

إشراك الهيئات والمراكز المتخصصة في وضع التشريعات كآلية لمواجهة التحديات والتحول الرقمي

Involving specialized bodies and centers in developing legislation as a mechanism to address digital challenges and transformations

عباس صادقي¹،

Abbes Sadeki¹,

sadeki.abbes@cuillizi.dz، المركز الجامعي إليزي (الجزائر)،¹

تاريخ الاستلام: 2024/09/30 تاريخ القبول: 2024/10/25 تاريخ النشر: 2025/03/22

ملخص:

إن مواجهة تحديات التحول الرقمي، لم يعد يتوقف عند حد التعاون في "إنفاذ القانون" فحسب، بل يمتد إلى التعاون في صياغة القوانين والمساهمة في إثرائها ضمن استراتيجيات الشراكة بين الهيئات الأمنية والهيئات التشريعية والقضائية وخبراء تكنولوجيا المعلومات والاتصالات.

وتسعى هذه الورقة العلمية لبيان أهمية هذه الآلية والتعريف بها، فعلى الصعيد الدولي، يشار إلى الدور الهام الذي تقوم به منظمة إنتربول بهذا الصدد، حيث أصدرت دليل "أدوات التكنولوجيا الحديثة وحماية البيانات"، أوضحت من خلاله المشروعات المعتمدة في نطاق عملها.

وتبين من خلال استعراض بعض هذه المشروعات، أنها تركز في تحقيق أهدافها على اتباع سياسة إشراك ذوو اختصاصات متعددة، كالحامين والقضاة وأساتذة القانون، وخبراء تكنولوجيا المعلومات، والضباط ورجال الشرطة والأمن المكلفون بالأمن السيبراني، والهيئات والجهات المختصة، للوصول إلى وضع أطر قانونية مناسبة لتأطير التحولات الرقمية، ولمواجهة الجرائم والتهديدات الإلكترونية، وتجاوز صعوبات مواجهتها.

كلمات مفتاحية: الهيئات المتخصصة؛ الخبراء؛ القانون؛ التحولات الرقمية؛ التحديات.

تصنيفات JEL: K420، K100.

Abstract:

Facing the challenges of digital transformation no longer stops at cooperation in "law enforcement" only, but extends to cooperation in drafting laws and contributing to their enrichment within partnership strategies between security agencies, legislative and judicial bodies, and information and communications technology experts.

This intervention seeks to explain the importance of this mechanism and introduce it. At the international level, the important role played by Interpol in this regard is noted, as it issued a guide to "Modern Technology Tools and Data Protection", through which it explained the projects approved within the scope of its work. Through reviewing some of these projects, it became clear that, in achieving their goals, they focus on following a policy of involving people with multiple specializations, such as lawyers, judges, law professors, information and communications technology experts, officers, police and security men in charge of cybersecurity, and competent bodies and authorities, to reach the development of appropriate legal frameworks for framing Digital transformations, to confront cyber crimes and threats, and to overcome the difficulties of confronting them technically and legally

Key Words: Specialized bodies; experts; law; digital transformations; challenges.

JEL Classification Codes: K420; K100.

المؤلف المرسل: عباس صادقي، الإيميل: sadeki.abbes@cuillizi.dz

1. مقدمة

القانون هو " مجموعة من القواعد العامة المجردة التي تنظم سلوك الإنسان وتتضمن جزاءً مادياً حالاً يُوقع ضد من يخالفها "¹. أما لفظ التشريع " فإنه يُستخدم لمعنيين: معنى عام يُقصد به وضع القواعد القانونية اللازمة لحكم العلاقات الاجتماعية بين الناس، ومعنى أخص من ذلك هو تعبير عن إرادة السلطة العامة إصدار قاعدة قانونية وإلزام الناس باحترامها وهذا هو المعنى المقصود بلفظ التشريع، باعتباره وسيلة

من وسائل تطور القانون "2. ويُقصد بالتشريع في الاصطلاح الشرعي والقانوني "سن القوانين التي تُعرفُ منها الأحكام لأعمال المكلفين وما يحدث لهم من الأفضية والحوادث"3

ومن الملاحظ أن تنوع وسائل التواصل والاعتماد على التقنيات الالكترونية الحديثة ودمجها في مختلف نواح الحياة، حتى أصبحت ركيزة لا يمكن الاستغناء عنها، وكأي منجز آخر من منجزات واختراعات العقل البشري تم استغلال الفضاء الالكتروني على نحو سلبي غير مشروع، سواء في تسهيل ارتكاب الجرائم التقليدية كالسرقات والاعتداءات بمختلف صورها، أو في استهداف وسائل ونظم التواصل الالكتروني في حد ذاتها، وكلا الأمرين ترتب عنه زيادة مذهلة في معدلات ارتكاب الجريمة، وفي استنساخ دائم لصور جديدة من الإجرام، جعلت من التشريعات والتدابير الأمنية في كثير من الحالات في مكانة متأخرة منها، وفي ملاحظة مرهقة وغير مجدية وعاجزة عن تغطية واحتواء مظاهر الاجرام الحديثة. ففي الوقت الذي تتعرض فيه الدول لاعتداءات وتهديدات متنامية وغير مألوفة، ويتعرض فيه الأفراد لانتهاك حقوقهم وخصوصياتهم، لازالت الكثير من التشريعات تراوح مكانها رغم الاصلاحات المتكررة.

وإذا كان لابد من إرساء استراتيجية تشريعية شاملة لتنظيم التحول الرقمي، ومواجهة الجرائم والتهديدات المرتبطة به، من خلال تحديث القوانين والنظم الحاكمة للتعاملات الرقمية، والمتابعات الجزائية والتحقيق والتفتيش والقبض والمحكمة، فكيف يتم هذا التحديث، هل وفقا للأنماط التقليدية بمبادرة من السلطات المختصة بالتشريع في كل دولة، أو وفق سياسة تشريعية متكاملة، تتم بشراكة حقيقية بين المشرعين لقواعد القانون والسلطات المنقذة له من جهة، وبينها وبين خبراء التكنولوجيا والاتصالات الالكترونية والهيئات المكلفة بالدفاع والأمن، على المستويين الدولي والوطني، من جهة ثانية؟

تسعى هذه الورقة العلمية للإجابة على التساؤل المذكور، باتباع المنهج التحليلي لمعرفة خلفيات ومبررات تحديث الترسنة القانونية لمواجهة التحديات والتحويلات الرقمية، والمنهج المقارن للاطلاع على بعض الجهود والتجارب الرائدة في هذا المجال.

ويتم التطرق للموضوع من خلال محورين أساسيين:

* واقع المواجهة التشريعية للتحديات والتحويلات الرقمية

* الدور الاستشاري والاستشاري للهيئات والمراكز المتخصصة وأهميته للسلطات التشريعية

2. واقع المواجهة التشريعية للتحديات والتحولات الرقمية

على الرغم من الاجماع حول خصوصية التعاملات الرقمية والافتراضية وكذا السلوكيات المجرمة المرتبطة بها، إلا أن التشريعات المؤطرة لها قد يتم سنّها بنفس القواعد العامة المقررة بهذا الشأن، وعليه فقد اتسمت بالقصور من ناحية وبعدم الفاعلية من ناحية أخرى.

1.2 قصور نصوص التجريم التقليدية السائدة عن الاحاطة بالتهديدات والجرائم المستحدثة

تسعى كافة النظم القانونية إلى الحد من السلوك الإجرامي، أو السلوك الذي يُهدّد بتدمير المجتمع، وإلا افتقد الناس الشعور بالأمان " لذلك فإنه عندما تتمتع الدولة بقدرٍ كافٍ من القوة فإنه يتوافر لديها الأسباب المقنعة للتدخل والسعي لتطبيق قواعد متحضرة. وتحاول معالجة السلوك الذي يُدبّر المجتمعات على نحو متسق ومحيد. فهي تقرر ماهية السلوك الذي يدعو لتدخلها وتجرّمه على أساس من القانون"⁴ ويرجع البعض⁵ قصور نصوص التجريم التقليدية السائدة عن الاحاطة بالتهديدات والجرائم المستحدثة كجرائم الكمبيوتر الى ثلاث حقائق اساسية؛ أولها أن جرائم الكمبيوتر تستهدف المعطيات ذات الطبيعة المعنوية، سواءً كان الكمبيوتر أداة للجريمة أو هدفاً أو مسرحاً لها. والحقيقة الثانية، هي أن مبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوفر النص القانوني، فلا جريمة ولا عقوبة إلا بنص، ومتى ما انتفى النص على تجريم مثل هذه الافعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصور في مكافحة هكذا جرائم. أما الحقيقة الثالثة، فمفادها أن القياس في النصوص الجنائية الموضوعية محظور وغير جائز، ويكاد ينحصر في الحقل الجنائي بنصوص الاجراءات الجنائية كلما كانت أصلح للمتهم.

ويختلف التعامل القانوني مع هذه الطائفة من الجرائم اختلافاً كبيراً عن الفهم التقني لها، حيث تميل الأحكام القانونية إلى أن تكون أكثر عمومية بكثير من أجل شمول أوسع مجموعة من الجرائم مع مراعاة أثر الابتكارات التكنولوجية في المستقبل. ومن ناحية أخرى، فإن المنظور التقني يتميز بنهج تفصيلي أو دقيق لفهم التقنيات المستخدمة في ارتكاب الجريمة، "ومن الواضح تماماً أن هذا النهج القانوني المعمم لا يتناسب مع التحليل الفني الدقيق والمفصل لحوادث أمن الحاسوب. ومن الواضح أيضاً أن المفاهيم والمصطلحات

القانونية لا علاقة لها بالمفاهيم المستخدمة في مجال أمن المعلومات. وعلاوة على ذلك، عندما يُستخدم نفس المصطلح في كل من القانون والعلوم، فإنه كثيرا ما يُستخدم بمعنى مختلف، والارتباك الناتج بينهما أمرٌ لا مفرَّ منه"⁶

ويُشار إلى أن تطور استخدام المصطلحات الدالة على الجرائم المرتكبة بواسطة تقنيات وأنظمة الكمبيوتر أو المستهدفة لها، تلازم بشكل جليّ مع زيادة استخدام النظم الحاسوبية في حد ذاتها، وتوسُّع الاعتماد عليها من مجرد تخزين ونقل وتبادل المعلومات والبيانات، إلى اعتبارها أهم وسيلة من وسائل التواصل التي فرضت نفسها في كافة مناح الحياة، لذلك فإن المحاولات الفقهية والتشريعية الأولى لمواجهة هذه الطائفة المستحدثة من الجرائم ركّزت على دور النظم الحاسوبية ومدى الاعتماد عليها أو استهدافها لتحقيق الأغراض الإجرامية؛ فقد تم تسميتها "جرائم إساءة استخدام الحاسوب"، وينطبق هذا الوصف على "كل الأعمال المعتمدة التي تتم باستخدام الحاسوب للإيقاع بضحية أو أكثر، ولتحقيق منافع غير مشروعة"⁷

وبقدر الاختلاف في تحديد تعريف جامع ومانع للجرائم والتهديدات والاعتداءات الالكترونية، بقدر الاتفاق حول خطورتها، وتفاقم أثارها، وضُعف أليات مواجهتها وحماية مستخدم الأنترنت من أضرارها. حيث أن تنامي الجرائم والتهديدات الالكترونية أخذ أبعادا خطيرة، فهي لم تصبح مُجرّد جرائم متفرقة تستهدف جني المال، أو الانتقام والتشفي، أو إشباع نزوات وأهواء فردية منحرفة. إن هجوما كالذي تعرّضت له عشرات الدول في شهر مايو 2017، مستهدفا بالأساس تعطيل مصالحها الحيوية، كالمؤسسات الصحية ومؤسسات النقل وغيرها، يؤكّد ما انتبه له جانب كبير من المختصين المهتمين بالتشريعات وبتكنولوجيا المعلومات. حيث توجّه العديد منهم إلى القول بأن وجود القوانين التي تحارب الجريمة الالكترونية على النحو المطبّق الآن "ليس كفيلا بمواجهتها مواجهة حقيقية فعّالة". إذ أن غالبية الدول المستهدفة وجدت نفسها في مواجهة "هجوم إلكتروني" واسع النطاق، على الرغم من وجود تلك القوانين والعمل بها منذ فترات متفاوتة.

2.2 الفوارق بين الأنظمة القانونية الحاكمة للجرائم والتهديدات الالكترونية

يشير البعض⁸ لأثار التطبيق الضيق لمبدأ شرعية الجرائم والعقوبات ومبدأ سيادة الدولة في مواجهة الجرائم الالكترونية، وكيف أن التحجج بالسيادة وانغلاق التشريعات العقابية الداخلية على نفسها وغياب قنوات الاتصال الفعّال بين الدول كانا سببان بارزان في إضعاف روح التعاون بين الدول في مكافحة الجرائم بصفة عامة والجرائم الالكترونية والمستحدثة بصفة أخص.

وهذه النتيجة المنطقية التي جنتها مختلف الأنظمة القانونية سواء الآخذة منها بنظام وحدة القانون الداخلي والدولي، أو الآخذة بنظام ازدواجيتهما، أظهرت ضعف في مواجهة الجرائم الالكترونية، وتلكؤ واضح في تفعيل الاتفاقيات الدولية المتعلقة بها، وبالتالي الركون إلى قواعد القانون الداخلي لمجابهتها، خاصة في الدول العربية. وهذا المسلك أثبت إخفاقه في التصديّ للجرائم الالكترونية، التي يتعدى نطاقها الجغرافي وضحاياها ووسائل اثباتها وحجز أدلتها حدود الدولة، إلى الحد الذي قد تمتنع فيه عن تجريم طوائف بأكملها من الجرائم المعتبرة إلكترونية، كنسخ المنتوجات والبرامج بطرق غير مشروعة ...

وعليه فقد أدركت غالبية الدول "أن التعاون القضائي الدولي في المسائل الجنائية وسيلة فاعلة لمواجهة ما هو سائد من أن "الحدود الدولية تعترض القضاة دون الجناة"، فهو يتصدى لظاهرة تدويل الجريمة وعبورها حدود الدولة في ضوء التطور التكنولوجي وتطور الاتصالات والمعلومات التي يشهدها العالم، الأمر الذي يحتم تدويل إجراءات الملاحقة الجنائية لمثل هذا النوع من الإجرام، ليكون المجرم على قناعة بأنه سيلاحق أينما حل أو ارتحل"⁹

وعليه يُذكر أن مواجهة التهديدات والجرائم المستحدثة في الوقت الراهن، لم تعد تتوقف عند حد التعاون في "إنفاذ القانون" فحسب، بل تمتد إلى التعاون في صياغة القوانين والمساهمة في إثرائها ضمن استراتيجيات الشراكة بين الهيئات الأمنية والهيئات التشريعية والقضائية وخبراء تكنولوجيا المعلومات والاتصالات. والاتجاه نحو إنشاء هيئات ضبطية قضائية متخصصة بمكافحة الجرائم الالكترونية. فما هي أبرز ملامح هذا التوجه الحديث؟

3. الدور الاستشاري والاستشاري للهيئات والمراكز المتخصصة وأهميته للسلطات التشريعية

تشمل الهيئات والمراكز المتخصصة كافة الوحدات البحثية والأمنية والتكنولوجية والتقنية والاجتماعية ذات العلاقة بتكنولوجيا المعلومات والاتصالات والأمن. ولعل من أهم أدواها وجهودها هو التشخيص الدقيق لمظاهر وتدابير مواجهة التهديدات الرقمية واقتراح حلول مواجهتها.

1.3 أهمية توحيد جهود تأطير ومواجهة تحديات التحول الرقمي

للتخفيف من وطأة "الفوارق بين الأنظمة الجنائية"، وأثرها البين في إضعاف مكافحة الجريمة الالكترونية، ينبغي الترويج لفهم أكثر عمقا لحقيقة التهديدات الالكترونية، ولتعدد المعوقات التي تحول دون تحول رقمي آمن، وبكون تلك التهديدات تطال مختلف الأفراد والدول، وأنها في استنساخ دائم، وهذه الحقيقة كفيلة بدفع الدول لتنشيط حركة التعاون فيما بينها، بما في ذلك التفتح نحو تبني نظم إجراءات جنائية أكثر فاعلية ومرونة من النظم القائمة حاليًا، والاعتماد شيئًا فشيئًا على ممارسة الاختصاص العالمي باعتباره ركيزة أساسية من ركائز ردع المجرمين حيثما كانوا.

ومن خلال النظر فيما تضمّنته اتفاقية بودابست لسنة 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، وللمحاولات الفقهية التي تسعى لتوحيد الجهود الدولية في مواجهة الجرائم الالكترونية، وكذا ممارسات الدول في تطبيق مبدأ الاختصاص العالمي يمكن ذكر بعض الوسائل القانونية:

أ- ضرورة التحديث الدوري لاتفاقيات التعاون القضائي وتعيين هيئات مكلفة بحسن تنفيذها.

ب- الاعتماد على أليات أكثر صرامة في تنفيذ الالتزامات الدولية التعاقدية، وبحث وسائل التنفيذ الالزامي للاتفاقيات المتعلقة بمكافحة الجرائم الالكترونية، كحضر التحفظ بشأن النقاط المتصلة بجوهر التعاون والتبادل المعلوماتي، والتبليغ الاجباري عن البيانات والمعلومات المتصلة بالجرائم الالكترونية، وربط تنفيذ تلك الاتفاقيات بالمعاملات الاقتصادية والتجارية بين الدول.

ت- الاعتماد على صياغة قانونية أكثر دقة للاتفاقيات الدولية المعنية بمكافحة الجرائم الالكترونية، بما في ذلك الأخذ بمفاهيم محدّدة متفق عليها لحرية التعبير والحق في الخصوصية وحرمة الحياة الخاصة واحترام الشعائر الدينية والثوابت الوطنية، وفقا لرؤية دولية مقاربة وليس وفقا لثقافة واحدة أو لاتجاه فكري معيّن،

حيث أظهر الواقع أن الدول تخشى من الالتزامات التي تتعارض مع مفاهيمها الدينية والاجتماعية وتحجم عن الانخراط في تنفيذها خاصة عند تناقضها الصريح مع تشريعاتها الداخلية.

ث-تضمن النصوص التشريعية الدولية والوطنية للقيم الأخلاقية والتربوية، وتشجيع الرقابة الذاتية كقيود طوعية وحضارية للحد من الجرائم الالكترونية، وحث الدول على اتخاذ التدابير التوعوية لمحاصرة الدعايات المغرضة والاشاعات، ودعوة مستخدمي الأنترنت لعدم متابعة الفضائح، والمواد الاباحية الخليعة، وعدم التفاعل مع المواقع المضللة، ومقاطعة المواقع الدعائية والطائفية والسياسية والفكرية المتطرفة، خاصة في أوساط النشء والشباب.

2.3 المشروعات المجسدة في إطار عمل المنظمة الدولية للشرطة الجنائية إنتربول

ينبغي الإشارة إلى الدور الهام الذي تقوم به منظمة إنتربول بهذا الصدد، حيث أصدرت سنة 2015 دليل "أدوات التكنولوجيا الحديثة وحماية البيانات"¹⁰، أوضحت من خلاله المشروعات المعتمدة في نطاق عملها، والهادفة لمواجهة شاملة للجرائم الالكترونية، تقوم أساسا على إشراك أكبر قدر ممكن من الهيئات والجهات المختصة للوصول إلى وضع أطر قانونية مناسبة لمواجهة الجرائم الالكترونية، وتحقيق الأمن في الفضاء السيبراني، وهذه المشروعات هي:

*مشروع (Smart)¹¹: ومن أهم أهدافه " توفير إطار قانوني فعّال لمواجهة الاعتداء على البيانات الرقمية"

*مشروع (Respect)¹²: الذي يسعى من خلاله إنتربول " لوضع الأسس القانونية التي تحدد كيفية تنظيم المراقبة الرقمية لوسائل مثل كاميرات المراقبة ومواقع التواصل الاجتماعي"

*مشروع (SIIP)¹³ المسمى المشروع المتكامل لتحديد هوية الشخص من صوته: ويركز إنتربول من خلاله على "تقنين استخدام هذه التكنولوجيا الناشئة في مواجهة الجرائم المرتكبة في الفضاء السيبراني"

*مشروع (Evidence)¹⁴: ويرمي إلى "وضع إطار قانوني مشترك ومنهجي لجمع الأدلة الالكترونية واستخدامها وتبادلها، ودراسة الأبعاد القانونية المحتملة لتطبيق التكنولوجيا الحديثة"

*مشروع (E-crime)¹⁵: ويهتم بدراسة الجريمة السيبرانية "وتداعياتها القانونية والاقتصادية" والبحث عن إجراءات ملموسة لمواجهتها.

*مشروع (Mapping)¹⁶: ويبحث مسائل الانتقال إلى المجتمع الرقمي وتطور الانترنت، من النواحي الاجتماعية والاقتصادية والقانونية والأخلاقية".

إن مثل هذه المشروعات، تركز في تحقيق أهدافها على اتباع سياسة الجمع بين الخبرات والرؤى والمنطلقات والمناهج ذات العلاقة بالجريمة الالكترونية، وعلى الخطط التفاعلية الواقعية التي يسهم في متابعتها ذوو اختصاصات متعددة، حيث تشمل المحامين والقضاة وأساتذة القانون، وخبراء تكنولوجيا المعلومات والاتصالات، والضباط ورجال الشرطة والأمن المكلفون بالأمن السيبراني. كما أنها تشكّل فضاءً خصبا لتبادل المعلومات والكفاءات والاطلاع عن كثب عن حقيقة التهديدات الالكترونية وعن صعوبات مواجهتها تقنيا وتكنولوجيا وقانونيا. ولا شك أن الكثير من دول العالم خاصة الدول العربية عليها أن تستفيد من هذه المشروعات باعتبارها أعضاء في منظمة إنتربول.

وكمثال على جهود الشراكة بين المؤسسات الأمنية والقائمين على تشريع القوانين والفاعلين في مجال تكنولوجيا المعلومات بصدد محاربة الإجرام الالكتروني، يُذكر على الصعيد العالمي، منتدى "التعاون من أجل الأمن"، الذي عُقد في 28 مارس 2017 بالشراكة بين حكومة دولة الإمارات العربية المتحدة والمنظمة الدولية للشرطة الجنائية "إنتربول" و"مؤسسة إنتربول" من أجل عالم أكثر أمانا، وقد التقى ممثلو الحكومات والمؤسسات الشرطية ورواد قطاع الأمن بهدف تحديد مسار أكثر فعالية لمواجهة التحديات الأمنية في ظلّ الترابط المتزايد بين الإرهاب والجريمة المنظمة والجرائم الإلكترونية"¹⁷. كما يمكن على الصعيد الوطني، وكمثال، الإشارة إلى الملتقى الأول حول "الدفاع السيبراني والأمن السيبراني" الذي تم تنظيمه من قبل وزارة الدفاع في الجزائر¹⁸ في يومي 15 و16-05-2017، وكان من بين أبرز أهدافه " تبادل الخبرات والمعارف ومناقشة المستجدات والتطورات في مجال الفضاء السيبراني، والتطرق للتشريعات الخاصة بذلك، من قبل مجموعة من الخبراء المدنيين والعسكريين"

هذا، ويرى المختصون بأن " الأمن السيبراني والدفاع معقدان لأن مسائل تحديد السلطات المختصة والمسؤوليات المشتركة بين القطاعين العام والخاص والتعاون الدولي الضروري، يجب فهمها وممارستها ووضعها قانونا كسياسات لإدارة الحوادث السيبرانية. فكثيرا ما لا يكون هناك وقت كاف لتوحيد جهود الاستجابة والتصدي لها حال وقوعها. ولذلك يجب أن تكون خيارات الأمن والدفاع والاستجابة السيبرانية محددة سلفا على عدة مستويات في شركات تكنولوجيا المعلومات والاتصالات ومكاتب إنفاذ القانون والاستخبارات والإدارات الأمنية العسكرية والمدنية ووكالات الشؤون الخارجية والتحالفات والمنظمات الدولية. ومع ذلك، تختلف الحكومات على نطاق واسع في مستويات الوعي بها فيما يتعلق بتطبيق الدفاع الإلكتروني للمفاهيم الرئيسية مثل تقسيم الأدوار بين الجيش وإدارات إنفاذ القانون، عند الاستجابة لحالات الطوارئ، وإذا لم تكن هذه التعقيدات مفهومة بشكل عام من قبل المشرعين وواضعي السياسات، فإن أي قوانين وسياسات جديدة للدفاع الإلكتروني قد ينتج عنها التداخل في الأدوار على نحو يضعف المواجهة الشاملة لحوادث الأمن الإلكتروني"¹⁹

لذلك، فإن مكافحة الجرائم الإلكترونية، ومظاهر الجرائم الأخرى، وتفعيل آليات التعاون الاقليمي والدولي بهذا الصدد، لا يمكن أن يكتمل إلا من خلال اتخاذ بعض الخطوات، أهمها مثل هذه المشروعات، تركّز في تحقيق أهدافها على اتباع سياسة الجمع بين الخبرات والرؤى والمنطلقات والمناهج ذات العلاقة بالتحويلات الرقمية، وعلى الخطط التفاعلية الواقعية التي يُسهم في متابعتها ذوو اختصاصات متعددة، حيث تشمل المحامين والقضاة وأساتذة القانون، وخبراء تكنولوجيا المعلومات والاتصالات، والضباط ورجال الشرطة والأمن المكلفون بالأمن السيبراني. كما أنها تشكّل فضاءً خصبا لتبادل المعلومات والكفاءات والاطلاع عن كثب عن حقيقة التهديدات والصعوبات المواجهة للتحويلات الرقمية وتنظيم مواجهتها تقنيا وتكنولوجيا وقانونيا. ولا شك أن الكثير من دول العالم خاصة الدول العربية عليها أن تستفيد من هذه المشروعات باعتبارها أعضاء في منظمة إنتربول

4. خاتمة:

إن الملاحظ أن انفراد السلطة التشريعية في وضع القوانين المرتبطة بالتحول الرقمي والتحسب والاستعداد للتهديدات والجرائم المرتبطة بذلك، وعدم ايلائها الاعتبار للجوانب التقنية التفصيلية، وعدم الاهتمام بنتائج البحوث والدراسات المتخصصة، وعدم تفعيل جانب الاستشارات المتعددة... كل ذلك يؤثر سلبا على فاعلية النصوص القانونية المتخذة بهذا الصدد. لتبقى طوائف من المعاملات الالكترونية خارج التغطية القانونية اللازمة.

كما ورد في دليل الاجراءات التشريعية لمواجهة إساءة استخدام الكمبيوتر لدول مجلس اوروبا: "ومن الواضح تماما أن هذا النهج القانوني المعمّم لا يتناسب مع التحليل الفني الدقيق والمفصل لحوادث أمن الحاسوب. ومن الواضح أيضا أن المفاهيم والمصطلحات القانونية لا علاقة لها بالمفاهيم المستخدمة في مجال أمن المعلومات. وعلاوة على ذلك، عندما يُستخدم نفس المصطلح في كل من القانون والعلوم، فإنه كثيرا ما يُستخدم بمعنى مختلف، والارتباك الناتج بينهما أمرٌ لا مفرّ منه"²⁰

لذلك لا بد من تفعيل تقنية إشراك الهيئات والمراكز المتخصصة الأمنية والبحثية والتقنية، والاستفادة من جهودها عند سن التشريعات والنظم، والعمل على حماية مستخدم الانترنت وتحقيق الأمن في الفضاء الالكتروني، وتجاوز عملية ادماج تقنيات التواصل الالكتروني في الحياة المعاصرة بسلاسة وبأمن. وذلك من خلال الاعتماد على تشريعات بمقدورها استيعاب وتجسيد الأبعاد الأمنية والقانونية للتطورات التقنية، ولها القدرة على ردع الجرائم والتهديدات المصاحبة لذلك.

5. قائمة المراجع:

*** الكتب:**

- صوفي حسن أبوبال، تاريخ النظم القانونيّة والاجتماعيّة، جامعة القاهرة، مصر، 2007.
- عبد الوهاب خلاف، خلاصة التشريع الإسلامي، دار القلم، الكويت، دون سنة طبع.
- توني أونوريه، آراء في القانون، ترجمة د. مصطفى رياض، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، مصر، 1998.

*** المقالات:**

- إمام حسنين خليل، التعاون القضائي الدولي لمواجهة الجريمة المنظمة. دراسة مقارنة بين الاتفاقيات الدولية لمكافحة الجريمة المنظمة عبر الوطنية والقانون الإماراتي، مجلة رؤى استراتيجية، عدد يناير 2015.

*مداخلات علمية:

-يونس عرب، قراءة في الاتجاهات التشريعية لمكافحة الجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، ورقة بحثية مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية 4-2 نيسان / ابريل 2006، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان.

-أشغال منتدى "التعاون من أجل الأمن"، الذي عُقد في 28 مارس 2017 بالشراكة بين حكومة دولة الإمارات العربية المتحدة والمنظمة الدولية للشرطة الجنائية "الإنتربول" و"مؤسسة الإنتربول" من أجل عالم أكثر أماناً. (تاريخ الاطلاع 2017-8-01 الساعة 8:00) متاح على الموقع:

<https://www.interpol.int/ar/2017/N2017-039/>

-أشغال الملتقى الأول حول "الدفاع السيبراني والأمن السيبراني" الذي تم تنظيمه من قبل وزارة الدفاع في الجزائر في يومي 15 و16-05-2017. (تاريخ الاطلاع 2023-8-01 الساعة 8:20) متاح على الموقع:

http://www.mdn.dz/site_principal/#

*الأدلة والمراجع باللغة الانجليزية:

-Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, Study for the European Commission Directorate-General Information Society (2002), ECSC-EC-EAEC, Brussels -Luxembourg 2003, p 22. (Date of view 30-7-2023 Time 15:40) Available on the website:

http://www.icsd.aegean.gr/website_files/metaptyxiako/133991949.pdf

-Computer Crime. Criminal Justice Resource Manual, Second Edition, National Institute of Justice, Department of Justice, USA,1989 , p 22. (Date of view:3-6-2023 Time 14:00) Available on the website:

<https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf>

-Scalable Measures for Automated Recognition Technologies (SMART) (Date of view 20-7-2023 Time 3:30) Available on the website: www.smartsurveillance.eu

Rules, Expectations & Security Throught Privacy-Enhanced Convenient Technologies (RESPECT) (Date of view 20-7-2023 Time 4:30) Available on the website: www.respectproject.eu

-Speaker Identification Integrated Project (SIIP) (Date of view 21-7-2017 Time 12:30) Available on the website: www.siip.eu

-ROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE. (Date of view 21-7-2017 Time 1:30) Available on the website: www.evidenceproject.eu

-E-CRIME PROJECT. (Date of view 21-7-2023 Time 1:30) Available on the website: www.ecrime-project.eu

-Managing Alternatives for Privacy, Property and Internet Governance. (Date of view 21-7-2023 Time 1:50) Available on the website: www.mappingtheinternet.eu

-Eneken Tikk & Kadri Kaska & Liis Vihul, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS, Cooperative Cyber Defence Centre

of Excellence (CCD COE), Tallinn, Estonia, 2010, p 7. (Date of view 2-8-2017 Time 2:10) Available on the website:

<https://ccdcoe.org/publications/books/legalconsiderations.pdf>

6. الهوامش والاحالات:

¹ صوفي حسن أبوطالب، تاريخ النظم القانونية والاجتماعية، جامعة القاهرة، مصر، 2007، ص 7.

² نفس المرجع. ص 137.

³ عبد الوهاب خلاف، خلاصة التشريع الإسلامي، دار القلم، الكويت، دون سنة طبع، ص 7.

⁴ توني أونوريه، آراء في القانون، ترجمة د. مصطفى رياض، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، مصر، 1998، ص 71.

⁵ يونس عرب، قراءة في الاتجاهات التشريعية لمكافحة الجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، ورقة بحثية مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية 2-4 نيسان / ابريل 2006، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، ص 26

⁶ Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, Study for the European Commission Directorate-General Information Society (2002), ECSC-EC-EAEC, Brussels -Luxembourg 2003, p 22. (Date of view 30-7-2023 Time 15:40) Available on the website:

http://www.icsd.aegean.gr/website_files/metaptyxiako/133991949.pdf

⁷ Computer Crime. Criminal Justice Resource Manual, Second Edition, National Institute of Justice, Department of Justice, USA, 1989, p 22. (Date of view: 3-6-2023 Time 14:00) Available on the website:

<https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf>

⁸ معتب بن عبد الله السند، المرجع السابق، ص 158.

⁹ إمام حسنين خليل، التعاون القضائي الدولي لمواجهة الجريمة المنظمة. دراسة مقارنة بين الاتفاقيات الدولية لمكافحة الجريمة المنظمة عبر الوطنية والقانون الإماراتي، مجلة رؤى استراتيجية، عدد يناير 2015، ص 10.

¹⁰ دليل أدوات التكنولوجيا الحديثة وحماية البيانات، صحيفة وقائع، منظمة إنتربول (1-OLA-03-2015/FS/COM) تاريخ الاطلاع: 20-7-2023 الساعة 3:00) متاح على الموقع:

[file:///C:/Users/DAR%20EL%20COMPUTER/Downloads/OLA01_03_2015_AR_web%20\(2\).pdf](file:///C:/Users/DAR%20EL%20COMPUTER/Downloads/OLA01_03_2015_AR_web%20(2).pdf)

¹¹ Scalable Measures for Automated Recognition Technologies (SMART) (Date of view 20-7-2023 Time 3:30) Available on the website: www.smartsurveillance.eu

¹² Rules, Expectations & Security Through Privacy-Enhanced Convenient Technologies (RESPECT) (Date of view 20-7-2023 Time 4:30) Available on the website: www.respectproject.eu

¹³ Speaker Identification Integrated Project (SIIP) (Date of view 21-7-2017 Time 12:30) Available on the website: www.siip.eu

¹⁴ ROPEAN INFORMATICS DATA EXCHANGE FRAMWORK FOR COURTS AND EVIDENCE. (Date of view 21-7-2017 Time 1:30) Available on the website: www.evidenceproject.eu

¹⁵ E-CRIME PROJECT. (Date of view 21-7-2023 Time 1:30) Available on the website: www.ecrime-project.eu <file:///C:/Users/DAR%20EL%20COMPUTER/Downloads/e-Crime%20project%20factsheet.pdf>

¹⁶ Managing Alternatives for Privacy, Property and Internet Governance. (Date of view 21-7-2023 Time 1:50) Available on the website: www.mappingtheinternet.eu

¹⁷ منتدى "التعاون من أجل الأمن"، الذي عُقد في 28 مارس 2017 بالشراكة بين حكومة دولة الإمارات العربية المتحدة والمنظمة الدولية للشرطة الجنائية "الإنترپول" و "مؤسسة الإنترپول" من أجل عالم أكثر أماناً. (تاريخ الاطلاع 2023-8-01 الساعة 8:00) متاح على الموقع: <https://www.interpol.int/ar/2017/N2017-039/>

¹⁸ الملتقى الأول حول "الدفاع السيبراني والأمن السيبراني" الذي تم تنظيمه من قبل وزارة الدفاع في الجزائر في يومي 15 و 16-05-2017. (تاريخ الاطلاع 2023-8-01 الساعة 8:20) متاح على الموقع: http://www.mdn.dz/site_principal/#

¹⁹ Eneken Tikk & Kadri Kaska & Liis Vihul, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS, Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, Estonia, 2010, p 7. (Date of view 2-8-2017 Time 2:10) Available on the website: <https://ccdcoe.org/publications/books/legalconsiderations.pdf>

²⁰ Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, Study for the European Commission Directorate-General Information Society (2002), ECSC-EC-EAEC, Brussels -Luxembourg 2003, p 22. (Date of view 3-7-2023 Time 15:40) Available on the website: http://www.icsd.aegean.gr/website_files/metaptyxiako/133991949.pdf