الآليات الإجرائية للكشف عن الجريمة المعلوماتية

Procedural mechanisms for detecting information crime

مجدوب نوال (*)
المركز الجامعي مغنية- الجزائر
doctrmedjdoub@gmail.com

تاريخ الاستلام: 2022/03/25 تاريخ القبول للنشر: 2022/11/09

****

ملخص:

كرس المشرع الجزائري جملة من الإجراءات التي من شأنها مساعدة جهات التحقيق في الكشف عن الجريمة المعلوماتية وإيجاد الدليل الرقمي الذي بموجبه يمكن متابعة مرتكب الجريمة، ومن ضمن الإجراءات نجد إجراء التفتيش كإجراء يخص الجرائم التقليدية، و يمكن تطبيقه على البيئة الرقمية مع مراعاة خصوصية هذه البيئة وطبيعتها.

بالإضافة إلى ذلك فقد استحدث المشرع إجراءات أخرى للكشف عن الجريمة المعلوماتية، ومن قبيل ذلك إجراء التسرب الإلكتروني والذي يقوم به ضباط الشرطة القضائية دعما لجهات التحقيق، بالإضافة إلى اعتراض المراسلات والمراقبة الإلكترونية، والحفظ والإفشاء العاجلان للمعطيات الإلكترونية، بالإضافة إلى إنتاج المعطيات المعلوماتية، وتجميع معطيات المرور بوقتها الفعلي.

الكلمات المفتاحية : الجريمة – المعلوماتية – البيئة الرقمية - الدليل الرقمي - التحقيق.

Abstract:

The Algerian legislature has devoted a set of procedures that will assist investigation authorities in uncovering information crime and creating digital evidence according to which the perpetrator of the crime can be followed up, and among the procedures we find the inspection procedure as a procedure for traditional crimes,

* مجدوب نوال .

and it can be applied to the digital environment, taking into account the privacy of this The environment and its nature.

In addition, the legislature has introduced other procedures to uncover information crime, such as the electronic leakage procedure that some judicial police officers perform in support of the investigation authorities, in addition to intercepting correspondence and electronic surveillance, and the urgent preservation and disclosure of electronic data, in addition to the production of data Informatics, and collecting traffic data in real time.

***Key words*:** crime - informatics - digital environment - digital evidence - investigation.

مقدّمة:

شهد العالم ثورة هائلة في مجال تقنية المعلومات، والتي أصبحت من أساسيات الحياة نظرا لإيجابياتها، إلا أن الاستخدام السلبي للمعلوماتية نجم عنه بروز إجرام جديد يرتبط بهذه البيئة ويصطلح عليه بالجريمة المعلوماتية.

وتختلف الجرائم المعلوماتية باختلاف استعمال الحاسوب، فقد يكون الحاسوب هدفا للإجرام المعلوماتي،و من صورها الهجمات الإلكترونية التي يرتكبها أفراد أو مجموعات على معرفة تقنية عالية.

في حين يتحول الحاسوب إلى أداة للإجرام المعلوماتي، ومن أبرز أمثلتها الاحتيال وسرقة الهوية، وحرب المعلومات، والتصيد، والبريد المزعج، ونشر المحتوى الفاحش أو المسيء مثل المضايقات والتهديدات، وكذلك تجارة المخدرات.

و عبر المشرع الجزائري على الجرائم المرتكبة عبر الإنترنيت (04/18، المؤرخ في 10 مايو 2018)، بتسمية " الجرائم المتصلة بتكنولوجيات الإعلام
والاتصال"، و التي عرفتها الفقرة أ من المادة رقم 02 من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام
والاتصال و مكافحتها (04/09، المؤرخ في 05 غشت 2009) على أنها" جرائم تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات،أو أي جريمة

أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصال الإلكتروني ".

ومن ثم و باعتبار أن الجريمة المعلوماتية ترتكب بالبيئة الرقمية فإن إجراءات الكشف عنها صعبة، مقارنة مع الجرائم التقليدية أو العادية، وهو الأمر الذي يتطلب تبني إجراءات توصل إلى الدليل الرقمي.

وبناءا على ما سبق فإن الإشكالية التي تدور حولها الدراسة تتجلى فيما يلي : هل تكفي الإجراءات المعتمد عليها في الجرائم العادية للوصول إلى الدليل الرقمي أم أن الأمر يتطلب إجراءات خاصة ؟.

ومن أجل الإجابة عن سالف الإشكال سيتم دراسة إجراء التفتيش والضبط كإجراء تقليدي (المبحث الأول)،مع الوقوف على الإجراءات الجزائية المستحدثة للكشف عن الجريمة المعلوماتية (المبحث الثاني).

المبحث الأول : التفتيش كإجراء تقليدي لضبط الدليل الرقمي

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

- تفتيش الكيانات المادية، ويشمل كل الكيانات المادية ذات الطابع المادي الملموس،و المرتبطة 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 (عربوز، 2019، صفحة 34).
  - التمييز بين ما إذا كانت مكونات الكمبيوتر المراد تفتيشها منعزلة عن غيرها من أجهزة الكمبيوتر، أو متصلة بمكان آخر.
- 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 (ليندا، جوان 2017، صفحة 490).

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).

المطلب الأول : أنواع التفتيش

باعتبار أن التفتيش من الإجراءات الجوهرية في عملية التحقيق، فقد حرصت جل التشريعات الإجرائية (442/20، 2020) على إحاطته بجملة من الضمانات القانونية لتفادي تعسف القائم به،

أو خرقه لحق الأفراد في الخصوصية، وعلى ذلك فضمانات التفتيش نوعان، إحداهما موضوعية (الفرع الأول)، و أخرى شكلية أو إجرائية (الفرع الثاني).

الفرع الأول : الشروط الموضوعية للتفتيش الإلكتروني

حتى يكون التفتيش صحيح يجب توافر ثلاثة شروط تتجلى في سبب التفتيش (أولا)، ومحل التفتيش (ثانيا)، والسلطة المختصة بالتفتيش(ثالثا)

أولا: سبب التفتيش

يعد عنصر السبب ضمانة قانونية لصحة و مشروعية إجراء التفتيش، و يتحقق هذا الأخير من خلال وقوع جريمة يتم بموجبها توجيه الاتهام إلى الشخص المراد تفتيشه،و ذلك بناءا على قرائن قوية تفيد تورطه بالجريمة.

ومن ثم يتحقق سبب التفتيش بالجريمة الإلكترونية بتوافر ثلاثة عناصر نلخصها في ما يلي :

- وقوع جريمة إلكترونية لها إما وصف الجناية أو الجنحة، و من ثم تستبعد المخالفات من دائرة التفتيش نظرا لعدم خطورتها (جمال، 2018/2017، صفحة 49).

وعلى ذلك فإن التفتيش لا يكون مشروعا إلا متى بني على أسباب جدية، تتجلى في الوقوع الفعلي للجريمة:

- اتهام شخص أو أكثر بمساهمته في إرتكاب الجريمة الإلكترونية، إما بوصفه فاعلا أصليا أو ثانويا،و بالتالي إذا لم يكشف قاضي التحقيق هوية المتهم بالشكوى، فإن ذلك كافي لحفظ ملف القضية، وإصدار أمر بأن لا وجه للمتابعة.
- توافر قرائن قوية توحي بوجود أدلة مادية تفيد في الكشف عن الجريمة،إذ لا يكفي وقوع جريمة بل يجب أن يستدل في التحقيق على قرائن قوية، تفيد أنه يوجد بالمجل المراد تفتيشه أجهزة أو أشياء أو مستندات إلكترونية تساعد في الكشف عن الجريمة (سلمى، صفحة 237).

ثانيا : محل التفتيش

يقصد بمحل التفتيش في البيئة الإلكترونية نظام الحاسب الآلي بكل مكوناته المادية أو المعنوية، أو شبكات الاتصال التي تشمل مكونات الحاسوب و مزود الإعلام الآلي، و الملحقات التقنية.

ثالثا : السلطة الخاصة بالتفتيش

باعتبار أن إجراء التفتيش سواء في الجريمة العادية أو في الجريمة الإلكترونية قد يمثل اعتداء على الحقوق والحريات، فقد خول القانون هذا الإجراء إلى جهات خاصة بالتحقيق.

إلا أنه و حرصا على سرعة اتخاذ أعمال التحقيق، وتسهيله

والاستفادة من خبرة رجال الضبطية القضائية أجاز المشرع لسلطة التحقيق تكليف أعوان الضبطية القضائية من أجل القيام بالتحقيق، مع إمكانية الاستعانة بأشخاص مؤهلين على النحو الذي نص عليه المشرع الجزائري بموجب المادة 49 من قانون الإجراءات الجزائية.

وبناءا على ما سبق فإنه يمكن لسلطة التحقيق إما القيام بالتحقيق بنفسها أو عن طريق الإنابة،و لها أيضا الاستعانة بخبير له دراية بالمجال المعلوماتي، وبالتدابير المتخذة لحماية المعطيات المعلوماتية (خليفة، ماي 2020، صفحة 33).

الفرع الثاني : الشروط الإجرائية و الشكلية

من أجل صحة إجراء التحقيق يتوجب مراعاة الضوابط الشكلية التالية:

أولا: احترام الميعاد الزمني لإجراء التفتيش

يقصد بالميعاد الزمني في التفتيش أن يتم إجراءه خلال الفترة الزمنية التي حددها المشرع،بهدف ضمان عدم الاعتداء على الجرية الفردية، وتضييق التعسف في استعمال السلطة.

وبذلك هو قيد زمني من أجل حماية الحقوق والحريات للأفراد، ويتوجب أن يكون التفتيش ما بين الساعة الخامسة صباحا إلى الثامنة مساءا (155/66، 08 جوان 1966)، ماعدا في الحالات الاستثنائية.

غير أنه يرد استثناء على القواعد العامة متى تعلق الأمر بالجريمة المعلوماتية،حيث يستبعد شرط الميعاد الزمني، وبالتالي يمكن لرجال الضبطية القضائية إجراء التفتيش في أي ساعة من الليل أو النهار (155/66، المتضمن قانون الإجراءات الجزائية).

ثانيا : وجود إذن بالتفتيش

يشترط وجود إذن سابق من وكيل الجمهورية متى تعلق الأمر بالتفتيش بالجرائم الإلكترونية، باعتبار أن التفتيش يمس خصوصية الأفراد من جهة، ومراعاة للطبيعة المستمرة لهذه الجريمة من حيث إمكانية ارتكابها في أي وقت من جهة أخرى، بالإضافة لكون أن أدلة الإثبات فيها سريعة و سهلة التلف و المحو (الصغير، 1988، صفحة 52).

ثالثا : أن يتم التفتيش بحضور المتهم

كقاعدة عامة يشترط أن يتم التفتيش بحضور المتهم، أو حضور من ينوب عليه، و ذلك بهدف تضييق نطاق الاعتداء على حرمة الحياة الخاصة للأفراد، و حرمة مساكنهم، تحت طائلة بطلان الإجراء.

إلا أن المشرع الجزائري خرج عن هذا الأصل عندما يتعلق الأمر بالتفتيش في الجرائم الإلكترونية، وذلك إقرارا منه بخصوصية جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، حيث أجاز لأعوان الضبطية القضائية إجراء التفتيش دون التقيد بشرط حضور المتهم، أو من ينوب عنه أو حتى الشهود.

وباعتبار أن التفتيش دخل ضمن أعمال التحقيق، فإنه يتوجب تحرير محضر يثبت ما أسفر عنه التفتيش، مع الإشارة أن المشرع لم يحدد شروط خاصة بمحضر التفتيش في البيئة الرقمية، مما يتطلب الرجوع للقواعد العامة أي المنصوص عليها في قانون الإجراءات الجزائية.

ويتجلى الفرق بين التفتيش في البيئة التقليدية والبيئة الرقمية في كون القائم بالتفتيش في الجرائم الإلكترونية هو شخص ملم بتقنية المعلوماتية، مع إمكانية استعانته بأهل الخبرة الفنية والاختصاص في هذا المجال من أجل مساعدته في صياغة المحضر وتغطية كل الجوانب الفنية للتفتيش (الغافري، 2009، صفحة 32).

المطلب الثاني :ضبط الأدلة في الجريمة الإلكترونية

يعد الضبط من إجراءات جمع الأدلة، فهو الأثر الذي تنتهي به عملية التفتيش، ويناط به وضع اليد على الأشياء والوسائل التي تم بموجبها إرتكاب الجريمة، والتي من شأنها تسهيل الكشف عن الحقيقة، ليتم بعدها وضعها المضبوطات في أحراز مختومة تقدم للقضاء كدليل إثبات (الحلبي، 2011، صفحة 169).

وقد تأخذ المضبوطات الصورة المادية في تلك الحالة التي يتعلق الأمر بعناصر مادية، ومن قبيل ذلك جهاز الحاسب الآلي وملحقاته، أو الأقراص الصلبة، أو الأشرطة الممغنطة، أو الطابعة، أو بطاقات الإئتمان، أو المعدات المستعملة في شبكة الإنترنيت مثل المودم .

كما قد تأخذ المضبوطات الصورة غير المادية أي المعنوية، مثل البرامج والبيانات المعالجة أليا، والمراسلات الإلكترونية، والدليل الموجود على مستوى البريد الإلكتروني (جمال، المرجع السابق، صفحة 46).

وبذلك إذا أسفر التحقيق على وجود دليل رقمي تم ضبطه فإن الإجراء المتخذ بعدها هو الحجز، كما عبر عنه المشرع الجزائري بموجب المادة 06 من القانون رقم 04/09 سابق الإشارة إليه،

والتي تنص 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 و الوضع في أحرار.

وفي كل الحالات يتوجب على السلطة التي تقوم بالتفتيش والحجز أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجرى بها العملية" (04/09 ا.، 2009).

مع الإشارة أنه في حالة استحال على السلطة القائمة بالتفتيش إجراء الحجز لأسباب تقنية، فإنه يتوجب عليها استعمال التقنيات المناسبة بهدف منع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها (04/09 ا.، 2009).

أما إن تعلق الأمر بمعطيات يشكل محتواها جريمة فإن القانون خول للسلطة التي تباشر التحقيق أن تتخذ أي إجراء لازم لمنع الإطلاع على هذه المعطيات (04/09 ا.).

ومن ثم فإنه سواء تعلق الأمر بمعطيات يشتبه فيها، أو بمحتوى يشكل جريمة فإنه يمتع تحت طائلة المسائلة الجنائية استعمال هذه المعطيات التي أسفر عنها التحقيق لأي غرض، ماعدا إن تعلق الأمر بالتحري أو التحقيق أو العمل القضائي ككل (04/06).

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 الماسة بأنظمة المعالجة الآلية للمعطيات (66/156، المؤرخ في 10 نوفمبر 2004) واحدة من الجرائم التي أجاز المشرع أن يتم الاعتماد فيها على إجراء التسرب من أجل التحري فيها وذلك بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية.

إذ عرف المشرع إجراء التسرب من خلال المادة 65 مكرر 12 من قانون الإجراءات الجزائية،على أنه " قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرط القضائية

المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

وبذلك فالتسرب هو إجراء أو تقنية تسمح لضباط الشرطة القضائية بالتوغل داخل جماعة إجرامية (أمينة، جوان 2019، صفحة 247)، و ذلك تحت مسؤولية ضباط الشرطة القضائية و بالتنسيق معهم.

ومن ثم يتم الانضمام إلى أشخاص مشتبه فيهم، من أجل الكشف عن نشاطهم الإجرامي وكسب ثقتهم مع إخفاء الهوية، وتقديم المتسرب نفسه على أنه شريك أو مساهم بالجريمة أو فاعل، وبذلك فهو من أخطر إجراءات التحقيق لما ينطوي عليه من خطورة على المتسرب (وردة، جوان 2017، صفحة 543).

ونشير في هذا السياق إلى أن المشرع الجزائري عبر على التسرب بالاختراق بموجب المادة 56 من القانون رقم 01/06 المتعلق بالوقاية من الفساد ومكافحته (06/01، المؤرخ في 20 فبراير 2006)، والتي تنص على أنه

" من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها بهذا القانون يمكن اللجوء إلى التسليم المراقب، وإتباع أساليب تحري خاصة، كالترصد الإلكتروني أو الاختراق على النحو المناسب، وبموجب إذن من السلطات المختصة ".

وكضمانة للمتسرب و بهدف حمايته وعائلته من مخاطر التعدي عليه، نصت المادة 65 مكرر من قانون الإجراءات الجزائية على أنه " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية اللذين يباشرون عملية التسرب تحت هيئة مستعارة في أي مرحلة من مراحل الإجراء " (06/22، المؤرخ في 20 ديسمبر 2006).

وحدد المشرع جملة من الضوابط الموضوعية (الفرع الأول) والإجرائية (الفرع الثاني) يستوجب مراعاتها من أجل القيام بإجراء، كالتالي :

الفرع الأول : الشروط الموضوعية لإجراء التسرب

هناك شرطين موضوعيين لإجراء التسرب نلخصهما فيما يلي :

أولا: عنصر التسبيب

يعد عنصر التسبيب ضمانة هامة كونه تتضح من خلاله الأسباب المبررة التي دفعت بوكيل الجمهورية لإصدار الأمر بإجراء التسرب، وذلك تحت طائلة بطلان الإذن وكل الإجراءات، أي أن مفاده تبيان المبررات وكذلك الحجج التي بموجبها منحت الجهة القضائية الإذن بالتسرب لضباط الشرطة القضائية.

ثانيا: تحديد نوع الجريمة

إذ يتوجب تبيان نوع الجريمة التي بموجبها تم طلب إجراء التسرب بهدف التحقيق فيها، مع ضرورة أن تكون هذه الجرائم من ضمن الجرائم الخطيرة، والمحددة على سبيل الحصر بموجب المادة 65 مكرر 05 سابق الإشارة إليها.

الفرع الثاني: الشروط الإجرائية لإجراء التسرب

وتتجلى الشروط الإجرائية لإجراء التسرب كوسيلة للكشف عن الجريمة المعلوماتية في مايلي :

أولا: الإذن القضائي

لا يجوز للعون القضائي مباشرة التسريب تلقائيا وبمحض إرادته، لأن ذلك مرهون على طلب الإذن المسبق من طرف وكيل الجمهورية قبل افتتاح التحقيق،باعتباره المكلف قانونا بإدارة نشاط الضبطية القضائية،

وممثلا للنيابة العامة (عمارة، جوان 2010، صفحة 248).

و تبقى العملية تحت الرقابة المباشرة للجهة المصدرة للإذن، وذلك من أجل الحد من التعسف في استعمال الحق في التسرب الإلكتروني.

ويشترط أن يكون الإذن مكتوبا و ليس شفويا (أمينة، المرجع السابق، صفحة 252)،و إلا عد إجراء التسرب باطلا، من منطلق أن العمل الإجرائي يجب أن يكون مكتوبا تحت طائلة البطلان، مع احتوائه لجملة البيانات المطلوبة، ومن ذلك تحديد نوع الجريمة المتخذ بشأنها التسريب، وكذلك اسم ضابط الشرطة القضائية الذي قامت العملية تحت مسؤوليته (نجيمي، 2011، صفحة 452).

ثانيا: تحديد مدة التسرب

إذ يتوجب أن يكون إجراء التسرب محدد بفترة زمنية، غير أنه إذا تقرر وقف العملية أو انقضت المهلة المحددة في الرخصة للتسرب، و لم يتم تمديدها يمكن للعون المتسرب مواصلة النشاطات للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف آمنة دون أن يكون مسؤولا جنائيا، على أن لا يتجاوز ذلك 04 أشهر (17).

وما تجدر الإشارة إليه هو أنه وبموجب المادة 26 من القانون رقم 05/20 المؤرخ في 28 أبريل 2020، والمتعلق بالوقاية من التمييز وخطاب الكراهية أجاز المشرع الجزائري لضباط الشرطة القضائية استعمال إجراء التسرب من أجل الكشف عن مرتكبي جرائم التمييز وخطاب الكراهية، وذلك عن طريق إيهامهم أنه فاعل معهم أو شريك لهم، وهو ما يعتبر من الصلاحيات المستحدثة للضبطية القضائية (20/05، المؤرخ في 28 أبريل 2020).

المطلب الثاني : اعتراض المراسلات و المراقبة الإلكترونية

إن دراسة عملية اعتراض المراسلات كآلية للكشف عن الجريمة المعلوماتية تتطلب بالضرورة تحديد مفهوم اعتراض المراسلات والمراقبة الإلكترونية (الفرع الأول)، بالإضافة إلى الوقوف على المراسلات التي يمكن أن تكون محلا لإجراء الاعتراض (الفرع الثاني)، مع تحديد الشروط الموضوعية والشكلية المتطلبة قانونا من أجل تبني عملية اعتراض المراسلات (الفرع الثالث).

الفرع الأول :مفهوم عملية اعتراض المراسلات

يناط باعتراض المراسلات، تلك العملية التي تسمح بمراقبة سرية المراسلات السلكية و اللاسلكية في إطار البحث و التحري عن الجريمة، وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في إرتكاب الجريمة.

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 (2000/03، 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 (ناجية، صفحة 293)[35]، من أجل استعمالها كدليل لمواجهته.

كما تعد المراسلات عبر البريد الإلكتروني مجالا خصبا للربط و الاتصال الإلكتروني (18/04) بين الأشخاص في مختلف أنحاء العالم وبوقت قياسي، ومن ثم يمكن إخضاعها لعلمية الاعتراض والمراقبة للكشف عن الجرائم الإلكترونية (18/04 ا.).

الفرع الثاني : 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.

مع الإشارة أن المشرع الجزائري لم يتبنى إجراء مراقبة الاتصالات الإلكترونية كإجراء للتحقيق القضائي،و كذلك التحري بموجب القانون رقم 04/09، 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 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها (09/04).

وبالتالي هي عبارة عن هيئة أو سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي ومقرها بالجزائر العاصمة، تم تحديد تشكيلتهاوعملها بموجب المرسوم الرئاسي رقم 261/15 (15/261، المؤرخ في 08 اكتوبر 2015).

الفرع الثالث : 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 (20/442، المؤرخ في 30 ديسمبر 2020)، 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 مع تحديد مدة الاعتراض والتي لا تتجاوز 04 أشهر قابلة للتجديد.

- التسبيب، أي تبيان دواعي اللجوء إلى الاعتراض و مراقبة المراسلات، و تبيان مدى جدية تلك الدواعي ودورها إظهار الجريمة والجناة.
- تحديد الجرائم محل الاعتراض والمراقبة و التي يتوجب أن لا تخرج عن ما هو مقرر قانونا، مع مراعاة سرية الإجراءات وكتمان السر المهني.

المطلب الثالث : الكشف عن الجريمة المعلوماتية عن طريق المعطيات

تلعب المعطيات دورا هاما في الكشف عن الجريمة المعلوماتية، ويتم الاستفادة منها إما عن طريق الحفظ و الإفشاء العاجلان(الفرع الأول)،أو عن طريق تجميعها بوقتها الفعلي (الفرع الثاني).

الفرع الأول :الحفظ و الإفشاء العاجلان للمعطيات الإلكترونية

يعد الحفظ و الإفشاء من الإجراءات المستحدثة للكشف عن الجريمة المعلوماتية والوصول إلى الدليل الرقمي، ونصت عليهما المادة 10 من القانون 04/09 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام و الاتصال
ومكافحتهما (09/04 ا.).

ومن ثم فإنه يقوم بهذا الإجراء مقدمي خدمات الإنترنيت، أين يقومون بالحفظ عن طريق الحيازة بالأرشيف بهدف حماية المعطيات التي سبق وجودها في شكل مخزن، مما يحول دون تلفها أو تجرديها من صفتها أو حتى حالتها الأصلية وفق النماذج التي تراها ملائمة لوضع عملية الحفظ وموقع التنفيذ.

ومن ثم هناك نوع من المعطيات يمكن أن تكون محل تحفظ،مع مراعاة جملة من الضوابط يتم التطرق إليها في ما يلي.

أولا : المعطيات محل التحفظ

حددت المادة 11 من القانون رقم 04/09 سابق الإشارة إليه، معطيات المرور التي يتعين على مقدم الخدمات التحفظ عليها بناءا على طلب من السلطات القضائية المختصة، والتي تتجسد في مايلي :

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات المستعملة بالاتصال، ومن ذلك الإشارة إلى الرقم التسلسلي للجهاز و كذلك نوعه و طرق تشغيله.

- المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم، ومن ذلك أرقام الهواتف أو عناوينهم.
- الخصائص التقنية و كذلك تاريخ و وقت و مدة الاتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المعلومة المستعملة و مقدميها.

ثانيا : الضوابط الواجب مراعاتها خلال عملية حفظ المعطيات

نظرا لكون عملية حفظ معطيات تمس الحق في الخصوصية، فقد حدد المشرع الجزائري ضوابط يتوجب على مقدم خدمة الانترنيت التقيد بها كالتالي :

- احترام المدة الزمنية المقررة لعملية الحفظ،و التي حددها المشرع الجزائري بموجب المادة 11 من القانون 04/09 بسنة واحدة، إبتداءا من تاريخ التسجيل، و بعد انقضاء المدة المقررة للحفظ يتوجب على مزود الخدمة السحب الفوري للمعطيات المخزنة من خلال اتخاذ التدابير التي تفيد عدم إمكانية الإطلاع عليها (09/04 ا.، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).
- مراعاة سرية عملية التحفظ، إذ يلتزم مقدمو الخدمات بالحفاظ على سرية كل الإجراءات،و التدابير التي تفرضها العملية طيلة الفترة المقررة، وتبقى الحكمة من هذا الالتزام هي مراعاة الحق في الخصوصية و تفادي تغيير البيانات أو محوها من طرف أشخاص.
- الإفشاء العاجل لمعطيات السير على النحو المنصوص عليه بموجب المادة 10 من القانون 04/09.

ونشير في هذا السياق إلى عملية أخرى فعالة في التحقيق والكشف عن الجريمة المعلوماتية والمتجسدة في إنتاج البيانات المعلوماتية فهو إجراء حديث يتماشى وطابع الدليل المعلوماتي (ناجية، المرجع السابق، صفحة 294).

إلا أن المشرع الجزائري لم ينص على هذا الإجراء كإجراء يمكن الاعتماد عليه في سبيل التحري، و هو ما يتطلب معه و على وجه الضرورة أن يتدارك المشرع الجزائري هذا السهو.

الفرع الثاني : تجميع معطيات المرور بوقتها الفعلي

يتم جمع المعلومات المساعدة في عملية التحري من طرف مقدم خدمة الانترنيت، و يعرف هذا الأخير على أنه "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة

منظومة معلوماتية أو نظام للاتصالات، أو هو أي كيان يقوم بمعالجة أو تخزين معطيات لفائدة خدمة الاتصال (09/04 ا.).

و بالتالي فإنه يقع على عاتق مقدم خدمة الانترنيت (09-04) التعاون مع جهات البحث والتحري بهدف الوصول إلى الدليل الرقمي وذلك من خلال قيامه بمايلي :

- حفظ المعطيات التي تسمح بالتعرف على مستعمل الخدمة، و كذلك الخصائص التقنية ومدة الاتصال، بالإضافة إلى المعطيات التي تسمح بالتعرف على المرسل إليهم و عناوينهم المواقع التي تم الإطلاع عليها (09/04 ا.).

- مراعاة أن يكون حفظ المعطيات لمدة سنة واحدة إبتداءا من تاريخ التسجيل، و تقديمها لجهات التحقيق فور طلبها.
- التدخل الفوري لسحب المحتويات التي يسهل الإطلاع عليها بمجرد علمهم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين،مع تخزينها أو جعل الدخول غليها غير ممكن.
- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة،أو إخبار المشتركين لديهم بوجودها.

ونشير في هذا السياق أن امتناع مقدم خدمات الإنترنيت على التعاون مع السلطات، من شأنه تعريضه للعقوبة الإدارية وللمسائلة الجنائية (09/04 ا.، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

ومع بروز القانون 05/20 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والذي يصبو لوضع حد لكل تمييز و خطاب كراهية بغض النظر عن الوسيلة المستعملة سواء كانت تقليدية أو إلكترونية، نجد أن المشرع الجزائري وبموجب 21 منه أجاز للجهات القضائية المختصة بمناسبة التحقيق في هذه الجرائم أن تأمر مقدمي خدمات الانترنيت أو أي شخص آخر بتسليمها المعلومات والمعطيات المخزنة باستعمال وسائل تكنولوجيات الإعلام والاتصال.

كما يمكنها إصدار أمر إلى مقدمي خدمات الإنترنيت بالتحفظ الفوري للمعطيات المرتبطة بهذا النوع من الجرائم نظرا لخطورتها (20/05 ا.).

خاتمة:

إن موضوع إجراءات الكشف عن الجريمة المعلوماتية من المواضيع التي فرضت نفسها، وذلك راجع لصعوبة الوصول إلى الدليل الرقمي وطبيعته الرقمية غير الملموسة.

وبالتالي كفل المشرع الجزائري طريقتين للوصول إلى الدليل الرقمي، إحداهما تتم عن طريق تبني الإجراءات التقليدية، والأخرى عن طريق إجراءات مستحدثة.

إذ كرس المشرع التفتيش كإجراء تقليدي للكشف عن الجريمة المعلوماتية، ورغم أهمية هذا الإجراء متى تعلق الأمر بالمكونات المادية للحاسوب، كونه قد يؤدي إلى الدليل الرقمي ومن ثم ضبطه، إلا أنه متى تعلق الأمر بالعناصر المعنوية للحاسوب كالبرامج و غيرها فإن دوره محدود.

وبالتالي فقد استحدث المشرع الجزائري إجراءات جزائية أكثر راهنية للكشف عن الجريمة المعلوماتية، ويندرج فيها كل من إجراء التسرب الإلكتروني، واعتراض المراسلات والمراقبة الإلكترونية،ناهيك عن الحفظ والإفشاء العاجلان للمعطيات الإلكترونية،بالإضافة إلى إنتاج المعطيات المعلوماتية، و تجميع معطيات المرور بوقتها الفعلي.

ورغم أهمية هذه الإجراءات ونجاعتها في الكشف عن الجريمة المعلوماتية، والوصول إلى مرحلة ضبط الدليل الرقمي،إلا أن التجربة التشريعية الجزائرية في مجال الجريمة المعلوماتية لا تزال فتية، ويتطلب الأمر عصرنة النصوص القانونية حتى تواكب ثورة الرقمنة.

وبناءا على ما سبق طرح بعض الاقتراحات على النحو التالي:

- من الضروري تكريس آليات وميكانيزمات أكثر عصرنة، من شأنها الكشف عن الجريمة المعلوماتية.
- من الضروري تفعيل دور أجهزة الوقاية من الجرائم المعلوماتية على أرض الواقع.

من الضروري تبني إجراء مراقبة الاتصالات الإلكترونية كإجراء للتحقيق القضائي.

الهوامش:

النصوص القانونية:

1- الأوامر التشريعية:

- الأمر رقم 155/66، المؤرخ في 08جوان 1966، المتضمن قانون الإجراءات الجزائية المعدل و المتمم.

2- القوانين :

- القانون قم 15/04 المعدل للأمر 156/66 المتضمن قانون العقوبات، المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية للجمهورية الجزائرية، العدد 71.

- القانون رقم 01/06، المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد .14، الصادرة في 08 مارس 2006.
- القانون رقم 09 /04 المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد .47، الصادرة في 16 غشت 2009 .
- القانون رقم 04/18 المؤرخ في 10 مايو 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 27، الصادرة بتاريخ 13 مايو 2018.
- القانون رقم 05/20، المتعلق بالوقاية من التمييز و خطاب الكراهية، المؤرخ في 28 أبريل 2020، الجريدة الرسمية للجمهورية الجزائرية، العدد .25، الصادرة في 29 أبريل 2020 .

3- المراسيم الرئاسية :

- المرسوم الرئاسي رقم 15/ 206، المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات تسيير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية، العدد .53، الصادرة في 18 أكتوبر 2015.
- المرسوم الرئاسي رقم 261/15، المؤرخ في 08 أكتوبر 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 53، الصادرة في 08 أكتوبر 2015.

- المرسوم الرئاسي رقم 442/20، المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء 01 نوفمبر 2020، الجريدة الرسمية للجمهورية الجزائرية، العدد. 82، الصادرة في 30 ديسمبر 2020.

الكتب والمؤلفات:

- جميل عبد الباقي الصغير، 1998، الجوانب الإجرائية للجرائم المتعلقة بالإنترنيت، دار النهضة العربية، القاهرة.
- جمال نجيمي، 2011، إثبات الجريمة على ضوء الإجتهاد (دراسة مقارنة)، دار هومة، الجزائر.

- حسين سعيد الغافري، 2009، السياسة الجنائية في مواجهة جرائم الانترنيت-دراسة مقارنة-، دار النهضة العربية، القاهرة.

- خالد عياد الحلبي، 2011، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، دار الثقافة للنشر والتوزيع، عمان

البحوث والمقالات:

- بن خليفة إلهام، 2020، التفتيش كإجراء تحقيق تقليدي لجمه الأدلة المتصلة بتكنولوجيات الإعلام و الإتصال، مقال منشور بالمجلة الدولية للبحوث القانونية والسياسية، المجلد.04، العدد.01.

- شيخ ناجية،2017، أساليب البحث والتحري المتخذة في القانون رقم 22/06، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري ، المجلة النقدية.

- شرف الدين وردة، 2017، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري، مقال منشور بمجلة المفكر،العدد 15.

- عربوز فاطمة الزهراء، 2019، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مقال منشور في مجلة جيل الأبحاث القانونية المعمقة، العدد.34.

- فدوي عمارة، 2010، إعتراض المراسلات وتسجيل الأصوات كإجراء قضائي في المواد الجنائية، مقال منشور بمجلة العلوم الإنسانية، العدد 33.

- بن طالب ليندا، 2017، التفتيش في الجريمة المعلوماتية، مقال منشور بمجلة العلوم القانونية والسياسية، العدد 16.

- مانع سلمى، التفتيش كإجراء للتحقيق في الجريمة المعلوماتية، مقال منشور في مجلة العلوم الإنسانية، العدد 21.

- معزيز أمينة، 2019، التسرب في قانون الإجراءات الجزائية الجزائري، مقال منشور في مجلة القانون و المجتمع، العدد 11.

- نوال مجدوب، 10 و 11 ابريل 2017، المسؤولية الجنائية عن الجريمة السبيرانية، مداخلة مقدمة بالملتقى الدولي حول الإجرام السبيراني، المنظم من طرف جامعة برج بوعريريج، الجزائر.