]- محمد امين الشوابكة، نفس المرجع السابق ، ص60

بحقوق الأفراد.

– الإفشاء العاجل للمعطيات : في بعض الحالات الطارئة التي تتطلب الكشف الفوري للمعطيات، يمكن للمشرع أن يسمح بالإفشاء العاجل لها، كما هو منصوص عليه في المادة 10 من القانون 04/09 هذا الإجراء يستدعي تقديم المعطيات فورًا إلى السلطات القضائية المختصة في حالات الجرائم ذات الطابع العاجل. [1]

ومع ذلك، تُعد عملية إنتاج البيانات المعلوماتية إجراء حديثا يتماشى مع طبيعة الأدلة الرقمية، وقد يتطلب اعتماد تقنيات جديدة تواكب التطور السريع في تكنولوجيا المعلومات. إلا أن المشرع الجزائري لم ينص بشكل صريح على هذا الإجراء في إطار قوانين التحقيقات الجنائية. وهذا السهو قد يؤدي إلى ضرورة تحديث التشريعات لتشمل تقنيات الحفظ الحديثة التي تواكب طبيعة الأدلة الرقمية التي تتغير بسرعة.

ثانيا : تجميع معطيات المرور بوقتها الفعلي

تعتبر عملية تجميع معطيات المرور في وقتها الفعلي من الإجراءات التقنية المتقدمة والمهمة في التحقيق في الجرائم الإلكترونية. [2]حيث تتطلب هذه العملية تعاون مقدمي خدمات الإنترنت السلطات القضائية للتحقق من طبيعة الجريمة المرتكبة وجمع الأدلة الرقمية بشكل دقيق. وتعرف خدمة الإنترنت بموجب المادة 04/09 من القانون الجزائري بأنها "أي كيان عام أو خاص يقدم لمستعمليه خدمات الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، أو أي كيان يقوم بمعالجة أو تخزين معطيات لفائدة خدمة الاتصال ".

[1]– خالد الممدوح ابراهيم ، فن التحقيق الجنائي في الجريمة الالكترونية ، دار الفكر الجامعي ، الاسكندرية ،مصر 2009 ،ص 126–

[2]- مر زبيحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر، ، 2011ص 131

1- ضرورة تعاون مقدمي خدمات الإنترنت

يمثل التعاون بين مقدمي خدمات الإنترنت والسلطات القضائية جانبا أساسيًا في التحقيقات الجنائية الإلكترونية. حيث يُلزم هؤلاء بتقديم المعطيات الخاصة بالاتصالات، مثل معطيات التعريف بالمستخدمين وخصائص الاتصال التقنية، وكذلك مدة الاتصالات وأوقات الاتصال. هذا التعاون يشمل العديد من المعطيات المهمة مثل:

- معطيات تعرف المستخدمين : مثل بيانات المستخدم الخاصة مثل أرقام الهاتف وعناوين البريد الإلكتروني.
- الخصائص التقنية : مثل نوع الجهاز، رقمه التسلسلي، وطريقة تشغيله، وكذلك بيانات تقنية أخرى تتعلق بنظام الاتصال.
- المعطيات الزمنية : مثل تاريخ ووقت ومدة الاتصال، التي تشكل معلومات أساسية في تحديد مواقع الأفعال الإجرامية.[1]

2- شروط حفظ معطيات المرور:

يشترط المشرع الجزائري أن تقوم خدمات الإنترنت بحفظ المعطيات التي يتم جمعها لفترة زمنية معينة، والتي تبلغ عامًا واحدًا ابتداءً من تاريخ التسجيل هذا الحفظ يتم بهدف توفير الأدلة الضرورية للمحققين في حالة الحاجة إليها لاحقا. بعد مرور المدة المحددة للحفظ، يجب على مقدمي الخدمات سحب المعطيات المخزنة بشكل فوري واتخاذ التدابير التي تمنع أي شخص غير مخول من الاطلاع عليها.[2]

[1]- زبيحة زيدان ، نفس المرجع السابق ، ص132

[2]- زبيحة زيدان ،نفس المرجع السابق ، ص134

- حفظ المعطيات لفترة سنة :يجب على مقدمي خدمات الإنترنت احترام المدة المحددة لاحتفاظهم بالمعطيات وهي سنة واحدة ابتداء من تاريخ التسجيل وهذه المدة تعد ضمانًا لوجود المعلومات الهامة عند الحاجة إليها في التحقيقات.
- تدخل فوري لسحب المحتويات : في حال علم مقدمي خدمات الإنترنت بوجود معطيات مخالفة للقانون، يجب عليهم اتخاذ إجراءات فورية لسحبها وحفظها بطريقة تمنع الوصول إليها إلا للجهات المخولة بذلك.[1]

3- الضوابط التقنية لمنع الوصول إلى المعلومات

من أجل ضمان تطبيق المعايير القانونية وحماية المعطيات الرقمية من العبث أو التعديل، يجب على مقدمي خدمات الإنترنت اتخاذ ترتيبات تقنية محددة لحصر إمكانية الدخول إلى الموزعات أو الأجهزة التي تحتوي على معطيات مخالفة. هذه الترتيبات تشمل:

- منع الدخول إلى الموزعات المخالفة : يجب أن تتخذ تدابير فنية تحظر الوصول إلى الموزعات التي تحتوي على معطيات مخالفة للنظام العام أو الآداب العامة. كما يمكن اتخاذ إجراءات لحظر الوصول إلى المواقع الإلكترونية التي تروج للأعمال الإجرامية.
- إبلاغ المشتركين بالمخالفات : يجب على مقدمي خدمات الإنترنت إبلاغ المشتركين لديهم إذا كانت هناك معطيات مخالفة للقوانين على شبكتهم، وذلك لتفعيل المسؤولية القانونية على الجهات التي تروج لمحتويات مخالفة.[2]

[1]- بن يحي اسماعيل، التحقيق الجنائي في الجرائم الإلكترونية رسالة دكتوراه، تخصص قانون الخاص،قسم حقوق كلية الحقوق و العلوم السياسية، جامعة أبي بكر الصديق بلقا يد تلمسان ، الجزائر ، سنة 2020-2021 ص66

[2]- بن يحي اسماعيل، نفس المرجع السابق ، ص67

4 – المسؤولية القانونية لمقدمي خدمات الإنترنت

في حال امتناع مقدمي خدمات الإنترنت عن التعاون مع السلطات في جمع المعطيات المطلوبة، فإنهم قد يعرضون أنفسهم لعقوبات قانونية حيث ينص القانون الجزائري في المادة 109/04 من قانون الوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال على معاقبة مقدمي الخدمات الذين يمتنعون عن التعاون في جمع المعطيات أو لا يقدمونها في الوقت المناسب. بالإضافة إلى ذلك، فإن التشريعات الأخيرة المتعلقة بحماية المعلومات تفرض عقوبات أشد ضد من يخالف قوانين تقديم المعطيات الرقمية.

5– تطبيق القانون في جرائم التمييز وخطاب الكراهية

بالإضافة إلى الجرائم المعلوماتية التقليدية أتاح المشرع الجزائري في القانون 05/20 المتعلق بالوقاية من التمييز وخطاب الكراهية استخدام نفس الإجراءات لجمع المعطيات والتحقيق في الجرائم التي تقع ضمن هذا الإطار. يُمكن للجهات القضائية المختصة إصدار أوامر لمقدمي خدمات الإنترنت بتسليم المعطيات المخزنة المتعلقة بهذه الجرائم، كما يمكنها إصدار أوامر بالتحفظ الفوري على هذه المعطيات. تعتبر هذه الصلاحيات ضرورية لمكافحة الجرائم التي تهدد النظام العام أو قد تؤدي إلى إحداث الفتنة الاجتماعية. [1]

[1]– رابحي عزيزة، الأسرار المعلوماتية و حمايتها الجزائية ، رسالة دكتوراه، تخصص قانون خاص ، قسم الحقوق،كلية الحقوق والعلوم السياسية ، جامعة ابوبكر بلقا يد ، تلمسان ، الجزائر ، 2017–2018 ص143

خلاص الفصل :

تناول الفصل الأول موضوع الكشف عن الجريمة المعلوماتية باستخدام الأدلة الرقمية من خلال استعراض الإجراءات القانونية والتقنية التي تساعد في جمع وتوثيق المعطيات الرقمية. بدأ الفصل بتعريف الأدلة الرقمية وكيفية ضبطها عبر التفتيش والحجز وفقًا للقوانين الجزائرية، خاصة قانون الإجراءات الجزائية والقوانين ذات الصلة بالجرائم المعلوماتية. كما تم التطرق إلى كيفية استخدام إجراءات التسرب الإلكتروني والرقابة على المراسلات كأدوات فعالة في التحقيقات الإلكترونية.

كما أشار الفصل إلى دور مقدمي خدمات الإنترنت في الكشف عن الجريمة المعلوماتية، من خلال إجراءات حفظ المعطيات والإفشاء العاجل وكذلك تجميع المعطيات في وقتها الفعلي، مع تحديد الضوابط القانونية التي يجب مراعاتها أثناء هذه العمليات. تضمن الفصل أيضا مناقشة مفهوم الاعتراض على المراسلات الإلكترونية كوسيلة لمراقبة الأنشطة الإجرامية في الفضاء الرقمي، وبيّن كيف أن هذه الإجراءات تخضع لقوانين توازن بين ضرورة التحقيق وحماية حقوق الأفراد.

في النهاية، يبرز الفصل الأول أهمية تطوير القوانين المتعلقة بالأدلة الرقمية في ظل التحديات التقنية المستمرة، وكذلك ضرورة تكامل الجهود بين السلطات القضائية ومقدمي خدمات الإنترنت لضمان تحقيق العدالة دون المساس بالحقوق الأساسية.

الفصل الثاني
الآليات المؤسساتية والتعاون الدولي في مواجهة الجريمة الإلكترونية

تمهيد:

الجريمة الإلكترونية هي جريمة حديثة، بسبب ارتباطها بالتكنولوجيا الحديثة وقد أدى ذلك إلى زيادة الغموض المحيط بها، لذا تم إنشاء جهاز خاص للتحقيق في الجريمة الإلكترونية ويتكون من وظائف متخصصة إلكترونيا وقانونيا، وفي الجزائر توجد هيئة ووحدات متخصصة للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال بالإضافة إلى وحدات تابعة للأمن والدرك الوطني وكذا هيئات قضائية متخصصة في البحث والتحري عن الجريمة تتمثل في الاختصاص الإقليمي للأقطاب الجزائية المتخصصة كما قمنا بالتطرق إلى تمديد الاختصاص المحلي هذا من جهة، ومن جهة أخرى حاولت الدول أن تبحث عن آليات مشتركة لتنسيق المواقف حول طرق ما يعرف بالتعاون الدولي والمساعدة القضائية الدولية لمواجهة هذا النوع من الجرائم.

المبحث الأول: الهياكل الخاصة لمواجهة الجرائم الإلكترونية

مع تزايد الجرائم المعلوماتية يوما بعد يوم، ونظرا إلى الطبيعة الخاصة التي ميزت هذه الجرائم، أصبح من الضروري تحديث أجهزة الشرطة القضائية لمواجهة هذا التطور الحاصل في مجال الجريمة الإلكترونية لذلك قامت معظم الدول بإنشاء وحدات خاصة لمكافحة هذا النوع من الجرائم، وقد تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الأنتربول واليوروبول والأفريبول.

أما بالنسبة للجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى الوحدات القضائية وأخرى تابعة لسلك الأمن والدرك الوطني وهذا ما سنبينه من خلال المطلبين الآتيين:[1]

[1]– بيكة باكة ، موساوي لمياء، آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر ، المركز الجامعي الشيخ أمود بن مختار إيليزي، معهد الحقوق قسم الحقوق 2022/2023، ص 30.

المطلب الأول: الهيئات الفنية المتخصصة في البحث والتحري عن الجريمة الإلكترونية

الهيئات المتخصصة في مكافحة الجريمة المعلوماتية تعتمد على وحدات تضم محققين من نوع خاص يتمتعون بصفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية، وهذه الوحدات تعمل على تنفيذ مهام الوقاية ومكافحة الجرائم الإلكترونية [1]، كما يحدد هوية مرتكبي هذه الجرائم رغما عن تعقيدات الأمر من الناحية التقنية نظرا لطبيعة الجريمة الإلكترونية وأدلتها. ونادرا ما يتغافل الجاني عن تركها وراءه، واعتمادا على ذلك فإن أمر التحقيق والبحث تقوم به جهات من نوع خاص من حيث التركيبة البشرية المكونة لها، ويتميز أفرادها بالخبرة العملية والكفاءة في مجال النظم المعلوماتية، وهذا ما يمكنهم من التحكم في مجريات التحقيق، من خلال خبرتهم في التعامل مع الوسائل الموضوعة تحت تصرفهم من أجهزة وحواسيب وبرامج تحكم خاصة، والتي تسمح لهم بملاحقة المجرمين المعلوماتيين واقتفاء آثرهم الإلكتروني إذ أنه المستحيل على رجال البحث والتحقيق في الجرائم التقليدية التعامل مع الجرائم المعلوماتية. وهذا ما أدى إلى ضرورة استحداث وحدات خاصة لأجل مجابهة فئة المعلوماتية، مجرمي لأنهم أخطر فئة من الناحية الإجرامية على أمن وسلامة النظم المعلوماتية، وأيضا بالنظر إلى تفاقم الظاهرة الإجرامية المعلوماتية من يوم لآخر وزيادة مدى خطورتها واتساع رقعة نشاطها لتشمل كل ما هو موصول بالشبكة سواء هيئات عمومية أو خاصة أو أفراد. انطلاقا من هذا لنا أن نتطرق إلى الفرعين الآتيين:

[1]– وشن لبني نباش ،مراد، دور رجال الضبطية القضائية في مكافحة الجريمة الإلكترونية، مذكرة ماستر، جامعة البشير الإبراهيمي، برج بوعريريج كلية الحقوق والعلوم السياسية قسم الحقوق، 2021/2022، ص44.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم الإلكترونية:

قام المشرع الجزائري باستحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والمعلومات ومكافحتها، كما تساعد الهيئة السلطات القضائية في التحقيقات المتعلقة بالجرائم المعلوماتية وتقوم بتجميع المعلومات وإنجاز الخبرات القضائية.[1]

أولا: التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تعرف حسب ما نصت عليه المواد من 01 إلى 04 من القانون 09-04 بأنها: "هيئة إدارية مستقلة بشخصية معنوية واستقلال مالي ويقع مقرها بالجزائر العاصمة". كما أنشأت الهيئة الوطنية بالجزائر بموجب المادة 13 من القانون 09-04 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاتصال والإعلام ومكافحتها، وبالضبط في نص المادة 13، لكنه ترك أمر تشكيل الهيئة وتنظيمها وكيفية سيرها للتنظيم الصادر بموجب المرسوم الرئاسي 15/261.[2]

كما تعتبر الهيئة سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة يترأسها وزير العدل وأساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن،

وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء وتضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية النابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين وفقا لقانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة

[1]– ربيعي لحسن، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة دكتوراه جامعة باتنة 1 ، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2015/2016، ص145.

[2]– سيد علي السيد محمد، الجرائم الإلكترونية (ماهيتها ، صورها إثباتها مكافحتها، دار التعليم الجامعي، الإسكندرية، 2020، ص107.

والوقاية للاتصالات الإلكترونية قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات والجرائم الأخرى تحت سلطة القاضي المختص. [1]

ثانيا مهام واختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

مهامها نصت المادة 14 من نفس القانون على أنه تتولى الهيئة المذكورة في المادة 13 خصوصا مجموعة من المهام نذكر منها:

1-الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تكمن إجراءات الوقاية بتوعية مستعملي تكنولوجيات الإعلام والاتصال وشرح مدى خطورة هذه الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، وعلى رأس هذه الجرائم جرائم التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء... [2]

2- مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

المادة 14 من القانون 09-04 يوجد نوعان من المكافحة تتولاها هذه الهيئة:

مد يد العون للسلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجربها بشأن هذه الجرائم.

تنشيط وتنظيم عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، تقديم المساعدة لمصالح الأمن والدرك الوطنيين ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة) تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعطيات

[1]- ربيعي لحسن ، مرجع سابق، ص147

[2]- مرجع نفسه، ص148.

المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم:

تقوم الهيئة وطنيا بتنسيق وتحفيز الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات (الهيئات) المشابهة لها على مستوى الدول بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم.[1]

اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: بينت الفقرة 02 من المادة 04 من المرسوم الرئاسي -15-261 المهام التي تتولاها الهيئة على سبيل الحصر والغاية منها هو الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ومن أبرز مهامها:[2]

- اقتراح العناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

تنسيق وتنشيط العمليات الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. مد يد المساعدة لمصالح الشرطة القضائية والسلطة القضائية في إطار مكافحة الجرائم الإلكترونية من خلال تزويدهم بالمعلومات والخبرات القضائية وضمان المراقبة الوقائية للاتصالات الإلكترونية لأجل الكشف عن الجرائم التي تتعلق بعمال الإرهابية والتخريبية التي تمس بأمن الدولة وذلك تحت سلطة القاضي وباستثناء أي هيئات وطنية أخرى.

[1]- ربيعي لحسن، نفس المرجع السابق ، ص148

[2]- ربيعي لحسن، نفس المرجع السابق ، ص150

-تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.[1]

ثالثا : تشكيل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

لكي تتمتع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بفعالية، يجب أن تتكون من جهاز إداري تنفيذي وذلك لأداء اختصاصاتها على أكمل وجه، يتكون الجهاز الإداري من مجلس توجيه ومديرية عامة وهذا يضمن أداء المهام المنوطة بها وفقا للقانون، يترأس مجلس التوجيه وزير الدفاع الوطني أو ممثلة وتتكون من الوزارات التالية:

- وزارة الدفاع الوطني. وزارة العدل.

- الوزارة المكلفة بالمواصلات السلكية واللاسلكية.

- الوزارة المكلفة بالداخلية.

إلا أنه، وما يجب التأكيد عليه أن مثل هذه الهيئات لا تعمل بمعزل عن الأهداف الحكومية الكبرى أو خارج نطاق السياسة العامة للدولة، لأن الغاية من إنشاؤها هو تحقيق سياسة الدولة في المجالات المعنية لذلك، حتى تنجح هذه المهمة تعمد الدولة إلى منح هذه الهيئات نوعا من الاستقلالية كقوة دفع لها حتى تتيح لها الفرصة للعمل بنجاعة. وتزود الهيئة بأمانة عامة تحت سلطة وزارة الدفاع الوطني، ويتكلف مجلس التوجيه على الخصوص بما يلي:

-التداول حول إستراتيجية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[1]- بوزبرة سهيلة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، مجلد ،17، العدد 2 ، 2022، ص565-567.

-التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

-تقييم حالة التهديد دوريا في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال للقدرة على تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بشدة.

-اقتراح النشاطات التي تتصل بالبحث وتقييم الأعمال المباشرة في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. [1]

-الموافقة على عمل الهيئة.

-دراسة التقرير السنوي لهذه الهيئة.

-تقديم الرأي في كل مسألة تتصل بمهام الهيئة.

-ضبط المعايير القانونية في مجال اختصاصه.

-دراسة مشروع الهيئة.[2]

وقد أكد المشرع على أن سير مجلس التوجيه تحدد بموجب قرار من وزير الدفاع:

وهذا ما يدل على سيطرة وزير الدفاع على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال حتى وبالتالي تبعية هذه الهيئة لوزارة الدفاع فلا يمكن القول باستقلاليتها.

[1]- زناتي محمد السعيد الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية ، مجلة إيليزا للبحوث والدراسات، مجلد 2، العدد 01، 2017،ص34

[2]- زناتي محمد السعي، نفس المرجع اللسابق ، ص36

الفرع الثاني: جهازي الأمن والدرك الوطني

قامت المديرية العامة للأمن الوطني وجهاز الدرك الوطني بإنشاء فرق خاصة لمكافحة الجرائم الإلكترونية وتدريب أفراد متخصصين في هذا المجال على مستوى الداخل والخارج يستخدمون أحدث التقنيات لكشف ومكافحة هذا النوع من الجرائم.[1]

أولا: جهاز الأمن الوطني:

المديرية العامة للأمن الوطني في الجزائر قامت بإنشاء مخابر مركزية بمركز الشرطة بشاطوف – الجزائر العاصمة ومخيرين بقسنطينة ووهران وتحتوي هذه المخابر على فروع تقنية خلية الإعلام الآلي، وفرق متخصصة للتحقيق والكشف عن جرائم الانترنت، هناك مخابر أخرى ثم تأسيسها في بشار ورقلة وتمنراست، كما يتم توسيع نشاط هذه المخابر لتغطية جميع أنحاء البلاد. ينظم المخبر الجهوي للشرطة العلمية مخبرا خاصا على مستوى قسنطينة يقوم بمهمة التحقيق في الجريمة الإلكترونية تحت اسم "دائرة الأدلة الرقمية والآثار التكنولوجية "ضمت 03 أقسام هي: قسم استغلال الرقمية الناتجة عن الحواسب والشبكات.

قسم استغلال الأدلة الناتجة عن الهاتف النقال.

قسم تحليل الأصوات ويكون بالاستعانة بأجهزة مادية للكشف عن الجرائم الإلكترونية. 1

ثانيا: جهاز الدرك الوطني:

الدرك الوطني يعتبر جزءا هاما من قوات الأمن في مكافحة الجريمة بشكل عام والجريمة الإلكترونية بشكل خاص. وقد تم تخصيص موارد بشرية ومادية لهذا الغرض وأصبحت مكافحة الجريمة الإلكترونية من أولويات الدولة الجزائرية وقد بدأت الجهود الفعلية لمحاربة الجريمة الإلكترونية بقيادة الدرك الوطني في عام 2004، وهذا ما يعكس التزام الدولة في

[1]– زناتي محمد السعي، نفس المرجع اللسابق ، ص36

الحفاظ على الأمن والطمأنينة في الفضاء السيبيراني الوطني، ليتم بعدها إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها والذي يعد اليوم العصب الذي يسير مهام المكافحة واليقظة وفرض احترام القوانين في الوقت الذي يبحر فيه الملايين من المستخدمين عبر صفحات الانترنت سواء من الخواص أو المؤسسات في الفضاء الإلكتروني.[1]

وقد عمل المركز السالف الذكر منذ إنشائه سنة 2008 على تأمين منظومة المعلومات لخدمة الأمن العمومي، بحيث يهدف ضباط وأعوان الشرطة القضائية المؤهلين في الدرك الوطني إلى تطبيق القوانين وجمع الأدلة وتحليل المعطيات وبيانات الجرائم الإلكترونية المرتكبة والبحث عن مرتكبيها ، وتحديد هوية أصحابها إن كانوا أشخاصا فرادى أو عبارة عن عصابات كما يعمل المركز على مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها في هذا الخصوص، كما يستطيع هذا المركز معالجة أكثر من 100 جريمة إلكترونية سنة 2014 وما يفوق 500 قضية رقمية سنة 2015، وفي الخمسة أشهر الأولى من سنة 2019 تم معالجة 1188 قضية بنجاح من مجموع 1515 قضية مسجلة مع توقيف 1512 متورط، وقد قامت قيادة الدرك الوطني بمجموعة من البرامج التوعوية بالتنسيق مع وزارة التربية الوطنية بتقديم دروس توعية في المدارس باعتبار أن الأطفال هم من أكثر الفئات العمرية تضررا من الجريمة الإلكترونية كخطوة أولية نحو زيادة وعي الطلاب بمخاطر الجريمة الإلكترونية وحمايتهم منها.

ولابد من السعي لمواكبة التطورات والمستجدات الحاصلة في مجال التكنولوجيات، فقد عمل جهاز الدرك الوطني على تكوين الإطارات وأعوان الدرك الوطني بشكل متواصل وذلك من خلال إنشاء مدارس ومعاهد لهذا الغرض، كمدرسة الشرطة القضائية التابعة للدرك الوطني والمعهد الوطني للشرطة القضائية.

[1]– زناتي محمد السعي، نفس المرجع اللسابق ، ص38

المطلب الثاني: الهيئات القضائية المتخصصة في البحث والتحري عن الجريمة الإلكترونية

تقوم السلطة القضائية بتسوية القضايا المتعلقة بالإجرام المتصلة بتكنولوجيات الإعلام والاتصال خاصة بعد اللجوء الكبير والمتزايد إلى الشبكات الرقمية والنظام القضائي الجزائري ويتجه نحو تثبيت فكرة القضاء المتخصص وذلك ما نص عليه القانون 04/14 المؤرخ في 10 نوفمبر 2010 المعدل والمتمم لقانون الإجراءات الجزائية من إمكانية تمديد دائرة الاختصاص للمحكمة وكذا الوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم، وذلك فيما يتعلق جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[1]

وقد نصت المادة 40 من قانون الإجراءات الجزائية على : تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد 40، 37، 329.

من هذا القانون ومراعاة أحكام المواد من 40 مكرر 01 إلى 40 مكرر 05 أدناه وتطبيقا لذلك صدر المرسوم التنفيذي رقم 06 348 الذي تضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق وقد نصت المادة 10 منه على[2]: تطبيقا لأحكام المواد و 40 و 329 من الأمر رقم 66/156 والمتضمن قانون الإجراءات الجزائية ويهدف هذا المرسوم إلى تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دوائر اختصاص محاكم أخرى كما هو محدد في المواد 2 و 3 و 4 و 5 أدناه في الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم

[1]– شنتير خضرة، المرجع السابق، ص 200 –202.

[2]– مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني، المجلد 06، العدد 02،2022، ص1074.

الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف. وقد سعى المشرع من وراء إنشائه للأقطاب الجزائية إلى سد العجز القائم على فكرة غياب هيئات قضائية متخصصة مؤهلة لمكافحة هذه الجرائم أو التقليل من آثارها وأبعادها الوخيمة على الصعيدين المحلي والدولي لاسيما بعد إثبات عجز القضاء العادي وعدم قدرته على حل هذا النوع الحديث من الجرائم وهذا ما سنبينه في الفرعين الآتيين:

الفرع الأول: الاختصاص الإقليمي للأقطاب الجزائية المتخصصة.

المشرع يضبط الحدود التي يمكن لقضاة النيابة والتحقيق والحكم العمل ضمنها وعادة ما يتم تحديد اختصاص محلي لكل محكمة استنادا على موقع وقوع الجريمة أو المكان الذي يقيم فيه المتهم أو مكان القبض عليه، وهذا ما وصت عليه المادة 329/01 ق.إ.ج.ج كما أن الأصل أن اختصاص الشرطة القضائية ووكيل الجمهورية المشرف عليهم يكون ضمن الحدود التي يباشرون ضمنها مهامهم في دائرة اختصاصهم وهو ما نصت عليه المادة 16 من ق.إ.ج.ج. [1]وقد ظهرت فكرة إنشاء محاكم ذات اختصاص موسع كأحد مخرجات برنامج إلى إصلاح العدالة وتطويرها، كما اتجه المشرع من جهة أخرى نحو سياسة تجريمية قصد تطويق أفعال تضر بالمصالح الحيوية للمجتمع، وتتجه نحو اتجاه التزامات الدولة الجزائرية كمكافحة الجريمة المنظمة العابرة للحدود الوطنية والجريمة الإلكترونية وغيرها من الجرائم التي تحتاج كفاءة مهنية عالية، وتقنيات تحري خاصة تحتاج إلى وسائل مادية وبشرية ذات نوعية.

وعلى هذا الأساس جاء القانون رقم 04/14 المؤرخ في 10/11/2004 المتضمن تعديل الأمر رقم 66-155 المتعلق بقانون الإجراءات الجزائية حيث قام بتعديل المواد 37، 40 و

[1]- عاشور أنيسة، بحيصة خديجة، الأقطاب الجزائية المتخصصة كآلية إجرائية لمكافحة جرائم الفساد، مذكرة ماستر، جامعة غرداية، كلية الحقوق والعلوم السياسية قسم الحقوق، 2023،ص 26

329 منه مؤسسا لإمكانية توسيع الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق والمحكمة إلى دائرة اختصاص محاكم أخرى تحدد عن طريق التنظيم، وهذا بمناسبة متابعة جرائم معينة بالتحديد.

وقد جسدت السلطة التنفيذية هذا الاتجاه نحو فكرة التخصيص القضائي بصدور المرسوم التنفيذي رقم 06-348 المؤرخ في 05/10/2006 وقد تضمن الجهات القضائية التي سيوسع اختصاصها المحلي، وقد حدد أربعة محاكم على المستوى الوطني وهي محكمة سيدي محمد بالجزائر العاصمة، محكمة قسنطينة، محكمة وهران، محكمة ورقلة. [1]

أولا: محكمة سيدي محمد: مقرها في الجزائر العاصمة، ويمتد إقليميا لتشمل اختصاص محاكم تقع في دائرة اختصاص مجالس قضائية لكل من الجزائر، الشلف الأغواط، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس وهي عشر مجالس قضائية[2].

ثانيا: محكمة قسنطينة: مقرها في مدينة قسنطينة ويمتد إقليمها إلى اختصاص محاكم التابعة للمجالس القضائية لكل من : قسنطينة، أم البواقي بجاية بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة وبرج بوعريريج.

ثالثا: محكمة وهران: مقرها في مدينة وهران ويتوسع اختصاصها الإقليمي إلى نطاق اختصاص المحاكم التابعة للمجالس القضائية لكل من وهران بشار ،تلمسان تيارت سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة عين تموشنت، غليزان.

رابعا: محكمة ورقلة: تقع في مدينة ورقلة ويمتد اختصاصها الإقليمي إلى نطاق اختصاص المحاكم التابعة للمجالس القضائية لكل من ورقلة أدرار ، تمنراست، إليزي، تندوف، غرداية.

[1]- بيكرارشوش محمد، الاختصاص الإقليمي في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، مجلد 8، العدد14 ، 2016، ص 315، ص 316

[2]- بيكرارشوش محمد، نفس المرجع السابق ، ص319

ويجب الإشارة إلى أنه وبالإضافة إلى ما سبق، فإن المحاكم الجزائرية يمتد اختصاصها المحلي إلى خارج حدود الإقليم الوطني إذا تعلق الأمر بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال الصادر بموجب القانون رقم 09-04 المؤرخ في 05 غشت 2009 في حال ارتكابها خارج الإقليم الوطني.

الفرع الثاني: تمديد الاختصاص المحلي.

من أهم القواعد الإجرائية لمواجهة الجرائم الإلكترونية تمديد الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق وضباط الشرطة القضائية:[1]

أولا: تمديد الاختصاص المحلي لوكيل الجمهورية:

يجوز تمديد الاختصاص المحلي لوكلاء الجمهورية حسب ما أقرته المادة 37/2 من ق.إ.ج إلى دائرة اختصاص محاكم أخرى، حينما يتعلق الأمر بجرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال، الإرهاب، جرائم الصرف والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[2]

وقد تم سحب نظام الملائمة من النيابة العامة في إطار متابعة هذا النوع من الجرائم، إذ يجب على وكيل الجمهورية تحريك الدعوى العمومية بقوة القانون .

[1]– بيكرارشوش محمد، نفس المرجع السابق ، ص320

[2]– بونار رويقة، الجريمة المعلوماتية في التشريع الجنائي الجزائري، مذكرة ماستر جامعة محمد الصديق بن يحي جيجل، كلية الحقوق والعلوم السياسية قسم الحقوق، 2020 /2021 ص 46

ثانيا : تمديد الاختصاص المحلي لقاضي التحقيق:

يجوز تمديد الاختصاص المحلي لقاضي التحقيق حسب ما أقرته المادة 40/2 من ق. إج إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالعرف.

ثالثا : تمديد الاختصاص المحلي لضباط الشرطة القضائية:

يتحدد الأصل المكاني أو الإقليمي لضبط الشرطة القضائية تحت سلطة وكيل الجمهورية الذي يقوم بإدارة أعمالهم في مرحلة جمع الاستدلالات، وبانتداب قاضي التحقيق في حال فتح تحقيق قضائي بالمكان الذي ارتكبت فيه الجريمة أو مكان توقيف المشتبه فيهم أو مكان إقامتهم طبقا للمواد 16/3 من ق .إج: يجوز لهم أيضا في حال الاستعجال أن يقوموا بمباشرة مهمتهم في جميع الأقاليم الوطنية إذ طلب منهم أداء ذلك من القاضي المختص قانونا، ويجب أن يساعدهم ضباط الشرطة القضائية الذي يمارس وظائفه في المجموعة السكنية المعنية. والمادة 16 مكرر ، المادة 40 مكرر 1 ، المادة 40 مكرر 2، المادة 40 مكرر 3، أي أن اختصاصهم يتسع ليشمل اختصاص إقليمي لمحاكم غير التي يباشرون فيها مهامهم في دائرة اختصاصها . [1]

[1]– بونار رويقة، نفس المرجع السابق ، ص48

المبحث الثاني: التعاون الدولي القضائي في مواجهة الجرائم الإلكترونية

بما أن الجريمة الإلكترونية تعد جريمة ذات بعد دولي أي أنها عابرة للحدود الوطنية فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي والجنائي، إضافة إلى ذلك فالتحقيقات المتبادلة في الجريمة الإلكترونية وملاحقتها قضائيا تبرز أهمية المساعدة القانونية بين الدول ،[1] لذلك تحرص الدول منذ فترة طويلة على عدم إفلات المجرمين من العقاب وذلك من خلال إبرام اتفاقيات ثنائية ومتعددة الأطراف لتعزيز التعاون القضائي في المجال الجنائي بين الدول كما تساهم في تحقيق المصلحة المشتركة وتقديم المجرمين للعدالة، واتخذت كمظاهر لهذا التعاون صورا متنوعة ، وأهمها التعاون الأمني على المستوى الدولي والذي سنوضحه في المطلب الأول والمساعدة القضائية الدولية من خلال عرضها في المطلب الثاني.

المطلب الأول: التعاون الأمني على المستوى الدولي.

ويشمل ذلك أربع صور والمتمثلة في ضرورة التعاون الأمني على المستوى الدولي وجهود المنظمة الدولية للشرطة الجنائية (الإنتربول)، بالإضافة لتبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة والقيام ببعض العمليات الأمنية والشرطية المشتركة وهذا ما سنبينه في الفروع التالية.[2]

[1]– بودربالة إلياس، التعاون الدولي كآلية لمكافحة الفساد، مجلة الحقوق والحريات، المجلد 9 ، العدد 2، 2021، ص499.

[2]– بودربالة إلياس، نفس المرجع السابق ، ص52

الفرع الأول: ضرورة التعاون الأمني الدولي.

إن الواقع العملي أثبت أن الدولة بمفردها لا تستطيع مواجهة التحديات الجرمية في هذا العصر المتطور في شتى ميادين الحياة، وبالتالي أصبحت هناك حاجة ماسة لوجود كيان يتولى مكافحة الجريمة الالكترونية، وتتعاون من خلاله أجهزة الشرطة في مختلف الدول خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة. [1]

الفرع الثاني: جهود المنظمة الدولية للشرطة الجنائية (الانتربول).

تعمل المنظمة على تعزيز التعاون بين أجهزة الشرطة في الدول الأطراف، كما تعمل المكاتب المركزية الوطنية للشرطة الدولية على تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وكذا التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها حول جرائم الأنترنت، وفيما يخص دور المنظمة في ما يتعلق بجرائم الانترنت نأخذ على سبيل المثال ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة من موقعه على شبكة الانترنت وذلك إثر تلقي النيابة اللبنانية برقية الانتربول في ألمانيا بهذا الخصوص. كما أولت المنظمة اهتماما خاصا بمكافحة الجريمة المنظمة بحيث تم اتخاذ العديد من القرارات الأساسية في الجمعية العامة للأنتربول، ومن أهم هذه القرارات القرار رقم RES/ MAGN57 /17 الذي تم اتخاذه من خلال دورة الجمعية العامة 57 المنعقدة في بانغوك سنة 1988 بعنوان الجريمة المنظمة. كما أعربت الجمعية العامة للأنتربول في جلستها 67 في القاهرة عام 1988 أن محاربة الجريمة المنظمة أحد أولويات الشرطة الدولية في قيامها بالدور الهام المتمثل بتنسيق تعاون الشرطة الدولية ضد الجريمة المنظمة.

[1]– محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 2 ، 2016، ص52.

يمكن تفعيل الأدوار التي تمارسها الأنتربول في مواجهة الجرائم المنظمة من خلال العديد من النشاطات التي تقوم بها المنظمة في مجال التعاون الأمني الدولي لمكافحة الجريمة المنظمة، ومنها :

-عقد ندوات ومؤتمرات: فقد عقدت عدة ندوات عالمية كالتي عقدت حول جرائم المخذرات، ومؤتمرات إقليمية وجهوية مثل المؤتمر الآسيوي والإفريقي والأوروبي، كما احتضنت الجزائر عام 1997 الندوة الجهوية الإفريقية لمنظمة الأنتربول.

-التحقق من المجرمين والكشف عن شخصية الجثث المجهولة فإثبات وتحقيق الشخصية يعد مظهرا من مظاهر التعاون الدولي الأمني.

الفرع الثالث: تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة:

الكوارث الضخمة قد تواجه كافة دول العالم وتكون صعبة التنبؤ بها كما يصعب مواجهتها بالإمكانيات القومية للدولة المنكوبة بمفردها، بالإضافة إلى ذلك فإن الوقت يلعب دورا حاسما في التعامل مع الكوارث فالواجب أن يتم تكثيف الجهود والخبرات والإمكانيات للتصدي للتحديات التي تواجهنا في وقت قصير، فالاستجابة السريعة والتنسيق الجيد يساعد في تخفيف الآثار السلبية للكوارث وتعزيز الاستعداد والاستجابة الفعالة وهذا ما يمكن تحقيقه إلا بتضافر الجهود لذلك لابد من التعاون الدولي.[1]

الفرع الرابع: القيام ببعض العمليات الشرطية والأمنية المشتركة

تعقب المجرم الإلكتروني وجمع الأدلة الرقمية وكذلك عمليات التفتيش العابرة للحدود تعتبر مكونات أساسية وعملية التحقيق الجنائي الحديث، حيث تستخدم الحواسيب والأنظمة المعلوماتية وشبكات الاتصال للبحث عن أدلة وبراهين تساعد في الكشف عن الجريمة

[1]- غربي أسامة، المنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مكافحة الجريمة المنظمة ، مجلة دراسات وأبحاث، المجلد3، العدد 3، 2011، ص 164-165.

المعلوماتية، فالعمليات الشرطية والأمنية تلعب دورا هاما في تطوير مهارات وخبرات القائمين على مكافحة تلك الجرائم من خلال التعاون والتنسيق بين الجهات المعينة مما يؤدي لتعزيز القدرة على مكافحتها ووضع حد لها.

المطلب الثاني: المساعدة القضائية الدولية.

المساعدة القضائية الدولية تهدف لتسهيل المحاكمة وكشف الحقيقة في جرائم معينة حيث تعمل السلطات المختصة في الدولة المطلوبة على تنفيذ إجراءات قضائية بناءا على طلب الدولة الطالبة، ووظف مصطلح المتبادلة لتبادل المساعدة القضائية الدولية في إطار القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .[1]

بالإضافة إلى أن المساعدة القضائية الدولية تلعب دورا هاما في ضمان عدم إفلات مرتكبي الجرائم من العقبات وهي السبيل الفعال للحصول على الدليل الإلكتروني سواء من خلال تبادل المعلومات بين الدول أو نقل الإجراءات أو تفويض جهات أخرى للقيام لأعمالها وهذا ما سنعرضه في الفروع التالية:

الفرع الأول: تبادل المعلومات.

تلعب المعلومة دورا حاسما في مواجهة أي ظاهرة وتحقيق أي إنجاز، والدول تدرك أهمية ذلك وتسعى لاكتساب معلومات أكثر لتعزيز التعاون الدولي ورغم وجود اتفاقيات تلزم الدول بالتعاون إلا أنه قد يكون هناك بعض الإحباطات في التنفيذ، سيما إذا ما تعلق الأمر بالإجرام الذي يتعدى نطاق الدولة الواحدة، ذلك أن المعلومات ذات الصلة في هذا الجانب

[1]– ناشف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، 2022، ص 438.

ترتبط بصورة أو أخرى بأمن الدولة القومي وسيادتها التي لا تريد التفريط بها، وتبالغ الدول عادة في الدفاع عن تلك السيادة.[1]

أقرت العديد من الاتفاقيات هذا النمط من التعاون، وأبرزها ما ورد في الفقرة الثانية من المادة الأولى لمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية وكذلك ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، إذ فرضت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي. والأمر نفسه بالنسبة لما قضت به المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية، وفي هذا المجال وضع اتفاق شنغن للإتحاد الأوروبي نظاما متكاملا لتبادل المعلومات. [2]

الفرع الثاني: نقل الإجراءات .

يقوم الدول بالتعاون واتخاذ إجراءات جنائية بناءا على اتفاقيات ومعاهدات لمكافحة الجرائم التي ترتكب في إقليم دولة أخرى ولمصلحة دولة أخرى وذلك عند توافر شروط معينة من أهمها التجريم المزدوج يعني أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها أي أن تكون هذه الإجراءات مقررة في قانون الدولة المطلوب إليها عن نفس الجريمة، كما يجب أن تكون الإجراءات المطلوبة ذات أهمية بالغة حيث تلعب دورا حاسما في الكشف عن الحقيقة. كما أقرت العديد من الاتفاقيات الدولية والإقليمية التي تهدف إلى

[1]– عصماني ليلى، صهيب سهيل غازي زامل المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، المجلد 9، العدد 2، 2020، ص16

[2]– شويرب جيلالي، مراد فائزة، الآليات الدولية والوطنية لمكافحة الجريمة السيبيرانية ، مجلة الدراسات القانونية والسياسية، المجلد 9، العدد 2، 2023، ص 165.

تعزيز التعاون الدولي في مجال المساعدة القضائية، مثل معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية سنة 2000 في المادة 21 منها، ونفس الشيء نجده في معاهدة المؤتمر الإسلامي لمكافحة الإرهاب الدولي سنة 1999 في المادة 9 منها ، وأيضا المادة 16 من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي عام.2003[1]

الفرع الثالث: الإنابة القضائية:

ويقصد بذلك طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، هذا الطلب يتم تقديمه من قبل الدولة الطالبة إلى الدولة المطلوب إليها للمساعدة في فصل مسألة معروضة على السلطة القضائية في الدولة الطالبة.[2]

يهدف هذا الطلب إلى تسهيل الإجراءات الجنائية بين الدول وضمان إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى مثل سماع الشهود أو إجراء التفتيش وغيرها من الإجراءات.

أولا : تنفيذ الإنابة القضائية:

بخصوص تنفيذ الإنابة القضائية الدولية فإنه إذا استقر القاضي على ضرورة اللجوء إلى الإنابة القضائية، كأن يرى القاضي الجزائري اتخاذ الإجراء القضائي موضوع الإنابة فيمكنه إرسال الطلب إلى الجهة القضائية المختصة في الخارج أو إلى البعثة الدبلوماسية أو

[1]– زغودي عمر، الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية، مجلة البحوث القانونية والاقتصادية، المجلد 3 ، العدد 2، 2020، ص 105.

[2]– غانم مرضي الشمري، مرجع سابق، ص99، ص 100.

القنصلية المتواجدة في الخارج حسب ما أكدت عليه المادة 112 من القانون 08-09 المتعلق بقانون الإجراءات المدنية والإدارية. [1]

أ- عن طريق السلطات القضائية:

الإنابة القضائية عادة ما توجه إلى السلطات في الدولة الأجنبية عن طريق النيابة العامة في البلدين أو أي جهاز قضائي آخر يعهد إليه بتنفيذ الإنابة ويتم إرسالها عن طريق وزارة العدل فوزارة الخارجية ثم وزارة العدل في الخارج أو عن طريق أحد أطراف الخصومة أنفسهم الذي يتقدم بطلب للجهات القضائية موضوعه تنفيذ إنابة قضائية في الخارج وهذا ما أقره الفقه والقضاء الفرنسيين وهذه الطريقة في تنفيذ الإنابة القضائية الأكثر اتفاقا مع طبيعة الإنابة.[2]

تنفيذ الإنابة القضائية الدولية بواسطة البعثات الدبلوماسية والقنصلية:

عند تنفيذ الإنابة القضائية يعين تحديد نطاق الهيئة المنابة ولمعرفة هذا النطاق يجب معرفة حدود الهيئة الدبلوماسية أو القنصلية من حيث أن سلطتها في تنفيذ الإنابة القضائية الدولية تشمل رعاياها فقط أم تمتد إلى رعايا دولة أخرى.

وبالإشارة إلى أن اتفاقية فينا للعلاقات القنصلية لعام 1963 اشترطت أن تكون طريقة إرسال الإنابة القضائية وتنفيذها على وفق قوانين وأنظمة الدولة المرسل إليها هذا الطلب والمراد تنفيذه على إقليمها إلا إذا أوجد اتفاق دولي بين الدول المعنية تحدد طريقة خاصة لهذا التنفيذ من قبل الممثل القنصلي على أن عدم وجود اتفاقية بين الدولتين لا يسمح بصورة مطلقة للدول طالبة الإنابة القضائية تنفيذها من قبل مبعوثها الدبلوماسي أو القنصلي في الدولة الأجنبية على وفق قوانين هذه الدولة فإذا قدر القاضي ضرورة اللجوء إلى الإنابة القضائية فعادة ما يلجأ إلى إحدى الطريقتين: اللجوء إلى ممثلي دولته الدبلوماسيين أو قناصلها في

[1]- زغودي عمر،نفس المرجع السابق ، ص103

[2]- زغودي عمر، مرجع سابق، ص 106.

الدولة المراد اتخاذ الإجراء فيها، على أن هذا اللجوء إلى هذه الطريقة رهن شرطين أولهما أن يجيز قانون دولة الممثل الدبلوماسي أو القنصلي للقيام بذلك العمل وثانيهما أن تسمح الدولة المعتمدين لديها بمباشرة الإنابة القضائية على إقليمها .[1]

ثانيا: تنفيذ الأحكام الأجنبية

عندما يتعلق الأمر بإعمال إقليمية القانون الجنائي بصورة مطلقة فإنه بالضرورة يقود إلى القول بإقليمية الأحكام الجنائية وبالتالي القاضي الجنائي لا يطبق سوى قانون دولته، كما أن الحكم الجنائي الأجنبي الصادر من قضاء دولة معينة لا يعترف له إلا داخل إقليم هذه الدولة، ومن ثم لا يجوز قوة الأمر المقضي به ولا يجوز تنفيذه، إلا أن إنشاء صور وأشكال الجريمة عبر الوطن اقتضى ضرورة الاعتراف بحجية الحكم الجنائي الأجنبي الصادر عن محاكم دولة أخرى. كما أن التعاون الدولي في تنفيذ الأحكام الجزائية الأجنبية مهم جدا في مكافحة الجريمة العابرة للحدود ومع ذلك هناك شروط محددة يجب توافرها لتنفيذ الحكم الجزائي الأجنبي في إقليم الدولة وتقرير الحالات التي لا يجوز فيها تنفيذ هذا الحكم.

أما في الجزائر يوجد تجسيد واقعي لتنفيذ الأحكام الجزائية الأجنبية من خلال بعض الاتفاقيات التي أبرمتها الجزائر والمتعلقة بالتعاون القضائي في المجال الجزائي على سبيل المثال اتفاقية الرياض العربية للتعاون القضائي والتي نصت على الشروط التي يجب توافرها من أجل التعاون الدولي بين الدول الأطراف في مجال تنفيذ الأحكام الجزائية في دولة غير الدولة التي أصدرت هذه الأحكام، عندما يكون المحكوم عليهم من مواطني الدولة المطلوب منها التنفيذ وذلك في حالة توافر الشروط، أن يوافق على طلب التنفيذ كل من الطرف المتعاقد الصادر عنه الحكم والمحكوم عليه، أو أن تكون العقوبة المحكوم بها سالبة للحرية

[1]– زغودي عمر، مرجع سابق، ص 108

لا تقل مدتها أو المدة المتبقية منها أو القابلة للتنفيذ على ستة أشهر أو أن تكون العقوبة من أجل إحدى الجرائم التي لا يجوز فيها التسليم طبقا للمادة 41 من هذه الاتفاقية.[1]

وفي نهاية هذا الفصل يتسنى لنا القول أن الجرائم الإلكترونية من المستجدات الإجرامية الحديثة حيث تستهدف الاعتداء على البيانات والمعلومات والبرامج الإلكترونية، لذا قام المشرع بإنشاء هياكل خاصة لردع هذا النوع من الإجرام وذلك بتخصيص هيئات فنية متخصصة في البحث والتحري عن الجريمة وكذا هيئات قضائية، بالإضافة إلى هذه الآليات لابد من تضافر جهود ولية متبادلة أي ضرورة التعاون الأمني القضائي للحد من هذه الجرائم باعتبارها عابرة للحدود ومن أبرز صور هذا التعاون، التعاون الأمني الدولي والمساعدة القضائية.

[1]– زغودي عمر، مرجع سابق، ص 110

خلاصة الفصل:

لقد كشف لنا هذا الفصل، من خلال تفكيك البنية المؤسساتية الوطنية والدولية، عن أن مكافحة الجريمة الإلكترونية لا يمكن أن تتم بفعالية ما لم تتوفر منظومة متكاملة من الهياكل الفنية والقضائية، مدعومة بإطار تعاون دولي محكم. فمن الجانب الوطني، اتضح أن الجزائر قد سعت إلى تدعيم مؤسساتها بهيئات متخصصة، على غرار الهيئة الوطنية للوقاية من الجرائم الإلكترونية، التي تُعد الذراع التقني الرئيسي لرصد وتتبع الأنشطة غير المشروعة عبر الفضاء السيبراني، إلى جانب ما تقوم به جهازي الأمن الوطني والدرك الوطني من دور محوري في الجانب التحري والتدخل الميداني.

وفي الشق القضائي، أظهرنا أهمية إنشاء الأقطاب الجزائية المتخصصة في تمكين القضاء من ممارسة اختصاص نوعي وإقليمي أكثر نجاعة في مواجهة الجرائم المعقدة، مثل الجرائم الإلكترونية، مع التأكيد على مرونة الاختصاص المحلي عبر آلية التمديد لمسايرة الطبيعة اللا–مكانية لهذه الجرائم.

أما على الصعيد الدولي، فقد برزت أهمية التعاون الأمني الدولي كإطار ضروري لمواجهة تحديات الجريمة الإلكترونية ذات الطابع العابر للحدود، حيث سلطنا الضوء على دور الإنتربول في التنسيق وتبادل المعطيات والقيام بعمليات شرطية مشتركة. كما أبانت الدراسة عن ضرورة تبني الدول لمبدأ المساعدة القضائية الدولية، خصوصًا في مجالات تبادل المعلومات، ونقل الإجراءات، والإنابة القضائية، باعتبارها آليات قانونية تسهم في سد الثغرات القانونية والإجرائية التي قد تعيق التتبع القضائي للمجرمين السيبرانيين.


الخاتمة

الخاتمة :

في ختام هذه الدراسة الموسومة بـ "الآليات الإجرائية في مكافحة الجريمة المعلوماتية في التشريع الجزائري"، يتضح أن تطور تكنولوجيا المعلومات والاتصال قد خلق بيئة خصبة لظهور أنماط جديدة من الإجرام، عُرفت بالجريمة المعلوماتية، والتي تجاوزت الحدود التقليدية للجريمة وأصبحت تهدد الأفراد، المؤسسات، والدول على حد سواء، بما تمثله من مخاطر على الأمن السيبراني والاقتصادي والاجتماعي. وقد عمل المشرّع الجزائري، شأنه شأن باقي التشريعات المقارنة، على مواجهة هذه الظاهرة من خلال إدراج أحكام قانونية وتنظيمية ضمن عدة نصوص،حيث أظهرت الدراسة أن الآليات الإجرائية المقررة في التشريع الجزائري تسعى إلى تحقيق نوع من التوازن بين حماية حقوق الإنسان من جهة، وتمكين الجهات القضائية والأمنية من وسائل فعالة للكشف عن هذه الجرائم وتعقب مرتكبيها من جهة أخرى، كالتفتيش الإلكتروني، مراقبة الاتصالات، وحجز الأدلة الرقمية. ومع ذلك، تبين من خلال التحليل أن هذه الآليات، رغم أهميتها، لا تزال تعاني من ثغرات على مستوى التطبيق العملي، وضعف التنسيق بين الجهات المختصة، ونقص التكوين التقني للضبطية القضائية والسلطة القضائية في المجال الرقمي.

كما أبرزت المقارنة مع بعض التشريعات الأجنبية المتقدمة في هذا المجال، على غرار التشريع الأوروبي والأمريكي، أن الجزائر بحاجة إلى تعزيز بنيتها التشريعية وتطوير نظم التحقيق الرقمي، ومواكبة الاتفاقيات الدولية، خصوصًا اتفاقية بودابست الخاصة بالجريمة السيبرانية، وتحديث القدرات التقنية والبشرية للهيئات المكلفة بإنفاذ القانون.

وبناءً عليه، فإن نجاح مكافحة الجريمة المعلوماتية في الجزائر لا يتوقف فقط على وجود نصوص قانونية، بل يتطلب إرادة سياسية واضحة، تفعيلًا عمليًا للآليات الإجرائية، تكوينًا متخصصًا ومستمرًا للفاعلين في العدالة، وتعاونًا إقليميًا ودوليًا فعّالًا، مع إشراك المجتمع المدني ووسائل الإعلام في التوعية والتحسيس بمخاطر هذه الجرائم وسبل الوقاية منها.

- الاقتراحات :

- ضرورة إصدار قانون موحد شامل للجريمة المعلوماتية يتضمن تعريفًا دقيقًا لها، ويغطي كافة صورها وأنماطها، مع تحديد الإجراءات الخاصة للتحري والتحقيق فيها.

- تعزيز التكوين والتدريب المتخصص لأعوان الضبطية القضائية والقضاة في مجال الجرائم الإلكترونية، لا سيما ما يتعلق بالتحقيق الرقمي وأدلة الجرائم المعلوماتية.

- تفعيل التعاون القضائي الدولي والإقليمي، والانضمام الرسمي لاتفاقية بودابست بشأن الجريمة السيبرانية، لتيسير تبادل المعلومات والمساعدة التقنية بين الدول.

- إنشاء وحدات متخصصة دائمة في الجرائم المعلوماتية داخل مصالح الأمن والدرك الوطني والنيابة العامة، مزودة بموارد بشرية وتقنية متطورة.

- الاستثمار في البنية التحتية التقنية اللازمة لتعقب الجرائم الإلكترونية وضمان تأمين الشبكات الوطنية ضد الاختراقات والتهديدات السيبرانية.

- تحديث وتوسيع الإجراءات الإجرائية التقليدية)كالتفتيش، الحجز، التنصت، المراقبة الإلكترونية) لتتلاءم مع طبيعة الجرائم الرقمية وتعقيداتها.

قائمة المصادر والمراجع

أولا : القوانين .

1. القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الامر 66-156 المتضمن قانون العقوبات الجزائري.
2. القانون رقم 01/06 المتعلق بالوقاية من الفساد ومكافحته المؤرخ في 20 فبراير 2006، الجريدة الرسمية.
3. القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 47، بتاريخ 16 أوت 2009.
4. القانون رقم 18-04 المؤرخ في 10 ماي 2018 يتضمن تعديل قانون العقوبات، بإدراج الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ضمن النصوص العقابية. الجريدة الرسمية للجمهورية الجزائرية، العدد 27 ،الصادرة بتاريخ 2018.ماي 16
5. القانون قانون الوقاية من التمييز وخطاب الكراهية رقم 05/20 المؤرخ في 28 أبريل 2020، الجريدة الرسمية.

ثانيا : المراجع باللغة العربية .

1. أحمد جمال، التحقيق في الجرائم الإلكترونية"، دار الفكر الجامعي، الإسكندرية 2017-2018،
2. أحمد خليفة الملط الجرائم المعلوماتية دار الفكر الجامعي للنشر والتوزيع، مصر 2006،
3. آمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الثانية ، دار هومه للطباعة والنشر والتوزيع، الجزائر ، سنة 2007 ،
4. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع الجزائر2007

5. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة للطباعة والنشر، الجزائر،2006

6. الحلبي، علي عبد القادر، شرح قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، 2011،

7. خالد الممدوح ابراهيم ، فن التحقيق الجنائي في الجريمة الالكترونية ، دار الفكر الجامعي ، الاسكندرية ،مصر 2009 ،

8. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر (أساليب وتغرات) ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر ، سنة 2010،

9. زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، سنة 2011

10. زبيحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى الجزائر، 2011

11. سيد علي السيد محمد، الجرائم الإلكترونية (ماهيتها ، صورها إثباتها مكافحتها، دار التعليم الجامعي، الإسكندرية، 2020،

12. صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،2003

13. عباس أبو شامة عبد المحمود، عولمة الجريمة االقتصادية، جامعة نايف العربية للعلوم أألمنية، الرياض،سنة 2007

14. عبد الرحمان خلفي محاضرات في القانون الجنائي العام، دار الهدى للطباعة والنشر والتوزيع الجزائر، دون طبعة

15. عفيفي عفيفي كامل، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية، ط1، دار الكتب القانونية، القاهرة 2002

16. الغافري عبد الحق، "التحقيق" في الجرائم المعلوماتية"، دار الخلدونية، الجزائر، 2009،

17. لصغير جميل عبد الباقي، القانون الجنائي والتكنولوجية الحديثة، ط1 دار النهضة العربية، القاهرة 1992،

18. مال، عبد الحميد، التحقيق الجنائي في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2015،

19. محمد صغير، "شرح قانون الإجراءات الجزائية"، دار هومة، الجزائر، 1988،

20. مر زبيحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر، ، 2011

21. نائلة عادل محمد فريد قورة – جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية – منشورات الحاتي الحقوقية2005 ص 90

22. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت،2005

23. نهلة عبد القادر مومني، الجرائم المعلوماتية، ط2 دار الثقافة للنشر والتوزيع ب س ن،

24. هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة 1992،

25. هشام محمد فريد رستم ، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة 2000،

26. وردة جوان ، إجراءات التحري في الجرائم الإلكترونية، الطبعة الثانية 2017،

ثالثا: المذكرات والأطروحات .

1. ابتسام موهوب، جرائم المساس بأنظمة المعالجة الآلية لمعطيات للتشريع الجزائري ، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي 2014-2015
2. بلعيد منصورية، النظام الإجرائي للجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، ميدان الحقوق والعلوم السياسية، تخصص قانون قضائي، جامعة عبد الحميد بن باديس 2019-2020،
3. بن زرط أسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، ميدان الحقوق والعلوم السياسية، تخصص قانون جنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم 2018-2019،
4. بن يحي اسماعيل، التحقيق الجنائي في الجرائم الإلكترونية رسالة دكتوراه، تخصص قانون الخاص،قسم حقوق كلية الحقوق و العلوم السياسية، جامعة أبي بكر الصديق بلقا يد تلمسان ، الجزائر ، سنة 2020-2021
5. بونار رويقة، الجريمة المعلوماتية في التشريع الجنائي الجزائري، مذكرة ماستر جامعة محمد الصديق بن يحي جيجل، كلية الحقوق والعلوم السياسية قسم الحقوق، 2020 /2021
6. بيكة باكة ، موساوي لمياء، آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر ، المركز الجامعي الشيخ أمود بن مختار إيليزي، معهد الحقوق قسم الحقوق 2022/2023،
7. رابحي عزيزة، الأسرار المعلوماتية و حمايتها الجزائية ، رسالة دكتوراه، تخصص قانون خاص ، قسم الحقوق،كلية الحقوق والعلوم السياسية ، جامعة ابوبكر بلقا يد ، تلمسان ، الجزائر ، 2017-2018

8. ربيعي لحسن، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة دكتوراه جامعة باتنة 1 ، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2015/2016،
9. سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم القانونية، جامعة الحاج لخضر باتنة، سنة دراسية 2102/2013.
10. سلمى عفيفي، "الضوابط القانونية للتفتيش الإلكتروني"، رسالة ماجستير ، جامعة الجزائر 1،
11. سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماجستير ، كلية الحقوق والعلوم السياسية، جامعة خيضر بسكرة 2014
12. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر 1 ، كلية الحقوق، 2011، 2012
13. عاشور أنيسة، بحيصة خديجة، الأقطاب الجزائية المتخصصة كآلية إجرائية لمكافحة جرائم الفساد، مذكرة ماستر، جامعة غرداية، كلية الحقوق والعلوم السياسية قسم الحقوق، 2023،
14. عبد العزيز أحمد ، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي والعلوم الجنائية كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي سعيدة 2021-2022
15. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر الطور الثاني ميدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير ، تخصص إدارة تحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح ورقلة 2018-2019
16. وشن لبني نباش ،مراد، دور رجال الضبطية القضائية في مكافحة الجريمة الإلكترونية، مذكرة ماستر، جامعة البشير الإبراهيمي، برج بوعريريج كلية الحقوق والعلوم السياسية قسم الحقوق، 2021/2022،

رابعا : المجلات

1. بثينة حبيباتي الطبيعة الخاصة للجريمة المعلوماتية ، دراسات مجلة وأبحاث، مجلد جامعة زيان عاشور، الجلفة، الجزائر، مجلد 12 عدد 03 جويلية 2020 ،
2. بودربالة إلياس، التعاون الدولي كآلية لمكافحة الفساد، مجلة الحقوق والحريات، المجلد 9 ، العدد 2، 2021،
3. بوزبرة سهيلة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، مجلد ،17، العدد 2 ، 2022،
4. بيكرارشوش محمد، الاختصاص الإقليمي في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، مجلد 8، العدد14 ، 2016، ص 315،
5. حمز خضري، عشاش ،حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، العدد 02، المجلد 6، جامعة محمد بوضياف المسيلة، جوان 2020
6. خضري حمز ، عشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجازئري، مجلة الدراسات القانونية والسياسية، العدد 02 المجلد 6 جامعة محمد بوضياف، المسيلة جوان 2020.
7. خليفة عبد القادر، التحقيق الجنائي في الجريمة المعلوماتية"، مجلة القانون والتكنولوجيا، ماي 2020،
8. زغودي عمر، الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية، مجلة البحوث القانونية والاقتصادية، المجلد 3 ، العدد 2، 2020،
9. زناتي محمد السعيد الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية ، مجلة إيليزا للبحوث والدراسات، مجلد 2، العدد 01، 2017،

10. شويرب جيلالي، مراد فائزة، الآليات الدولية والوطنية لمكافحة الجريمة السيبيرانية ، مجلة الدراسات القانونية والسياسية، المجلد 9، العدد 2، 2023،
11. عصماني ليلى، صهيب سهيل غازي زامل المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، المجلد 9، العدد 2، 2020،
12. عميور خديجة، قواعد اختصاص ألقطاب الجزائية للنظر في جرائم الفساد، مجلة دراسات في الوظيفة العامة، العدد 02 جامعة جيجل 2014. ،
13. غربي أسامة، المنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مكافحة الجريمة المنظمة ، مجلة دراسات وأبحاث، المجلد3، العدد 3، 2011،
14. محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 2 ، 2016،
15. محمد زروقي، إجراءات التفتيش في الجرائم الإلكترونية ، المجلة الجزائرية للقانون والعلوم السياسية، العدد 2، 2020،
16. مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني، المجلد 06، العدد 02،2022،
17. ناشف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، 2022،

ملخص الدراسة :

تتناول هذه الدراسة موضوع الآليات الإجرائية في مكافحة الجريمة المعلوماتية، وذلك في ظل التطور التكنولوجي المتسارع الذي أدى إلى بروز هذا النوع من الجرائم كخطر يهدد الأفراد والدول على حد سواء.

تُركّز الدراسة على تحليل الإجراءات القانونية والأمنية المتبعة في التصدي لهذا النوع من الجرائم، بدءًا من جمع الأدلة الرقمية، والتحقيقات الإلكترونية، والتعاون الدولي، والتشريعات الخاصة بمكافحة الجريمة السيبرانية، إلى جانب دور الجهات المختصة مثل النيابة العامة، وأجهزة إنفاذ القانون، والهيئات القضائية المتخصصة.

كما تتناول الدراسة الصعوبات العملية والقانونية في تطبيق هذه الآليات، ومنها الطبيعة العابرة للحدود للجريمة المعلوماتية، ونقص الخبرة التقنية، والحاجة إلى تطوير القوانين الوطنية بما يتماشى مع الاتفاقيات الدولية.

وخلصت الدراسة إلى أهمية تعزيز التنسيق بين الدول، وتطوير البنية القانونية والتقنية، وزيادة الوعي المجتمعي، وتكثيف التدريب المتخصص لمواجهة هذا التهديد المتنامي.

الكلمات المفتاحية:

الجريمة المعلوماتية – الإجراءات الجنائية – الأدلة الرقمية – الأمن السيبراني – التعاون الدولي – التحقيق الإلكتروني – التشريعات الحديثة.

Study Summary :

This study addresses the topic of procedural mechanisms in combating cybercrime, within the context of rapid technological advancement that has made such crimes a growing threat to both individuals and states.

The research focuses on analyzing the legal and security procedures adopted to combat cybercrime, including digital evidence collection, cyber investigations, international cooperation, and cybercrime-specific legislation, as well as the role of competent authorities such as public prosecution, law enforcement agencies, and specialized judicial bodies.

The study also examines the practical and legal challenges in implementing these mechanisms, such as the cross-border nature of cybercrime, lack of technical expertise, and the need to update national legislation in line with international agreements.

It concludes by emphasizing the need to enhance international coordination, develop legal and technical infrastructure, raise public awareness, and intensify specialized training to effectively counter this growing threat.

Keywords:

Cybercrime – Criminal procedures – Digital evidence – Cybersecurity – International cooperation – Cyber investigation – Modern legislation