

التحديات القانونية لاثبات الجريمة المعلوماتية

Legal challenges to prove cybercrime

الأستاذ الدكتور عبد الغني حسونة⁽¹⁾

مخبر أثر الاجتهاد القضائي على حركة التشريع

جامعة محمد خيضر - بسكرة (الجزائر)

maitrehassouna@gmail.com

تاريخ النشر	تاريخ القبول:	تاريخ الارسال:
30 مارس 2023	14 مارس 2023	26 نوفمبر 2022

الملخص:

على الرغم من التأثير الايجابي للنظم المعلوماتية على حياة ونشاط الأشخاص، إلا أنها لم تسلم من الاستغلال السيئ وغير المشروع باستغلال ما توفره هذه النظم المعلوماتية من تقليص للأبعاد الجغرافية والمكانية وسرعة في التنفيذ والانتشار، وضعف التأطير القانوني لهذه السلوكات غير المشروعة. وبرغم من كل الجهود التي تبذلها السلطات المختصة في كل دول العالم سواء بشكل منفرد أو في إطار تنسيق جماعي لأجل إثبات مختلف الجرائم المعلوماتية، والتحقيق فيها بغية الوصول إلى تحديد مرتكبها ومحاكمته في إطار تحقيق حماية المصلحة العامة، وكذا الحفاظ على المصالح الخاصة لضحايا هذه الجرائم، إلا أن كل هذه المجهودات تصطدم بجملة من التحديات القانونية والتي تحول دون استكمال الأهداف المرجوة من تلك التحريات والتحقيقات. وهنا تبرز أهمية البحث في موضوع هذا المقال انطلاقا من ضروره تحديد موقف المشرع الجزائري في معالجته لهذه التحديات التي تشكل حاجز أمام الحد من الجرائم المعلوماتية ومكافحتها.

الكلمات المفتاحية: الجريمة المعلوماتية - الخصوصية - نظم معلوماتية - البيانات - التحقيق

الجزائي

Abstract:

Despite the positive impact of information systems on lives and activities of individuals, they have not been spared from bad and illegal exploitation by exploiting the geographical and spatial dimensions provided by these information systems, the speed of implementation and spread, and the weak legal framework for these illegal behaviors. Regardless of all the efforts made by the competent authorities in most countries, whether individually or within the framework of collective coordination in order to prove various information crimes, and investigate them in order to reach the identification and prosecution of the perpetrator within the framework of achieving the protection of the public interest, as well as preserving the private interests of the victims, all these efforts collide with a number of legal challenges that prevent completion of the desired goals of these investigations. The importance of researching the subject of this article is based on the need to determine the position of the Algerian legislator in addressing these challenges, which constitute a barrier to reducing and combating cybercrimes.

key words: Cybercrime – Privacy -Information systems –data- Criminal Investigation



مقدمة :

لقد كان لاستخدام النظم المعلوماتية المختلفة والناجمة عن التطور التكنولوجي الكبير الذي عرفته البشرية تأثير واضح وإيجابي على حياة ونشاط الأشخاص طبيعيين كانوا أو معنويين، إذ أدى استخدام واستغلال هذه النظم إلى تيسير حياتهم الشخصية والمهنية بالنظر إلى ما توفره هذه النظم المعلوماتية من بيانات ومعلومات هائلة في كافة مناحي الحياة الاقتصادية والاجتماعية والثقافية.

وعلى الرغم من التأثير الإيجابي لهذه النظم المعلوماتية، إلا أنها لم تسلم من الاستغلال السيئ وغير المشروع من طرف العديد من الأشخاص والكيانات مستغلين ما توفره من خصائص لتقليص الابعاد الجغرافية والمكانية وسرعة في التنفيذ والانتشار، وضعف التأطير القانوني لهذه السلوكات غير المشروعة.

وبرغم من كل الجهود التي تبذلها السلطات المختصة في كل دول العالم سواء بشكل منفرد أو في إطار تنسيق جماعي لأجل إثبات مختلف الجرائم المعلوماتية المرتكبة، والتحقيق فيها بغية الوصول إلى تحديد مرتكبها ومحاكمته في إطار تحقيق حماية المصلحة العامة وكذا الحفاظ على المصالح الخاصة لضحايا هذه الجرائم، إلا أن كل هذه الجهود تصطدم بجملة من التحديات القانونية والتي تحول دون استكمال الأهداف المرجوة من تلك التحريات والتحقيقات.

وفي هذا الصدد عمل المشرع الجزائري باعتباره معني بالتصدي لهذا النوع من الاجرام على وضع تنظيم قانوني مسترشدا في ذلك بالتنظيم الدولي ذي الصلة والمعني بتنظيم استغلال النظم المعلوماتية ومكافحة الاعتداء عليها، وهنا تبرز أهمية البحث في موضوع هذا المقال انطلاقا من ضرورة تحديد موقف المشرع الجزائري في معالجته لهذه التحديات التي تشكل حاجز أمام الحد من الجرائم المعلوماتية ومكافحتها.

ولأن عمليات التحقيق في الجرائم المعلوماتية وإثباتها تشكل انطلاقة العمل الإجرائي المتعلق بالمتابعة حيث تتخذ هذه التحديات صور وأوضاع مختلفة والتي يمكن تصنيفها ضمن مجموعتين أساسيتين، حيث تتخذ جملة من هذه التحديات وصف الطابع الشخصي، في حين تأخذ مجموعة أخرى من هذه التحديات وصف الطابع الموضوعي.

وفي إطار كل ما سبق تتمحور إشكالية هذا المقال حول مدى فعالية تدخل المشرع الجزائري في معالجة التحديات القانونية المرتبطة بعمليات إثبات الجرائم المعلوماتية ٩.

ولمعالجة موضوع هذا المقال سنعتمد على المنهج الوصفي ببيان المفاهيم ذات الصلة بالتحديات المتعلقة بإثبات الجريمة المعلوماتية وأبعادها، وكذا المنهج التحليلي من خلال قراءة

في النصوص القانونية التي وضعها المشرع الجزائري في مجال تأطير الجريمة المعلوماتية وتحليلها ومناقشتها.

وفي الأخير ومن من أجل الإجابة على إشكالية هذا المقال وبالنظر إلى خصوصية عناصر موضوعه سنعمد خطة ثنائية تقوم على مبحثين أساسيين: المبحث الأول: التحديات القانونية ذات الطبيعة الشخصية. أما المبحث الثاني: التحديات القانونية ذات الطبيعة الموضوعية.

المبحث الأول: التحديات القانونية ذات الطبيعة الشخصية

تبرز التحديات القانونية ذات الطابع الشخصي والمعرقلة لإثبات الجريمة المعلوماتية في إشكالات تثار نتيجة تدخل عوامل شخصية إما ذات صلة بالضحية أو مرتبطة بالجاني أو متعلقة بالسلطات المختصة بعملية التحقيق، أو تعد مساس بحرمة الحياة الشخصية للمشتبه به أو لغيره.

حيث تظهر هذه التحديات في ضعف مستوى التبليغ عن الجرائم المعلوماتية، بالإضافة إلى اعتماد المجرم المعلوماتي لتدابير حمائية لإخفاء هويته، وكذا ضعف الخبرات المعلوماتية لهيئات التحقيق ذات الاختصاص العام فضلا عن اصطدام إجراءات التحقيق مع حرمة الحياة الخاصة.

المطلب الأول: ضعف مستوى التبليغ عن الجرائم المعلوماتية

يعرف التبليغ على أنه القيام بإبلاغ السلطات المختصة بواقعة يعاقب عليها القانون، سواء كانت الواقعة وقعت على المبلغ نفسه أو على ماله أو شرفه، ويمكن أن تكون قد وقعت على الغير أو ماله أو شرفه، قد تكون الدولة أو ملكياتها محل الاعتداء¹.

وعلى الرغم من أهمية التبليغ في الكشف عن الجرائم ومتابعة مرتكبيها وتسليمهم إلى العدالة لإحكامتهم، إلا أن اكتشاف الجريمة المعلوماتية غالبا ما يتم بالصدفة، حيث لا يميل المجني عليه في هذا النوع من الجرائم إلى تبليغ السلطات المختصة في إثبات الجريمة والكشف عنها، وحتى في حالة الاكتشاف للجريمة المعلوماتية من قبل السلطات المختصة، فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرّة وضياح ثقة المساهمين، حيث يظهر المجني عليه في الجرائم المعلوماتية عادة في شكل بنك أو مؤسسة مالية أو مشروع صناعي ضخم يهيمه المحافظة على ثقة عملائه وعدم اهتزاز سمعته، أكثر من اهتمامه بالكشف عن الجريمة ومرتكبها، لذلك يميل المجني عليه على تقديم ترضية سريعة لعميله، وينهي الأمر بشكل داخلي وودي حتى لا يفقده.²

كما يعود أيضا إحصاء المجني عليه من التبليغ عن الاعتداء الواقع عليه في الجريمة المعلوماتية إلى عدم إدراكه أن مثل هذه الأفعال والتعديلات تشكل جرائم يمكن معاقبة مرتكبيها عليها بموجب القواعد التشريعية والتنظيمية المعمول بها هذا من جهة، من جهة أخرى الرغبة في إخفاء الأسلوب الذي تمت به الجريمة المعلوماتية لكي لا يتم تقليده من الآخرين مستقبلا.³

وبالعودة إلى القانون الجزائري نسجل غياب تدخل المشرع لمعالجة هذا التحدي وإيجاد آليات لتحفيز وإلزام ضحايا الجرائم المعلوماتية بالقيام بالتبليغ عن هذه الأخيرة والتي تقع عليهم، وفي هذا الإطار ندعوا إلى ضرورة تدخل المشرع على نحو ما ذهب إليه التشريعات المقارنة في هذا المجال، كما هو الحال بالنسبة لفرض إدراج بنود في عقود التأمين المبرمة بين شركات التأمين والمؤمنين تقضي بضرورة التبليغ عن الجريمة المعلوماتية لدى سلطات الضبط القضائي كإجراء مسبق قبل تسوية ملف التعويضات عن الأضرار الناجمة عن هذه الجريمة المعلوماتية، أو إلزام أعوان المؤسسات المالية بالتبليغ عن كل الثغرات المالية التي يكتشفونها بمناسبة أداء عملهم تحت طائلة ترتيب عقوبات جزائية.

المطلب الثاني: اعتماد المجرم المعلوماتي لتدابير حماية لإخفاء هويته

يتصف المجرمون المعلوماتيون غالبا بالذكاء والخبرة الواسعة مقارنة بنظرائهم من المجرمين التقليديين، كما يتصفون بالخشية الكبيرة من انكشاف جرائمهم وفضح سلوكياتهم، وعلى الرغم من أن هذا الخوف يصاحب غالبية المجرمين بمختلف أنواعهم، إلا أنه يزيد لدى المجرمين المعلوماتيين لما يترتب من اكتشاف أمرهم من تأثير على فقدان مراكزهم الوظيفية والاجتماعية، هذا ويساعدهم على الحفاظ على سرية أفعالهم الإجرامية طبيعة الأنظمة المعلوماتية نفسها.⁴

حيث أنه وعلى الرغم من أن التقنيات المتطورة في هذا المجال قد ساهمت في إمكانية تحديد مكان أو موقع النظام الآلي الذي تمت منه العمليات أو السلوكات المجرمة للجريمة المعلوماتية محل البحث، ومن ثم الكشف عن الجاني على اعتبار أن صاحب الجهاز المعلوماتي كأصل عام هو القائم بالفعل الإجرامي، غير أن هذا الافتراض غير صحيح في كل الأحوال، لأن ما يمكن التوصل إليه من خلال التقنيات المتطورة في هذا المجال تكشف فقط موقع تواجد الجهاز المعلوماتي، حيث لا يمكن وفق هذا الافتراض وحده إسناد السلوك الإجرامي إلى صاحب الجهاز المعلوماتي.

إذ أن المجرم المعلوماتي المتمرس يجتهد في إخفاء هويته للحيلولة دون تعقبه أو اكتشاف أمره، بحيث تظل أنشطته مجهولة ويمنأى عن علم السلطات المختصة بمكافحة هذه الجريمة، وفي هذا الإطار تبرز مظاهر وصور الممارسات التي يعتمدها المجرم المعلوماتي في هذا الشأن، من استعمال المجرم المعلوماتي لجهاز معلوماتي غير جهازه الشخصي كما هو الحال بالنسبة للحواسيب

الموجودة في مقاهي الأنترنت، على اعتبار أن حرية استعمال الحواسيب الموجودة في هذه المقاهي تتم دونما وجود قيود تتعلق بتحديد هويته مستخدميه، كما أن استخدام شبكة الانترنت اللاسلكي "الوي فاي" يعزز بدوره من صعوبة تحديد شخص المجرم المعلوماتي.⁵

وفي إطار تجاوز هذا التحدي عمل المشرع الجزائري بالأخذ بما اعتمدته التشريعات المقارنة لا سيما ما يتعلق بفرض التزام على الكيانات الضامنة للتزويد بخدمات الانترنت والاتصال، حيث يتعلق بتحديد هوية مستعمل الخدمة وكذا المعطيات التي تسمح بالتعرف على هوية المرسل إليه وكذا عناوين المواقع المطلع عليها فضلا على تحديد تاريخ وتوقيت كل اتصال.⁶

المطلب الثالث: ضعف الخبرات المعلوماتية لهيئات التحقيق ذات الاختصاص العام

تقتضي العدالة الجنائية أن يكون أفراد الأجهزة والهيئات المسؤولة عن المعاينة والضبط والتحقيق في الجرائم على قدر من المسؤولية في معرفة وتحديد الجناة والتحقيق معهم، إلا أن هناك جملة من التحديات تواجه عمل أفراد هذه الهيئات، وبخاصة الأفراد غير المختصين أو غير ذوي الكفاءة والخبرة الفنية في مجال الجرائم المعلوماتية، والذين انحصرت معارفهم وخبراتهم في الجرائم التقليدية من قتل وسرقة وتزوير، ذلك أن أفراد هاته الهيئات لن يكونوا قادرين على معالجة هذه الجرائم المعلوماتية، كونها ترتكب بواسطة أسلوب تقني وفني.

وما يزيد في صعوبة إثبات الجرائم المعلوماتية ضعف الخبرة الفنية لسلطات التحقيق على اختلاف صورها من سلطات الضبط القضائي لا سيما ذات الاختصاص العام إلى جهات الاتهام والتحقيق القضائي، حيث يظهر هذا الضعف في تحديد الدليل المعتبر الذي يعد حاسما في إثبات الجريمة المعلوماتية أو في انتشار ذلك الدليل من النظام المعلوماتي والحفاظ عليه.⁷

ونخلص في الأخير إلى أن الخبرة الفنية في الجرائم المعلوماتية اليوم، تحتاج إلى إدارة خاصة يعمل بها مختصون في أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية، وهو ما يتطلب إنشاء إدارة خاصة للخبرة والمعاينة في الجرائم المعلوماتية، حيث لا يتم الاكتفاء فقط بمجرد تدريب القائمين على إدارة الخبرة الجنائية.⁸

وفي الإطار نسجل أنه وعلى الرغم من إحداث المشرع الجزائري للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها في إطار القانون 09-04،⁹ والتي عهد إليها مهمة الوقاية من الجرائم المعلوماتية، وكذا تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها هذه الأخيرة في الجرائم ذات الصلة، دون أن يكون للهيئة أو لخبرائها الممارسين والمنتمين إليها صفة الضبطية القضائية بما يمنح لهم صلاحية الضبط والتدخل بشكل مباشر، وهنا ندعو المشرع الجزائري إلى إسناد صفة الضبطية

القضائية للخبراء المعلوماتيين الذي تتوفر عليهم الهيئة المذكورة أعلاه، كون تدخلهم في التحقيق وهم يتمتعون بصفة الضبطية القضائية سوف يكون أكثر نجاعة وفعالية في إثبات الجرائم المعلوماتية منه تدخل أعوان الضبطية القضائية ذات الاختصاص العام المحددين في قانون الاجراءات الجزائية.

المطلب الرابع: اصطدام إجراءات التحقيق مع حرمة الحياة الخاصة

تشكل الحياة الخاصة عنصرا أساسيا وجوهريا، ولا يمكن المساس به بأي شكل حتى لو كان ذلك على محض الصدفة، ويرجع ذلك إلى اعتبار الحياة الخاصة مستودع أفراد وجزء من كياناتهم وشخصيتهم، ونظرا لأهمية ذلك أولت التشريعات الوطنية المختلفة بالحياة الخاصة، فجعلته حقا لكل إنسان على كل شخص طبيعي أو معنوي يتعين احترامه وعدم التعرض له أو المساس به إرساء لحماية الإنسان وصون حياته الخاصة.¹⁰

ولأنه لا يمكن إنكار الدور الأساسي والهام للدليل الرقمي في عملية الإثبات الجنائي، غير أنه في مقابل ذلك لا يمكن إغفال مدى تأثير هذا الدليل على الخصوصية المعلوماتية، لاعتبار الدليل الرقمي ذو طبيعة تقنية، ويعتمد في تحصيله بشكل أساسي وكبير على نظام المراقبة الالكترونية، هذه الأخيرة تشكل مساس واضح بالخصوصية المعلوماتية، وتظهر حدو هذا المساس عندما يترتب على المراقبة الالكترونية في إطار البحث على الدليل الرقمي نتيجة سلبية، على نحو قيام سلطات البحث والاستدلال المختصة بالولوج إلى حسابات المشتبه فيه والاطلاع على محتوى رسائله الشخصية وحساباته المصرفية المبحوث عنها، ثم يتضح فيما بعد أنه لا وجود لأي علاقة تربط بين الجريمة المعلوماتية محل البحث والتحقيق وتلك البيانات والمعلومات المتضمنة في حسابات المشتبه به.¹¹

وتزداد الحدة أكثر من ذلك ولأن النظم المعلوماتية متداخلة ومتشابكة مع بعضها البعض، فإن عملية البحث من أجل اثبات الجريمة المعلوماتية قد يتجاوز محله النظام المعلوماتي للمشتبه به إلى أنظمة أخرى مرتبطة بنظام المشتبه به، ولا شك أن البحث سيمس في التصميم بالحق في الخصوصية المعلوماتية لأصحاب هذه النظم المعلوماتية¹²، والذين ليس لهم علاقة نهائيا بهذه الجريمة لا من قريب ولا من بعيد، وكل ما في الأمر أنهم وجدوا أنفسهم مرتبطين بحاسوب بشكل أو بآخر بالنظام المعلوماتي للمشتبه به محل البحث.

وفي هذا الاطار حاول المشرع الجزائري إيجاد نوع من التوازن بين ما تتطلبه حرمة الحياة الخاصة المعلوماتية من حماية، وما تفرضه أو تقتضيه حماية المصلحة العامة في الحد من الجرائم المعلوماتية بإعمال الاجراء المتعلق بالمراقبة الالكترونية، حيث ضبط المشرع

الجزائري ممارسة الرقابة الالكترونية من قبل السلطات المختصة بجملة من الضوابط تضمن تحقيق المصلحة العامة وكفالة الحد اللازم من الخصوصية المعلوماتية.

ومن جملة الضوابط التي وضعها المشرع الجزائري في هذا الصدد ما جاء في القانون 04-09 سالف الذكر، والتي قام المشرع من خلاله ابتداء بحصر الحالات التي يمكن اللجوء فيها إلى الرقابة الالكترونية في ما يلي:¹³

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن اعتداء على منظومة معلوماتية على نحو يهدد الصالح العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما وضع المشرع الجزائري وفي نفس السياق ضابط آخر لإعمال المراقبة الالكترونية ويتمثل في إلزامية الحصول على ترخيص مكتوب من طرف السلطات القضائية المختصة، هذا وقد أفرد المشرع الحالة الأولى التي تجوز فيها المراقبة الالكترونية بأحكام خاصة على مستوى الجهة القضائية المختصة بمنح ترخيص إعمال إجراء المراقبة الالكترونية وكذا آجالها فضلا عن الترتيبات التقنية الخاصة بها وفقا لما جاء في الفقر 06 و 07 من المادة 04 من القانون 04-09 سالف الذكر.

إذن فمفهوم المخالفة تعد مراقبة الكترونية غير مشروعة تلك المراقبة التي تتم خارج الضوابط المذكورة أعلاه على نحو غياب الترخيص القضائي اللازم للقيام بالمراقبة، أو القيام بها خارج الحالات المذكورة أعلاه، أو خارج الآجال المنصوص عليها إما في إطار القانون 04-09 سالف الذكر، أو الآجال المنصوص عليها في أحكام قانون الإجراءات الجزائية والمحددة بأربعة أشهر قابلة للتجديد حسب مقتضيات القضية.¹⁴

المبحث الثاني: التحديات القانونية ذات الطبيعة الموضوعية

تبرز التحديات القانونية ذات الطابع الموضوعي والمعركة لإثبات الجريمة المعلوماتية في إشكالات تثار نتيجة تدخل عوامل غير شخصية وإنما تعود لطبيعة الجريمة المعلوماتية ذاتها والآثار المترتبة عنها.

حيث تظهر هذه التحديات في غياب الآثار المادية للجريمة المعلوماتية وسهولة محوها إن وجدت، وكذا طبيعة وخصوصية مسرح الجريمة المعلوماتية، بالإضافة إلى كبر حجم البيانات

التي يتعين البحث فيها، فضلا عن عدم تناسب إجراءات التحقيق الكلاسيكية مع الجرائم المعلوماتية.

المطلب الأول: غياب الآثار المادية للجريمة المعلوماتية وسهولة محوها إن وجدت

بالنظر إلى الطابع الخاص الذي تتميز به الجرائم المعلوماتية، فإن إثباتها يحيط به الكثير من التحديات، والتي من بينها صعوبة اكتشاف هذه الجرائم، كونها لا تترك آثارا مادية خارجية، حيث يغيب استعمال العنف بمختلف صوره وأساليبه عن الجرائم المعلوماتية، من سفاك للدماء أو آثار اقتحام لسرقة الأموال وغيرها...، بل هي جرائم فنية وهادئة ويتم فيها الاعتماد على البيانات والأرقام والتي يمكن وبكل سهولة ويسر من تغييرها ومحوها من السجلات المخزنة في ذاكرة الحواسيب وليس لها أي أثر خارجي مرئي¹⁵.

وفي ذات السياق يشكل تحديا لإثبات الجريمة المعلوماتية سهولة إخفاء الجناة لأدلة الإدانة أو محوها أو تدميرها، إذ يستخدمون في ذلك التلاعب غير المرئي في النبضات والذبذبات الالكترونية التي يتم تسجيل البيانات عن طريقها، وما يزيد في من إمكانية وسهولة إخفاء هذا الدليل أنه يمكن محوه في زمن قصير جدا لا يستغرق بضعة دقائق، وربما بعض أجزاء من الدقيقة، وبشكل لا يمكن معه إقامة الدليل على المجرم المعلوماتي من قبل سلطات التحقيق عند بلوغ إلى مسامعها وقوع الجريمة المعلوماتية.¹⁶

وفي إطار تخفيف حدة التحدي المتعلق بسهولة محو الآثار المادية للجريمة المعلوماتية، حتى وإن كانت قد تمت عملية المحو هذه على مستوى النظم المعلوماتية للجناة أو لضحايا هذه الجريمة، فإننا نسجل تدخل المشرع الجزائري من خلال القانون 09-04 بإلزام مقدي الخدمات بحفظ كل المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وكذا المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، بالإضافة إلى الخصائص التقنية وكذا تاريخ ووقت ومدد كل اتصال، فضلا عن المعطيات المتعلقة بالخدمات التكميلية المطلوبة المستعملة

ومقدميها، يضاف إليها المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وكذا عناوين المواقع المطلع عليها.¹⁷

إن الزام المشرع الجزائري لمقدمي الخدمات بحفظ كل المعطيات المذكورة أعلاه، يساهم ولو بشكل نسبي في الحفاظ على الآثار التقنية على مستوى الكيانات المقدمة للخدمات والتي يمكن الاستعانة بها في تتبع مسار الجريمة المعلوماتية وإثباتها، وحتى وإن تم محو أو اتلاف الآثار التي شكلت الركن المادي للجريمة المعلوماتية.

المطلب الثاني : طبيعة مسرح الجريمة المعلوماتية

يعرف مسرح الجريمة بشكل عام على أنه الفضاء الجغرافي الذي عايش كل أو بعض من أطوار الفعل الإجرامي، وخلف عنده الجاني مجموعة من الآثار التي قد تكون واضحة أو مخفية، والتي تدل على فعل يصب في خانة الجرائم، مما يستدعي تدخل مجموعة من المحققين الجنائيين والخبراء الفنيين لفك الألغاز وأسرار الجريمة موضوع التحقيق¹⁸.

مع ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر مختلف الدول، إذ أن القدرة التي تتمتع بها النظم والتجهيزات المعلوماتية في نقل وتبادل كميات كبيرة من المعلومات والبيانات بين نظم معلوماتية يفصل عنها آلاف الأميال، قد أدى إلى نتيجة مفادها أن كيانات وشركات متواجدة في دول مختلفة قد تتأثر بالجريمة المعلوماتية في وقت واحد¹⁹.

وتأكيدا على ما سبق تزداد المسألة تعقيدا حينما يكون محل البحث عن اثبات الجريمة المعلوماتية هو شبكة الانترنت إذ يصبح ضبط الدليل والبحث عنه أمرا في غاية الصعوبة إذا لم يكن مستحيلا أحيانا، على اعتبار أن عمليات التفتيش والضبط في هذه البيئة الافتراضية يتطلب أن يتم خارج حدود الدولة وفي نطاق دولة أخرى، مما يتطلب الحصول على إذن مسبق بذلك من سلطاتها، لما ينطوي عليه من مساس بسيادة هذه الدولة، ناهيك عن ما يسفر عنه البحث من انتهاك لخصوصية الآخرين ممن تتعلق بهم البيانات أو المعلومات محل الضبط أو التفتيش²⁰.

وفي هذا الصدد وفي إطار تجاوز هذا التحدي المتعلق بطبيعة مسرح الجريمة المعلوماتية يتعين على الدول من خلال سلطاتها المختصة أن تعمل على التنسيق المسبق فيما بينها من خلال إبرام اتفاقيات التعاون الأمني والقضائي في مجال مكافحة هذا النوع من الجرائم، بما يكفل تعزيز التدخل السريع لإثبات الجريمة المعلوماتية وضبط المجرم المعلوماتي.

وهو ما جسده المشرع الجزائري من خلال قانون 09-04 المتعلق بالوقاية من تكنولوجيات الاعلام والاتصال في المادة 05 منه في فقرتها الثالثة على مبدأ التعاون مع السلطات المختصة للدول الأجنبية في إطار الاتفاقيات ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

كل هذا إعمالا وانسجاما مع ما تضمنته اتفاقية بودابست²¹ من أنه يتعين على كل الأطراف التعاون على تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك على مستوى القانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة

بالجرائم الجنائية للشبكات والبيانات المعلوماتية وكذا بشأن الحصول على الأدلة في الشكل الإلكتروني مثل هذه الجرائم²².

المطلب الثالث: كبر حجم البيانات التي يتعين البحث فيها

كما هو معلوم تتميز الأنظمة المعلوماتية على اختلاف أنواعها بقدراتها الهائلة على تخزين البيانات بما يوازي مئات الآلاف من الصفحات الورقية، حيث أنه وببساطة لو أتيح لسلطات الضبط والتحقيق مثلاً، طباعة محتويات أحد الأقراص الصلبة، فإن ذلك يستلزم كميات ضخمة من الأوراق، وقد تكون النتيجة رغم كل ذلك سلبية وبرغم كل هذا الجهد بحيث لا يمكنها كشف الدليل المراد ضبطه أو تحصيله، وهذا سببه عدم وجود آلية للفرز الذاتي للملفات المخزنة حتى يمكن الوقوف على الملفات غير المشروعة.²³

لذلك يشكل الكم الهائل للبيانات التي يجري تداولها في الأنظمة المعلوماتية إحدى الصعوبات البارزة التي تعيق التحقيق وإثبات الجرائم التي تقع عليها أو بواسطتها، إذ عادة ما يتطلب البحث عن الأدلة في حاسب آلي واحد الإطلاع والفحص الدقيق لكل المعطيات التي تتضمنها آلاف الملفات المخزنة في ذاكرة هذا الحاسب الآلي، الأمر الذي يكلف المحققين وقتاً كبيراً وجهداً معتبراً، وهو ما ينعكس سلباً على مردود سلطات البحث والتحقيق بسبب الملل والضجر، ويؤدي بهم حتى إلى عدم مواصلة البحث والتحري من أجل إثبات الجريمة المعلوماتية محل البحث.²⁴

و في حقيقة الأمر، أن هذا التحدي الموضوعي والمتعلق بحجم البيانات الكبير المحيط بجوانب الجريمة المعلوماتية، لم يعرف له تدخلاً من قبل المشرع الجزائري في إيجاد تسوية تخفف من حدته، وإنما تركه لتقدير سلطات الاستدلال حسب ظروف كل قضية، وهو أمر منطقي كون أصل هذا التحدي يعتبر إشكال ذو طابع تقني، ويتعين تسويته بشكل تقني وليس بشكل قانوني.

المطلب الرابع: عدم تناسب إجراءات التحقيق الكلاسيكية مع الجرائم المعلوماتية

يعد التطور السريع في المجال المعلوماتي من أهم التحديات التي تحول دون مكافحة الجريمة المعلوماتية والتحقيق فيها بطريقة فعالة، حيث تبرز في كل يوم جديد تقنيات جديدة للقرصنة والتحايل والاختراق بشكل يصعب مسايرته من طرف السلطات المختلفة في الدولة، حتى أصبح العالم اليوم يعيش في إطار ما يسمى بالطوفان الرقمي.²⁵

هذا وتجدر الإشارة إلى أنه لا يتوقف الأمر عند قصور النصوص العقابية في مواجهة الجرائم المعلوماتية، بل يتعدى إلى القوانين الإجرائية، إذ أن معظم إجراءات التحقيق والمتابعة التي تتضمنها التشريعات التقليدية لا تتلاءم مع طبيعة هذه الجرائم المعلوماتية، وأحياناً

تتعارض حتى مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها المعلومات أو البيانات بشتى أنواعها، وهذا الأمر يشكل عقبة كبيرة أمام سلطات التحقيق.²⁶

ويتأكد المعنى المذكور أعلاه من خلال جملة من التطبيقات الإجرائية على نحو عملية أو إجراءات التفتيش التي تختلف طبيعتها في الجرائم المعلوماتية عنها في الجرائم التقليدية، كون إجراء التفتيش في الجرائم المعلوماتية سيتم في الكيانات المنطقية للنظم المعلوماتية، ولأن عملية التفتيش تستهدف بشكل أساسي ضبط العناصر المادية ذات العلاقة بالجريمة محل البحث، ولما كانت الكيانات المنطقية للنظم المعلوماتية على نحو البرامج والبيانات تعد عناصر معنوية غير مادية، فإن إجراء التفتيش بالمعنى المادي لا ينسجم وخصوصية هذه الكيانات المنطقية، وعليه فإن هذه الأخيرة لا يمكن ضبطها وتفتيشها إلى إذا تم تضييقها في كيان مادي محسوس على نحو طباعتها على ورق أو تخزينها على دعائم مادية، ومن ثم ضبطها لكي يتم إخضاعها للتفتيش.

في ذات السياق ووفقا للقواعد العامة للإجراءات الجزائية، أحاط المشرع الجزائري بإجراء التفتيش بجملة من الضوابط تبدأ إلزاميا بحضور صاحب المسكن محل التفتيش أو من يمثله وعند الاقتضاء حضور شاهدين²⁷، هذا وإن كانت هذه الضوابط منسجمة مع عمليات التفتيش المادي، فإن ذلك ليس له ما يبرره في الجرائم المعلوماتية، لا سيما عندما تتم عمليات التفتيش عن بعد عبر شبكات الاتصال المختلفة، وعليه ندعوا المشرع في هذا الإطار إلى استثناء إجراء التفتيش عن بعد في الجرائم المعلوماتية من الضوابط الواردة في المادة 45 من قانون الإجراءات الجزائية المذكورة أعلاه.

من جهة أخرى وفي الإطار المتعلق بالتقادم والذي يتم احتسابه وفقا للقواعد العامة ابتداء من تاريخ ارتكاب السلوك المادي للجريمة²⁸، على اعتبار أن اكتشاف الجريمة يكون في العادة مصاحبا لارتكاب السلوك المادي لها أو قريب منها زمنيا، فإن هذا لا ينطبق غالبا على الجرائم المعلوماتية بالنظر إلى غياب الآثار المادية الناجمة عن ارتكابها، وكذا إحجام الضحايا المتضررين عن الإبلاغ عن الاعتداء الواقعة عليهم جراء هذه الجريمة، الأمر الذي يترتب عليه مرور مدة طويلة بين تاريخ إتيان السلوك الاجرامي وتاريخ اكتشافه وهي فترة يمكن أن تستغرق مدة التقادم الخاص بالجريمة محل البحث أو التحقيق، وبالتالي تملص المجرم المعلوماتي من المتابعة، وعليه ندعوا المشرع الجزائري في هذا الإطار إلى تخصيص حكم إجرائي خاص بالتقادم في الجرائم المعلوماتية يبدأ من تاريخ اكتشاف الفعل الاجرامي لا من تاريخ إتيانه.

خاتمة:

في ختام هذا البحث نخلص إلى القول بأن المشرع الجزائري قد سعى جاهدا إلى معالجة التحديات القانونية المتعلقة بإثبات الجريمة المعلوماتية من خلال تدخله بإصدار القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث وفق إلى حد بعيد في التخفيف من حدة هذه الإشكالات، مع تسجيل بعض التحفظات، وبشكل أكثر تفصيل نخلص إلى النتائج التالية:

1- تسجل غياب تدخل المشرع لمعالجة التحدي المتعلق بضعف التبليغ عن الجرائم المعلوماتية وإيجاد آليات لتحفيز وإلزام ضحايا الجرائم المعلوماتية بالقيام بالتبليغ عن هذه الأخيرة والتي تقع عليهم.

2- في إطار تجاوز إشكالية إخفاء هوية المجرم المعلوماتي باعتداده لتدابير حمائية، عمل المشرع الجزائري على إلزام الكيانات الضامنة للتزويد بخدمات الانترنت والاتصال، بتزويد السلطات المختصة بالتحقيق بالمعلومات المتعلقة بهوية مستعمل الخدمة وكذا المعطيات التي تسمح بالتعرف على هوية المرسل إليه وكذا عناوين المواقع المطلع عليها فضلا على تحديد تاريخ وتوقيت كل اتصال.

3- قام المشرع الجزائري باستحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته في إطار القانون 09-04، والتي عهد إليها مهمة الوقاية من الجرائم المعلوماتية، وكذا تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها هذه الأخيرة في الجرائم ذات الصلة، دون أن يكون للهيئة أو لخبرائها الممارسين والمنتهمين إليها صفة الضبطية القضائية بما يسمح لهم صلاحية الضبط والتدخل بشكل مباشر.

4- حاول المشرع الجزائري إيجاد نوع من التوازن بين ما تتطلبه حرمة الحياة الخاصة المعلوماتية من حماية، وما تفرضه أو تقضيه حماية المصلحة العامة في الحد من الجرائم المعلوماتية بإعمال الإجراءات المتعلقة بالمراقبة الالكترونية، حيث ضبط ممارسة هذه الأخيرة بجملة من الضوابط على نحو حصر الحالات التي يمكن اللجوء فيها إلى الرقابة الالكترونية، وكذا إلزامية الحصول على ترخيص مكتوب من طرف السلطات القضائية المختصة.

5- أفرد المشرع في إطار معالجة التحدي المتعلق بحماية الحياة الخاصة بأحكام خاصة بالجهة القضائية المختصة بمنح ترخيص إعمال إجراء المراقبة الالكترونية، وكذا آجالها فضلا عن الترتيبات التقنية الخاصة بها، وهذا عند التحقيق في الجرائم ذات الصلة بالأفعال الإرهابية

والتخريبية والماسة بأمن الدولة وفقا لما جاء في الفقرة 06 و 07 من المادة 04 من القانون 09-04.

6- في إطار تجاوز التحدي المتعلق بطبيعة مسرح الجريمة المعلوماتية يتعين على الدول من خلال سلطاتها المختصة أن تعمل على التنسيق المسبق فيما بينها من خلال إبرام اتفاقيات التعاون الأمني والقضائي في مجال مكافحة هذا النوع من الجرائم، وهو ما جسده المشرع الجزائري من خلال قانون 09-04 في المادة 05 منه في فقرتها الثالثة على مبدأ التعاون مع السلطات المختصة للدول الأجنبية في إطار الاتفاقيات ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

7- عدم ملائمة العديد من إجراءات التحقيق والمتابعة التي تتضمنها التشريعات التقليدية مع طبيعة الجرائم المعلوماتية، وأحيانا تتعارض حتى مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها المعلومات أو البيانات بشتى أنواعها، وهذا الأمر يشكل عقبة كبيرة أمام سلطات التحقيق.

8- إن إلزام المشرع الجزائري لمقدمي الخدمات بحفظ معطيات محددة، يساهم ولو بشكل نسبي في الحفاظ على الآثار التقنية على مستوى الكيانات المقدمة للخدمات والتي يمكن الاستعانة بها في تتبع مسار الجريمة المعلوماتية وإثباتها، وحتى وإن تم محو أو إتلاف الآثار التي شكلت الركن المادي للجريمة المعلوماتية.

و بناء على نتائج هذه الدراسة نخلص إلى جملة التوصيات التالية :

1- في إطار معالجة ضعف التبليغ عن الجرائم المعلوماتية ندعو إلى ضرورة تدخل المشرع على نحو ما ذهب إليه التشريعات المقارنة في هذا المجال، كما هو الحال بالنسبة لفرض إدراج بنود في عقود التأمين المبرمة بين شركات التأمين والمؤمنين تقضي بضرورة التبليغ عن الجريمة المعلوماتية لدى سلطات الضبط القضائي كإجراء مسبق قبل تسوية ملف التعويضات عن الأضرار الناجمة عن هذه الجريمة المعلوماتية، أو إلزام أعوان المؤسسات المالية بالتبليغ عن كل الثغرات المالية التي يكتشفونها بمناسبة أداء عملهم تحت طائلة ترتيب عقوبات جزائية.

2- ندعو المشرع الجزائري إلى إسناد صفة الضبطية القضائية للخبراء المعلوماتيين الذي تتوفر عليهم الهيئة المذكورة أعلاه، كون تدخلهم في التحقيق وهم يتمتعون بصفة الضبطية القضائية سوف يكون أكثر نجاعة وفعالية في إثبات الجرائم المعلوماتية منه تدخل أعوان الضبطية القضائية ذات الاختصاص العام المحددين في قانون الإجراءات الجزائية.

3- ندعو المشرع إلى استثناء إجراء التفتيش عن بعد في الجرائم المعلوماتية من الضوابط الواردة في المادة 45 من قانون الإجراءات الجزائية لغياب ما يبرر وجود تلك الضوابط.

4- ندعوا المشرع الجزائري إلى تخصيص حكم إجرائي خاص بالتقادم في الجرائم المعلوماتية يبدأ من تاريخ اكتشاف الفعل الاجرامي للجريمة المعلوماتية، لا من تاريخ إتيانه.

الهوامش:

- 1- بلقاسم محمد، التبليغ عن جرائم الفساد في الاتفاقيات الدولية واثره على التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 58، عدد 04، ص 136.
- 2- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديد للنشر، الاسكندرية، 2004، ص 54.
- 3- أنيس حسيب السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية والرقمية: دراسة مقارنة دار الفكر الجامعي، الاسكندرية، 2016، ص 97.
- 4- غريبي بشري، خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، المركز الجامعي مغنية، المجلد 02، العدد 02، ص 105.
- 5- أنيس حسيب السيد المحلاوي، مرجع سابق، ص 91.
- 6- المادة 11 من القانون 09-04 المؤرخ في 05-08-2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج ر، عدد 47.
- 7- جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية: دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2010، ص 92.
- 8- عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية: دراسة مقارنة، رسالة لنيل درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص 81.
- 9- المادة 13 من القانون 09-04، مرجع سابق.
- 10- بلعابد عيّد، الدليل الرقمي بين حتمية الاثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق علمية، المركز الجامعي تمنراست، المجلد 11، العدد 01، ص 142.
- 11- بلعابد عيّد، مرجع سابق، ص 145.
- 12- غانم مرضي الشمري، الجرائم المعلوماتية، الطبعة الأولى، الدار العلمية الدولية النشر والتوزيع، عمان، 2016، ص 175.
- 13- المادة 04 من القانون 09-04.
- 14- المادة 65 مكرر 7 ف 2 من الأمر 66-155 المؤرخ في 08-06-1966 المعدل والمتمم والمتضمن قانون الإجراءات الجزائية، ج ر، عدد 48.
- 15- محمد علي العريان، مرجع سابق، ص 53.
- 16- بثينة حبابنتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، جامعة قسنطينة، عدد 50، ص 88.
- 17- المادة 11 من القانون 09-04، مرجع سابق.
- 18- ميهوب يوسف وريطاب عز الدين، بروتوكول معاينة الطبيب الشرعي لسرح الجريمة، مجلة دراسات وأبحاث، جامعة الجلفة، المجلد 7، العدد 21، ص 482.
- 19- طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديد، الاسكندرية، ص 172.
- 20- أنيس حسيب السيد المحلاوي مرجع سابق، ص 97.

- ²¹ – تجدر الإشارة إلى أنه على الرغم من هذا الانسجام بين اتفاقية بودابست والقانون 09-04، إلا أنه أن الجزائر لم توقع على هذه الاتفاقية بشكل رسمي.
- ²² – المادة 23 من اتفاقية بودابست المتعلقة بالجريمة الالكترونية، الموقعة بتاريخ 22 نوفمبر 2001 الصادرة في إطار مجلس أوروبا.
- ²³ – أنيس حسيب السيد المحلاوي، مرجع سابق، ص 96.
- ²⁴ – براهيم جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه في القانون، جامعة تيزيوزو، 2018، ص 218.
- ²⁵ – حوالف حليلة ومهاجي فاطمة الزهراء، معالم الجريمة المعلوماتية في القانون الجزائري ، مجلة البحوث القانونية والسياسية، جامعة سعيدة، مجلد 03، عدد 16، ص 145.
- ²⁶ – براهيم جمال، مرجع سابق، ص 145.
- ²⁷ – المادة 45 من الأمر 66-155، مرجع سابق.
- ²⁸ – المادة 07 و08 و09 من الأمر 66-155، مرجع سابق.

