

انتهاك الجرائم الإلكترونية للحق في الخصوصية

من منظور القانون الدولي

Cybercrime violation of the right to privacy under international law

يحي عبد الرحمن*، مخبر التطبيقات التكنولوجية الحديثة على القانون، كلية الحقوق والعلوم السياسية

جامعة لمين دباغين - سطيف 2-

yahia.arahmane@gmail.com

قرقرور نبيل، مخبر التطبيقات التكنولوجية الحديثة على القانون، كلية الحقوق والعلوم السياسية

جامعة لمين دباغين - سطيف 2-

nabil201334@gmail.com

تاريخ إرسال المقال: 2024/03/08 تاريخ قبول المقال: 2024/04/09 تاريخ نشر المقال: 2024/05/18

الملخص:

نعالج من خلال هذا البحث مسألة بالغة الأهمية في الوقت الحالي، تتمثل في كثرة الهجمات الإلكترونية لا سيما مع الانتشار الواسع للأدوات التكنولوجية التي تستغل بشبكة الأنترنت، وهذا ما أفرز العديد من المخاطر والتهديدات على الحق في الخصوصية، حيث يلجأ القراصنة إلى اختراق شبكات الأنترنت وما تحتويه من بريد الكتروني وحسابات شخصية قصد الاستلاء على معلومات خاصة بهم، لغرض مادي أو قصد استغلال تلك المعلومات من أجل الإضرار بأصحابها أو ابتزازهم، وهذا ما أفرز العديد من الآثار على خصوصية ضحايا هذه الهجمات الإلكترونية، وما زاد من خطورة المسألة هو أن بعض الدول أصبحت تقف هي الأخرى وراء العديد من الهجمات الإلكترونية مستهدفة بذلك دولا أخرى أو أشخاص معنوية أو طبيعية، كما حدث مع روسيا وإسرائيل اللتان أصبحتا تستخدم الهجمات السيبرانية ضد خصومها من الدول والأشخاص أو باقي الكيانات الأخرى، إضافة إلى الحرب التجارية والاقتصادية بين الصين والولايات المتحدة الأمريكية التي أخذت أبعادا أخرى في إطار المجال السيبراني.

الكلمات المفتاحية: انتهاك - الإلكترونية - الخصوصية - الدولي.

Abstract

Through this research, we are addressing a very important issue, distinguished by the cyber attacks, especially with the wide spread of technological tools that operate on the internet, that resulted in many risks and threats to the right to privacy, as hackers resort to hacking the internet

* المؤلف المرسل

networks and personal accounts in order to seize their private information, for a physical purpose or with the intention of exploiting that information in order to harm or blackmail its owners, this has resulted in many impacts on the privacy of victims of these cyber-attacks, what has increased the seriousness of the issue is that some countries have become the other behind many cyber attacks Targeting other countries or legal persons, as happened with Russia and Israel, which have begun to use cyber attacks against their opponents from other countries, in addition to the trade and economic war between China and the United States of America, which has taken on other dimensions within the cyber sphere.

Key words: Violation - cybercrime- privacy - international.

المقدمة:

أصبح الفضاء الإلكتروني يستخدم على نطاق واسع في أغلب مظاهر الحياة اليومية للأفراد، سواء على مستوى الأفراد أو على المستوى الرسمي، حيث باتت الحكومات تنتهج ما يسمى "بالحكومات الإلكترونية" والتي تعني التسيير الرقمي لمختلف شؤون الدولة من إدارات عمومية وهيئات وغيرها. وقد أفرز هذا الوضع الجديد العديد من التحديات ذات الصلة باستخدام شبكة الإنترنت والوسائل التكنولوجية المرتبطة بها، أبرزها انتهاك أسرار الدول إضافة إلى خصوصية الأفراد نتيجة للجرائم الإلكترونية المختلفة التي ينفذها الأفراد (القراصنة)، أو جهات تدعمها الدول كما حدث مع استونيا عام 2008 حينما تعرضت لهجوم سيبراني من طرف روسيا نتج عنه شلل شبه كلي لمختلف مظاهر التسيير الحكومي آنذاك.

والسبب في ذلك هو سهولة شن مثل هذه الهجمات نتيجة للترابط الكبير بين الشبكات إضافة إلى ضعف أمن العديد منها، وهذا ما يعرض خصوصية الأفراد إلى خطر الاختراق، وهذا على الرغم من أن هذا الحق يعد من الحقوق الأساسية للأفراد التي يستوجب على الدول حمايتها بكل الوسائل من كل ما يهددها، وفي مقدمة ذلك الجرائم الإلكترونية التي أصبحت تشكل أكبر خطر على الحق في الخصوصية. وما زاد من حدة الاعتداءات والجرائم السيبرانية وتداعياتها الخطيرة على حقوق الأفراد لا سيما الحق في الخصوصية، هو انتشار الأدوات التكنولوجية في المجتمعات إضافة إلى انتهاج غالبية الدول لرقمنة مختلف القطاعات، خاصة في ظل عدم مواكبة بعض التشريعات للتطورات الحاصلة في مجال التكنولوجيا والذكاء الاصطناعي وغيرها من أوجه التكنولوجيا الأخرى التي أصبحت في متناول الجميع.¹

وبالتالي فإن حماية الأفراد في الفضاء السيبراني يستوجب إبرام العديد من الصكوك الدولية ذات الصلة، وذلك كي يتسنى توفير حماية فعالة لمستخدمي تكنولوجيات الاعلام والاتصال، لاسيما بعد التطور الذي وصل إليه الذكاء الاصطناعي بمختلف تطبيقاته التي ما فتئت تنتشر في المجتمعات، إلى درجة أن أصبحت من الأدوات الفردية التي لا يمكن للأفراد الاستغناء عنها في العديد من جوانب الحياة اليومية. ومن هذا المنطلق، فإن حق مستخدمي الفضاء السيبراني في حمايتهم من مختلف التهديدات التي يمكن أن يتعرضوا لها، باتت ضرورة ملحة تفرض نفسها على المجتمع الدولي كافة، بما في ذلك الحكومات،

لذلك تم استحداث اتفاقيات دولية لمواجهة هذه التحديات من بينها: اتفاقية بودابست لمكافحة الجريمة الإلكترونية لسنة 2001، الاتفاقية الإفريقية حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2000، وقد سارت التشريعات المقارنة لمختلف الدول على هذا المنوال من خلال اعتماد مضمون هذه النصوص الدولية في تشريعاتها الداخلية، فضلا عن سن قوانين داخلية نابعة من رؤية السياسة التشريعية لكل دولة.

ولمعالجة المسألة سألنا الذكر طرح التساؤل التالي:

- ماهي الآثار التي يمكن أن ترتبها الجرائم الإلكترونية على الحق في الخصوصية؟ وما موقف قواعد القانون الدولي من ذلك ؟

وقصد الإجابة عن إشكالية الدراسة نتبع المنهج التحليلي لتسليط الضوء على الآثار المترتبة عن انتهاك الصكوك الدولية المنظمة لاستخدام شبكة الأنترنت بصفة عامة، سواء أكانت اتفاقيات ثنائية أو إقليمية أو دولية متعددة الأطراف.

1- ماهية الحق في الخصوصية وأثر التكنولوجيا الحديثة عليه

1.1- مفهوم الحق في الخصوصية

يقصد بالخصوصية لغة حالة الخصوص، والخصوص نقيض العموم،² أما من الناحية الاصطلاحية فيقصد بها حق الفرد في الاستئثار بسرية شؤونه الخاصة، سواء تعلق الأمن بكيانه المادي والمعنوي كصورته وسمعته أو بمحيطه الذي يعيش فيه كبيته ومن يشاركه فيهم أفراد أسرته وحياته الخاصة في إطار الفضاء الأسري، كما يمكن تعريفه بأنه حق الفرد في حماية معلوماته ومعطيات الشخصية من الاطلاع عليهما دون إذن منه، ويكتسي الحق في الخصوصية أهمية بالغة باعتباره حقا من حقوق الإنسان، مكرس في مختلف الاتفاقيات الدولية.

ومعنى ذلك أن الحق في الخصوصية يتضمن العديد من العناصر التي يسميها البعض بمظاهر أو صور الحق في الخصوصية، والتي نوجزها في: حرمة المسكن، حرية المراسلات والاتصالات، حق حماية البيانات الشخصية، فكل هذه المسائل تدخل ضمن نطاق خصوصية الفرد، بحيث إذا ما تم انتهاكها أو خرقها نكون بصدد الاعتداء على حق خصوصية هذا الفرد أو ذاك.

أما فيما يتعلق بخصوصية الأفراد في المجال الرقمي، فتقتضي حماية معطياتهم ذات الطابع الشخصي من السرقة أو الاختراق سن نصوص قانونية لضمان تلك الحماية، لذلك دفعت الجريمة الإلكترونية بالمشروع نحو حماية المعطيات الشخصية باعتماد ترسانة من النصوص القانونية، وذلك نظرا لتزايد اعتماد الهيئات العامة والخاصة في أداء مهامها وجميع نشاطاتها على أجهزة الحاسوب وشبكات الأنترنت، إلى جانب شيوع استخدام تكنولوجيا المعلومات في مختلف المعاملات الإدارية والمالية والصحية

وغيرها.³ وذلك في إطار استراتيجية الدول الرامية إلى تعميم رقمنة التسيير الإداري لهيئاتها ومؤسساتها الرسمية.

وهذا ما زاد من حجم المعطيات الشخصية والقائمين عليها وأغراض حمايتها، الأمر الذي يؤدي إلى تعاضم المخاطر التي تهدد الحياة الخاصة للأفراد من خلال معالجة معطياتهم ذات الطابع الشخصي (données à caractère personnel) أو كما يحب البعض تسميتها المعطيات الشخصية (données personnelles)، حيث عرفها المشرع الجزائري في المادة 03 الفقرة 01 من القانون 18-17 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخص على أنها: "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معروف أو قابل للتعرف عليه ...".⁴

وقد انتشرت تكنولوجيا المعلومات والاتصالات بشكل عملي في جميع جوانب الحياة، وكانت أولوية الوصول إليها تعتبر في بداية الأمر ضرباً من الرفاهية، وقد صار من المتفق عليه حالياً أن الاستثمار في الوصول الميسور التكلفة إلى تكنولوجيا المعلومات والاتصالات ضروري لتحقيق أهداف التنمية المستدامة، إلا أن النجاحات والإخفاقات المختلفة لتكنولوجيا المعلومات والاتصالات أظهرت أن التكنولوجيا نفسها ليست إيجابية ولا سلبية أو محايدة بالضرورة،⁵ وهذا ما يتطلب فرض رقابة دائمة ومستمرة على استخدام التكنولوجيا الرقمية قصد تجنب أي إساءة لاستخدامها.

ومن بين إيجابيات التكنولوجيات الحديثة نشر ثقافة حقوق الإنسان والترويج للمسائل ذات الصلة، فتقاسم المعلومات ونقلها يؤدي إلى إتاحة فرص كثيرة من أجل الترويج لقضايا حقوق الإنسان،⁶ ونشر كل ما له علاقة بترقية وتطوير حقوق الإنسان في أي منطقة يراد تسليط الضوء على وضعية حقوق الإنسان فيها، بالإضافة إلى إمكانية استخدام التكنولوجيا الرقمية بصفة عامة كآلية للإنذار المبكر عن أي انتهاك لحقوق الإنسان في أي منطقة من العالم خاصة تلك التي تعاني التوترات والنزاعات المسلحة.

ونتيجة لما سبق يتم العمل حالياً على تمكين الدول والمنظمات الحكومية وغير الحكومية من استخدام المواقع الإلكترونية، بهدف إتاحة المعلومات المتعلقة بالمعايير القانونية المنظمة لحقوق الإنسان لأوسع جمهور ممكن.⁷ ويعكس هذا الاتجاه الاهتمام المتزايد بالتكنولوجيا الرقمية وتسخيرها لحماية وترقية حقوق الإنسان بدلاً من أن تكون عامل من عوامل تهديد حقوق الإنسان كما يريده الذين يسيئون استخدامها.

ورغم الإيجابيات الكثيرة التي تتمتع بها التكنولوجيات الحديثة وفي مقدمتها ما تتيحه شبكة الإنترنت من خدمات، إلا أنها تنطوي على آثار سلبية كثيرة أيضاً تمس على وجه الخصوص الحق في الخصوصية، حيث تكون الوسائل التكنولوجية المختلفة عرضة للعديد من الهجمات والجرائم الإلكترونية نتيجة لعدة أسباب وعوامل، بعضها شخصي والآخر موضوعي، ففي مثل هذه الحالات تتحول الأدوات التكنولوجية من أدوات

صديقة للإنسان تسهل له حياته اليومية إلى سبب من أسباب انتهاك كيانه المعنوي المتمثل في حقه في الخصوصية، كما قد تتسبب في أحيانا أخرى في إلحاق الأذى حتى بكيانه المادي.

2.1- تهديد الجرائم الإلكترونية للحق في الخصوصية:

تعد جريمة الدخول غير المصرح به أو التعسفي أو غير المشروع من بين الصور الكثيرة للجرائم الإلكترونية الماسة بالحق في الخصوصية من خلال المساس بالبيانات الشخصية المعالجة إلكترونياً؛ وكذا الانحراف عن الغرض القانوني للمعالجة الآلية للبيانات،⁸ كإفشاء المعلومات والبيانات التي تتم السيطرة عليها من دون أي رخصة من الجهات المختصة لمساومة أو ابتزاز أصحابها أو قصد الإساءة إليهم بأي طريقة كانت.

إلا أنه من بين الاستثناءات الواردة على قاعدة عدم جواز إفشاء المعلومات⁹ هي ضرورة الحصول على رخصة مسبقة وأن يكون هذا الإجراء يهدف إلى الكشف عن جريمة أخرى، وإلا وقع المنتهك تحت طائلة المسائلة القانونية ومن ثم تقوم مسؤوليته القانونية المترتبة عن هذا الانتهاك.

وتكريسا للحق في الخصوصية تنص المادة 17 من العهد الدولي للحقوق المدنية والسياسية على حق كل شخص في عدم التعرض على نحو تعسفي أو غير مشروع للتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس بشرفه أو سمعته، وفي هذا السياق ترى اللجنة المعنية بالحقوق المدنية والسياسية أنه يستلزم ضمان هذا الحق في مواجهة جميع التدخلات والاعتداءات سواء أكانت صادرة عن سلطات الدولة أو عن أشخاص طبيعيين، ومن ثم فإن الالتزامات التي تفرضها هذه المادة تقتضي أن تعتمد الدولة تدابير تشريعية وغيرها من التدابير اللازمة لإعمال الحظر المفروض على تلك التدخلات والاعتداءات فضلا عن حماية هذا الحق.¹⁰ خاصة عندما يكون جانب من تشريعات وقوانين بعض الدول لا تتوافق مع الاتفاقيات الدولية ذات الصلة باحترام خصوصية الأفراد.

2- النصوص الدولية الخاصة بمكافحة الجرائم الإلكترونية:

1.2- الصكوك العالمية الخاصة بحماية الحق في الخصوصية:

لم تعد مسألة ارتكاب الاعتداءات السيبرانية تقتصر على الأفراد والتنظيمات الإجرامية فحسب، بل باتت أيضا ترتكب من طرف بعض الدول، سواء أكان ذلك في فترة النزاعات المسلحة أو في مجالات أخرى كالحروب التجارية والاقتصادية والسياسية التي تشنها الدول بين بعضها البعض كما حدث بين الصين والولايات المتحدة الأمريكية، وكذلك بين روسيا والولايات المتحدة الأمريكية أثناء فترة الانتخابات الرئاسية التي فاز بها الرئيس الأمريكي السابق "دولاند ترامب"، حيث اتهمت الإدارة الأمريكية روسيا بانتهاكها لقواعد بيانات الناخبين بالولايات وإجراء تغييرات على عدد المصوتين لترجيح الكفة لصالح ترامب، بالإضافة لقيام الصين بشن هجمات على شركات أمريكية على إثر الخلافات التي ثارت بين البلدين بخصوص بعض المسائل التجارية والاقتصادية.

وتبعاً لما سبق بيانه، تثار عدة مسائل بخصوص حقوق الأفراد أثناء الهجمات الإلكترونية التي تنفذها الدول، حيث يتضرر هؤلاء بشكل أو بآخر نتيجة لهذه الصراعات المعاصرة التي أصبحت تهدد العديد من الحقوق الشخصية للأفراد، كالحق في الخصوصية وكذا الحق في الغذاء على سبيل المثال، الذي يتضرر نتيجة لاستهداف مواقع شركات اقتصادية عالمية، بالإضافة لمسألة ارتفاع الأسعار العالمية للغذاء والدواء وغيرها من المستلزمات الأخرى الضرورية لحياة الأفراد.

وتجدر الإشارة إلى أن الحقوق سالفة الذكر محمية بموجب قواعد القانون الدولي المتمثلة في العديد من الصكوك والاتفاقيات الدولية، أبرزها الإعلان العالمي لحقوق الإنسان المعتمد سنة 1948 والذي يعد من أهم المواثيق الدولية الخاصة بتكريس وحماية حقوق الإنسان، وعلى منواله سارت بقية الاتفاقيات الدولية والإقليمية التي أبرمت بعده كالعهد الدولي للحقوق المدنية والسياسية لعام 1966، حيث تطرقت هذه المواثيق لنفس المبادئ والحقوق التي تضمنها الإعلان الذي يعد الوثيقة المرجعية في مجال الحقوق والحريات الأساسية التي ينبغي للدول احترامها وحمايتها.

وقد تطرق الإعلان العالمي لحقوق الإنسان للحق في الخصوصية من خلال المادة 12، كما أشار العهد الدولي للحقوق المدنية والسياسية المعتمد سنة 1966 للحق في الخصوصية من خلال الفقرة الأولى من المادة 17، حيث دعت الوثيقتين إلى حق الفرد في الخصوصية وضرورة احترامها وحمايتها من كل مل يمكن الإساءة إليها، ولا تقتصر هذه الخصوصية على الفرد بل تتعداه إلى أسرته وبيته أيضاً وغيرها من الجوانب المتعلقة بالفرد.

وقد أشارت أيضاً أغلب الاتفاقيات الإقليمية لحماية حقوق الإنسان لضرورة حماية الحق في الخصوصية، وفي مقدمة هذه الاتفاقيات؛ الاتفاقية الأوروبية لحقوق الإنسان لعام 1953، التي تطرقت لضرورة صيانة هذا الحق في الفقرة الأولى من المادة 8 التي تنص على أن: "لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته".

أما الاتفاقية الأمريكية لحقوق الإنسان لعام 1969؛ فقد عالجت مسألة الحق في الخصوصية من خلال المادة 11، حيث نصت الفقرة الأولى منها على أن لكل إنسان الحق في أن يحترم شرفه وتضام كرامته، وعلى نهج الاتفاقيات المذكورة سار أيضاً الميثاق الأفريقي لحقوق الإنسان والشعوب لسنة 1981، فقد أشار من خلال المادة 4 إلى ضرورة حماية واحترام حياة الأفراد وسلامتهم البدنية والمعنوية ومنع من حرمانهم بطريقة تعسفية من هذا الحقوق.

2.2- الصكوك العالمية والإقليمية الخاصة بالجرائم الإلكترونية:

نظرا لخطورة الجرائم الإلكترونية ونفسيها على الساحة الدولية، تم إصدار العديد من الوثائق الدولية وكذا إبرام اتفاقيات أخرى إقليمية للتصدي لهذه الجريمة.

وتأتي وثائق الأمم المتحدة الخاصة بحماية الحق في الخصوصية من الجرائم الإلكترونية في مقدمة النصوص الدولية التي تصدرت لهذا النوع من الجرائم؛ كلوائح مجلس حقوق الإنسان في مجال حماية الحق في الخصوصية، حيث أكد المجلس في لائحته رقم: A/HRC/RES/32/13 المؤرخة في 2016/07/01 بعنوان: تعزيز وحماية حقوق الإنسان على الانترنت والتمتع بها، لا سيما فقرتها الثامنة، على دعوة الدول إلى التصدي للمسائل الأمنية على الانترنت وفقا لالتزاماتها الدولية في مجال حقوق الإنسان، من أجل ضمان حرية التعبير والحق في الخصوصية وغيرها من الحقوق الأخرى على الانترنت.¹¹

وفي ذات السياق اتخذ مجلس حقوق الإنسان خطوة هامة بتعيين مقرر خاص بحماية الحق في الخصوصية، وذلك في سبيل حماية هذا الحق على شبكة الأنترنت، وهذا بموجب القرار A/HRC/28/27 المؤرخ في 2015/03/26،¹² وقد ساهمت أيضا مفوضية الأمم المتحدة السامية لحقوق الإنسان في الدعوة لحماية هذا الحق من خلال بعض تقاريرها.¹³ إضافة إلى تقارير المقرر الخاص بتعزيز وحماية حقوق الإنسان والحريات الأساسية،¹⁴ بالإضافة إلى باقي هيئات الأمم المتحدة وفروعها ذات الصلة بحماية حقوق الإنسان بصفة عامة.

وتعزيزا لهذا الحق وضعت منظمة اليونسكو استراتيجية لحماية الحق في الخصوصية، حيث تركز منذ تسعينات القرن الماضي على المسائل الأخلاقية ذات الصلة بمجتمع المعلومات ومجال الانترنت، وعلى إثر ذلك تم تنظيم سلسلة من المؤتمرات في الفترة الممتدة بين (1997-2000) بعنوان: "أخلاقيات الأنترنت"، وقد تبع هذه المؤتمرات في السنوات العشر الأخيرة عدد من الاجتماعات الإقليمية لوضع أطر أخلاقية للقرارات السياسية، منها على سبيل المثال "مدونة أخلاقيات لمجتمع المعلومات" التي اقترحها عام 2011 المجلس الدولي الحكومي لبرنامج المعلومات للجميع (إيفاب).¹⁵

كما عمدت منظمة الأمم المتحدة على إصدار العديد من الوثائق الخاصة باستخدام التقدم العلمي والتكنولوجي لصالح السلم وخير البشرية، وتجنب إساءة استخدام هذه التقنية على نحو يمكن أن يهدد أمن وسلامة البشرية، فقد تطور الأمر أن صار بإمكان التهديدات السيبرانية تهديد السلم والأمن الدوليين، خاصة أن العديد من المجالات الحيوية أصبحت تعتمد على شبكة الانترنت كمحطات الكهرباء والمفاعلات النووية، وغيرها من البنى التحتية التي أصبحت تدار باستخدام شبكة الأنترنت، فضلا عن الإدارات والمؤسسات العمومية والخاصة التي اعتمدت أغلبها الاستراتيجية الرقمية في تسيير شؤونها، بحيث أن استهداف هذه المعطيات يؤدي لا محالة إلى تضرر المعطيات الشخصية للأفراد، بالتالي انتهاك خصوصيتهم ومعلوماتهم التي تشكل مجملها الخصوصية الرقمية، وما يزيد من خطورة هذه الاعتداءات هو إمكانية الاستيلاء على هذه المعلومات لاستخدامها في أغراض إجرامية غير مشروعة.

كما انعقدت عدة مؤتمرات دولية خاصة من أجل التصدي للجرائم الإلكترونية أبرزها: القرار 11 لمؤتمر طهران المنعقد في الفترة الممتدة من 22 أبريل إلى 13 ماي 1968، والمتضمن حماية حق الإنسان في حياته الخاصة، كما انعقد مؤتمر بمونترال في الفترة من 14 إلى 18 أكتوبر 1968، تطرق إلى البحث في الآثار السلبية التي يشكلها التقدم التكنولوجي على خصوصية الأفراد،¹⁶ وقد جاء هذا المؤتمر نتيجة لإساءة استخدام بعض الدول في مرحلة الحرب الباردة لبعض الوسائل التكنولوجية في مجال التجسس على الدول والأفراد على حد سواء.

وفي ذات السياق اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ عام 1976، وفي عام 1996 أنشأت اللجنة الأوروبية لمسائل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة السيبرانية، حيث عملت اللجنة بين سنة 1997 و 2000 على اتفاقية جرائم الإنترنت التي اعتمدها البرلمان الأوروبي في أبريل 2001، والتي أسست لإبرام اتفاقيات إقليمية أخرى متعلقة بحماية خصوصية الأفراد ومكافحة الجرائم الإلكترونية.

وفي سياق الحديث عن الجهود الإقليمية لمكافحة الجرائم الإلكترونية، تم اعتماد دليل تالين سنة 2017 من طرف مجموعة من الخبراء القانونيين والعسكريين، للتأكيد على تطبيق القانون الدولي الإنساني على الحروب السيبرانية، ولتحديد الدور الذي ستلعبه قواعد القانون الدولي الإنساني في حالة شن هجوم سيبراني وما قد يشكله من تهديدات على المستوى الدولي وكذا الداخلي، بما في ذلك مسألة انتهاك خصوصية الأفراد.

ومع تزايد صور وحجم الخسائر والأضرار الناجمة عن الجرائم المعلوماتية، التي تتخطى في أغلب الأحيان الحدود لتتطال اعتداءاتها دولا ومؤسسات أخرى ما يجعلها تتميز بالعالمية وبكونها عابرة للحدود، فقد أثبت الواقع العملي أن الدول لا تستطيع بجهودها المنفردة مواجهة الجريمة المعلوماتية، لذلك عملت الدول على توحيد جهودها لمكافحتها.¹⁷

ومعنى ذلك أن مكافحة الجرائم المعلوماتية لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي والجنائي، وينبغي هنا الإشارة إلى أن التعاون المذكور يجب أن تشارك فيه الدول وكذا مختلف الكيانات الدولية الأخرى من منظمات حكومية وغير حكومية، ويتمحور هذا التعاون في تبادل الخبرات وكذا المعلومات إضافة إلى تسليم وتبادل المجرمين.

وقد بدل الاتحاد الإفريقي هو الآخر جهودا في هذا المجال، حيث طلب المؤتمر الاستثنائي لوزراء الاتحاد الإفريقي المسؤولين عن تكنولوجيا المعلومات والاتصالات المنعقد في جنوب إفريقيا في نوفمبر 2009 من مفوضية الاتحاد الإفريقي، القيام بالاشتراك مع لجنة الأمم المتحدة الاقتصادية الخاصة بإفريقيا بإعداد اتفاقية حول التشريع القضائي على أساس احتياجات القارة، والالتزام بالمسائل القانونية والتنظيمية للمعاملات الإلكترونية والأمن الإلكتروني وحماية البيانات الشخصية، كما أوصت بضرورة توفير

الحماية القانونية لأنظمة المعلوماتية التي تكتسي قيمة بالنسبة للمجتمع، مما يجعل من الضروري سن تشريعات لمكافحة الجريمة الإلكترونية، وعلى هذا الأساس اجتمع مجموعة من قادة الاتحاد الإفريقي في يونيو 2014، وعلى إثر ذلك تمت الموافقة على اتفاقية الاتحاد الإفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية.¹⁸

أما على المستوى العربي؛ فمن أبرز ما يمكن أن يقال عن الجهود العربية المبذولة على مستوى الدول العربية لمكافحة الجرائم الإلكترونية التي تضررت منها العديد من الدول، يمكن ذكر الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المعتمدة في 2010/12/21 المتضمنة لـ 43 مادة، بالإضافة إلى الاتفاقيات الخاصة بالقارة الإفريقية والتي تشمل العديد من الدول العربية التي تقع بالقارة، كالاتفاقية الإفريقية حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2000، والإعلان الإفريقي لحقوق وحرريات الإنترنت لسنة 2002، وكذا الإعلان الإفريقي لتسيير الإنترنت الصادر بالجزائر سنة 2017.

واستكمالا لهذه الجهود فقد عقد المكتب الإقليمي العربي لاتحاد الاتصالات اجتماعه الأول في الجزائر يومي 25 و 26 فيفري من عام 2013، حيث تم على إثر ذلك تشكيل فريقا للعمل حول حماية الأطفال على الإنترنت في المنطقة العربية، يهدف إلى تنسيق الجهود وتوحيد الرؤى في المنطقة العربية من أجل التوصل إلى وضع مبادئ توجيهية لإطار قانوني لحماية الطفل في المنطقة العربية من فضاء الإنترنت، وقد تم الاتفاق على أن تكون مهمة الفريق تتمحور حول تحديد الأفعال التي تشكل خطرا على الأطفال في الفضاء السيبراني، وكذا وضع المبادئ التوجيهية للإطار القانوني الإقليمي لحماية الأطفال في هذا الفضاء في إطار التعاون والتنسيق الإقليمي في المنطقة العربية، إضافة إلى تقديم توصيات عامة حول الاسترشاد بالمبادئ التوجيهية على المستوى الوطني لكل دولة عند صياغة قوانينها الخاصة.¹⁹

كما اعتمدت جامعة الدول العربية قوانين نموذجية عبر الأمانة العامة لمجلس وزراء العدل العرب، أطلق عليها اسم القوانين العربية الاسترشادية الخاصة بمكافحة الجرائم الإلكترونية،³⁷ وذلك في إطار مواكبة التطورات التشريعية والقانونية الإقليمية والعالمية فيما يتعلق بحماية خصوصية الأفراد في المجال السيبراني. كما لا يفوتنا أن نذكر في هذا السياق بجهود المنظمة الدولية للشرطة الجنائية "الإنتربول"، والتي تهدف إلى محاربة الجريمة المنظمة بمختلف صورها ووسائله، فقد تعرضت المادة 2 من دستور المنظمة الدولية للشرطة الجنائية الدولية لبيان الهدف الأساسي للمنظمة والمتمثل في: تأكيد وتشجيع التعاون المتبادل بين سلطات الشرطة الجنائية، سواء أكان ذلك على المستوى المحلي أو على المستوى الدولي، وذلك في إطار القوانين القائمة في البلاد وكذا الاتفاقيات الدولية ذات الصلة، والتي تستمد مضامينها من روح الإعلان العالمي لحقوق الإنسان.

الخاتمة:

في الختام نخلص إلى أن الجرائم الإلكترونية بمختلف صورها المتمثلة أساساً في جريمة الدخول غير المصرح به، والجرائم المتعلقة بالبيانات الشخصية المعالجة إلكترونياً؛ باتت تشكل أحد أهم المخاطر التي تهدد الحياة الخاصة للأفراد وكذا أمن الدول على حد سواء، ومن ثم يستوجب على الجميع أخذ كافة التدابير والاحتياطات التي من شأنها ضمان حماية ووقاية خصوصية الأفراد من أي انتهاك محتمل، وهذا من خلال التركيز على مسألتين أساسيتين، تتمثل الأولى في الجانب القانوني أما الثاني فتتعلق بالجانب التقني.

فالجانب القانوني يقتضي تعزيز الصكوك الدولية الخاصة بحماية الحق في الخصوصية وكذا تلك المتعلقة بمكافحة الجرائم الإلكترونية، أما الجانب التقني فينتطلب تطوير الإمكانيات التقنية للدول وكذا المجتمع الدولي الخاصة بمكافحة الجرائم الإلكترونية وتعقب المجرمين في الفضاء الإلكتروني، بالإضافة إلى تطوير الأنظمة الرقمية الخاصة بحماية أمن الشبكات والمعطيات الرقمية الخاصة بالدول والأفراد على حد سواء.

وفي ختام هذه الدراسة ومن أجل التصدي للجرائم الإلكترونية ومن ثم حماية الحق في الخصوصية؛ نقدم التوصيات التالية:

- إبرام مزيداً من الاتفاقيات الدولية ذات الصلة بمكافحة الآثار السلبية للجرائم الإلكترونية على الحق في الخصوصية، والتي من شأنها الأخذ بعين الاعتبار التطورات الحاصلة في مجال الجرائم الإلكترونية.
- تعزيز التعاون الدولي والإقليمي من أجل ملاحقة القراصنة وتسليمهم للدول المعنية.
- مساعدة الدول الفقيرة تقنياً ومدها بالتكنولوجيات الحديثة قصد تمكينها من مواجهة الجرائم الإلكترونية بمختلف صورها.
- تعزيز السلطات الرسمية للدول لأمن الشبكات كي تتجنب اختراق قواعد بيانات إدارتها العمومية المختلفة، لا سيما الحساسية منها كالمؤسسات السيادية والأمنية، إضافة إلى الحالة المدنية والبنوك المؤسسات المالية والمصرفية وغيرها.

الهوامش:

- 1 - لامية طالة، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، معالم للدراسات القانونية والسياسية، المجلد 2، العدد 4، ديسمبر 2020.
- 2 - محمد بن مكرم بن منظور، لسان العرب، المجلد الخامس، الطبعة الأولى، دار صادر للطباعة، والنشر، بيروت، 2000، ص 80.
- 3 - عبد الحليم بوقرين وصورية قلالي، أثر الجريمة الإلكترونية على الحياة الخاصة للأفراد، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 3، العدد 2، سبتمبر 2019، ص 69.
- 4 - القانون رقم 18-07 المؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ج ر 34، راجع: عبد الحليم بوقرين وصورية قلالي، مرجع سبق ذكره، ص 69.

5 - الأمم المتحدة، وقائع الأمم المتحدة، التكنولوجيات الجديدة والأهداف العالمية، متاح على الرابط التالي: [HTTPS://WWW.UN.ORG/AR/61413](https://www.un.org/ar/61413)، آخر زيارة للموقع بتاريخ: 2020/09/11، على الساعة: 00 و43 د.

6 - تقرير المقرر الخاص المعني بحالات الإعدام خارج نطاق القضاء أو بإجراءات موجزة أو تعسفاً، السيد كريستوف هاينز بعنوان: استخدام تكنولوجيات المعلومات والاتصالات لضمان الحق في الحياة، الدورة التاسعة والعشرون، البند 3 من جدول الأعمال بعنوان: تعزيز وحماية جميع حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية، أنظر الوثيقتان: A/HRC/26/36 و A/67/275 المؤرختان في 2015/04/24.

7 - نفس المرجع.

8 - عبد القادر عيمير، الحماية الجنائية للحق في الحياة الخاصة في البيئة الرقمية، المجلة الإلكترونية القانون والأعمال، متاح على الرابط التالي: [HTTPS://WWW.DROITENTREPRISE.COM](https://www.droitentreprise.com)، آخر زيارة للموقع بتاريخ: 2021/04/12، على الساعة: 14 سا و22 د.

9 - نفس المرجع.

10- اللجنة المعنية بالحقوق المدنية والسياسية، الدورة الثانية والثلاثون لعام 1988، الفقرة 1 من التعليق العام رقم 16 على المادة 17 (الحق في حرمة الحياة الخاصة)، 1988.

11 - عبد اللطيف دحية وأحمد بن بلقاسم، الدور الجديد لمنظمة الأمم المتحدة في حماية الحق في الخصوصية في ظل العصر الرقمي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 8 المجلد 2، ديسمبر 2017، ص 502

12 - مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، 20 جوان 2014، A/HRC/27/37

13 - نفس المرجع، ص 501

14 - عبد اللطيف دحية وأحمد بن بلقاسم، مرجع سبق ذكره، ص 501

15 - نفس المرجع، ص 504.

16 - صفية بشاتن، الحماية القانونية للحياة الخاصة: دراسة مقارنة، رسالة دكتوراه في القانون، جامعة تيزي وزو، 2012، ص 308.

17 - فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد 2، 2015، ص 11.

18 - نفس المرجع، ص 18.

19 - أنظر موقع الاتحاد الإفريقي: WWW.AFRICAN-UNION.ORG، آخر زيارة للموقع بتاريخ 2022/01/12.

