

الوقاية من الجرائم الالكترونية في ظل القانون رقم 04-09 يتضمن القواعد الخاصة للووقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

عبد الصديق شيخ ،

¹ جامعة يحي فارس بالمدينة-كلية الحقوق والعلوم السياسية المدية (الجزائر)، الإيميل abdelseddik@yahoo.fr

تاريخ النشر: 2020/06/15

تاريخ القبول: 2019/12/09

تاريخ الاستلام: 2019/09/09

ملخص:

أدى التطور الكبير في عالم تكنولوجيا المعلوماتية وأجهزة الاتصال واتساع استعمال الشبكة الانترنت إلى احتلالها مساحة واسعة في الحياة اليومية للمواطنين، لكن في المقابل ساهمت في بروز العديد من الجرائم المتصلة بها، التي أصبحت تشكل هاجسا حقيقيا للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الذي دفعها إلى العمل على إيجاد حلول سريعة لمكافحتها والحد من انتشارها، سواء من خلال إبرام اتفاقيات دولية أو سن تشريعات وطنية، ولأن أفراد قانون خاص للحد ومكافحة الجرائم الالكترونية بات اليوم أكثر من ضرورة، حاولت الجزائر استحداث آليات قانونية تسمح بالحد من انتشار هذه الجرائم، من خلال وضع منظومة قانونية متكاملة تركز أساسا على كل من قانوني العقوبات والإجراءات الجزائية، وتم تدعيمها بالقانون رقم 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

كلمات مفتاحية: الجرائم الالكترونية-آليات الوقاية-التفتيش-المراقبة

Abstract:

The enormous development in the world of information technology has greatly increased its role, and computers and the Internet have become indispensable, and multiple applications contributed to the emergence of many crimes, these crimes are a real concern for many countries as one of the most serious cross-border crimes, which In this context.

Algeria has worked to develop legal mechanisms to limit the spread, prevention and control of such crimes through the establishment of a system of law, of integrated mainly based on both legal sanctions and penal procedures, including rules for the prevention of crimes related to information and communication technologies and control.

Keywords: : information- technology- prevention- control

المؤلف المرسل: عبد الصديق شيخ، الإيميل abdelseddik@yahoo.fr

١ . مقدمة:

أدى التطور الهائل في عالم تكنولوجيا المعلوماتية ووسائل والاتصال إلى تعاظم دورها بشكل كبير في شتى مجالات الحياة، وأصبحت الحواسيب وشبكة الانترنت تحتل مساحة هامة في الحياة اليومية للمواطن، وبات يعتمد عليها بشكل شبه كلي في تسيير شؤونها اليومية، وتسيير مختلف المرافق الإدارية والعلمية والاقتصادية، الأمر الذي يتطلب توفير أقصى درجات الحماية لهذه الوسائل الحديثة وما يحيط بها، تجنباً لتعطيل سير تلك المرافق الحيوية أو الاعتداء عليها بما يؤثر على المصالح والخدمات التي باتت تقدمها في عالم اليوم .

رغم الإيجابيات والفوائد الكثيرة لهذا التطور في التكنولوجيات الحديثة، فلقد إلى بروز العديد من المشكلات والسلبيات التي ظهرت نتيجة الاستعمال الواسع للحواسيب ووسائل الاتصال المختلفة، أبرزها على الإطلاق الجرائم الالكترونية المقترفة من بعض مستخدمي هذه الوسائل الحديثة التي تتميز بخطورتها وسهولة استعمالها، وبذلك فقد ساهم الانتشار الواسع لتكنولوجيا المعلوماتية واتاحة استعمال التقنيات الحديثة دون ضوابط صارمة في ظهور هذه الجرائم ، وهي تعد من الجرائم الخطيرة التي يصعب اكتشافها ومكافحتها لاسيما بعد اتساع استعمال الأجهزة ومختلف الوسائط الالكترونية بشكل كبير وغير مسبوق.

لقد أصبحت هذه الجرائم تشكل هاجساً حقيقياً للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الذي دفعها إلى العمل بشكل جاد على مكافحتها، سواء من خلال إبرام اتفاقيات ثنائية أو وضع تشريعات وطنية للحد منها ومكافحتها .

كما أدى هذا التطور الذي عرفته تكنولوجيا المعلوماتية وتطبيقاتها المتعددة، إلى بروز مشاكل قانونية جديدة، تطلب حلها البحث في الأوضاع القانونية القائمة ومدى وملاءمتها لمواجهة هذه المشاكل، خاصة وأن القاضي الجزائي مقيد عند نظره في الدعوى العمومية بمبدأ الشرعية، فهو لا يستطيع أن يجرم أفعالا لم ينص عليها المشرع، حتى ولو كانت على درجة عالية من الخطورة الإجرامية.

لذلك فقد بات اليوم أفراد قانون خاص للحد ومكافحة الجرائم الالكترونية أكثر من ضروري، حيث حاول المشرع استحداث آليات قانونية تسمح بالحد من انتشار هذه الجرائم والوقاية منها ومكافحتها بشكل فعال، من خلال وضع منظومة قانونية متكاملة تركز أساسا على كل من قانوني العقوبات والإجراءات الجزائية، وتم تدعيمها بالقانون رقم 04-09 مؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تلاه صدور المرسوم الرئاسي رقم 261-15 مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث تم إرساء قواعد إجرائية جديدة تتضمن تحكما جيدا في أساليب مكافحة هذا النوع من الجرائم.

بناء على ما تقدم فإن هذه الدراسة تهدف إلى تقديم رؤية قانونية حول الجريمة الالكترونية، وكيف حاول المشرع الوقاية منها ومكافحتها من خلال إبراز أهم الآليات القانونية التي جاء بها القانون رقم 04-09 السالف الذكر في مجال الوقاية، حيث تم اتباع في ذلك كل من المنهج الوصفي والتحليلي المناسبين لطبيعة الموضوع الذي يعتمد على إظهار أهم الآليات التي جاءت في هذا القانون، والوقوف على مفهوم وأركان وخصائص الجريمة الالكترونية، وإبراز أهم الآليات التي أوجدها المشرع لمكافحتها والوقاية منها.

بناء على ما تقدم يتسنى لنا طرح الإشكالية التالية:

ما هي آليات الوقاية من الجرائم الالكترونية في ظل القانون رقم 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؟ وكيف يمكن أن تساهم هذه الآليات في مكافحتها والوقاية منها؟

سنتناول دراسة هذا الموضوع من خلال محورين اثنين وهما:

المحور الأول: مفهوم الجرائم الالكترونية

المحور الثاني: آليات الوقاية من الجرائم الالكترونية

المحور الأول: مفهوم الجريمة الالكترونية

وجد الفقه صعوبة كبيرة في إيجاد تعريف دقيق للجريمة الإلكترونية بسبب حداثها وسرعة وتيرة تطور تكنولوجيا المعلوماتية ووسائل الاتصال، وتباين الدور الذي تؤديه في الجريمة، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة ووسيلة لارتكابها تارة أخرى.

كما أن حداثة الجرائم الالكترونية واختلاف الثقافات والنظم القانونية بين الدول صعب من إيجاد مصطلح موحد للدلالة عليها، وهو ما أدى إلى عدم وضع تعريف موحد لهذه الظاهرة الإجرامية¹، حيث يتم استعمال العديد من المصطلحات والعبارات للتعبير أحيانا على نفس الجريمة كالجريمة المعلوماتية والجريمة المتصلة بوسائل الإعلام والاتصال.

أولاً: تعريف الجريمة الالكترونية

تعددت آراء الفقهاء بشأن تعريف الجريمة الإلكترونية، وكل رأي تبني مفهوماً بالنظر إلى الزاوية التي ينظر منها، فهناك جانب من الفقه عرفها من زاوية فنية، وأخرى قانونية، وهناك جانب آخر حاول تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استناداً لمعايير مختلفة.

1-التعريف الفقهي:

قدم الفقه العديد من التعاريف للجريمة الإلكترونية، من بينها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"²، وفي تعريف آخر بأنها " كل فعل غير مشروع يؤدي فيه جهاز الحاسوب دوراً مهماً لإتمام السلوك غير المشروع على أن يكون هذا الأداء أو الدور مؤثراً ومؤدياً إلى ارتكاب الجريمة"³، كما عرفت بأنها " كل أشكال السلوك أو الفعل غير المشروع والذي يرتكب بواسطة جهاز الحاسوب"⁴.

2-التعريف التشريعي:

استعمل المشرع للدلالة على الجريمة الإلكترونية عبارة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال⁵، وعرفها في المادة الثانية من القانون رقم 04-09 السالف الذكر، بأنها " يقصد في مفهوم هذا القانون بما يأتي:

أ-الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

إن ما يمكن ملاحظته على التعريف الذي جاء في المادة الثانية أعلاه، أنه واسع وغير دقيق ولا يتضمن جميع العناصر التي تتميز بها الجرائم الإلكترونية، وإن كان المشرع قد اعتمد على البعض منها للدلالة على الجريمة الالكترونية، منها وسيلة الجريمة المتمثلة في نظام الاتصالات الالكترونية، ومعيار موضوع الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات.

لذلك ومما تقد من تعريفات، يمكن القول بأن الجريمة الالكترونية هي عبارة عن أفعال غير مشروعة تهدف إلى تحقيق مكاسب مختلفة، يكون الحاسوب ومختلف وسائل الاتصال والأجهزة الالكترونية الحديثة والمتطورة محال لها أو وسيلة لارتكابها.

ثانيا: خصائص الجريمة الالكترونية

تعتبر الجرائم الإلكترونية جرائم حديثة إذ أنها لم تظهر إلا بعد اتساع التغطية بشبكة الانترنت والانتشار الواسع للحواسيب والوسائط الالكترونية ومختلف وسائل الاتصال الحديثة لا سيما الهواتف النقالة، لذلك فهي تنفرد بخصائص لا نجدها في غيرها من الجرائم وتميزها عن الجرائم التقليدية، ومنها:

1-يتطلب ارتكاب الجريمة الالكترونية وجود جهاز الكتروني والتحكم بتقنية استخدامه:

تتميز الجرائم الالكترونية عن غيرها من الجرائم بأنها تعتمد أساسا على جهاز الكتروني متطور يشكل أداة الجريمة ووسيلة تنفيذها، فبدون هذا الجهاز تنتفي الجريمة الالكترونية، كما أنها تتطلب تكوين وتحكم ودراية كافية بتكنولوجيا المعلوماتية وخاصة الانترنت، حيث أن أغلب الجرائم الالكترونية تتم عبر هذه الشبكة⁶، كما لا يتصور ارتكابها دون استخدام التقنية المعلوماتية لأن هذه الأخيرة تشكل عنصراً من عناصرها، مثل الاختراق وتدمير الشبكات وتحريف البيانات أو التلاعب بها وإساءة استخدام المعلومات المتحصل عليها.

كما أنه إذا كانت الجرائم الإلكترونية تتشابه مع الجرائم التقليدية في استخدام الجناة لوسائل غير مشروعة لارتكاب جرائمهم، فإنها تتميز كذلك بارتكابها من طرف مجرمين على قدر كبير من الذكاء والمهارة والمعرفة الدقيقة بالتقنيات الحديثة لأحدث تكنولوجيات الاتصال، والتي يتم استخدامها بصورة سيئة من طرفهم.

لذلك فإن الجرائم الإلكترونية تتطلب توفر تكوين علمي وفني عالي المستوى، ودراية تامة بالجوانب التقنية والفنية لاستخدام الحاسوب والانترنت ومختلف أجهزة الاتصال الحديثة، حيث أنه كلما زادت الخبرة والتكوين في هذه المجالات كلما ازدادت صعوبة اكتشاف هذه الجرائم.

لقد أكد الواقع العملي أن أغلب الجرائم الإلكترونية أصبحت ترتكب عن طريق الهواتف النقالة، لاسيما منها الهواتف الذكية المزودة بتكنولوجيات فائقة الجودة، وهي في الحقيقة عبارة عن أجهزة حاسوب صغيرة موصولة بشبكة الانترنت، يتم تخزين ونقل المعلومات فيها بكل سهولة وبسرعة فائقة، بل أنه أحيانا تتفوق الهواتف الذكية على أجهزة الحاسوب حيث تسمح بالاتصال والتواصل مع الغير خلافا لأجهزة الحاسوب.

كما لا بد من الإشارة بأن موضوع الاعتداء يتمثل بشكل أساسي في البيانات والمعطيات المخزنة في الحواسيب والهواتف الذكية ومختلف الوسائط الإلكترونية، والتي يمكن نقلها وتخزينها من جهاز لآخر، مما يجعلها عرضة للسرقة والاتلاف بكل سهولة، الأمر الذي يتطلب سرعة تدخل المشرع ولتوفير حماية قانونية فعالة لها⁷.

2- تعد الجرائم الإلكترونية جرائم عابرة للحدود:

أدى التطور التكنولوجي في مجال المعلوماتية والاتصالات وتزايد الاعتماد على الأقمار الصناعية وشبكات المعلومات الدولية، إلى تزايد التواصل والارتباط بين الدول، إذ يكاد يشكل العالم اليوم مجتمعا واحدا، حيث الانتشار السريع للمعلومات وسهولة انتقال الأموال والأشخاص، الأمر الذي يسر تحرير التجارة الدولية وإزالة الحواجز الجمركية، وأصبحت الحدود الاقتصادية مفتوحة أمام تدفقات رؤوس الأموال والاستثمارات الدولية، وتمدد الشركات متعددة الجنسيات، وهي ظروف هيأت مناخاً مشجعاً لارتكاب الجريمة المنظمة عبر الحدود، يتم التخطيط لها وتنفيذها من طرف جماعة إجرامية منظمة تمارس أنشطتها الإجرامية في أكثر من دولة.

لقد استطاعت شبكة الانترنت إزالة كل الحدود الجغرافية بين الدول بعد أن أصبحت متاحة لجميع الأشخاص سواء طبيعيين أو معنويين، وجعلت العالم عبارة عن قرية صغيرة، وأصبح التواصل بين أفرادها لا يكلف سوى شراء حواسيب وأجهزة اتصال متطورة ووصلها بهذه الشبكة، لكن في مقابل ذلك أصبحت الجريمة الالكترونية، جريمة عابرة للحدود.⁸

كما أن انتشار الوسائل التكنولوجية الحديثة وشيوع استخدامها بين أفراد المجتمع والتوسع في التعامل من خلالها، أعطى لدى كل فرد القدرة على التفاعل والتواصل دون أي مانع إقليمي أو جغرافي، مع توافر القدرة على نقل وتلقي كم هائل من المعلومات والمعطيات والولوج والاطلاع على البيانات والبرامج بكل سهولة ويسر.

لذلك فإن الجرائم الإلكترونية تعد من الجرائم غير المرتبطة بمنطقة جغرافية معينة، فقد ترتكب في أي وقت وهي غير مقيدة بدولة معينة، حيث يتم ارتكابها باستعمال مختلف الأجهزة الإلكترونية وعلى رأسها جهاز الحاسوب باستعمال شبكة الأنترنت⁹، ومما زاد في تعقيدها وصعوبتها أنه يتم التخطيط لها في دولة معينة ويتم تنفيذها في دولة أخرى، وغالبا ما يكون الجاني أو المجني عليه في دولة ثانية وقد يقع الضرر في دولة ثالثة، كحالة اختراق واتلاف مواقع الانترنت لاسيما السرية منها أو حالة سرقة البيانات والمعلومات وحتى الأموال، مما يجعل مكافحة هذه الجريمة بالوسائل التقليدية أمرا في غاية الصعوبة، لتعدد الأماكن التي تتعلق بالجريمة وتنازع قوانين الدول الواجبة التطبيق، واختلاف الإجراءات الجزائية من دولة لأخرى وصعوبة ملاحقة الجناة، الأمر الذي يتطلب تعاون دولي نشيط للقبض على الجناة وتقديمهم للجهات القضائية المختصة بالنظر والفصل في النزاع¹⁰.

3-صعوبة إثبات الجرائم الإلكترونية:

تمتاز الجرائم الإلكترونية كذلك بصعوبة اثباتها، وصعوبة إيجاد الدليل الذي يدين مرتكب الجريمة، حيث يسهل محو الأدلة والتلاعب فيها، لأنها لا تترك أثارا خارجية مادية ملموسة، ومما زاد من صعوبة اكتشافها البعد الجغرافي بين الجاني والمجني عليه، واستخدام الجاني في جريمته لوسائل تقنية وفنية حديثة.

كما أنه ومما يزيد من صعوبة إثبات واكتشاف الجرائم الإلكترونية، أنها ترتكب في وقت سريع جدا قد لا يتعدى بضعة ثواني، ويمكن محو آثارها بكل سهولة ويسر نتيجة التطور الرهيب في الحواسيب ومختلف أجهزة ووسائل الاتصال، وقد يلجأ المجرمون في أحيان كثيرة إلى استئجار قراصنة متخصصين لسرقة بيانات ومعلومات هامة وبيعها لمن يطلب الاستفادة منها، ويضاف إلى ذلك ضعف تكوين وخبرة عناصر الضبطية القضائية في مجال المعلوماتية وتكنولوجيات الاتصال، وافتقارهم للأجهزة التقنية المتطورة في متابعة الجرائم الإلكترونية وضبط أدلتها، وهو ما انعكس سلبا على مجريات التحريات والتحقيقات التي يباشرونها عند اكتشافهم لوقوع الجريمة الإلكترونية، وصعب عليهم انجاز مهامهم بالفعالية اللازمة والمطلوبة في هذا النوع من الجرائم.

إضافة إلى نقص الوسائل والأجهزة الحديثة التي تعوق عمليات البحث والتحقيق في الجرائم الإلكترونية، نسجل كذلك نقص الخبرة والكفاءة في المعرفة التقنية الحديثة والمتجددة لدى القائمين بالبحث والتحقيق في هذه الجرائم، مما يجعلهم غير قادرين على أداء مهامهم على أحسن ما يرام، وهو ما يعد من الأسباب الرئيسية في الإخفاق في كشف الجرائم الإلكترونية وجمع أدلتها، ويظهر ذلك بشكل واضح في الدول التي لا تزال تتعامل مع هذه الجرائم بإجراءات البحث والتحقيق التقليدية، وغالبا ما لا يقتنع القضاة بأدلة الاثبات التي يقدمونها بها.

لذلك يتعين على الدول وضع برامج تدريب وتأهيل لعناصر الضبطية القضائية على أساليب الوقاية من الجرائم الإلكترونية، لتسهيل أدائهم لمهامهم في التحري والبحث عن الجرائم المرتكبة والعمل على كشفها، وتفعيل التدابير المانعة لوقوعها وتوظيف وتدريب أشخاص مختصين ومؤهلين فنيا وتقنيا في مجال المعلوماتية وتكنولوجيات الاتصال، وتزويدهم بالإمكانات المادية والتقنية اللازمة، من أجهزة وبرامج حديثة تسمح لهم بمكافحة هذه الجرائم.

4- قلة الإبلاغ عن الجرائم الإلكترونية: يعتبر قلة الإبلاغ عن الجرائم الإلكترونية من الخصائص التي تزيد في صعوبة الكشف عنها، وهذا ما يفسر قلة القضايا التي تطرح على

القضاء مقارنة مع غيرها من الجرائم التقليدية، حيث غالبا ما يتم اكتشافها صدفة وبعد مدة طويلة من ارتكابها.

ذلك أن الجريمة الإلكترونية تقع في مجال المعالجة الآلية للمعلومات والبيانات وتستهدف أساسا المعنويات لا الماديات، وهي بالتالي أكثر صعوبة في الكشف والإثبات لأن مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه، وهذا ما يصعب من إجراءات اكتشاف هذه الجريمة ومعرفة مرتكبها، بخلاف الجريمة التقليدية التي عادة ما تترك وراءها دليلا ماديا أو شهادة شهود أو غيرها من أدلة الإثبات، كما أن موضوع التفتيش والضبط قد يتطلب أحيانا امتداده إلى أشخاص آخرين غير المشتبه فيهم أو المتهمين.

كما يرتبط قلة الإبلاغ عن هذه الجرائم أساسا بشخصية المجني عليه، إذ غالبا ما يحجم هذا الأخير عن طلب مساعدة الجهات القضائية المختصة في إثبات الجريمة والكشف عنها، خوفا من التداعيات النفسية والاجتماعية لاسيما عندما نكون أمام حالة ابتزاز والتهديد بنشر معلومات وصور خاصة بضحيا هذا الابتزاز.

المحور الثاني: آليات الوقاية من الجريمة الالكترونية

تثير الجرائم الالكترونية الكثير من المشكلات القانونية، بدءا من مرحلة التحريات والتحقيقات وجمع الأدلة حتى صدور الحكم القضائي، لاسيما فيما يتعلق بإثبات الجرائم المرتكبة عبر الإنترنت وصلاحيات الدليل الرقمي للإثبات ومدى شرعية الأدلة المتحصلة عليها بواسطة الأنترنت وقبولها لدى القاضي الفاصل في النزاع.

لذلك أوجد المشرع بموجب القانون رقم 04-09 السالف الذكر، العديد من الآليات للوقاية من الجرائم الالكترونية، وهي تتمثل أساسا في كل من الوقاية والتفتيش والحجز، على ألا تستعمل المعلومات المتحصلة عليها أثناء عملية المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، وهذا تحت طائلة العقوبات المنصوص عليها في ذات القانون¹¹.

أولاً: الرقابة

تعد الرقابة من أهم آليات الوقاية من الجرائم الإلكترونية، حيث يمكن مراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها عند الحالات التالية¹²:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، إذ يختص النائب العام لدى مجلس قضاء الجزائر، بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، إذنا لمدة ستة أشهر قابلة للتجديد، وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

- تكون الترتيبات التقنية الخاصة بهذه الحالة موجهة حصرياً لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها، وهذا تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

- عند توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

- عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، لمقتضيات التحريات والتحقيقات القضائية.

- عند تنفيذ طلبات المساعدة القضائية المتبادلة.

كما لا بد من الإشارة بأن المشرع قد منع إجراء عمليات المراقبة المنصوص عليها في المادة 4 من القانون رقم 04-09 السالف الذكر، إلا بإذن مكتوب من السلطة القضائية المختصة،

ثانياً: التفتيش

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق، يهدف إلى البحث عن الأدلة لإثبات وقوع جريمة ما في مكان معين، حيث أنه ونظراً لخطورته تشترط أغلب التشريعات الحصول على رخصة للتفتيش من الجهة القضائية المختصة¹³.

إذا كان الالتزام بقواعد التفتيش في الجرائم التقليدية لا يثير إشكالات كبيرة، فإن الأمر ليس كذلك بالنسبة للجرائم الإلكترونية، خاصة وأن نظم المعالجة الآلية تتكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات اتصال متطورة ومعقدة¹⁴. كما أن إجراء التفتيش في الجريمة الإلكترونية يحتاج إلى تقنيات ومهارات خاصة يختلف عن الجرائم التقليدية، فتفتيش الحواسيب وأجهزة الاتصال يتطلب دراية وتحكم دقيق في هذه الأجهزة وكيفية إخفاء المعلومات فيها، وهي عملية ليست بال بسيطة والسهلة وتتطلب وقت وجهد كبيرين، بل أحيانا لا بد من الاستعانة بالخبرات الفنية والتقنية المتخصصة سواء تعلق الأمر بتفتيش المكونات المادية والمعنوية للحاسوب أو تفتيش الشبكات المعلوماتية المتصلة بالحاسوب عن بعد، وكذلك مختلف وسائل الاتصال كالهواتف وغيرها من الأجهزة الإلكترونية.

لقد أجاز المشرع للسلطات القضائية ولضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وضمن حالات المراقبة المنصوص عليها في المادة 4 من القانون رقم 04-09 السالف الذكر، الدخول بغرض التفتيش ولو عن بعد في الحالتين التاليتين¹⁵: -تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها. -تفتيش منظومة تخزين معلوماتية.

بالنسبة للحالة الأولى، فإذا كانت هناك أسباب تدعو إلى الاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى يمكن الدخول إليها انطلاقا من المنظومة الأولى، فيجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام الجهة القضائية المختصة بذلك.

أما إذا تبين مسبقا، بأن المعطيات المبحوث عنها التي يمكن الدخول إليها انطلاقا من المنظومة الأولى، هي مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فيمكن الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

كما يمكن للسلطات المكلفة بالتفتيش، تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، بغرض مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها. وبذلك يكون المشرع قد أعطى للمحققين والمتحررين عن الجرائم الإلكترونية، وسائل هامة تسمح لهم بالتدخل بشكل فعال لتقديم الأدلة اللازمة لإدانة المتهمين.

ثالثاً: الحجز

يعتبر إجراء الحجز من أخطر وأهم آليات الوقاية من الجرائم الإلكترونية التي جاء بها القانون رقم 04-09 السالف الذكر، ويتم في حالتين رئيسيتين هما¹⁶:

1- حجز المعطيات المعلوماتية: أجاز المشرع للسلطة المكلفة بالقيام بعملية التفتيش في أي منظومة معلوماتية، حجز المعطيات المخزنة التي تكون مفيدة في الكشف عن الجرائم أو مرتكبها فقط، إذا كان ليس من الضروري حجز المنظومة بأكملها، وهذا بالقيام بما يلي:

- نسخ المعطيات محل البحث وكذا جميع المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية، تكون قابلة للحجز والوضع في أحراز وفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية.

- تسهر السلطة التي تقوم بعملية التفتيش والحجز على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

- يجوز للسلطة التي تتولى عملية التفتيش والحجز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل المعطيات محل البحث، لتصبح قابلة للاستغلال لأغراض التحقيق، شريطة ألا يؤدي ذلك إلى المساس بمحتوى هذه المعطيات.

2- الحجز عن طريق منع الوصول إلى المعطيات: يتم الحجز في هذه الحالة إذا استحال حجز المعطيات المعلوماتية لأسباب تقنية، وفي هذه الحالة يتعين على السلطة التي تتولى عملية التفتيش، استعمال التقنيات المناسبة للوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

كما يمكن للسلطة التي تباشر عملية التفتيش، أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، وهذا عن طريق تكليف أي شخص مؤهل لاستعمال الوسائل التقنية المناسبة لذلك¹⁷.

الخاتمة:

تبقى الحماية الفنية والتقنية مهما بلغت درجتها عاجزة عن التطور الرهيب الذي تشهده تقنيات اختراق الأجهزة الالكترونية لاسيما الحواسيب، وهو ما أدى إلى استفحال الجريمة الالكترونية وتسبب في أضرار مادية ومالية وحتى نفسية للعديد من الضحايا. تبين لنا من خلال هذه الدراسة مدى خطورة الجرائم الإلكترونية وصعوبة اكتشافها، حيث وقفت مختلف النظم القانونية عاجزة عن مكافحتها، نظرا للعدد الهائل من هذه الجرائم المتزايدة بشكل غير مسبوق.

كما أن الجهود الوطنية والدولية لمكافحة الجرائم الإلكترونية لا تزال في بداياتها الأولى، ولا ترقى إلى المستوى المطلوب، وأمام هذه الوضعية حاول المشرع الحد من هذه خطورة هذه الجرائم، من خلال إدراجه لتعديلات هامة على قانون العقوبات وقانون الإجراءات الجزائية، وسن القانون رقم 04-09 للوقاية ومكافحة هذه الجريمة.

ومن بين النتائج المتوصل إليها نجد ما يلي:

- تعد الجرائم الإلكترونية من الجرائم المستحدثة التي تعتمد على التقنية الحديثة والمتطورة، لذلك يتطلب مكافحتها الاعتماد على وسائل تقنية لا تقل حداثة عن الوسائل المستعملة في ارتكابها.
- تظهر خطورة الجرائم الإلكترونية في كونها جرائم عابرة للحدود وصعبة الاكتشاف والإثبات ويصعب فيها تحديد الاختصاص القضائي، نتيجة لكون شبكة الانترنت هي المجال الحيوي لارتكابها.
- ترتكب الجرائم الإلكترونية في عالم افتراضي غير ملموس ماديا لكن له وجود حقيقي، أهم خصائصه هي أنه غير مقيد بحدود زمنية ومكانية، وهو ما يتطلب ضرورة إعادة النظر في الكثير من القواعد والمسلمات القانونية مثل قواعد الاختصاص القضائي وغيره من المبادئ القانونية.

- رغم المحاولات الجديرة بالاحترام التي قام بها المشرع الجزائري إلا أنها تبقى غير كافية بسبب التطور الكبير في مختلف الأجهزة الإلكترونية.

أما فيما يخص الاقتراحات، فيمكن تقديم ما يلي:

- الإسراع في وضع آليات قانونية ردعية للوقاية ومكافحة انتشار الجرائم الإلكترونية.
- توفير الإمكانيات البشرية والمادية والتقنية الحديثة للمراكز والأجهزة المتخصصة في مكافحة الجرائم الإلكترونية.
- إدراج الجرائم الإلكترونية في المناهج التعليمية والتربوية في مختلف المستويات التعليمية، لزيادة الوعي الاجتماعي بخطورة هذه الجرائم.
- وضع برامج تأهيل لعناصر الضبطية القضائية ورجال الأمن المكلفين بعمليات البحث والتحري، حول كيفية التعامل مع الأدلة وضبطها، والاستعانة بذوي التخصصات الدقيقة من التقنيين والفنيين في أنظمة الحاسوب والإنترنت وشبكات الاتصال الأخرى.
- باعتبار أن الجرائم الإلكترونية تعد من الجرائم العابرة للحدود يتعين تكثيف التعاون الدولي، فهو السبيل الوحيد للحد من امتدادها وانتشارها.

التهميش

¹ أشرف عبد القادر قنديل، 2015، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ص 92.

² محمد أمين أحمد الشوابكة، 2004، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ص 7.

³ نائلة عادل محمد فريد، 2005، الجرائم المعلوماتية على شبكة الإنترنت، منشورات الحلبي الحقوقية، بيروت، ص 28 و 29.

⁴ يوسف حسن يوسف، 2011، الجرائم الدولية للإنترنت، المصدر القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، ص 13.

⁵ المادة الأولى من القانون رقم 04-09.

⁶ أنظر كل من:

- رامي متولي القاضي، 2011، مكافحة الجرائم المعلوماتية، دار النهضة العربية، الطبعة الأولى، القاهرة، ص 53.

- محمد الألفي، المواجهة الأمنية والتشريعية لجرائم الإرهاب عبر الإنترنت، المكتبة المصرية الحديثة، القاهرة، 2011، ص 82.

عنوان المقال.: الوقاية من الجرائم الالكترونية في ظل القانون رقم 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

- ⁷ خالد عياد الحلبي، 2011 إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان، ص 55.
- ⁸ خالد عياد الحلبي، المرجع السابق، ص 55.
- ⁹ لورنس سعيد الحوامدة، 2017، الجرائم المعلوماتية أركانها آليات مكافحتها دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانون، ص 9.
- ¹⁰ محمود أحمد عبابنة، 2009، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ص 35.
- ¹¹ المادة 9 من القانون رقم 04-09.
- ¹² المادة 3 من نفس القانون.
- ¹³ أنظر المواد من 44 إلى 47 من الأمر رقم 154-66 يتضمن قانون الإجراءات الجزائية، المعدل والمتمم.
- ¹⁴ عبد الفتاح بيومي حجازي، 2006، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ص 378.
- ¹⁵ المادة 5 من القانون رقم 04-09.
- ¹⁶ المادة 6 و 7 من نفس القانون.
- ¹⁷ المادة 8 من نفس القانون.

قائمة المراجع والمصادر:

-المؤلفات:

- أشرف عبد القادر قنديل، 2015، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية.
- محمد أمين أحمد الشوابكة، 2004، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان.
- نائلة عادل محمد فريد، 2005، الجرائم المعلوماتية على شبكة الانترنت، منشورات الحلبي الحقوقية، بيروت.
- رامي متولي القاضي، 2011، مكافحة الجرائم المعلوماتية، دار النهضة العربية، الطبعة الأولى، القاهرة.

- محمد محمد الألفي، 2011، المواجهة الأمنية والتشريعية لجرائم الإرهاب عبر الانترنت، المكتبة المصرية الحديثة، القاهرة.
- خالد عياد الحلبي، 2011، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011.
- محمود أحمد عبابنة، 2009، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان.
- عبد الفتاح بيومي حجازي، 2006، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية.
- يوسف حسن يوسف، 2011، الجرائم الدولية للإنترنت، المصدر القومي للإصدارات القانونية، الطبعة الأولى، القاهرة.
- المقالات:
- لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها آليات مكافحتها دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانون، 2017.
- النصوص القانونية:
- القانون رقم 04-09 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، صادر في الجريدة الرسمية العدد 47 بتاريخ 16 أوت 2009.
- النصوص التنظيمية:
- المرسوم الرئاسي رقم 15-261 مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، صادر في الجريدة الرسمية العدد 53 بتاريخ 8 أكتوبر 2015.