الفصل التاسع

التعاون الدولي للتجارة الالكترونية

obeikandl.com

obeikandl.com

أمام انتشار الجرائم الالكترونية ومحاولات القضاء علي الاقتصاد الرقمي كظاهرة عالمية، بات من الضروري البحث في كيفية إيجاد حلول فعالة وإ تخاذ تدابير وقائية منها وردعية لوقف الزحف الخطير لهذه الكوارث التقنية التي باتت تهدد اقتصاديات أمن واستقرار الدول بعد تطور الجريمة الالكترونية من إطارها الكلاسيكي المعروف إلى التقنية العلمية الحديثة لتصبح تجارة الكترونية رائجة وهو ما اصطلح عليه بالاقتصاد الرقمي، وهو ما تفسره نسبة الشكاوى الرسمية التي اعتمدها المركز العالمي لشكاوى الانترنت والتي كلفت سنة ٢٠٠٠ خسارة مادية فادحة قدرت بـ١٢ بليون دولار جراء النتائج التدميرية التي تسببت فيها فيروسات إتلاف برامج المعلوماتية. وقد قدرت مجمل الشكاوى الرسمية التي قدمها الضحايا للمركز بـ ٢٧٥٢٨٤ شكوى ولهذا ومن أجل حماية فعالة لبرامج المعلوماتية وقاعدة للبيانات يجب اعتماد السبل القانونية الوقائية من خلال الدخول إليها عن طريق كلمات مرور سرية يجتنب فيها استخدام كلمات سر مكونة من كلمات عادية مع الحرص على تغييرها دوريًا كل شهر إن تطلب الأمر ذلك، مع تكثيف برامج الرقابة على نوادي ومقاهي الانترنيت، والعمل على ترصد وحجب المواقع الإباحية كما هو الحال بالعربية السعودية وتونس، مع اعتماد برامج خاصة مضادة للفيروسات التدميرية واستعمالها بشكل مستمر.

١. التعاون الدولي للحد من جرائم المعلوماتية:

أمام الفراغات التشريعية التي أضحت تؤرق كاهل الدول بعد استفحال جرائم المعلوماتية والحاسب الآلي، خاصة مع استخدام تقنية الإنترنيت "الشبكة العنكبوتية" ونظراً لخصوصيتها المميزة، بات من الضروري إيجاد إطار فعال يضمن استحداث آليات للتعاون الدولي في مجال مكافحة هذا النوع من الجرائم من خلال التشجيع على تبادل الخبرات من أجل الضبط الجنائي لها، باعتبارها جرائم افتراضية، مع تكوين مختصين في المجال سواء الضبطية القضائية أو القضاء بوجه عام، وإيجاد تشريع دولي خاص لمواجهة هذا الخطر، وتبني منظومة معلوماتية موحدة تعتمد على إنشاء مكتب عالمي أو إقليمي للتوثيق الالكتروني، مع تسجيل كافة البرامج المعلوماتية وحفظها واعتماد الدلائل أو القرائن الرقمية كدلائل إثبات الجريمة ومن ثمة إدانة مقترفيها والحرص على إدراج مثل هذه الجرائم ضمن اختصاصات المحكمة الجنائية الدولية نظراً لطابعها العالمي، باعتبارها حرب عوالم ذات القدرة التدميرية الخطيرة على اقتصاديات وأمن الدول.

التشريع الدولي المنشود يجب أن يبنى على أطر قانونية موحدة يتم فيها عولمة القوانين وصلاحيات الاختصاص المفتوحة والمشتركة بين جميع دول العالم.

تعتبر عُمان أول دولة عربية سنّت قوانين خاصة بمكافحة الجريمة الالكترونية، تلتها الإمارات العربية المتحدة ثم السعودية، غير أنها قوانين غير فعالة نظراً لطابعها المحلي من جهة، والثغرات القانونية الموجودة بها، لذا أصبح من الضروري الدعوة للعمل على سن قانون دولي فعال شامل يكون مبنيًا على قاعدة معلومات ومعطيات بيانية معلوماتية موثقة شاملة، تخص هذا الجانب مع تكثيف التعاون العربي الدولي من خلال عقد مؤتمر عالمي موحد لاحتواء هذا الخطر الزاحف، وتدعيم أجهزة الأمن بما فيها الشرطة الجنائية الدولية "الأنتربول" بكافة المعطيات اللازمة بتكوين خبراء مختصين في التقنية الالكترونية، إلى جانب تكريس وتشجيع البحث العلمي العربي، وتكثيف حجم التبادل في الخبرات وسن القوانين ذات الشمولية الدولية، وإدراج جرائم المعلوماتية ضمن الإستراتيجية الأمنية العربية.. والجزائر كغيرها من الدول العربية حاولت مسايرة حجم التطور الحاصل في الوسائط المعلوماتية، لذا حاول المشرّع الجزائري ضبط الأطر القانونية لمواجهة هذه الجرائم خاصة ما تعلق منها بالسطو على البرامج المعلوماتية، والقرصنة وإدراجها ضمن قانون حماية الملكية الأدبية والفنية، وسن عقوبات لها تتأرجح بين السجن النافذ والغرامة المالية المشددة كتعويض عن الضرر، غير أن هذا يبقى غير كافي، حيث لازالت معظم القوانين الموجودة لا تتماشى وحجم الكوارث المرتكبة يوميًا، لذا من الواجب من الآن، إعادة النظر في المنظومة القانونية الخاصة وإدراج قوانين جديدة للتصدي لظاهرة تنامي الجريمة الالكترونية في أبعادها المختلفة.

جرائم الإنترنت تتعدى تفجيرات ١١ سبتمبر.. هكذا هي نظرة العالم الآن إلى شبكة الإنترنت بعد أن أصبح الدخول إليها مخاطرة غير محسوبة العواقب حيث انتشر الهاكرز على جنباته منتظرين الانقضاض على أول فريسة تقابلهم.

وتغير الإنترنت من مفهومه التقليدي كوسيلة إعلامية إلى ساحة قتال اختلفت فيها الأسلحة، إلا أن النتيجة واحدة وهي الخسائر الفادحة للضحية وغنائم الحرب للقراصنة.

وفي خطوة اعتبرها البعض بداية صحيحة لطريق طويل ملئ بالعقبات، يعتزم الاتحاد الأوروبي وضع خطة جديدة يقوم بموجبها بتفتيش أجهزة الكمبيوتر عن بعد وذلك لمكافحة جرائم الانترنت.

وستشمل خطة العمل الخمسية للاتحاد خطوات للقضاء على الزيادة المطردة في السرقة الالكترونية وفي عدد الأجهزة المستخدمة في نشر الرسائل غير المرغوب فيها وغير ذلك من البرامج الخبيثة.

كما ستشجع الخطة تبادل المعلومات بين قوات الشرطة الالكترونية لملاحقة ومقاضاة المجرمين، وستنسق هذه القوات المعروفة باسم "يوروبول" عملها الاستقصائي، كما ستوجه تحذيرات حول موجات الجريمة الالكترونية.

وقد حظيت الخطة الخمسية بدعم وزراء الاتحاد الأوروبي في اجتماع تقرر فيه أيضًا منح يوروبول مبلغ ٣٠٠ ألف يورو لتنشئ جهازًا لتجميع تقارير الإجرام وإصدار تحذيرات حول الأخطار المحدقة.

ودعم الاجتماع الوزاري إستراتيجية مكافحة الجريمة الالكترونية التي ستنشئ فرق تحقيق تعمل عبر الحدود وترخص استخدام دوريات افتراضية لضبط بعض النواحي في الانترنت، بحسب بي بي سي.

ومن "الإجراءات العملية" الأخرى للخطة تشجيع تبادل أفضل للمعلومات بين قوات الشرطة في الدول الأعضاء في الاتحاد والشركات الخاصة حول طرق التحقيق واتجاهاته.

وتهدف الإستراتيجية بشكل خاص إلى مكافحة التجارة في صور الأطفال أثناء تعرضهم للإيذاء الجنسي.

وقال الاتحاد في بيان يضع الخطوط العامة لإستراتيجيته "إن نصف جرائم الانترنت تشمل إنتاج وتوزيع وبيع صور إباحية للأطفال".

كما ستشارك هذه القوات في "تفتيش أجهزة الكمبيوتر عن بعد" وتسيير دوريات على الانترنت لملاحقة المجرمين، وأكد الاتحاد الأوروبي أن الضوابط موجودة لضمان احترام قوانين حماية المعلومات أثناء جمعها وتبادلها.

وقد حث جاك بارو نائب رئيس الاتحاد الأوروبي على الالتزام التام بإستراتيجية مكافحة الجريمة "إذا أردنا أن نجعلها أكثر فعالية".

وكان "الاتحاد الدولي للاتصالات" قد استحدث دليلاً الكترونيًا لتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة على الانترنت، ويعتمد على مفهوم أن تنهض جهة مفردة بذلك التتبع، ما يمكّن المعنيين من الرجوع إليها ومتابعتها بسهولة.

ووُصف الدليل بأنه "خريطة طريق" فيما يتعلق بمعايير الأمن الخاصة بتكنولوجيا المعلومات والاتصالات حيث يستطيع أن يلاحق المعلومات عن أحدث المعايير الأمنية المتجددة باستمرار، ثم يصبها في قاعدة بيانات تُفتح أمام المعنيين، ما يُسهل مهمة البحث عن المعلومات المطلوبة، وفقًا للبيان الصحفي للـ"الاتحاد الدولي للاتصالات".

وتم وضع الدليل بالتعاون المشترك بين "الاتحاد الدولي للاتصالات" و"الوكالة الأوروبية المختصة بأمن الشبكات والمعلومات" وأطراف دولية أُخرى مهتمة بشؤون الأمن المعلوماتي على شبكة الانترنت.

ويعرض الدليل أسماء المنظمات المعنية بتطوير المعايير وما تنشره من صيغ خاصة بأمن الإنترنت، ما يُجنّب تكرار الجهود، كما يسهل مهمة مهندسي أمن الشبكة الالكترونية في كشف الثغرات التي تُمكن العابثين من تهديد أمنها.

ويضم الدليل خمسة أقسام تُحدّثُ بصفة مستمرة وتتناول منظمات تطوير المعايير الخاصة بتكنولوجيا المعلومات والاتصالات وأعمالها والصيغ المعتمدة لتلك المعايير وطرق إقرار الاتفاق على تلك المعايير، والحاجات المستقبلية.

٢. صعوبة أكتشاف الدليل الرقمي:

نظراً للخصائص المميزة التي تتّسم بها الجريمة الالكترونية في كونها عابرة للحدود، تحدث في مكان معين وضحاياها في مكان آخر، إلى جانب السرعة في تنفيذها والسرعة في إتلاف الأدلة ومحو آثارها، ناهيك عن كونها ترتكب من طرف أشخاص غير عاديين يتمتعون بذكاء خارق وتقنية عالية في التعامل مع التقنية المعلوماتية وأجهزة الحاسوب، كل هذه العوامل تشكل عائقًا حقيقيًا أمام مهمة المحققين في التوصل إلى ضبط الدليل الرقمي[1] للإثبات والإدانة للجناة، إلى جانب كونها تقع في بيئة افتراضية عابرة للحدود، حتى وصفت أحيانًا بالجرائم التخيلية، كجرائم الخداع التخيلي بغرض النصب والاحتيال والسطو على أموال الغير والخلاعة التخيلية كالإباحة الجنسية والتشهير والتحريض على تعاطي الرذيلة، مما يصعب في أغلب الحالات إثبات هذا النوع من الجرائم، نظراً لسهولة التخلص وإتلاف الأدلة المادية وبسرعة فائق، حيث أن معظم الجرائم التي تم الكشف عنها ومعالجتها تمت عن طريق الصدفة لا غير، خاصة وأنها عادة ما تقترن بنوع من الخصوصية أو الحرية الشخصية، وتتعدى إقليمية الاختصاص كأن

(1) د. عبد الفتاح بيومي حجازي الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت المرجع السابق.

تحدث في مصر مثلاً وضحاياها في السعودية فأي القوانين يمكن تطبيقها في هذه الحالة، القانون المصري أم السعودي؟[٢].

٣. محاولات للحد من الخطورة:

وفي نفس السياق وللحد من الخطر القادم عبر الشبكات، تسارع لدول إلى وضع ضوابط وحماية وإنشاء أمن خاص للشبكات حيث شكلت وزارة الداخلية المصرية "دوريات أمنية" من خلال الشبكة، ومهامها منع الجريمة قبل وقوعها.

واستطاعت هذه الدوريات من ضبط تنظيم للشواذ يمارس جرائمه عبر الانترنت، وكذلك ضبط العديد ممن يحاول استخدام بطاقات ائتمان مسروقة.

الحكومة البريطانية أيضًا شكلت وحدة من قوات الشرطة وكلفت بمتابعة المجرمين الذين يستخدمون أجهزة الكمبيوتر وبعد اقتناع تام بالخطر القادم ومداولات استمرت أربع سنوات قامت ثلاثون دولة أوروبية بتوقيع معاهدة لتوحيد الجهود في محاربة جرائم الانترنت.

ومطلوب من أجهزة الأمن العربية أن تواجه هذا التحدي وتطور قدراتها وتحدث برامجها للقضاء أو للحد من مثل هذه الجرائم.

"كولن روز" خبير في إحدى الشركات الاسكتلندية حذر من الإرهاب عبر شبكة الانترنت وقال: "إنه الخطر الذي يمثل المرتبة الثالثة بعد الأسلحة الكيميائية والنووية".

وفي السعودية، تفرض الحكومة عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن ٥٠٠ ألف ريال فيما يعادل ١٣٣ ألف دولار لجرائم القرصنة المرتبطة بالانترنت وإساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح.

وأكد بيان صادر عن الحكومة السعودية موافقتها على مشروع قانون بخصوص جرائم تكنولوجيا المعلومات كان مجلس الشورى السعودي قد اقترحه العام الماضي.

وبموجب مشروع القانون، توقع العقوبة على الدخول غير المشروع الى موقع الكتروني أو الدخول إلى موقع الكتروني لتغيير تصميم هذا الموقع أو إلغائه أو إتلافه أو تعديله، كما يجرم مشروع القانون "المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف المحمولة المزودة بكاميرا أو ما في حكمها بقصد التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة".

(2) د. هشام رستم شرح قانون العقوبات ـ القسم العام ـ المرجع السابق.

يذكر أن الدولة تفرض رقابة صارمة على استخدام الانترنت من خلال تعقب المستخدمين وحظر المواقع الجنسية وبعض المواقع ذات المحتوى السياسي، حيث تم إغلاق بعض منتديات الانترنت التي يستخدمها ذوي الاتجاهات السياسية المتطرفة، ونظراً للخصائص المميزة التي تتّسم بها الجريمة الالكترونية في كونها عابرة للحدود، تحدث في مكان معين وضحاياها في مكان آخر، إلى جانب السرعة في تنفيذها والسرعة في إتلاف الأدلة ومحو آثارها، ناهيك عن كونها ترتكب من طرف أشخاص غير عاديين يتمتعون بذكاء خارق وتقنية عالية في التعامل مع التقنية المعلوماتية وأجهزة الحاسب، كل هذه العوامل تشكل عائقًا حقيقيًا أمام مهمة المحققين في التوصل إلى ضبط الدليل الرقمي للإثبات والإدانة للجناة، إلى جانب كونها تقع في بيئة افتراضية عابرة للحدود، حتى وصفت أحيانًا بالجرائم التخيلية، كجرائم الخداع التخيلي بغرض النصب والاحتيال والسطو على أموال الغير والخلاعة التخيلية كالإباحة الجنسية والتشهير والتحريض على تعاطي الرذيلة، مما يصعب في أغلب الحالات إثبات هذا النوع من الجرائم، نظراً لسهولة التخلص وإتلاف الأدلة المادية وبسرعة فائق، حيث إن معظم الجرائم التي تم الكشف عنها ومعالجتها تمت عن طريق الصدفة لا غير، خاصة وأنها عادة ما تقترن بنوع من الخصوصية أو الحرية الشخصية.

هناك العديد من المشكلات والصعوبات العملية والإجرائية التي تظهر عند ارتكاب أحد جرائم الإنترنت، ومن هذه المشكلات:

١ـ صعوبة إثبات وقوع الجريمة[٣].

٢ـ صعوبة التوصل إلى الجاني[٤].

٣ـ صعوبة إلحاق العقوبة بالجاني المقيم في الخارج.

٤ـ تنازع القوانين الجنائية من حيث المكان.

٥ـ صعوبة تحديد المسؤول جنائيًا عن الفعل الإجرامي.

٦ـ القصور في القوانين الجنائية القائمة.

٧ـ افتراض العلم بقانون جميع دول العالم.

(3) د. عبد الفتاح بيومي حجازي الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت المرجع السابق.

(4) د. هشام رستم شرح قانون العقوبات ـ القسم العام ـ المرجع السابق.