

الدليل الجنائي.. نقطة ضعف في إثبات الجرائم الإلكترونية



تحقيق: محمد الماحي

تعدّ الجرائم الإلكترونية من أكثر القضايا القانونية حداثة وإثارة لمخاوف رواد المواقع ومنصات التواصل والشركات والبنوك التي تعدّ هدفاً ثميناً للهجمات السيبرانية ومرتكبي الجرائم التقنية

كما باتت تأخذ منحى أكثر رواجاً مع التقدم التكنولوجي الكبير الذي أدخل أبعاداً جديدة إلى مفهوم الجريمة. ومع تداخل المعلوماتية والأجهزة الحاسوبية في مختلف الأنشطة الحياتية، أصبحت الجرائم الرقمية أكثر خطورة وحساسية، فضلاً عن تعقيداتها، ووسائل التخفي في ارتكابها

وقد كان المشرع الإماراتي من أوائل المشرعين الذين أطروا الجرائم الإلكترونية في أحكام وقوانين تعنى بمكافحة الجريمة المعلوماتية، تفصّل في أحكامها طبيعة هذه الجرائم وآلياتها، وسلوكات مرتكبيها وأهدافهم والعقوبات المستحقة وتعويضات ضحايا الجرم الإلكتروني، وتشكّل رادعاً قانونياً للحدّ منها، في المقابل هنالك صعوبات عدّة ومتجددة تواجه القائمين على مكافحة الجرائم الإلكترونية من حيث اكتشافها والتحقيق، وجمع الاستدلالات اللازمة

لإثباتها وكيفية مباشرة إجراءات الدعوى الجنائية فيها أمام المحاكم

حدد قانونيون عدداً من التحديات التي تعطل إثبات الجرائم الإلكترونية، بسبب غياب الدليل الجنائي وصعوبة تتبع المتهمين بسبب قدرتهم على إخفاء أي أدلة تؤكد تورطهم في القضية أو وجودهم خارج حدود الدولة، وغياب التزام الشركات المزودة لخدمات التواصل الاجتماعي بتوفير تسهيلات للجهات القضائية بهدف الحصول على معلومات وبيانات تخص المتهمين، وعدم وجود قوانين تحمي البيانات الشخصية لمستخدمي «الإنترنت» عالمياً

وركزوا على تحدّي يرتبط بصعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ يستطيع المجرم المعلوماتي، في أقل من ثانية، أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكمبيوتر

وأكدوا أن المجني عليه، خصوصاً في جرائم الابتزاز الإلكتروني، يتكتم على الجريمة ولا يبلغ السلطات المختصة عنها، خوفاً من التشهير، وعندما يكون المجني عليه مصرفاً، أو مؤسسة مالية، أو مشروعاً صناعياً أو تجارياً ضخماً، لا يبلغ عن تلك الجريمة والسبب في ذلك يرجع إلى أن الإبلاغ عن تلك الجرائم ربما يؤدي إلى إحاطة المجرمين عمداً بنقاط الضعف في أنظمتها، ورغبة منها في تفادي الخسائر التي قد تلحق بها من جراء هذا البلاغ وتأثير ذلك في ثقة العملاء بها



ويقول المستشار القانوني عبدالله الكعبي: إن إدانة الجريمة الإلكترونية تنبع من طبيعة الجريمة التي تحدد الإجراءات، إذ تختلف عن نظيرتها التقليدية بطبيعتها وطرق إثباتها وجمع الأدلة واتخاذ الضبطية القضائية في تتبع الجريمة

وأضاف: هناك عدد من التحديات التي تعطل إثبات الجرائم المعلوماتية أبرزها عدم التزام الشركات المزودة لخدمات التواصل، بتوفير تسهيلات للجهات القضائية، وصعوبة الاحتفاظ الفني بدليل الجريمة، إذا يستطيع المجرم المعلوماتي حذف البيانات والمعلومات. مشدداً على تضافر الجهود بين المؤسسات الخاصة والحكومية، ومنها على سبيل المثال تنظيم الاتصالات والتنمية الاقتصادية والصحة للحدّ من الجريمة الإلكترونية



وأشار إلى أن المتهمين في الجرائم الإلكترونية على إمام بطبيعة الأجهزة التي يتعاملون معها، وكيفية تطبيق الجريمة من دون ترك أي دليل يثبت تورطهم، لذلك يجب تطوير القوانين مع تطور الجريمة الإلكترونية التي تتطور مع تقدم الأجهزة التي تتعامل معها، وأن تصدر القوانين لسد الثغرات التي تواكب تطور الأجهزة

وطالب الكعبي هيئة الاتصالات بتحديث الرقابة وإيجاد بيئة آمنة لخدمات البيانات وحجب المواقع والتطبيقات التي تسبب مشكلات، أو تمثل تقنيات ضارة، أو برامج انتهاك لخصوصية



ويتفق المحامي والمستشار القانوني عبيد الصقال مع ما سبق، ويضيف إليه: هناك صعوبات في إثبات الدليل الإلكتروني والعبث بالدليل لا يترك أثراً مادياً مثلما هو في الدليل العادي، لأن المجني عليه في جرائم الابتزاز الإلكتروني يتكتم على الجريمة ولا يبلغ السلطات المختصة عنها، خوفاً من التشهير وهذا يساعد المجرم في الإفلات

وقال إن أبرز المصاعب للتوصل إلى الدليل عند تعامل العميل مع شركات كبيرة مزودة لمواقع التواصل، وهذه الشركات تحافظ على خصوصية عملائها، ولا تشارك البيانات بسهولة، ما يؤخر إثبات الأدلة

وطالب بإلزام الشركات المزودة لخدمات التواصل، بتوفير تسهيلات للجهات القضائية للحصول على بيانات المتهمين في قضايا الابتزاز والاحتيال والجرائم الإلكترونية

وأضاف: هنالك زيادة ملموسة في البرمجيات الخبيثة والروابط غير الآمنة، خلال العام الأول من تفشي الفيروس، ما يعني تخلي الناس عن حذرهم مقابل رغبتهم في معرفة معلومات إضافية عن الفيروس، سواء كانت حقيقية أو زائفة

تحديات عدة



أما المحامية إيمان الرفاعي، فتري أنه تترتب على ظاهرة الجريمة الإلكترونية تحديات عدة، منها ظهور وتنامي الأنشطة الإجرامية الإلكترونية واستخدام مرتكبيها تقنيات جديدة غير مسبوقة في تكنولوجيا المعلومات والاتصالات، يسرت لهم ارتكاب هذه الأنشطة داخل حدود الدولة وخارجها، ما أدى إلى تبني الدولة للمؤتمرات الدولية بهذا النوع من الجرائم ودعوتها للدول التصدي لها ومكافحتها

وأضافت «بدراسة الأبعاد السكانية والاقتصادية واتجاهات السكان وسلوكهم، وغيرها من النواحي الأخرى على الشبكة، «يمكن التنبؤ بمعدلات الجرائم وأنواعها

وطالبت بضرورة إشراك الشرطة في الأبحاث العالمية للشركات الكبرى عند طرح أي خدمات جديدة إلكترونية لصقل الخبرات والتوعية لحماية الحقوق

مؤكد أن المعرفة التكنولوجية مفتاح الحل وسلاح الحماية، خصوصاً أن الجريمة الحديثة لا تحكمها جغرافيا، وربما مستقبلاً ستوفر خدمات أسرع في هذا المجال لرصد البصمات الإلكترونية للمجرمين التي توثق دخولهم لأي موقع إلكتروني أو هاتف، وتسهّل القبض عليهم

أبرز الثغرات

وأفاد الدكتور أحمد فلاح العموش، أستاذ علم الجريمة في جامعة الشارقة، بأن اليوم لم يعد «الهاكرز» يعمل في الخفاء، بل يواجه الضحية، ويخبره أنه يهاجمه ويقاوضه على مبادلة المعلومات بالمال، ومنها نظام الفدية الذي انتشر أخيراً. والأموال تحول عبر «الأموال الافتراضية» التي لا يمكن تعقب متسلمها ولا دليل على إدانته

وحدد أبرز الثغرات الموجودة في الأنظمة التي يسهل اختراقها وهي الاستخدام غير الآمن، والذي يتيح لأشخاص غير

مرخصين الدخول على أنظمة المعلومات واختراق الأنظمة وأخذ مواصفات المشغل، وعندها يمتلكون خاصية الدخول وسرقة المعلومات أو تدميرها لأسباب تخريبية.

وطالب بتأسيس قاعدة بيانات عالمية يمكن بها أخذ بصمات إلكترونية تحدد الذي يدخل للشبكة العنكبوتية أو الذي يستخدم منصات التواصل، تحت غطاء شخصية وهمية وأن تغذى تلك المنصة من مختلف الدول بالمعلومات المطلوبة عند الحاجة. وأظهر تقرير جديد أصدرته مؤسسة دبي للمستقبل بعنوان «الحياة بعد كوفيد 19: مستقبل الأمن السيبراني»، تزايداً ملحوظاً في الهجمات السيبرانية، والجرائم الإلكترونية، خلال المرحلة الماضية، مع ظهور ثغرات أمنية في أنظمة البنى التحتية القائمة، في ظل تفشي فيروس «كورونا» المستجد في مختلف دول العالم. وأرجع التقرير - الذي يأتي ضمن سلسلة التقارير التي تنشرها المؤسسة لاستشراف مستقبل القطاعات الحيوية - الزيادة في حجم التهديدات السيبرانية إلى سعي المخترقين المتواصل للوصول إلى المعلومات، التي تجمعها الدول والحكومات لتتبع المصابين، والحد من انتشار الفيروس، وتوظيفها في الهجمات الإلكترونية، التي ينفذونها ما يضع أمن المعلومات أمام تحديات كبيرة. واستعرض مجموعة من تقارير شركات متخصصة بأمن المعلومات، كشفت عن تصاعد الجرائم الرقمية بنسب عالية، بما في ذلك تقرير صادر عن شركة «مايم كاست»، بعنوان «100 يوم من فيروس كورونا» ذكر أن عدد الجرائم الإلكترونية ارتفع بنسبة 33 %، منذ مطلع العام الحالي حتى نهاية مارس/ آذار الماضي، مع ازدياد عدد زيارات الروابط غير الآمنة أكثر مما كان قبل تفشي الوباء.

ولاحظ أن قطاع الرعاية الصحية يأتي على رأس القطاعات التي تعرضت للهجمات السيبرانية عبر هجمات برامج الفدية، خصوصاً أن مرتكبي الهجمات الإلكترونية كانوا يعتقدون أن المؤسسات الصحية ستضطر إلى دفع الأموال «الفدية»، لاستعادة أنظمتها التي تعتمد عليها في مواجهة انتشار الفيروس.

تدابير حماية

ولا تألو الجهات والمؤسسات كافة، المعنية بدولة الإمارات، جهداً في اتخاذ جميع التدابير التي تحمي الدولة، ومؤسساتها، وأفرادها، من خطر الجرائم الإلكترونية بمختلف صورها. وتعاونت الهيئة العامة لتنظيم الاتصالات، مع شركتي «اتصالات» و«دو»، بحجب 3934 موقعاً إلكترونياً ومحتوى خاصاً بالإنترنت خلال عام 2020، مقابل 1688 % موقعاً خلال عام 2019، بزيادة نسبتها 133

وتضم فئات المحتوى المحظور 19، وشملت المواقع المحجوبة مواقع تدرج تحت 16 فئة من فئات المحتوى المحظور، بينما خلت القائمة من حجب أي مواقع تدرج تحت ثلاث فئات أخرى

وأوضحت الهيئة في تقرير عن المحتوى المحظور خلال عام 2020، أن عدد مواقع النصب والاحتيال والتصيد الإلكتروني التي حجبت خلال العام الماضي بلغ 534، بنسبة 13.6 %، لتحل بذلك المركز الثاني، مقابل 436 موقعاً عام 2019، بارتفاع 22.5 %.

وعن دور الشرطة للحد من هذه الجرائم، أطلقت شرطة أبوظبي الدورة الرابعة من الحملة الإعلامية التوعوية «خلِّك حذر» لتعزيز وعي المجتمع بالأشكال المستجدة للجرائم الإلكترونية المتمثلة بعدة أنواع مثل «النصب الهاتفي» والاحتيال والابتزاز، والتنمر، والتسول الإلكتروني، والتوظيف الوهمي.

وأوضح العميد محمد سهيل الراشدي، مدير قطاع الأمن الجنائي، أن الحملة في عامها الثالث وتستمر مدة شهر، تركز

على زيادة الوعي لدى الجمهور من مستخدمي «الإنترنت» والأجهزة الذكية بضرورة المحافظة على بياناتهم ومعلوماتهم الخاصة وعدم الإفصاح عنها، تجنباً للوقوع ضحايا لتنظيمات هدفها زعزعة الاستقرار والأمن وإحداث الفوضى في المجتمع. وذكر أن الحملة تستهدف تحذير جميع شرائح المجتمع بأخطار الجرائم الإلكترونية. مؤكداً الحرص على تضيق الخناق على المحتالين، وضبطهم والتصديّ لأساليبهم الإجرامية المتجددة بتدابير احترازية أمنية متقدمة

وأوضح أن الجرائم الإلكترونية من الجرائم التي تتعامل معها الأجهزة الأمنية بأولوية خاصة، مؤكداً تضافر جهود جميع الإدارات المعنية في شرطة أبوظبي للتصدي للجرائم الإلكترونية مهما اختلفت أشكالها وأنواعها وطرائق ارتكابها

ودعا الأسر إلى أهمية مراقبة أبنائهم من الابتزاز الإلكتروني وابتزاز الذين ينتحلون صفة الفتيات واستدراجهم بصور صداقة، ثم يبدأ الابتزاز الجنسي والمالي عن طريق وسائل التواصل الاجتماعي وكشف العقيد سعيد الهاجري، مدير إدارة مكافحة الجرائم الإلكترونية بالإدارة العامة للتحريات والمباحث الجنائية في شرطة دبي، جرائم إلكترونية استُحدثت خلال بداية جائحة «كورونا»، واستهدفت قطاعات حيوية، مثل القطاع الصحي، إذ استغل مجرمون جهل أفراد المجتمع وقلقهم من الجائحة، للاحتيال عليهم وخداعهم

وقال إن شرطة دبي ضبطت عصابات استغلت الجائحة في الترويج عبر الإنترنت لكمامات وأجهزة تنفس، وتبين أنهم محتالون وقبض عليهم وأحيلوا إلى الجهات المختصة

وأفاد بأن مؤشر البلاغات والاتصالات المتعلقة بجرائم إلكترونية، ارتفع بنسبة تصل إلى 3000% منذ إطلاق منصة «إي كرايم»، قبل ثلاثة أعوام. مؤكداً أن المشروع الاستراتيجي لشرطة دبي نافذة حيوية للتعرف إلى الاختراقات والوسائل الإجرامية الحديثة، ويعكس درجة عالية من الوعي لدى أفراد المجتمع. وأن أكثر من 25 ألفاً زدوا شرطة دبي بمعلومات قيّمة خلال العام الماضي، حوّل 20% منها إلى بلاغات اتخذت مساراً قانونياً، وضبط المتورطون فيها الموجودون داخل الدولة، فيما تستخدم 80% منها لتعزيز حماية المجتمع من الجرائم والممارسات المشبوهة