الاجتماع التاسع

للمتخصصين في أمن وسلامة الفضاء السيبراني (الإنترنت)

بيروت 2020/9/28

ورقة عمل

د. لينا الشلالدة أ. حنان ياغي/ وزارة العدل في دولة فلسطين

المحور الأول: الأدلة الرقمية وحجتها

دأبت دولة فلسطين إلى تحسين تشريعاتها لتواكب التطور السريع في المجال التكنولوجي، والذي أفرد بظلاله على كل جوانب الحياة بما فيها القانونية والقضائية، حيث عرف الدليل الالكتروني في الفقه القانوني على أنه البرهان أو الحجة التي تظهر صحة واقعه ما أو تنفيها، حيث أن الدليل هو الذي يمكن القاضي من التوصل للحقيقة التي يبني عليها حكمه، وجاء في قانون الجرائم الالكترونية الفلسطيني ان الدليل الناتج بأية وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الالكترونية أو البيانات والمعلومات الالكترونية من أدلة الاثبات.

وباستعراض للمنظومة التشريعية الفلسطينية ذات الصلة فقد نص قانون البينات في المواد المدنية والتجارية رقم (4) لسنة 2001، على سريان أحكام الفصل المتعلقة بالسندات غير الموقع عليها، وهي تعتبر من الأدلة الكتابية، على وثائق نظم الحاسب الالي، حيث ساوى القانون الفلسطيني في الاثبات بين الوثيقة المادية الرقمية المكتوبة باستخدام الحاسوب.

أما فيما يتعلق بقانون الإجراءات الجزائية، فقد نص بوضوح على أن تقام البينة في الدعاوى الجزائية بجميع طرق الاثبات إلا إذا نص القانون على خلاف ذلك بإشتراط طريقة معينه للاثبات، حيث أن الاثبات الالكتروني جائز في الدعاوى الجزائية طالما لم ينص القانون على طريقة معينة للاثبات واقتنع القاضي بالدليل الالكتروني.

كما تضمن قانون المعاملات الالكترونية 2017، يكون للمعاملات الالكترونية والسجلات والتواقيع الالكترونية أثرها القانوني وتعتبر صحيحة ونافذة، شأنها في ذلك شأن الوثائق المكتوبة، ولها صلاحية الاثبات.

وقد اثمرت الجهود التشريعية في فلسطين في سن قانون الجرائم الالكترونية المعدل 2018، والذي عالج في نصوصه موضوع الأدلة الرقمية وحجيتها، حيث يتولى مأموري الضبط القضائي في وحدة الجرائم الالكترونية في جهاز الشرطة عملية ضبط وجمع الأدلة بأمر من النيابة العامة أو المحكمة المختصة، واشترط القانون ان يكون مأمور الضبط القضائي مؤهلا للتعامل مع الطبيعة الخاصة للجرائم الالكترونية، كما ونظم القانون عدد من الاجراءات التي يتعين على الجهات ذات العلاقة اتخاذها، ومنها إجراءات عملية محددة ملزمة لمزود الخدمة اتخاذها، كما أجاز القانون للنيابة التفتيش والمراقبة والتسجيل والاعتراض ضمن شروط محددة والبحث عن أي دليل يساعد في كشف الحقيقة، كما يجيز للنيابة ضبط أي وسيلة تساعد في عملية التحقيق، والتحفظ عليها كاملة

او جزء منها أو نسخها واستخدام أي وسيلة تقنية لمصلحة التحقيقات، والحصول على الأجهزة والبيانات والمعلومات والاتصالات كما أجاز القانون بالاستعانة بذوي الخبرة، ويتوجب على الجهات المعنية الالتزام بكل تدابير الحماية للحفاظ على صحة الأدلة وسلامتها، ويعاقب في القانون كل من أقدم على العبث بالأدلة الرقمية من تعديل او إخفاء او اتلاف وغيره.

كما تُعتبر الأدلة المتحصل عليها من دول أخرى بمعرفة الجهة المختصة أدلة اثبات وفقا لبروتوكولات التعاون الدولي.

ولابد من الإشارة الى التقدم التقني الذي يتمتع به مأموري الضبط القضائي الفلسطيني ونيابة الجرائم الالكترونية في مجال ملاحقة المجرمين وكشف الجريمة بسرعة فائقة، هذا وتعمل كافة الأجهزة الحكومية على رفع قدرات العاملين في أجهزة انفاذ القانون من جهة، وتقديم برامج توعوية للمجتمع من جهة أخرى، وفي خطوة رائدة تقدم الجامعات الفلسطينية برامج دراسات عليا متخصصة في علم الجريمة وتحليل الأدلة الجنائية الرقمية بمختلف أنواعها من تشفير وشبكات وقواعد بيانات ونظم التشغيل والوسائط المتعددة والأجهزة اللوحية والنقالة والبيئة السحابية والخبير الرقمي في المحكمة وما الى ذلك من مواضيع متخصصة في علم الجريمة الالكترونية.

هذا ومع توسع الأنشطة الإنسانية في الفضاء السيبراني، ومع سرعة تطور وتنوع الأنشطة الاجرامية واستحداث وابتكار تقنيات جرمية جديدة، فإن الأدلة الرقمية تبقى لا حصر لها، حيث أن الابتكار الجرمي الالكتروني عادة ما يسبق الجهود التحقيقية، الا أن وجود برامج للتعاون العربي والدولي سيساعد في الإحاطة بنوعية الأدلة المستحدثة، وعليه يمكن على سبيل المثال لا الحصر – اعداد قائمة بالأدلة الرقمية مرفقة بالإجراءات الرقمية التي يتعين اتخاذها لكل دليل، وآلية حفظها وتخزينها ومعالجتها وضمان حمايتها، مع تحديثها بشكل مستمر وتبادلها في نطاق بروتوكول تعاون قضائي، أو يمكن تبادل برمجيات من شأنها ضبط الأدلة الرقمية بدون الاخلال بسلامة البيئة الرقمية.

وتسعى دولة فلسطين إلى اعداد قوانين ناظمة وضامنة لحقوق الانسان وبالتحديد لتوفير بيئة آمنة في ظل ازدياد وتيرة الجرائم الالكترونية مثل قانون حماية البيانات الشخصية وحق الحصول على معلومات.

المحور الثاني: الجرائم السيبرانية والجرائم المعلوماتية

بشكل عام، فإن **الجريمة السيبرانية** هي أي نشاط اجرامي يحدث في نطاق الفضاء السيبراني، سواء فعل جرمي رقمي ضد هدف رقمي، أو استخدام وسيلة رقمية لارتكاب نشاط اجرامي تقليدي.

وبناء على ذلك فإنه يمكن تقسيم الجرائم السيبرانية إلى نوعين أساسيين - النوع الذي يستهدف فيه المجرمون الشبكات والانظمة بحد ذاتها، والنوع الذي يرتكب فيه الأشخاص أعمالًا إجرامية باستخدام طرق رقمية.

أما **النوع الأول** الذي يستهدف الأنظمة الرقمية فقد أصبح المشهد الجرمي أكثر تعقيدًا وخطورة، فعلى سبيل المثال الحروب الكترونية او الاعتداءات الالكترونية واسعة النطاق التي من شأنها تعطيل وتدمير شبكات وأنظمة أمنية أو دفاعية الكترونية ذات طابع هام. ونظرًا لأن القدرة الرقمية أصبحت واسعة جدًا، فقد تطورت طبيعة الجرائم وفقًا لذلك.

وفي نفس السياق، فهناك افعال رقمية متعلقة بالعملات المشفرة حيث يتم الحصول على الأصول الرقمية بدون وجه حق أو التلاعب بها بشكل غير قانوني أو تضليل المستثمرين، وهذا النوع جديد

نسبيا لأن الأصول الرقمية نفسها لم تكن موجودة أما الآن فكل أنواع الأصول الإلكترونية موجودة في محافظ رقمية.

أما **النوع الثاني**، وحيث تُستخدم الوسائل الرقمية لتنفيذ أنشطة إجرامية تقليدية، فهناك سلسلة واسعة من العمليات الإجرامية التي تنطبق على ذلك، ويمكن توجيه الأنظمة لتضر الأشخاص جسديًا، كالاتجار بالبشر او تجارة الأعضاء او الجنس، وهناك ترويج المخدرات، المقامرة، تهريب الأموال، التشهير، التحريض، التنمر، الابتزاز، تقديم خدمة غير مرخصة، وما الى ذلك.

ان الجرائم المعلوماتية هي تلك التي تستهدف المعلومات بحد ذاتها وهي جزء لا ينفصل عن الجريمة السيبرانية، حيث تستخدم أساليب التحايل الرقمية لأنشطة غير قانونية تتعلق بالمعلومات الرقمية، فمثلا هناك عمليات دخول غير مشروع على قواعد البيانات تهدف الى شطب المعلومات أو تحريفها وهناك اعتداءات حاصلة على حقوق الملكية الفكرية، وسرقة المنشورات والأبحاث، أو التعديل على محتوى المواقع الالكترونية أو شطبها، وهناك عمليات التزوير في السندات والمعاملات، أو سرقة التواقيع الالكترونية أو تزويرها، وأيضا سرقة معلومات شخصية خصوصية ونشرها، التشهير والقدح والذم الالكتروني من حيث نشر معلومات بدون وجد حق او تصريح، التجسس للحصول على معلومات وبيعها أي تجارة المعلومات، أو بث معلومات تحريضية او عنصرية وبث خطاب الكراهية وما الى ذلك من الأمثلة التي لا يمكن حصرها.

ومما ذكر نرى ان كل جريمة معلوماتية تعتبر في نطاق الجرائم السيبرانية، ولكن لا يمكن اعتبار ليست كل الجرائم السيبرانية معلوماتية.

وتجدر الإشارة الى انه ورد في نصوص قانون الجرائم الالكترونية الفلسطيني تجريم العديد من الأفعال الرقمية، الا ان القانون لم يميز أو يصنف هذه الجرائم، فهي حتى الآن متداخلة أو لا يوجد تصنيف عالمي دقيق ومحدد للجريمة المستحدثة خاصةً.

وزارة العدل
فلسطين