

الجرائم السيبرانية وتحدياتها القانونية Cybercrimes and their legal challenges

سعيد عبد الحميد ♦

جامعة تيارت / الجزائر

مخبر البحث في تشريعات حماية النظام البيئي

abdelhamid.saidi@univ-tiaret.dz

سعيد عبد القادر

جامعة الزيتونة - ليبيا

kadisaidi72@gmail.com

تاريخ النشر: 2025/12/25

تاريخ القبول: 2025/11/19

تاريخ الإرسال: 2025/10/10

الملخص:

رغم الفوائد الكبيرة للنظم المعلوماتية في تسهيل حياة الأفراد وأنشطتهم، إلا أنها لم تخل من الاستخدام غير القانوني، حيث يتم استغلال إمكاناتها في تقليص الحدود الجغرافية، وسرعة التنفيذ والانتشار، مع ضعف الأطر القانونية لضبط هذه السلوكيات، وعلى الرغم من الجهود التي تقوم بها الجهات المختصة عالمياً سواء بشكل فردي أو من خلال تعاون دولي، للكشف عن الجرائم المعلوماتية والتحقيق فيها بهدف تحديد مرتكبيها ومحاكمتهم لحماية المصلحة العامة والمصالح الخاصة للضحايا، فإن هذه الجهود تواجه عقبات قانونية تعيق تحقيق الأهداف المنشودة. ومن هنا، تظهر أهمية دراسة موقف المشرع الجزائري في التعامل مع هذه التحديات التي تعوق الحد من الجرائم المعلوماتية ومكافحتها.

الكلمات المفتاحية: الجريمة المعلوماتية، الخصوصية، النظم المعلوماتية، البيانات، التحقيق الجنائي.

Abstract:

Despite the significant benefits of information systems in facilitating individuals' lives and activities, they have not been free from unlawful use. Their capabilities such as diminishing geographical boundaries, enabling rapid execution and widespread dissemination are often exploited in the absence of robust legal frameworks to regulate such behavior. Although competent authorities around the world, whether individually or through international cooperation, have made efforts to detect and investigate cybercrimes with the aim of identifying perpetrators and bringing them to justice in order to protect both the public interest and the private rights of

victims, these efforts continue to face legal obstacles that hinder the achievement of their intended goals.

Against this backdrop, the importance of examining the approach adopted by the Algerian legislator emerges, particularly in addressing the challenges that impede the prevention and suppression of cybercrime.

Keywords: Cybercrime; Privacy; Information systems; Data; Criminal investigation.

مقدمة:

أحدث التطور التكنولوجي تأثيرا كبيرا وإيجابيا على حياة الأفراد والمؤسسات، سواء كانوا أشخاصا طبيعيين أو معنويين من خلال استخدام النظم المعلوماتية التي سهلت الأنشطة الشخصية والمهنية. فقد وفرت هذه النظم كميات هائلة من البيانات والمعلومات التي تخدم مختلف الجوانب الاقتصادية والاجتماعية والثقافية. ومع ذلك، لم تخل هذه النظم من الاستخدامات غير المشروعة، حيث استغلها البعض لأغراض سلبية مستفيدين من قدرتها على تقليص الحدود الجغرافية، وسرعة تنفيذ العمليات وانتشارها، إلى جانب ضعف الأطر القانونية التي تحد من هذه السلوكيات.

ورغم الجهود التي تبذلها السلطات في مختلف الدول، سواء بشكل مستقل أو من خلال التعاون الدولي، للكشف عن الجرائم المعلوماتية والتحقيق فيها بهدف الوصول إلى مرتكبيها ومحاكمتهم لحماية المصلحة العامة والخاصة، فإن هذه الجهود تواجه تحديات قانونية تعرقل تحقيق الأهداف المرجوة.

وفي هذا السياق عمل المشرع الجزائري على وضع إطار قانوني لمواجهة هذه الجرائم، مسترشدا بالتشريعات الدولية ذات الصلة التي تنظم استخدام النظم المعلوماتية وتحد من الاعتداء عليها. ومن هنا تبرز أهمية دراسة موقف المشرع الجزائري في مواجهة هذه التحديات التي تقف عائقا أمام الحد من الجرائم المعلوماتية.

وتشكل عمليات التحقيق وإثبات الجرائم المعلوماتية نقطة انطلاق الإجراءات القانونية، حيث تتعدد أشكال التحديات ويمكن تصنيفها إلى نوعين رئيسيين: تحديات ذات طابع شخصي، وأخرى ذات طابع موضوعي.

وتتمحور إشكالية هذا المقال حول مدى فعالية تدخل المشرع الجزائري في التعامل مع التحديات القانونية المرتبطة بإثبات الجرائم المعلوماتية، ولمعالجة هذا الموضوع سيتم اعتماد المنهج الوصفي لتوضيح المفاهيم المتعلقة بهذه التحديات وأبعادها، إلى جانب المنهج التحليلي من خلال دراسة النصوص القانونية التي وضعها المشرع الجزائري وتحليلها ومناقشتها.

وأخيرا للإجابة على إشكالية المقال ونظرا لخصوصية الموضوع، سيتم اعتماد خطة ثنائية تتضمن مبحثين: الأول يتناول التحديات القانونية ذات الطابع الشخصي، والثاني يركز على التحديات ذات الطابع الموضوعي.

المبحث الأول: التحديات القانونية ذات الطبيعة الشخصية

تُظهر العقوبات القانونية ذات الطابع الشخصي- التي تعرقل إثبات الجرائم المعلوماتية في مشكلات ناتجة عن عوامل تتعلق إما بالضحية أو بالمتهم أو بالجهات المسؤولة عن التحقيق، أو تؤثر على خصوصية حياة المشتبه به أو أطراف أخرى، تتجلى هذه العقوبات في انخفاض معدل الإبلاغ عن الجرائم المعلوماتية، واستخدام المجرمين لوسائل لإخفاء هوياتهم، إلى جانب محدودية المهارات التقنية لدى فرق التحقيق العامة، فضلا عن تعارض إجراءات التحقيق مع حماية الحياة الخاصة.

المطلب الأول: ضعف مستوى التبليغ عن الجرائم المعلوماتية

يعرف التبليغ بأنه إخبار الجهات المختصة بحادثة يجرمها القانون، سواء أصابت هذه الحادثة المبلغ نفسه أو ممتلكاته أو كرامته، أو طالت شخصا آخر أو ممتلكاته أو سمعته، أو حتى استهدفت الدولة أو أملاكها¹.

رغم أهمية التبليغ في كشف الجرائم وملاحقة مرتكبيها وتقديمهم للعدالة، إلا أن اكتشاف الجرائم المعلوماتية غالبا ما يحدث بالمصادفة، فالضحية في هذه الجرائم تميل إلى عدم إبلاغ الجهات المختصة، وحتى عندما تكتشف السلطات الجريمة، فإن الضحية قد لا تتعاون مع التحقيق خوفا من الدعاية السلبية أو فقدان ثقة المساهمين. عادة، تكون الضحية مؤسسة مالية أو بنكاً أو مشروعا صناعيا كبيرا يركز على الحفاظ على سمعته وثقة عملائه أكثر من السعي لكشف الجريمة ومعاقبة الجاني، لذا يفضل الضحية في كثير من الأحيان تقديم تعويض سريع للعميل والتسوية داخليا بطريقة ودية لتجنب خسارته².

يرجع تردد الضحية في الإبلاغ عن الاعتداء الذي تعرض له في الجرائم المعلوماتية إلى عدم وعيه بأن هذه الأفعال تُعد جرائم يمكن معاقبة مرتكبيها وفقا للأنظمة والقوانين المعمول بها، كما يسعى البعض إلى إخفاء طريقة تنفيذ الجريمة لمنع تقليدها من قبل آخرين في المستقبل³.

بالنظر إلى القانون الجزائري نلاحظ غياب تدخل المشرع لمعالجة هذا التحدي ووضع آليات تشجع أو تلزم ضحايا الجرائم المعلوماتية بالإبلاغ عنها، في هذا السياق ندعو إلى ضرورة تدخل المشرع على غرار ما تتبعه التشريعات المقارنة، مثل إدراج شروط في عقود التأمين بين شركات التأمين والمؤمن لهم، تفرض الإبلاغ عن الجريمة المعلوماتية لدى الجهات القضائية كشرط أساسي لتسوية ملفات التعويض عن الأضرار الناتجة عنها، أو إلزام موظفي المؤسسات المالية بالإبلاغ عن أي ثغرات مالية يكتشفونها أثناء عملهم، مع تحديد عقوبات جزائية في حال عدم الالتزام.

¹ - بلقاسم محمد، التبليغ عن جرائم الفساد في الاتفاقيات الدولية واثرة على التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 58 عدد 04، ص 136

² - محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة 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

المطلب الثاني: اعتماد المجرم المعلوماتي لتدابير حماية لإخفاء هويته

يتميز المجرمون المعلوماتيون عادةً بذكاء ومهارة عالية مقارنةً بالمجرمين التقليديين، كما يتسمون بحذر شديد من انكشاف جرائمهم وتعرض سلوكياتهم للفضح. ورغم أن هذا الخوف يشترك فيه معظم المجرمين بمختلف أنواعهم، فإنه يكون أكثر حدة لدى المجرمين المعلوماتيين بسبب ما يترتب على كشف أمرهم من فقدان لوظائفهم أو مكانتهم الاجتماعية. وتساهم طبيعة النظم المعلوماتية ذاتها في تمكينهم من الحفاظ على سرية أفعالهم الإجرامية¹. رغم أن التقنيات المتقدمة في هذا المجال ساهمت في إمكانية تحديد موقع النظام الآلي المستخدم في تنفيذ الأفعال أو السلوكيات التي تشكل الجريمة المعلوماتية محل التحقيق، مما يساعد على كشف الجاني بافتراض أن صاحب الجهاز هو الذي ارتكب الفعل الإجرامي، فإن هذا الافتراض ليس دقيقاً في جميع الحالات. فالتقنيات الحديثة تتيح فقط معرفة مكان وجود الجهاز المعلوماتي، دون أن يكون ذلك كافياً لتأكيد أن صاحب الجهاز هو مرتكب الجريمة.

يسعى المجرم المعلوماتي الماهر إلى إخفاء هويته لمنع تتبعه أو كشف أمره، مما يجعل أنشطته الإجرامية بعيدة عن متناول السلطات المختصة بمكافحة هذه الجرائم. وفي هذا السياق، تتجلى الأساليب التي يتبعها المجرم المعلوماتي، مثل استخدامه لأجهزة معلوماتية لا تخصه، كالحواسيب الموجودة في مقاهي الإنترنت، حيث يتم استخدام هذه الأجهزة دون قيود تتعلق بتسجيل هوية المستخدم. كذلك، يزيد استخدام شبكات الإنترنت اللاسلكية "الواي فاي" من صعوبة تحديد هوية المجرم المعلوماتي².

لتجاوز هذا التحدي، اعتمد المشرع الجزائري نهج التشريعات المقارنة، من خلال فرض التزامات على الجهات المزودة بخدمات الإنترنت والاتصالات. تتضمن هذه الالتزامات تحديد هوية مستخدم الخدمة، وتسجيل البيانات التي تتيح معرفة هوية المستقبل، بالإضافة إلى عناوين المواقع التي تم زيارتها، وتسجيل تاريخ وتوقيت كل اتصال³.

المطلب الثالث: ضعف الخبرات المعلوماتية لهيئات التحقيق ذات الاختصاص العام

تتطلب العدالة الجنائية أن يتمتع أفراد الأجهزة المسؤولة عن المراقبة والاضبط والتحقيق في الجرائم بمستوى عالٍ من المسؤولية لتحديد الجناة والتحقيق معهم. لكن هناك عقبات تواجه عمل هذه الجهات، خاصة لدى الأفراد غير المتخصصين أو من يفكرون إلى الخبرة الفنية في مجال الجرائم المعلوماتية. فهؤلاء، الذين غالباً ما

¹ - غربي بشري، خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، المركز الجامعي مغنية، المجلد 02، العدد 02، ص 105.

² - أنيس حسيب السيد المخلوي، مرجع سابق، ص 91.

³ - المادة 11 من القانون 04-09 المؤرخ في 05-08-2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 47.

سعيد عبد الحميد، سعيد عبد القادر

تقتصر- معارفهم على الجرائم التقليدية كالقتل والسرقة والتزوير، يجدون صعوبة في التعامل مع الجرائم المعلوماتية التي تتطلب مهارات تقنية وفنية متخصصة.

ترداد صعوبة إثبات الجرائم المعلوماتية بسبب محدودية الخبرة التقنية لدى جهات التحقيق المختلفة، بما في ذلك أجهزة الضبط القضائي، خاصة ذات الاختصاص العام، وصولاً إلى جهات الاتهام والتحقيق القضائي. يتجلى هذا النقص في صعوبة تحديد الأدلة المعتبرة قانونياً، والتي تعد حاسمة لإثبات الجريمة المعلوماتية، أو في استخراج هذه الأدلة من النظم المعلوماتية والحفاظ عليها¹.

نستنتج في النهاية أن التعامل مع الجرائم المعلوماتية يتطلب خبرة فنية متخصصة، تقوم عليها جهات تتمتع بكفاءات في أنظمة المعلومات وبصلاحيات الضبط القضائي. وهذا يستلزم إنشاء إدارة خاصة للخبرة والمعاينة في هذا المجال، بدلاً من الاكتفاء بتدريب العاملين في إدارة الخبرة الجنائية العامة. وفي هذا السياق، نلاحظ أن المشرع الجزائري قد أسس الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب القانون 04-09².

أوكلت إلى الهيئة الوطنية مهمة الوقاية من الجرائم المعلوماتية، ودعم السلطات القضائية وأجهزة الشرطة القضائية في تحقيقاتها المتعلقة بهذه الجرائم. لكن هذه الهيئة، وكذلك خبراءها المنتسبون إليها، لا يتمتعون بصفة الضبطية القضائية التي تتيح لهم التدخل المباشر واتخاذ إجراءات الضبط. لذا، ندعو المشرع الجزائري إلى منح الخبراء المعلوماتيين في هذه الهيئة صفة الضبطية القضائية، حيث إن تدخلهم بهذه الصفة سيكون أكثر فعالية في إثبات الجرائم المعلوماتية مقارنةً بأعوان الضبطية القضائية ذوي الاختصاص العام المحددين في قانون الإجراءات الجزائية.

المطلب الرابع : اصطدام إجراءات التحقيق مع حرمة الحياة الخاصة

تُعد الحياة الخاصة ركيزة أساسية لا يجوز التعدي عليها بأي شكل، حتى لو حدث ذلك عن طريق الصدفة، لأنها تمثل جزءاً جوهرياً من كيان الإنسان وشخصيته. ونظراً لهذه الأهمية، منحت التشريعات الوطنية المختلفة الحياة الخاصة مكانة خاصة، معتبرة إياها حقاً أصيلاً لكل فرد، يجب على الأشخاص الطبيعيين والمعنويين احترامه وعدم الاعتداء عليه، وذلك لضمان حماية الإنسان وصون خصوصيته³.

لا يمكن إنكار الأهمية الكبيرة للدليل الرقمي في عملية الإثبات الجنائي، لكن في المقابل، لا يمكن تجاهل تأثيره على الخصوصية المعلوماتية. فالدليل الرقمي، بطبيعته التقنية، يعتمد بشكل رئيسي على أنظمة المراقبة الإلكترونية، التي

1 - جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية: دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2010، ص 92.

2 - المادة 13 من القانون 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، عدد 47.

3 - بلعابد عيدة، الدليل الرقمي بين حماية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق علمية المركز الجامعي تمارست المجلد 11، العدد 01، ص 142.

الجرائم السيبرانية وتحديثها القانونية

تشكل انتهاكها واضحاً للخصوصية. وتتجلى خطورة هذا الانتهاك عندما تؤدي المراقبة الإلكترونية، أثناء البحث عن الأدلة الرقمية، إلى نتائج سلبية، مثل قيام الجهات المختصة بالاطلاع على حسابات المشتبه به الشخصية، بما في ذلك رسائله الخاصة أو حساباته المصرفية، ليتبين لاحقاً عدم وجود أي صلة بين هذه البيانات والجريمة المعلوماتية محل التحقيق¹.

يشند الأمر تعقيداً بسبب ترابط النظم المعلوماتية وتداخلها، حيث قد تمتد عملية البحث لإثبات الجريمة المعلوماتية من نظام المشتبه به إلى أنظمة أخرى مرتبطة به. وهذا التوسع قد ينتهك بشكل مباشر خصوصية أصحاب تلك الأنظمة المعلوماتية والذين لا تربطهم أي صلة بالجريمة المعلوماتية، لا من قريب ولا من بعيد، وإنما وجدوا أنفسهم مرتبطين بنظام المشتبه به بطريقة ما في هذا السياق، سعى المشرع الجزائري إلى تحقيق توازن بين حماية الخصوصية المعلوماتية وضرورة المصلحة العامة في مكافحة الجرائم المعلوماتية من خلال تنظيم إجراءات المراقبة الإلكترونية. وقد وضع المشرع ضوابط قانونية لضمان تحقيق هذه المصلحة مع الحفاظ على مستوى مناسب من الخصوصية. من بين هذه الضوابط ما نص عليه القانون 04-09، الذي حدد الحالات التي يجوز فيها استخدام المراقبة الإلكترونية²:

- 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.
- لملتقيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

حرص المشرع الجزائري، في الإطار ذاته، على وضع ضوابط محددة لتنفيذ إجراءات المراقبة الإلكترونية، من أبرزها اشتراط الحصول المسبق على إذن مكتوب من الجهة القضائية المختصة. كما خصص أحكاماً دقيقة للحالة التي يسمح فيها باللجوء إلى هذا النوع من المراقبة، من حيث تحديد الجهة المخولة بمنح الترخيص، ومدته الزمنية، إلى جانب الضوابط التقنية الواجب اتباعها، وذلك استناداً إلى ما نصت عليه الفقرتان 6 و 7 من المادة 4 من القانون رقم 04-09.

وبناء على ذلك، يستنتج أن أي مراقبة إلكترونية تنفذ خارج هذه الضوابط تعد غير قانونية، سواء تعلق الأمر بغياب الترخيص القضائي، أو تنفيذ الإجراء في غير الحالات المحددة قانوناً، أو تجاوز المدد المنصوص عليها،

¹ - بلعابد عيدة، مرجع سابق، ص 145.

² - المادة 04 من القانون 04-09 المؤرخ في 05-08-2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 47.

سواء تلك الواردة في القانون 04-09 أو المدد المقررة في قانون الإجراءات الجزائية، والتي تُحدد بأربعة أشهر قابلة للتجديد بحسب ظروف كل قضية¹.

المبحث الثاني: التحديات القانونية ذات الطبيعة الموضوعية

تتمثل أبرز التحديات القانونية ذات الطابع الموضوعي التي تعيق عملية إثبات الجريمة المعلوماتية في إشكاليات ناتجة عن خصائص هذه الجريمة نفسها، وليس عن عوامل شخصية. إذ تُعزى هذه الصعوبات إلى طبيعة الجريمة المعلوماتية وما ينجم عنها من آثار، حيث تتجلى في انعدام أو محدودية الأدلة المادية، وسهولة طمسها أو محوها في حال وجودها، إلى جانب خصوصية البيئة الرقمية التي تُرتكب فيها هذه الجرائم. كما تزداد الصعوبة نتيجة ضخامة حجم البيانات الواجب تحليلها أثناء التحقيق، بالإضافة إلى عدم ملائمة الآليات التقليدية للتحقيق مع خصوصيات الجرائم المعلوماتية، الأمر الذي يستدعي تطوير أدوات وإجراءات أكثر توافقاً مع هذا النوع المستحدث من الإجرام.

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

نظراً للطابع الخاص للجرائم المعلوماتية، يكتنف إثباتها جملة من الصعوبات. من أبرز هذه التحديات صعوبة الكشف عنها لغياب الآثار المادية التقليدية، إذ لا يصحبا استعمال للعنف بأشكاله المعهودة كالاغتداء الجسدي أو اقتحام الممتلكات. فهذه الجرائم تعتمد بالأساس على مهارات تقنية ومعالجات رقمية، وتقوم على بيانات وأرقام مخزنة إلكترونياً يمكن تعديلها أو محوها بسهولة في سجلات الحواسيب، لذلك لا تترك غالباً أثراً خارجياً مرئياً يمكن الاعتماد عليه في الإثبات².

يشكل سهولة إخفاء الأدلة أو محوها أو تلافيها أحد التحديات الجوهرية في إثبات الجرائم المعلوماتية. فالجناة يعتمدون تقنيات تلاعب دقيقة وغير مرئية في النبضات والذبذبات الإلكترونية التي تُخزن من خلالها البيانات، مما يتيح لهم حذف أو تعديل آثار الجريمة خلال فترات زمنية وجيزة قد لا تتجاوز دقائق أو أجزاء من الدقيقة، ونظراً لهذه السرعة والدقة في طمس الأدلة، قد تصل معلومات وقوع الجريمة إلى جهات الضبط متأخرة بحيث يصبح من الصعب أو المستحيل استرجاع الآثار اللازمة لإثبات التهمة³.

وفي سياق التصدي لأحد أبرز التحديات التي تعيق إثبات الجريمة المعلوماتية، والمتمثل في سهولة محو أو إتلاف الأدلة الرقمية، حتى وإن تم ذلك داخل الأنظمة المعلوماتية التابعة للجنة أو الضحايا، جاء تدخل المشرع الجزائري من خلال القانون رقم 04-09، ليضع التزاماً صريحاً على عاتق مقدمي خدمات الاتصالات الإلكترونية،

¹ - المادة 65 مكرر 7 ف 2 من الأمر 155-66 المؤرخ في 08-06-1966 المعدل والمتمم والمتضمن قانون الإجراءات الجزائية، ج ر عدد 48

² - محمد علي العريان، مرجع سابق، ص 53.

³ - بنية حبابتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، جامعة قسنطينة، عدد 50، ص 17.

الجرائم السيبرانية وتحديثها القانونية

يلزمهم قانونا بالاحتفاظ بجملة من البيانات التقنية ذات الطابع الحاسم في تتبع النشاط المعلوماتي وتحديد المسؤولين.

ويشمل هذا الالتزام حفظ كل المعطيات التي تتيح التعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة في الاتصال، فضلا عن الخصائص التقنية لكل اتصال، بما في ذلك تاريخه وتوقيته ومدته، إلى جانب البيانات المرتبطة بالخدمات التكميلية المستعملة وهوية مقدميها، وكذلك المعلومات التي تسمح بتحديد هوية المرسل أو المرسل إليه، وعناوين المواقع الإلكترونية التي تم الولوج إليها، ويمثل هذا الإجراء آلية وقائية هامة تهدف إلى ضمان قابلية استرجاع الأدلة الرقمية عند الاقتضاء، وتمكين سلطات التحقيق من ملاحقة مرتكبي الجرائم المعلوماتية، رغم الطابع المتغير والزائل للمادة الجرمية الرقمية¹.

إن الزام المشرع الجزائي لمقدمي الخدمات بحفظ كل المعطيات المذكورة أعلاه، يساهم ولو بشكل نسبي في الحفاظ على الآثار التقنية على مستوى البيانات 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 بوجه عام على أنه الحيز المكاني الذي شهد ارتكاب الجريمة كليا أو جزئيا، ويمثل المجال الذي يترك فيه الجاني أثارا مادية أو رقمية، ظاهرة أو خفية، يمكن أن تسهم في الكشف عن طبيعة الفعل المرتكب وظروفه. ويُعد هذا الفضاء عنصراً جوهرياً في عملية الإثبات الجنائي، لما يوفره من دلائل مادية تستدعي تدخل فرق متخصصة من المحققين الجنائيين والخبراء التقنيين، قصد جمع القرائن وتحليلها وفك شيفرة الملابس المحيطة بالجريمة موضوع التحقيق².

مع التطور المتسارع في مجال شبكات المعلومات، انتفت الحدود الجغرافية التقليدية أمام انتقال وتداول البيانات، حيث أضحت النظم والتجهيزات المعلوماتية قادرة على تبادل كميات ضخمة من المعلومات بين أطراف تفصل بينها مسافات شاسعة تمتد عبر قارات مختلفة، وقد ترتب على هذه الخصوصية التقنية أن أصبحت الجريمة المعلوماتية ذات امتداد عابر للحدود، بحيث يمكن أن تستهدف في الوقت ذاته أنظمة وكيانات اقتصادية أو مؤسسية تقع في دول متعددة، مما يعقد من مهمة التتبع والتحقيق ويثير إشكاليات قانونية تتعلق بتحديد الاختصاص القضائي وسرعة التعاون الدولي في مجال مكافحة هذا النمط من الإجرام المستحدث³.

¹ - المادة 11 من القانون 04-09 المؤرخ في 05-08-2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 47.

² - ميهوب يوسف وربطاب عز الدين برتوكول معاينة الطبيب الشرعي لمسرح الجريمة، مجلة دراسات وأبحاث جامعة الجلفة، المجلد 7، العدد 21، ص 482

³ - طارق ابراهيم السوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الاسكندرية، ص 172.

سعيد عبد الحميد، سعيد عبد القادر

وتعزيزاً لما تم بيانه سابقاً، فإن تعقيد إثبات الجريمة المعلوماتية يبلغ ذروته عندما يكون مسرح هذه الجريمة هو شبكة الإنترنت، حيث يغدو ضبط الدليل الرقمي والبحث عنه مهمة شاقة، وقد تكون في بعض الأحيان شبه مستحيلة، ويعزى ذلك إلى الطابع العابر للحدود الذي يميز الفضاء السيبراني والذي يستلزم في كثير من الحالات تنفيذ إجراءات التفتيش أو الضبط خارج الإقليم الوطني، أي داخل أراضي دولة أجنبية، وهو ما يفرض ضرورة الحصول على إذن مسبق من سلطات تلك الدولة المعنية، نظراً لما يشكله هذا النوع من الإجراءات من مساس بسيادتها.

وعلاوة على ذلك، قد تفضي- هذه العمليات إلى المساس بحقوق وخصوصيات أشخاص لا علاقة لهم بالفعل الجرمي، باعتبار أن البيانات أو المعلومات المستهدفة بالتفتيش قد تكون مرتبطة بأطراف ثالثة، مما يثير إشكالات قانونية دقيقة تتعلق بمدى مشروعية الإجراء وحدوده ومدى احترامه للضمانات القانونية المكفولة للأفراد¹.

وفي هذا الإطار، وللتغلب على التحديات الناجمة عن الطابع العابر للحدود لمسرح الجريمة المعلوماتية، يتعين على الدول، من خلال سلطاتها القضائية والأمنية المختصة، التنسيق المسبق فيما بينها عبر إبرام اتفاقيات تعاون أمني وقضائي متخصصة في مكافحة هذا النوع من الجرائم. يهدف هذا التنسيق إلى تعزيز سرعة وكفاءة التدخل لإثبات الجريمة المعلوماتية والقبض على مرتكبيها.

وقد جسد المشرع الجزائري هذا المبدأ من خلال أحكام القانون رقم 04-09 المتعلق بالوقاية من تكنولوجيات الإعلام والاتصال، حيث نصت الفقرة الثالثة من المادة الخامسة على وجوب التعاون مع السلطات المختصة في الدول الأجنبية ضمن إطار الاتفاقيات ذات الصلة، وذلك وفق مبدأ المعاملة بالمثل.

وتتسق هذه القواعد مع ما ورد في اتفاقية بودابست، التي أكدت على ضرورة تعاون جميع الأطراف لتطبيق الوسائل الدولية المناسبة للتعاون الدولي في المجال الجنائي، واستحداث ترتيبات تستند إلى تشريعات موحدة ومتبادلة. كما شددت الاتفاقية على أهمية التعاون على المستوى الوطني بأوسع نطاق ممكن، بهدف تسهيل التحقيقات والإجراءات المتعلقة بالجرائم المعلوماتية، وبخاصة تلك المتعلقة بالحصول على الأدلة الرقمية ذات الصلة².

المطلب الثالث: كبر حجم البيانات التي يتعين البحث فيها

تتميز الأنظمة المعلوماتية، مهما اختلفت أنواعها، بقدرتها الهائلة على تخزين كم هائل من البيانات يعادل مئات آلاف الصفحات الورقية. وللتوضيح، إذا أتيح لسلطات الضبط والتحقيق طباعة محتويات قرص صلب واحد، فإن ذلك يتطلب موارد ضخمة من الأوراق والوقت، وقد تفضي- هذه العملية، رغم الجهد المبذول، إلى

¹ - أليس حسيب السيد المحلاوي مرجع سابق، ص 97.

² - المادة 23 من اتفاقية بودابست المتعلقة بالجريمة الالكترونية، الموقعة بتاريخ 22 نوفمبر 2001 الصادرة في إطار مجلس أوروبا.

الجرائم السيبرانية وتحديثها القانونية

نتائج سلبية في الكشف عن الأدلة الجنائية المرجوة. ويرجع ذلك أساسا إلى غياب آليات فعالة لفرز وتصنيف الملفات المخزنة بشكل ذاتي، مما يصعب على المحققين التمييز بين الملفات المشروعة وتلك غير المشروعة أو المرتبطة بالجريمة موضوع التحقيق¹.

يشكل الكم الهائل من البيانات المتداولة والمخزنة في الأنظمة المعلوماتية إحدى العقبات الرئيسية التي تعترض سير التحقيقات وإثبات الجرائم المرتكبة بواسطة هذه الأنظمة أو من خلالها. فعادة ما يتطلب الكشف عن الأدلة الرقمية في جهاز حاسوب واحد إجراء فحص دقيق وشامل لمحتويات آلاف الملفات المخزنة في ذاكرته، وهو ما يستلزم وقتا طويلا وجهدا كبيرا من المحققين. وينعكس هذا العبء على فعالية عمل سلطات البحث والتحقيق، إذ قد يؤدي طول هذه العملية إلى شعور المحققين بالإرهاق والملل، مما قد يحد من عزمهم على مواصلة جمع الأدلة والتحريات اللازمة لإثبات الجريمة المعلوماتية موضوع التحقيق².

في الواقع، لم يتدخل المشرع الجزائري بشكل مباشر لمعالجة التحدي الموضوعي المرتبط بكم البيانات المرتبطة بالجريمة المعلوماتية، إذ ترك هذا الأمر لتقدير سلطات الاستدلال بناء على ظروف كل قضية على حدة. ويعد هذا الموقف منطقيا، باعتبار أن جوهر هذا التحدي ينبع من طبيعة تقنية بحتة، تستوجب إيجاد حلول تقنية للتعامل معها، بدلا من محاولات تنظيمها عبر الأطر القانونية، التي قد لا تكون كافية لمعالجتها بشكل فعال.

المطلب الرابع : عدم تناسب إجراءات التحقيق الكلاسيكية مع الجرائم المعلوماتية

يعتبر التطور السريع والمستمر في المجال المعلوماتي أحد أبرز التحديات التي تعترض جهود مكافحة الجرائم المعلوماتية والتحقيق فيها بفعالية. إذ تظهر يوميا تقنيات وأساليب جديدة للقرصنة والاختراق والاحتيال الرقمي، تتسم بالتعقيد والابتكار، مما يصعب على الجهات المختصة مواكبتها والتصدي لها بشكل مناسب. وقد أدى هذا التطور المتسارع إلى بروز ما يعرف بـ «الطوفان الرقمي»، الذي يشير إلى الكم الهائل والمتزايد من البيانات والمعلومات المتداولة عبر الشبكات الرقمية، مما يضاعف من تعقيد مهمة مكافحة الجريمة المعلوماتية³.

ولا يقتصر الأمر على قصور النصوص العقابية في مواجهة الجرائم المعلوماتية، بل يمتد إلى التشريعات الإجرائية أيضا، حيث إن غالبية إجراءات التحقيق والمتابعة المنصوص عليها في القوانين التقليدية لا تتناسب مع خصوصية الجرائم المعلوماتية وطبيعتها التقنية. وفي بعض الأحيان، تتعارض هذه الإجراءات مع الوسائل التقنية

¹ - أنيس حسيب السيد المحلاوي، مرجع سابق، ص 96.

² - براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه في القانون، جامعة تيزيوزو، 2018، ص 218

³ - حوالم حليمه ومهاجي فاطمة الزهراء، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، جامعة سعيدة، مجلد 03، عدد 16، ص 145.

المستخدمة في ارتكاب الجرائم التي تستهدف المعلومات أو البيانات بمختلف أشكالها، مما يشكل عائقاً جوهرياً يعيق عمل سلطات التحقيق ويجد من فعاليتها في كشف الجريمة وملاحقة مرتكبيها¹.

يتجلى المعنى المشار إليه أعلاه بوضوح من خلال مجموعة من التطبيقات الإجرائية، لا سيما فيما يتعلق بإجراءات التفتيش، التي تختلف طبيعتها في الجرائم المعلوماتية عنها في الجرائم التقليدية. إذ يتم في الجرائم المعلوماتية إجراء التفتيش على الكيانات المنطقية للنظم المعلوماتية، والتي تشمل البرامج والبيانات، وهي عناصر معنوية وغير مادية بطبيعتها. وبما أن إجراءات التفتيش تقليدياً تستهدف ضبط العناصر المادية المرتبطة بالجريمة، فإن هذا التعريف المادي لا يتناسب مع خصوصية الكيانات المنطقية، التي لا يمكن ضبطها وتفتيشها إلا بعد تحويلها إلى شكل مادي محسوس، مثل طباعتها على ورق أو تخزينها على وسائل مادية قابلة للحجز والتفتيش.

وفي سياق متصل نص المشرع الجزائري، وفقاً للقواعد العامة للإجراءات الجزائية، على مجموعة من الضوابط التي تحكم إجراء التفتيش، ومنها إلزامية حضور صاحب المسكن موضوع التفتيش أو من يمثله، إضافة إلى حضور شاهدين عند الاقتضاء، وهو ما يضمن احترام الضمانات القانونية أثناء تنفيذ هذه الإجراءات² رغم أن هذه الضوابط تتلاءم مع طبيعة عمليات التفتيش المادي التقليدية، إلا أنها لا تجد مبرراً كافياً في سياق الجرائم المعلوماتية، خصوصاً عندما تتم عمليات التفتيش عن بعد عبر شبكات الاتصال المختلفة. ومن هذا المنطلق، نرى ضرورة دعوة المشرع إلى استثناء إجراءات التفتيش عن بعد في الجرائم المعلوماتية من تطبيق الضوابط المنصوص عليها في المادة 45 من قانون الإجراءات الجزائية، وذلك تماشياً مع خصوصية البيئة الرقمية ومتطلباتها التقنية الفريدة.

ومن جهة أخرى، وبخصوص مسألة التقادم، فإنها تحسب وفق القواعد العامة، حيث يبدأ احتسابها من تاريخ ارتكاب السلوك المادي للجريمة، مما يطرح تحديات خاصة في الجرائم المعلوماتية التي قد تدسم بطابع مستمر أو خفي يصعب تحديد وقت وقوعها بدقة³، على الرغم من أن اكتشاف الجريمة يكون عادة مصاحباً أو قريباً من تاريخ ارتكاب السلوك المادي لها، إلا أن هذا المبدأ لا ينطبق في أغلب الأحيان على الجرائم المعلوماتية، نظراً لغياب الآثار المادية الظاهرة الناتجة عن ارتكابها، فضلاً عن إجماع الضحايا المتضررين عن الإبلاغ عن الاعتداءات التي لحقت بهم جراء هذه الجرائم. هذا الأمر يؤدي إلى مرور فترة زمنية طويلة بين تاريخ ارتكاب الفعل الإجرامي وتاريخ اكتشافه، وهي فترة قد تمتد إلى حد التقادم الخاص بالجريمة موضوع البحث، مما يتيح للمجرم المعلوماتي التملص من الملاحقة القضائية.

¹ - براهيمي جمال، مرجع سابق، ص 145

² - المادة 45 من الأمر 155-66 المؤرخ في 08-06-1966 المعدل والمتمم والمتضمن قانون الإجراءات الجزائية، ج ر عدد 48.

³ - المادة 07 و 08 و 09 من الأمر 155-66 المؤرخ في 08-06-1966 المعدل والمتمم والمتضمن قانون الإجراءات الجزائية

الجرائم السيبرانية وتحديثها القانونية

وبناء عليه، نرى ضرورة دعوة المشرع الجزائري إلى اعتماد قاعدة إجرائية خاصة بالتقادم في الجرائم المعلوماتية، بحيث يبدأ حساب مدة التقادم من تاريخ اكتشاف الفعل الإجرامي وليس من تاريخ ارتكابه، بما يحقق التوازن بين حقوق الضحايا وفعالية العدالة الجنائية في مواجهة هذه الجرائم الحديثة.

خاتمة:

في ختام هذا البحث، يتبين أن المشرع الجزائري بذل مجهودا ملحوظة لمعالجة التحديات القانونية المتعلقة بإثبات الجريمة المعلوماتية من خلال إصدار القانون رقم 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. فقد تمكن إلى حد بعيد من التخفيف من حدة هذه الإشكالات، مع وجود بعض التحفظات التي يمكن تلخيصها كما يلي:

1. يلاحظ غياب تدخل تشريعي لمعالجة مشكلة ضعف التبليغ عن الجرائم المعلوماتية، وعدم توفير آليات تحفيزية أو إلزامية لضحايا هذه الجرائم للقيام بالتبليغ عنها.
2. وفي سبيل مواجهة إشكالية إخفاء هوية المجرم المعلوماتي، فرض المشرع الجزائري على مزودي خدمات الإنترنت والاتصال تقديم معلومات تفصيلية للسلطات المختصة تشمل هوية مستخدمي الخدمة، والبيانات المتعلقة بالمرسل إليهم، وعناوين المواقع التي تم الاطلاع عليها، إلى جانب تحديد تاريخ ووقت كل اتصال.
3. أنشأ المشرع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التي تعهد إليها بمهام الوقاية والمساعدة في التحريات، إلا أن هذه الهيئة وخبرائها لا يتمتعون بصفة الضبطية القضائية، مما يحد من صلاحياتهم في التدخل المباشر.
4. سعيا لتحقيق توازن بين حماية الحياة الخاصة والحاجة إلى مكافحة الجرائم المعلوماتية، وضع المشرع ضوابط صارمة لإجراءات المراقبة الإلكترونية، من بينها حصر الحالات المسموح بها والحاجة إلى ترخيص قضائي مكتوب.
5. خصص المشرع أحكاما خاصة بتنظيم جهة منح ترخيص المراقبة الإلكترونية، والآجال، والترتيبات التقنية المتعلقة بها، لا سيما في الجرائم ذات الطابع الإرهابي أو التي تمس أمن الدولة.
6. لمواجهة تعقيدات مسرح الجريمة المعلوماتية، أكد المشرع على أهمية التعاون الدولي من خلال اتفاقيات أمنية وقضائية، بما يتوافق مع مبدأ المعاملة بالمثل، لتعزيز فعالية التحقيقات.
7. تظهر صعوبة ملائمة إجراءات التحقيق التقليدية مع خصوصيات الجرائم المعلوماتية، حيث تعارض أحيانا الوسائل التقليدية طبيعة الوسائل التقنية المستخدمة في ارتكاب هذه الجرائم، مما يشكل عقبة أمام تحقيق العدالة.

8. يساهم إلزام مقدمي الخدمات بحفظ معطيات تقنية محددة في الحفاظ على آثار رقمية يمكن الاعتماد عليها في إثبات الجريمة، حتى في حال محاولة محوها أو إتلافها.
- وعليه، نقدم التوصيات التالية:

1. في سبيل معالجة ضعف التبليغ، نوصي المشرع بالاستفادة من التجارب المقارنة، مثل تضمين بنود في عقود التأمين تلزم بالتبليغ عن الجرائم المعلوماتية قبل صرف التعويضات، أو إلزام موظفي المؤسسات المالية بالإبلاغ عن الثغرات المالية التي يكتشفونها تحت طائلة العقوبات الجزائية.
2. ندعو إلى منح صفة الضبطية القضائية للخبراء المعلوماتيين التابعين للهيئة الوطنية، لما يتمتعون به من كفاءة تقنية تسهم في تحقيق أكثر فعالية في التحقيقات.
3. نوصي باستثناء إجراءات التفتيش عن بعد في الجرائم المعلوماتية من الضوابط التقليدية المنصوص عليها في المادة 45 من قانون الإجراءات الجزائية، نظرا لخصوصية هذا النوع من التفتيش.
4. اقترح تخصيص حكم إجرائي خاص يتعلق بالتقادم في الجرائم المعلوماتية، يبدأ من تاريخ اكتشاف الفعل الإجرامي، لا من تاريخ ارتكابه، لتعزيز مبدأ العدالة وفعالية ملاحقة مرتكبي هذه الجرائم.

المصادر والمراجع:

الكتب:

1. أنيس حسيب السيد المحلاوي الخبرة القضائية في الجرائم المعلوماتية والرقمية، دراسة مقارنة دار الفكر الجامعي الاسكندرية 2016.
2. جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية: دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2010.
3. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية.
4. غانم مرضي الشمري، الجرائم المعلوماتية، الطبعة الأولى الدار العلمية الدولية النشر والتوزيع، عمان، 2016.
5. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية، 2004.

الرسائل الجامعية:

6. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية: دراسة مقارنة، رسالة لنيل درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.
7. براهمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه في القانون، جامعة تيزوزو، 2018.

المجلات العلمية:

8. -بلقاسم محمد، التبليغ عن جرائم الفساد في الاتفاقيات الدولية وأثره على التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 58 عدد 04.

الجرائم السيبرانية وتحديثها القانونية

9. غريبي بشرى خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، المركز الجامعي مغنية، المجلد 02، العدد 02.
10. بلعابد عيدة الدليل الرقمي بين حتمية الاثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق علمية المركز الجامعي تلمسان المجلد 11، العدد 01.
11. بشينة حباتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، جامعة قسنطينة، عدد 50.
12. ميهوب يوسف وريطاب عز الدين برتوكول معاينة الطبيب الشرعي لمسرح الجريمة، مجلة دراسات وأبحاث جامعة الجلفة، المجلد 7، العدد 21.
13. حوالف حليلة ومحاجي فاطمة الزهراء، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، جامعة سعيدة، مجلد 03، عدد 16.

القوانين:

14. القانون 04-09 المؤرخ في 05-08-2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 47.
15. الأمر 155-66 المؤرخ في 08-06-1966 المعدل والمتمم والمتضمن قانون الإجراءات الجزائية، ج ر عدد 48.

الاتفاقيات:

16. المادة 23 من اتفاقية بودابست المتعلقة بالجريمة الالكترونية، الموقعة بتاريخ 22 نوفمبر 2001 الصادرة في إطار مجلس أوروبا.