الجرائم المعلوماتية وقضاياها المستجدة*

تشهد المملكة العربية السعودية تسارعاً ملحوظاً في استخدام تقنية المعلومات في مجالات الحياة المختلفة، ومع تزايد الاعتماد على تلك التقنية، استجدت قضايا متنوعة تمس الأفراد والمؤسسات وتؤثر بصورة مباشرة سلباً وإيجاباً على أمن البلد ونظامه الاجتماعي، وبالرغم من قلة هذه القضايا في المملكة مقارنة ببقية دول العالم لما حباها الله من الاعتماد على الكتاب والسنّة في جميع شؤون الحياة، فإن الحاجة قد باتت ماسة لوضع أحكام وأنظمة معلوماتية ولوائح تحكم مختلف تلك الأعمال الإلكترونية في حياتنا، وجاء نظام مكافحة الجرائم الإلكترونية منظماً لتلك الأعمال ويحد من استغلالها السيء لحفظ الحقوق والتبعات.

وفي هذه الندوة نسلط الضوء على عدد من الصور الإجرامية التي خلفت كثيراً من الخسائر المادية والأخلاقية بسبب شيوع استخدام وسائل التقنية الحديثة والمستجدة التي قد تنشأ في الخطأ وتمس الحقوق العامة والخاصة ويصل الأمر إلى أن تطال معطيات الكمبيوتر المخزنة والمعلومات المبرمجة أو المنقول عبر شبكات ونظم كما هو الحال في عالم الإنترنت وتهدد الأمن والسيادة الوطنية وتقضي على إبداع العقل البشري وتشيع فقدان الثقة بالتقنية.

ويسر العدل أن تلقي الضوء على هذا النوع من القضايا.

---

* إشراف مدير التحرير محمد الدبيان – إعداد الباحث في المجلة حمد الخنين

لمحة تاريخية:

أدركت حكومة المملكة أهمية الثورة المعلوماتية وخروج الحاسسبات الآلية، فقامت بجهود مباركة ففي عام ١٤١٧هـ ١٩٩٧م صدر قرار مجلس الوزراء رقم ١٦٣ في ١٤١٧/١٠/٢٤هـ الذي أناط بمدينة الملك عبدالعزيز للعلوم والتقنية مهمة إدخال خدمة الإنترنت العالمية وتبعاً لذلك أنشأت وحدة خدمات الإنترنت التي تولت كافة الإجراءات اللازمة لإدخال هذه الخدمة وتشغيل الشبكة وتسجيل مقدمي الخدمة وترشيح المحتوى وتأهيل القطاع الخاص، وقد بدأت الخدمة في المملكة في ١٤١٩/٨/٢٦هـ حيث تم ربط الجامعات وشركات تقديم الخدمة المحلية بهذه الشبكة من خلال مركز معلومات الشبكة ومركز تشغيل الشبكة وقسم الخدمات المساندة وعلاقات الخدمة ومركز أمن المعلومات وبذلك انطلقت الخدمات الحاسوبية في كافة المصالح والمؤسسات وسابقت الزمن، حيث الحكومة الإلكترونية.

شارك في الندوة:

١ - الشيخ عبدالله بن محمد اليحيى - وكيل وزارة العدل.

٢ - د. سليمان بن عبدالملك آل الشيخ - مدير عام الحاسب الآلي ومركز المعلومات بوزارة العدل.

٣ - د. زيد بن محمد الرماني - عضو هيئة التدريس بجامعة الإمام محمد بن سعود الإسلامية.

٤ - د. عبداللطيف بن محمد السبيل - القاضي بديوان المظالم.

٥ - د. رضا متولي وهدان - أستاذ الأنظمة المشارك في المعهد العالي للقضاء بالرياض.

٦ - د. محمد بن المدني بوساق - وكيل مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية.

٧ - محمد بن عبدالعزيز المهيزع - مدير عام إدارة المستشارين بوزارة العدل.

٨ - فهد بن إبراهيم المفرج - مدير إدارة الإشراف البنكي بمؤسسة النقد العربي السعودي.

٩ - د. عبد الرحمن بن عبدالله السند - استاذ الفقه المساعد بالمعهد العالي للقضاء

١٠ - د. إبراهيم أحمد زمزمي - المحامي والمستشار القانوني.

١١ - صالح بن غرم الله الزهراني - وكيل كلية علوم الحاسب والمعلومات بجامعة الإمام محمد بن سعود الإسلامية.

الحاسب الآلي:

يعد الوسيلة الأولى والأهم لفبركة الصور ومعالجتها وتعديل ملفات الصوت والفيديو للحصول على أهداف معينة وأغراض غير شريفة وهو آلة سهلة لممارسة الجرائم الإلكترونية مما قلل الفائدة المرجوة من خلاله.

الإنترنت:

فتح آفاقاً جديدة وعصراً فريداً وأذهل العالم باختراعه ثم فيه تقارب المسافات والأوقات اللازمة لإنجاز المهمات وساعد على أداء الأعمال عن بعدوقلب فلسفة التجارة والتعليم والخدمات الحكومية.

البريد الإلكتروني:

من أقوى الوسائل التي اتبعها منفذو الجرائم الإلكترونية كوسيلة للإيقاع بالضحايا ومن أهمها: الغش وإرسال الفيروسات وقصف البريد الإلكتروني، والتهديد والابتزاز، نظراً إلى أنها أسرع وأسهل الطرق لنشر الفيروسات والتروجانات «ملفات التجسس» عبر الإنترنت بعناوين مثيرة لإقناع المتلقي بفتح الرسالة وتشغيل المرفق وبالتالي يتم زرع الفيروس أو ملف التجسس في الجهاز ويمكن تعرض البريد الإلكتروني للقصف وذلك بإرسال رسائل بكميات كبيرة من الرسائل الإلكتروني مما يؤدي إلى تدميره، كما أن البريد الإلكتروني وسيلة قوية للتشهير أو الافتراء بهدف الانتقام وإثارة البلبلة، لذلك فإن البريد الإلكتروني وسيلة مهمة يجب الحذر من التعامل معه.

تعريف الجرائم المعلوماتية:

نوع من أنواع الجرائم فاعلها يكون ملماً بتقنيات الحاسوب ونظمه والهاتف النقال في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع لمنافاتها الأخلاق العامة.

تصنيف الجرائم المعلوماتية:

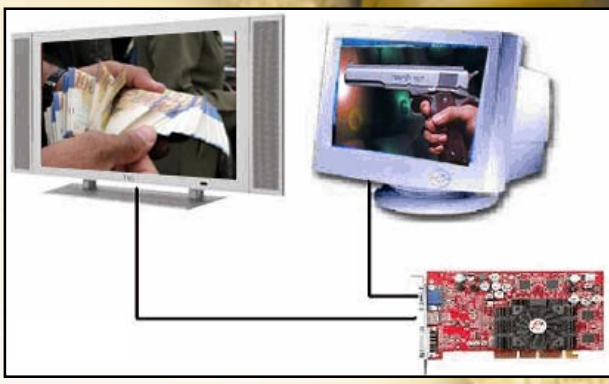
١ - حسب التنفيذ: (فردي - فردي)، (فردي - جماعي)، (جماعي - فردي)، (جماعي - جماعي).

٢ - حسب النوع: «التسلل والتجسس، الاتلاف والتدمير، التزوير والتغيير، الخداع والتغرير».

٣ - حسب الأهداف: «إثبات الذات، التشفي والانتقام، الضغط والابتزاز».

٤ - حسب الدوافع: «نفسية، جنسية، عقائدية، عنصرية».

٥ - حسب الوسائل: «البريد الإلكتروني، الحاسب الآلي، الهاتف النقال، الشبكات».



أهداف الجرائم الإلكترونية:

١ - الوصول إلى المعلومات بشكل غير قانوني، كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.

٢ - الوصول إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو تخزينها وعادة ما تتم هذه العملية على مواقع الإنترنت.

٣ - الحصول على معلومات تغيير عناوين مواقع الإنترنت بهدف التخريب على المؤسسات العامة وابتزازها.

٤ - الوصول إلى الأشخاص أو الجهات المستخدمة للتكنولوجيا بغرض التهديد أو الابتزاز كالبنوك والدوائر الحكومية والأجهزة الرسمية والشركات بكافة أشكالها.

٥ - الاستفادة من تقنية المعلومات من أجل كسب مادي أو معنوي أو سياسي غير مشروع كعمليات تزوير بطاقات الائتمان وعمليات اختراق مواقع إلكترونية على الشبكة العنكبوتية.

٦ - استخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة أو نشر الأفكار التي يمكن أن تؤسس إلى فكر تكفيري.

معلومات جنائية:

أعلن مركز بلاغات جرائم الإنترنت complain center internet cnime (ic٣)

في تقريره السنوي لعام ٢٠٠٧م أن مقدار ما تم خسارته في تكاليف الاستقبال للبلاغات الناتجة من سوء استخدام الإنترنت هو ١٩٨.٤ مليون دولار وذلك بزيادة قدرها ١٥.٣ مليون دولار عن السنة التي قبلها، وهذه الأرقام والإحصائيات الرسمية ليست نتائج الجرائم المعلوماتية، بل فقط لتسجيلها وتدوينها، أما ما أحدثته الجرائم من آثار ما الله به عليهم، ناهيك عن الآثار المعنوية والنفسية وغيرها من الآثار التي أصبحت عائقاً أمام التطور

❖ اليحيى:

• وزارة العدل تسعى لتضمين الدورات القضائية موضوعات ومحاور عن المستجدات وجدوى تطبيقها وتنزيل الأحكام عليها
• توثيق الصلة بين القضاء الشرعي وفقه الواقع مسلك محمود

البشري من خلال استخدامات التقنية بالصورة التي يجب أن تكون عليه.

المؤتمر العالمي لمواجهة الجرائم الإلكترونية:

يقام سنوياً، ويقدم أفكاراً وحلولاً متقدمة وإستراتيجيات يمكن نشرها من قبل الشركات العالمية والحكومات لمواجهة الجريمة الإلكترونية. وهو مخصص للمهتمين في مجال أمن المعلومات ومكافحة الجرائم الإلكترونية، حيث يشارك فيه أكثر من (٥٠٠) مشارك من كبار شركات التقنية وكبار مسؤولي الحكومات في العالم، موقع المؤتمر www.e-crimecongress.org

محاور الندوة

في البداية تحدث **فضيلة وكيل وزارة العدل الشيخ عبدالله بن محمد اليحيى** عن دور الوزارة في إطلاع القضاة وتعريفهم بكنه الجرائم الإلكترونية عبر الحاسوب وعبر شبكة «الإنترنت» والهواتف المحمولة. وغيرها فقال:

إن توثيق الصلة بين القضاء الشرعي وفقه الواقع مسلك اجتهادي محمود يضمن حسن التنزيل على الواقعات وصون مآلات الأحكام المتمخضة لخير الإنسان من التعطيل، ذلك أن فقه النص ليس بكافة وحده في تسديد العملية الاجتهادية وتفعيل الحياة بها ما لم يلتحم بفقه الواقع في سبيكة رائعة يمكن الاصطلاح عليها «بالمعادلة الصعبة» في الاجتهاد الفقهي.

والإلمام بمبادئ العلوم الإنسانية المعاصرة كالطب والاقتصاد والكيمياء وغيرها بوصفها مفاتيح لتحقيق المناط الخاص في الوسائل المستجدة وهي من الأدوات المعينة لسبر فقه الواقع على نحو يتيح الفهم العميق والتفسير المعقول للواقعات الاجتماعية والاقتصادية والعلمية المعاصرة.

والوزارة بتوجيه من معالي الوزير -حفظه الله- تسعى

❖ *آل الشيخ:*

• تتفاوت الأساليب الإجرامية المتعمدة في الوسائل الإلكترونية لتفاوت أسبابها
• وجود الآليات الفنية وتطويرها تساهم في الحد من جرائم المعلوماتية

لتضمين الدورات المعقودة لتدريب أصحاب الفضيلة القضاة سواء في المعهد العالي للقضاء أو جامعة نايف العربية للعلوم الأمنية أو المعهد المصرفي عدداً من المحاور والموضوعات المعينة على التصور والوصف للوقائع التي يتعرض إليها القاضي أثناء عملية التطبيق وتنزيل الأحكام على القضايا المنظورة وهذه المحاور والموضوعات تكون على النحو التالي:

أ - محاور تعنى بالحدود والتعريفات والاصطلاحات الفقهية الفروعية والأصولية ذات العلاقة بالأبواب والمباحث العلمية المساندة للنظر القضائي في أثناء التعامل مع النوازل القضائية.

ب - محاور تعنى بتعريف المصطلحات المعاصرة في التخصصات ذات العلاقة للنظر القضائي كالاصطلاحات الاقتصادية والحاسوبية وما يقابلها من الأوصاف الفقهية وكالمصطلحات الطبية والمهنية والقانونية وغيرها.

ج - محاور تعنى بالقواعد الإجرائية والمواد النظامية الواردة في أنظمة الدولة والاتفاقيات الدولية المتعلقة بالاختصاصات النوعية للقضاء لتأدي وظائف مختلفة ونتائج متنوعة ويستأنس بها القاضي في الأحكام من خلال تأكيدها في مضامين الحكم وتسبيباته أو بتأسيس مبادئ ينطلق منها المشاركون في العمل القضائي وكذا المستفيدون من المحامين والدارسين للقانون.

وهذا النوع من الأطروحات والندوات تعد من المعينة على الاجتهاد القضائي المعاصر ومن ضروراته ووسائل النهوض به، بل إن ذلك يعد من جواد التأهيل المستصحب والتدريب المرافق للقاضي والباحث الشرعي وكل هذا لا شك أنه سيعود على البيئة القضائية بالتطور والارتقاء في الجوانب النظرية والعملية.

التنوع في أساليب الجريمة ومستجداتها

وحول الجديد في تقنية الحاسوب في مجال الاستدلال إلى كنه وأساليب المجرمين في استخدام (الإنترنت) وأجهزة الاتصالات حول ذلك أبان **سعادة مدير عام إدارة الحاسب الآلي ومركز المعلومات بوزارة العدل د. سلمان بن عبدالملك آل الشيخ** أن تقنية الحاسب والاتصالات سلاح ذو حدين، فمع كونها تساهم في تقديم خدمات عديدة لا يكاد يستغني عن معظمها الكثير من الأفراد والجهات فإن إساءة استخدامها أدى إلى مفهوم الجريمة الإلكترونية والتي تعد من نوازل هذا العصر، وتتعدد الوسائل الحديثة المستخدمة في هذه الجرائم مثل الحاسب الآلي وأجهزة الجوالات ومن خلال البرامج والشبكات السلكية واللاسلكية بما فيها الإنترنت والبريد الإلكتروني، ويمكن الحد بشكل كبير من هذه الجرائم من خلال التعرف على أشهر أساليب المجرمين والعمل على الوقاية منها من خلال اتباع الآليات التي تساهم في منعها أو الحد من آثارها.

أساليب متنوعة

وتتفاوت الأساليب الإجرامية المعتمدة على التقنية كما تتفاوت أسبابها من التعمد إلى التسلية أو الخطأ غير المقصود، وتعتمد كثير من جرائم المعلوماتية على أساليب فنية بينما في المقابل يعتمد بعضها على استغلال نقاط الضعف البشرية أو الاستخفاف بالعقول.

فمن جهة الأساليب المعتمدة على التقنية فإنها تشمل التجسس على الشبكات ونشر الفيروسات والاعتماد على جهاز وسيط والإغراق بالطلبات واستغلال الثغرات الأمنية واستخدام برامج للبحث عن كلمات المرور وتقليد شاشات وصفحات مواقع، ويكون التجسس على الشبكات -سواء كانت سلكية أم لاسلكية- من خلال التنصت واعتراض البيانات عبر الشبكات ببرامج وأجهزة خاصة، أما الفيروسات وما شابهها من البرامج المتطفلة والديدان وأحصنة طروادة وبرامج التجسس فهي برمجيات تنتقل إلى الأجهزة الحاسوبية عن طريق الشبكات أو أقراص الوسائط الإلكترونية أو الرسائل الإلكترونية بحيث تعمل على هذه الأجهزة بشكل خفي لسرقة أو لتدمير البيانات أو لتعطيل الأجهزة، وتقوم بعض الأساليب التقنية بالاعتماد على جهاز وسيط لتنفيذ الجريمة الإلكترنية بحيث يكون لمقترف الجريمة القدرة على إصدار الأوامر من جهازه إلى الجهاز الوسيط والذي بدوره ينفذ الأوامر الإجرامية، وبعد الانتهاء يقوم صاحب الجريمة بحذف بيانات الجهاز الوسيط والتي تمكن من التعرف عليه، والهدف من ذلك هو إعاقة تعقبه وتحديد مصدر الجريمة، ومن جهة أخرى تهدف بعض البرامج إلى إرسال الطلبات أو الرسائل الإلكترونية بشكل مكثف إلى الأجهزة أو المواقع الإلكترونية أو العناوين البريدية الإلكترونية مع مرفقات كبيرة الحجم بهدف تعطيلها أو التأثير

على خدمتها واستجابتها للآخرين، كما أن أحد أهم الأساليب الإجرامية المعتمدة على التقنية تقوم على استغلال الثغرات الأمنية الناتجة عن الأخطاء والعيوب البرمجية في الأنظمة التشغيلية والشبكية فور اكتشافها والتي عادة ما يغفل عنها معظم المستفيدين من التقنية، إضافة إلى ذلك تستخدم برامج متخصصة للبحث عن كلمات المرور «السر» وفحص المداخل أو البوابات «ports» أو لالتقاط المفاتيح المضغوطة على لوحة المفاتيح ومن ثم تمريرها بهدف التعرف على المعلومات الشخصية، ومن الأساليب التي لا يتنبه لها البعض فتح شاشات أو صفحات مواقع على الإنترنت على أنها من قبل جهة موثوقة وذلك من خلال تقليدها لواجهات مواقع مشهورة وعند كتابة كلمات المرور أو أرقام البطاقات الائتمانية تمرر إلى الموقع الأصلي بعد حفظ نسخة منها.

أما من جهة الأساليب المعتمدة على النواحي البشرية فهي تعتمد على الاتصال المباشر بالأفراد سواء بالبريد الإلكتروني أو رسائل الجوال بغرض استغفال أو رثارة الآخرين، وذلك من خلال الوعد بتحقيق أرباح طائلة أو عرض معلومات شيقة، فعادة ما يحاول بعض المجرمين الحصول على بيانات شخصية للآخرين من خلال إرسال بريد إلكتروني يتضمن قصة مشروع تجاري ويطلب معلومات شخصية مثل أرقام حسابات بنكية أو بطاقات ائتمانية بهدف تحقيق الربح المشترك، وخاصة أن مثل هذه المحاولات لا تكلف أكثر من تجميع عناوين للبريد الإلكتروني وإرسال رسالة لها، إضافة إلى ذلك تتضمن بعض الرسائل وصفحات المواقع عبارات مثيرة للقارئ أو يرفق مع الرسائل الإلكترونية ملفات تظهر على أنها مستندات أو صور والتي ما أن يقوم القارئ بالدخول عليها أو فتحها حتى يقع ضحية دون أن يشعر.

ومعرفة القاضي ودرايته بما يستجد من نوازل تقنية أملتها المتغيرات أمر في غاية الأهمية، فعلى سبيل المثال مسألة التلصص على البطاقات الائتمانية ومن ثم استخدامها في سداد الفواتير أو شراء البضائع هو من باب السرقة وإن كان ينظر لها أنه ليس من حرز، ولكنه ينافي الحفاظ على أحدى الضرورات الخمسة التي حافظ عليها الإسلام وهي ضرورة حفظ المال، ومن الأمثلة الأخرى مسألة استخدام الجوال في قذف أو تهديد الآخرين عبر رسائل الجوال والتي تتنافى ضرورة العرض أو النفس.

طرق الحد من الجريمة:

وتوجد الكثير من الطرق والآليات التي تساهم في الحد من هذه الجرائم أو التخفيف من الآثار المترتبة عليها، ومع أهمية التركيز على الطرق والآليات الوقائية التي تهدف إلى منع وقوع هذه الجرائم ابتداء فإنه تجدر الإشارة إلى ضرورة تبني الطرق العلاجية التي تهدف إلى إيقاف انتشار هذه الجرائم والحد من آثارها مع سرعة علاجها، ويمكن تقسيم هذه الطرق حسب طبيعتها إلى جوانب نظامية وجوانب توعية للمجتمع والأفراد إضافة إلى الآليات الفنية.

فالنواحي النظامية تشمل العقوبات الرادعة ووضع واتباع سياسات وإجراءات لأمن المعلومات، فإيقاع العقوبات لمرتكبي هذه الجرائم سيكون رادعاً لضعاف النفوس عن الشروع فيها وقد صدرت في المملكة مجموعة من الأنظمة ذات العلاقة في هذا المضمار مثل نظام التعاملات الإلكترونية ونظام مكافحة جرائم المعلوماتية، وهي بلا شك جهد مشكور ولبنة بناءة، ومن الأمور المهمة التي ينبغي للجميع الاهتمام بها وضع سياسات وإجراءات لأمن المعلومات داخل المنشأة ومراجعتها بشكل دوري والتأكد من مدى الالتزام بها التي تشمل على العديد من الجوانب على حسب طبيعة الاحتياج والأعمال مثل تحديد البرامج المسموحة على الأجهزة وتحديد المستفيدين من الشبكة وكيفية التعامل مع الإنترنت والبريد الإلكتروني وآلية النسخ الاحتياطي للبيانات وتحديد صلاحيات الوصول إلى الأنظمة والبيانات بل حتى آلية الوصول الشخصي إلى المواقع والأجهزة داخل المباني.

ومن ناحية أخرى فإن لتوعية المجتمع والأفراد أهمية قصوى وبالغة، وهي تشمل التثقيف بأمن المعلومات بهدف اتباع الإرشادات والتحذير من مغبة التصرفات غير الواعية، فالمجتمع بحاجة إلى زيادة التثقيف بمبادئ علم أمن المعلومات والمختص بوسائل وإجراءات حماية المعلومات من التهديدات والمخاطر بأنواعها وتأكيد صحتها وسلامة محتواها من التعديل مع منع الاطلاع عليها من قبل غير المصرح لهم، ويشمل ذلك التأكيد على عدم إفشاء المعلومات عبر الوسائل الإلكترونية أو حتى حفظها على الحاسب بشكل مباشر.

وكذلك عدم فتح البريد الإلكتروني مجهول المصدر وعدم

الدخول إلى المواقع المجهولة، مع البعد عن التخاطب مع المجهولين والذي عادة ما يبدأ بدافع الفضول وحب الاستطلاع، ومن أفضل الممارسات في هذا المجال التعود على إقفال الحاسب حال البعد عنه بحيث لا تنقل منه بيانات من خلال الاتصال بالإنترنت، وكذلك استخدام قرص صلب خارجي لحفظ الملفات الشخصية عليه وفصله عن الحاسب عند الاتصال بالإنترنت، وأما فيما يتعلق بالشبكات اللا سلكية فمن الضروري تشفير هذه الشبكات - وهذا أمر سهل - وعدم تركها مفتوحة يسهل الدخول عليها والتلصص على بياناتها وهذا عادة ما يهمل في الاتصال المنزلي بالإنترنت لاسلكياً، وبالمثل فإن معظم أصحاب الأجهزة يهملون الأسماء وكلمات المرور الافتراضية فتترك كما هي والأفضل تعديلها بحيث لا تكون مدخلاً للآخرين على الأجهزة.

الآليات الفنية الوقائية

آخر جوانب الآليات التي تساهم في الحد من جرائم المعلوماتية هي الآليات الفنية مثل الجدر النارية والبرامج المضادة للفيروسات واستخدام الشبكات الافتراضية وسجلات المتابعة وتحديث البرامج والأنظمة التشغيلية مفتوحة المصدر والتوقيع الإلكتروني وطرق التحقق من الهوية، فالجدر النارية - سواء كانت برمجية أم أجهزة- تقوم بمنع دخول المتسللين وفلترة البيانات الواردة أو الخارجة، أما البرامج المضادة للفيروسات فتقوم بفحص أجهزة الحاسب وأقراص الوسائط الإلكترونية ورسائل البريد الإلكتروني، ومن جهة أخرى فإن الشبكات الافتراضية تساهم في تحويل العمل على شبكة الإنترنت كشبكة غير امنة إلى شبكة افتراضية امنة خاصة تشفر البيانات عبرها ولا يتاح الاطلاع عليها إلا للمصرح لهم، ومن الوسائل الفنية الأخرى حفظ ملفات وسجلات المتابعة بأنواعها وعلى جميع المستويات التي تضم التعرف على عناوين الأجهزة المرسلة لطلبات من عناوين شبكية وفيزيائية وكذلك بيانات التعديل والحذف ومن أجراها للرجوع إليها عند الحاجة، ومن الأمور المهمة تحديث البرامج بشكل دوري بما فيها أنظمة التشغيل والبرامج المضادة للفيروسات، ومن الأمور التي يمكن الاستفادة منها في هذا المضمار على مستوى وطني برامج الأنظمة التشغيلية مفتوحة المصدر بحيث تغلق جميع المنافذ الافتراضية وتضاف برمجيات مساندة لأمن المعلومات فلا يتاح حتى لمصممي البرامج التشغيلية اختراق المعلومات السرية، وكذلك تفعيل دور التوقيع الإلكتروني بمفهومه الصحيح والمبني على المفاتيح العمومية والخصوصية لكل مستفيد مع استخدام برامج التشفير في التراسل، ومن الطرق الفنية الأخرى التأكد من شخصية المستفيد ومشروعية عمله من خلال كلمات المرور وبطاقات التعريف الذكية إضافة إلى السمات الحيوية كالبصمة وغيرها.

ويحسن التنبيه إلى أن تقنية الحاسب الآلي أصبحت خياراً إستراتيجياً وليست مجرد ترف، وإن وقوع بعض جرائم المعلوماتية ليس مسوغاً للتهرب من تفعيل هذه التقنية والاستفادة منها، ولكن المطلوب التعرف على كيفية التعامل معها بالشكل السليم والذي يجني ثمارها بأفضل وجه متاح.

للتوعية دورمهم

وحول محور التوعية ضد جرائم المعلوماتية شاركنا برأيه **المستشار الاقتصادي وعضو هيئة التدريس بجامعة الإمام محمد بن سعود الإسلامية د. زيد بن محمد الرماني** مشيراً إلى صعوبة الحصول على تحديد دقيق للمقصود بالجرائم، وتساءل الرماني:

لماذا تثار هذه الضجة الكبيرة حول قرصنة البرامجيات أو ما يعرف بشكل أشمل بالجرائم الإلكترونية؟!

من الصعوبة الحصول على تحديد دقيق للمقصود بالجرائم الإلكترونية، وذلك لتعددأساليب ارتكاب الجريمة الإلكترونية، وتتعدد أنماطها وظهور أشكال جديدة مستحدثة.

بَيْدَ أنَّ بعض الجهات العالمية والعلمية حاولت تعريف الجريمة الإلكترونية بأنها: فعل غير مشروع يرتكب متضمناً استخدام أي جهاز إلكتروني أو شبكة معلوماتية خاصة أو عامة كالإنترنت.

ولا يخفى أن أشكال الجرائم الإلكترونية كثيرة ومتنوعة، منها على سبيل المثال تلك الجرائم التي يكون فيها النظام المعلوماتي موضوع الجريمة، وذلك كما في حالة إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدميرها أو إعاقة الوصول إلى الخدمة، أو اختراق أو تدمير المواقع الإلكترونية أو اختراق البريد الإلكتروني.

❖ الرماني:

• ينبغي وضع عقوبات رادعة ضد التزوير الفكري

• نظام مكافحة الجرائم المعلوماتية سوف يتحسن بتحسن البيئة النظامية لاستخدامات تقنية المعلوماتية

• الصحوة الأخلاقية مطلوبة لإنقاذ إنجازات القرن التقنية

كما أن هناك جرائم يكون فيها النظام المعلوماتي أداة لارتكاب الجريمة ووسيلة لتنفيذها، كما في حالة استغلال الحاسب الآلي أو الشبكة المعلوماتية للاستيلاء على الأموال أو التشهير بالآخرين وتشويه سمعتهم أو الاعتداء على حقوق الملكية الفكرية.

البرمجيات وسرقتها

وتشير الوقائع إلى أن سرقة البرمجيات تسجّل تزايداً مستمراً يتزامن مع الانتشار والازدهار المستمر الذي تحققه صناعة الحاسوب.

وغزت الأسواق بضاعة فكرية مزورة دفعت العالم إلي موقف المواجهة مع تجار التزوير الفكري، مما دعا كثير من الدول إلى تطبيق عقوبات صارمة جراء ذلك بحق تجارة التزوير الفكري، من خلال مقاضاة مرتكبي جرائم التزوير الفكرية، بل وصل الأمر بمداهمة الشرط أوكارهم لضبط بضائع مزورة ومصادرتها، وفي أحيان كثيرة يتم إتلافها على مرأى من الناس.

حقائق شرعية

أولاً: الاعتداء على الحياة الخاصة والتجس على مخاطبات ومراسلات المتعاملين بالشبكة المعلوماتية محرم شرعاً، لقوله سبحانه: ﴿ يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ ﴿١٢﴾ ﴾ [الحجرات: ١٢] ولأن في ذلك تتبعاً للعورات وكشفاً للمستور.

ثانياً: الاعتداء على الأشخاص بالسب والقدح والتشهير مما حرمته الشريعة الإسلامية ونهت عنه، قال تعالى: ﴿ وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بِغَيْرِ مَا اكْتَسَبُوا فَقَدِ احْتَمَلُوا بُهْتَانًا وَإِثْمًا مُّبِينًا ﴾ [الأحزاب: ٥٨].

ومما يلاحظ في الآونة الأخيرة، وللأسف، أن هناك من يحرّض غيره على بعض الجرائم الإلكترونية كالدخول إلى أجهزة الآخرين بغير حق أو يقوم بشرح كيفية نشر المواقع المعادية أو الداعية إلى الرذيلة.

يقول الدكتور عبدالله بن عبدالعزيز العجلان في ذلك: «إن هذا يعد مخالفة صريحة للنظام، ويضيف قائلاً إن من أهم مميزات تقنية المعلومات سهولة تبادل المعلومات وتداولها، وهذه الميزة كغيرها من مميزات التقنية تستغل من بعض الناس لنشر أفكارهم الهدامة وممارسة هواياتهم الضارة بالآخرين.

حقوق ملكية البرمجيات

أما البرامجيات هاجساً يثير قلق الشركات دائماً وأبداً، ويثير هذا الموضوع جملة تساؤلات: من الذي يملك الحق في البرامجيات؟ هل هو الشخص الذي كتب البرامجية أو الشركة التي يعمل لحسابه؟ وهل يملك الشخص الذي كتب البرامجية حق نسخ البرامجيات لصالح شركات أخرى؟

إن هذه الأسئلة وغيرها كانت محور نقاش حصيلته اتفاق الرأي أحياناً والاختلاف أحياناً، ولكن تم الاتفاق على أن البرامجية تكون من حق رب العمل إذا كان المبرمج يشغل وظيفة لدى رب العمل، وحين تكون وظيفة المبرمج يحكم الاستشاري يحدد الاتفاق المبرم بين الطرفين شكل الانتفاع من البرامجية.

وأخيراً تتعارض الآراء وترتفع الأصوات بنغمات متنافرة، ولكن الجميع يتفق على أن صحوة أخلاقية هي المفتاح للخروج من أزمة ما يسمى بقرصنة البرامجيات، بل إن هذه الصحوة الأخلاقية مطلوبة لإنقاذ إنجازات القرن التقنية كلها من أعدائها، ومن ذاتها أولاً، خاصة عندما تتسم هذه الذات بالأنانية والاندفاع والسعي إلى الاحتكار المعرفي والاقتصادي على السواء.

المنافع والمضار

وفي محور ما توفره الشبكة العالمية من منافع ومضار يمكن من خلالها أن تستغل من ضعاف النفوس في التعدي على حقوق الآخرين والإضرار بهم قال **الدكتور عبداللطيف بن محمد السبيل القاضي بديوان المظالم** أن الشريعة الإسلامية تضمنت من القواعد الكلية والأحكام الشاملة ما يكون كفيلاً للحكم على كل مسألة حادثة أو نازلة واقعة يتعرف أهل العلم والبصيرة حكمها من خلال تلك القواعد والأحكام غير أن بعض الحوادث والمسائل النازلة في هذا العصر لم يكن لها مثيل فيما مضى من العصور السالفة بفضل ما هيأ الله سبحانه لعباده من المخترعات والمكتشفات الحديثة نظراً للتطور العلمي في هذا العصر الذي بدوره أدى إلى ظهور جرائم جديدة نشأت بسبب استخدام تلك الوسائل المبتكرة في مجالات عدة من أهمها مجال المعلومات أو ما يسمى بشبكة المعلومات العالمية والتي من خلالها يستغل ضعاف النفوس في ارتكاب الجرائم المعلوماتية ومنها الاختراق والتزوير والتشهير والابتزاز وتشويه السمعة مما جعل ولي الأمر يسن أنظمة لمكافحة تلك الجرائم والتحقيق فيها ومراقبتها وضبطها والتركيز على ضرورة التعاون والتكاتف الاجتماعي لمنع وقوع مثل هذه الجرائم.

وقد اقتضت حكمة الله عزَّ وجلَّ أن يفرض من العقوبات ما يردع بها كل من تسول له نفسه المساس بأعراض الناس وسمعتهم وأموالهم وقيمهم فشرع الإسلام العقوبات المقدرة المتمثلة في الحدود والجنايات وشرع العقوبات غير المقدرة المتمثلة في التعزير الذي أوكل لولي الأمر تقديرها وتحديد ما يناسبها من عقوبة بحسب المصلحة ومن تأمل العقوبات الشرعية عموماً وتدبرها وجدها الدواء النافع والعلاج الحاسم للشر والفساد وفيها رفع الظلم عن العباد ولا أدل على هذا من واقعنا المعاصر في ملكتنا العربية السعودية، فالمرء فيها آمن مطمئن على عرضه ونفسه وماله

❖ *السبيل :*

• الوازع الديني النابع من الرقابة الذاتية له دور مهم في عملية الردع والحد من الجرائم المعلوماتية

• سن الأنظمة في النوازل والمستجدات غاية في الأهمية

• الشريعة الإسلامية جعلت لولي الأمر تقرير العقوبة المناسبة

بفضل الله عزَّ وجلَّ أولاً ثم بتطبيق أحكام الشرع.

تقرير العقوبة

الشريعة الإسلامية جعلت لولي الأمر تقرير العقوبة المناسبة لبعض الجرائم المستحدثة التي لا نص فيها مراعاة للمصلحة وسداً للذرائع تحت ما يسمى بالتعزير وهو حق الإمام يعاقب به الجناة والمجرمين بالحبس أو بالجلد أو بالمال بما يراها الحاكم مناسباً مشروع بالكتاب والسنَّة والإجماع.

واتفق الفقهاء على أن الحبس يصلح عقوبة في التعزير وما جا في هذا المقام أن عمر بن الخطاب رضي الله عنه سجن الشاعر الحطيئة على الهجو لمنع الأذى عن المسلمين بهجوه والمحافظة على أعراضهم، بل قد يكون التعزير بالتهديد والتوعد بالعقوبة كما في تهديد الزبير وعلي رضي الله عنهما للمرأة التي حملت كتاب حاطب بن أبي بلتعة إلى قريش، حيث هدداها بتفتيشها وتجريدها من ملابسها إن لم تخرج الكتاب وأما التعزير بالجلد فدليله قوله ﷺ: «لا يجلد أحد فوق عشرة أسواط إلا في حد من حدود الله تعالى» قال بعض أهل العلم إن التعزير بالجلد يكون بحسب المصلحة وعلى قدر الجريمة فيجتهد فيه ولي الأمر على ألا يبلغ فيما فيه حد مقدر فالتعزير على سرقة ما دون النصاب مثلاً لا يبلغ به القطع والسنة دلت على هذا فقد حكم عمر بن الخطاب رضي الله عنه فيمن قلد خاتم بيت المال بضربه ثلاثمائة على مرات، وأما التعزير بالمال فهو سائغ إتلافاً وأخذاً واستدل لذلك بأقضية للرسول ﷺ كإباحته سلب من يصطاد في حرم المدينة لمن يجده وأمره (بكسر دنان الخمر وتضعيفه الغرامة على من سرق من غير حرز، وأخذ شرط مال مانع الزكاة كما أن التعزيز بالمال قد يكون بحبسه أو بإتلافه أو بتغيير صورته أو بتمليكه الغير.

في سن الأنظمة وقاية

سن الأنظمة التي تُجرِّم من يعتدي على أعراض الناس أو ممتلكاتهم وتشويه سمعتهم وبتزازهم عبر المواقع الإلكترونية بكافة الطرق واستخدام وسائل التشهير بهم سواء كان بنشر الصور أو كشف العورات يعد مخالفة شرعية تجاه الغير وكبيرة من كبائر الذنوب سواء كان التشهير صحيحاً أو باطلاً إذ توعده الله سبحانه بالعذاب في الدنيا وفي الآخرة وحذر من الوقوع في مثل تلك الآثام قال تعالى: ﴿إِنَّ الَّذِينَ يُحِبُّونَ أَن تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ﴾ [النور: ١٩] ولا شكَ أن فرض العقوبات وتجريم تلك الأفعال وملاحقتهم في سبيل القضاء على تلك التصرفات المشينة التي تؤدي إلى التشهير وتشويه السمعة والمساس بالحياة الخاصة وإغلاق مواقعها أمر في غاية الأهمية، حيث أصبحت قضايا التشهير والابتزاز باستخدام الوسائل الحديثة كالحاسب الآلي وملحقاته وبرامجه والشبكات بمستوياتها المحلية والعالمية وكذا الهاتف الجوال جميعها من الجرائم المقلقة والمثيرة للجدل وتحتاج البلاد إلى جهة متخصصة ومؤهلة للتعامل مع تلك الجرائم تحقيقاً وضبطاً ووقاية على أنه وبكل الأحوال يجب أن لا يركن إلى الأنظمة واللوائح والتعليمات الصادرة بهذا الشأن دون غيرها من الوسائل الأخرى إذ إنها ليست وحدها العلاج الكافي أو الرادع بل لا بد من التوعية والنصح والإرشاد وهذا جانب مهم جداً، فالوقاية خير من البحث عن العلاج خاصة ونحن جميعاً في ظل بيئة محافظة يغلب عليها الوازع الديني النابع من الرقابة الذاتية التي لها دور مهم في عملية الردع والحد من تلك الجرائم ومن الأهمية بمكان أن تؤخذ بالحسبان عند طرح أخلاقيات التداول والتعامل مع شبكة المعلومات كنوع من الضوابط الشرعية التي تحكم أخلاقيات المستخدم عبر الشبكة العالمية أو غيرها من الوسائل الحديثة التي تردع المرء ذاتياً عن ارتكاب تلك الجرائم المعلوماتية ومن ثم ينبغي لنا أن نركز على ضرورة الالتزام بالضوابط الشرعية والأخلاقيات المرعية في هذا الشأن فالذي لا وازع ديني يمنعه ولا ضمير إنساني يردعه قد أتيحت له وسيلة سهلة في توصيل أفكاره ونشر مفاسده بذات الدرجة المتاحة أمام مبتغي الخير والنفع للناس فالنفس أمارة بالسوء والشيطان يجري مع ابن آدم مجرى الدم والعقوبة هي على من يضعف وازعه الديني ليجد أمامه الرادع الدنيوي بالمرصاد فتكون إصلاحاً لحال الناس إذ إن في تنفيذ العقوبة تأديب للجاني وإرضاء للمجني عليه وزجراً للمقتدي بالجناة.

إثبات الجرائم المعلوماتية

الأدلة الجنائية للجرائم الإلكترونية داعم قوي لجهات العدالة في إثبات هذه الجرائم وحول هذا المحور شاركنا في بيانه **الدكتور رضا متولي وهدان أستاذ الأنظمة المشارك في المعهد العالي للقضاء** وحصرها في صعوبة إثبات هذه الجرائم وسلطة القاضي في قبول الدليل المعلوماتي فإلى مشاركته:

بداية يجب أن نعترف بأن هذا النوع من الإجرام المعاصر، يثير العديد من المشكلات، أهمها: صعوبة الاكتشاف والإثبات، وترجع الصعوبة إلى خصائص هذه التقنية، التي منها السرعة الفائقة التي ترتكب بها الجرائم، وسهولة طمس معالمها، وآثارها

قبل أن تكتشف، وإذا وجد دليل على الإدانة، فيمكن للجاني أن يقوم بتدميره في ثوان، وإن تم اكتشاف الجريمة، لا يكون إلا بمحض الصدفة، وماتم الإبلاغ عنه، أو ما تم اكتشافه، لا يكاد يذكر على مستوى العالم، فالجرائم من هذا النوع تكون عابرة للحدود القارية، ويمكن للجاني استخدام وحدات طرفية، من خلالها يصدر تعليمات للحاسب، تخترق شبكات المعلومات، في مناطق على بعد آلاف الكيلومترات، ويتم ارتكاب الجريمة في هدوء.

ويزداد الأمر صعوبة، عندما تصطدم أجهزة العدالة الجنائية بتكنيك معلوماتي غير مسبوق، سواء كمحل للجريمة، أو كوسيلة مستحدثة، كما يغلب على أجهزة جمع الاستدلالات، أو التحقيق والادعاء أو المحاكمة، عدم المعرفة الفنية للتعامل مع هذا النوع المعقد من الإجرام.

أما سلطة القاضي في قبول الدليل المعلوماتي:

فالنظم الإجرائية تعرف نظامين للأدلة المقبولة في الإثبات بوجه عام: الأدلة الشرعية أو النظامية، والأدلة الاقناعية، الأولى محددة من حيث النوع والقيمة مسبقاً، والقاضي مقيد بها، وهذا النوع يعمل به في الإثبات المدني، وبعض نظم الإثبات الجنائي.

أما الأدلة الاقناعية، فترتبط بما يكونه القاضي من حقيقة حول واقعة معينة وبما يمليه عليه وجدانه وضميره، وكل الأدلة في ذلك سواء، وفي مجال الإثبات الجنائي يسود مبدأ حرية الإثبات، ولهذه الحرية وجهان:

الأول: أن القاضي الجنائي له سلطة قبول أي دليل يكون اقتناعه.

الثاني: أن القاضي بنفسه يقدر حسب اقتناعه الذاتي قيمة الدليل.

وأضاف أن الأدلة المعلوماتية تقوم على الاستعانة بالطرق الفنية، بواسطة الخبراء، وهذه القرائن تخضع للفحص العلمي الدقيق، وتكون دليلاً قطعياً يثبت الإدانة أو البراءة، وهذا الدليل بمفرده غير كاف، حيث يجب أن يقوم معه نظام الاقتناع القضائي، حتى يتم الفصل في الدعوى الجنائية.

وهذه الأدلة، يجب أن يحدد الإطار الذي ستقدم فيه، وتحديد مدى صحتها وصدقها، ومدى مطابقتها للأصول المرعية، فيجب أن توثق هذه الأدلة، حتى تكون بينة قاطعة لا تفتقر إلى إثبات.

فالدليل المعلوماتي يشكل بينة حقيقية ظاهرة للعيان، عندما يستخدم ظرفياً، أي مستمداً من الظروف المادية الدقيقة، المتصلة بالجريمة، ومعيار قبوله يتمثل في الدقة التي تعمل بها مثل هذه الآلات، والدليل المستخرج منها يعد دليلاً حقيقياً، ليس في مرتبة الشهادة السماعية، لكنه يرقى إلى مستوى الشهادة الشفوية، ويتأصل ذلك بشهادة من مشغل الآلة، وممن قام ببرمجتها، وممن قام باختبار صلاحيتها، فإذا كانت الشهادة مقنعة لقاضي فلا يوجد

❖ **وهدان:**

• للقاضي سلطة قبول الدليل الذي يكون القناعة الذاتية في قيمته

• نظام مكافحة الجرائم المعلوماتية نقلة نوعية وحضارية للحد من تلك الجرائم

• الأدلة المعلوماتية تقوم على الاستعانة بالطرق الفنية بواسطة الخبراء وتكون دليلاً قاطعاً يثبت الإدانة أو البراءة

حينئذ سبب معقول لاستبعاد مثل هذا الدليل الذي ارتقى إلى درجة اليقين.

وعملاً يمكن لأجهزة العدالة الجنائية، أن تستعين بشركة أو أكثر، متخصصة في مجال التقنية، كي تنشئ موقعاً إلكترونياً، يقوم بعملية الأرشفة لكافة البيانات الداخلة والخارجة، لكافة المواقع المشاركة على الشبكة المعلوماتية، وبالتالي يمكن الرجوع إليها وقت الحاجة إلى تقديم الدليل العلمي أمام القضاء، كشاهد حضوري، للكشف عن غموض مثل هذه الجرائم، وهذا ما نصت عليه المادة الرابعة عشرة من نظام مكافحة جرائم المعلوماتية، الذي يعد بحق نقلة نوعية وحضارية في هذا المجال.

التدريب والتأهيل

وشاركنا الحوار **د. محمد بن المدني بوساق - وكيل مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية** حول أهمية التدريب والتوعية في مجال العلوماتية لمكافحة جرائمها ووضع ضوابط محددة للعدالة وضرورة مواكبة القضاة والعلماء والمحققين التقنيات العصر فأبان أن الجرائم الرقمية حظيت باهتمام عالمي شامل وصارت محل عناية من كافة الدول وعدلت كثير من الدول العربية قوانينها لتشمل ما يتصل بجرائم الحاسب الآلي والإنترنت.

ولما اشتد التحدي الرقمي وتجاوزت الأساليب الإجرامية بالتقنية الإلكترونية الرقمية الحدود وتعددت أنواعها وطرقها مع

التطور المذهل والمتجدد باستمرار في مجال صناعة الحاسبات الآلية، ووسائل الاتصال ولأجل ذلك كله نجد هناك فزعاً حقيقياً، واستعداداً فائقاً لدى بعض الدول للتصدي لهذه الظاهرة ومن الأمثلة على ذلك إذا قام المجرم الإلكتروني الرقمي بالسيطرة على نظام الإشارات الضوئية في إحدى المدن بحيث يجعل الإشارات الضوئية كلها خضراء في الوقت نفسه، فإن حدوث تصادم بين السيارات عند التقاطعات سيكون من صنع أيديهم، ونظراً لاحتمال وفاة الأشخاص الموجودين في السيارات المتصادمة، فإن المجرم الإلكتروني الرقمي قد يواجه حكماً بالسجن مدى الحياة ومع هذا كله يبقى القانون الوضعي قاصراً عن ملاحقة الجرائم بالتقنية الرقمية ولن يستطيع سد الفراغ القانوني وسيفلت عدد كبير من المجرمين من المساءلة القانونية واستحقاق الجزاء الرادع ما لم يزخذ بنظرية الفقه الإسلامي في التفويض القضائي.

الشريعة الإسلامية تستوعب النوازل:

ويهدف التشريع الإسلامي إلى تحقيق السعادة العاجلة والآجلة للبشرية ولذلك لم يترك مصلحة حقيقية نافعة إلا وطلبها ولا مفسدة واقعة أو متوقعة إلا ودفعها، فأوجب إقامة العدل والقسط بين الناس وحرم البغي والعدوان أياً كان مصدره وبأي وسيلة وقع ومهما اختلفت نتائجه الضارة، فقد أوجب الشارع محاربة كل خطر وضرر وسوء ومنع الجور والفساد والميل عن ميزان العدل.

ولذلك استوعبت تشريعات الإسلام بمبادئها العامة ومقاصدها جميع ما يقع من الإنسان من خير أو شر وتضمنت الشريعة الغراء التوجيه لمواجهة كل ذلك بما يناسبه في وقته وإبانه وذلك عن طريق الاكتشاف بواسطة الاجتهاد الذي هو البحث العلمي الذي أمر به الله تعالى، فإن العقل البشري إذا استوعب المنهج الصحيح وجعله مرآته فسيصل في مواجهة الجرائم بعامة والرقمي منها بخاصة إلى أصوب ما يمكن وأصلح ما يمكن وأنسب ما يمكن.

فكما استطاع العقل البشري أن يكتشف في عالم التسخير عجائب الثورة الرقمية فلن يعجز عن اكتشاف ما يواجه به المفاسد التي قد يحدثها سوء استعمالها، وفيما يلي أعرض السبل لمواجهة الجريمة الرقمية:

مواجهة الجرائم الرقمية عن طريق الوقاية:

المنهج الإسلامي التكاملي يحقق بلا ريب أعلى درجات الوقاية والمنع من الجريمة بعامة والجريمة الرقمية بخاصة لأنه لا ينتظر وقوع الجريمة حتى يهب لمحاربتها، وإنما سعى في تشريع أحكامه إلى إيجاد مجتمع متكامل تسوده المحبة ويقوم على الولاء العقدي ويسلم من الآفات وبواعث الإجرام بداية بالفرد الذي هو مصدر جميع الأفعال الضارة والصالحة مروراً بالأسرة وامتداداً إلى جميع طبقات المجتمع، ومن هنا وجدنا التشريع الإسلامي يهتم بالفرد ويجعله مركز الاهتمام ويعمل على تركيز أسس الإيمان في قلبه لأنها بمثاب قاعدة المعلومات الأساسية في أجهزة الحاسوب تجعل المرء ميالاً لكل خير نافراً من كل شر سريع الاستجابة للأمر والنهي والتحذير والتنبيه.

وعليه فإن منهج الوقاية من الجرائم بعامة والجرائم الرقمية منها بخاصة يعمل على إصلاح الفرد بالتربية والتعليم والعبادات والتزكية ودعم الضمير «القلب» بما يجعله يقظاً شديد الرغبة في الخير وشديد الكراهية للشر، وبذلك يصبح الفرد صالحاً مصلحاً طاهراً في نفسه مطهراً لغيره.

ولتحقيق الوقاية المنشودة ينبغي إصلاح المجتمع كذلك برقامة جميع فروض الكفاية ونعني بها المصالح المشتركة بما يحقق التكافل ومحاربة الفقر والتشجيع على العمل ومحاربة البطالة وحماية الأسرة من التفكك بتنمية روابطها والمحافظة على ثوابتها التي تحفظ خصائص النوع البشري وهويته والعناية بالمرأة وإعطائها حقوقها التي أعطاها الله تعالى وتحقيق العدل والمساواة فإن العدل يهب الأمن وتنقية البيئة الاجتماعية من المهيجات الجنسية والمسكرات وملء أوقات الفراغ وسد أبواب الكسب الحرام، ومنع مسببات العداوة والبغضاء بين الناس وتطهير المجتمع من عوامل وأسباب الانحراف الفكري، ونشر منهج الوسطية السمحة التي يرجع إليه الغالي ويحلق بها التالي.

ومن الوقاية أيضاً فيما يتصل بجرائم الحاسوب أن تعمل

❖ بوساق :

• الجرائم الرقمية معظمها جرائم تعزيرية وعقوبتها تفويضية

• قضايا الجرائم الرقمية حظيت باهتمام عالمي شامل

• يهدف التشريع الإسلامي إلى تحقيق السعادة العاجلة والآجلة للبشرية

• منهج الوقاية من الجريمة يعمل على إصلاح الفرد بالتربية والتعليم

الجهات المختصة على إتقان تلك المصنوعات فقد قال النبي ﷺ: «إن الله يحب إذا عمل أحدكم عملاً أن يتقنه».

ومن وجوه الإتقان فيها أن يراعى في تصنيعها وتثبيت برامجها تأمين معطياتها واستعمالها بما يجعل اختراقها وإلحاق الضرر بها صعباً على كل من يحاول الإساءة والضرر، فالتأمين للأجهزة ينبغي أن يكون كجهاز المناعة لجسم الإنسان فلولاه لهلك الناس لأتفه الإصابات.

مواجهة التشريع الجنائي الإسلامي للجرائم الرقمية عن طريق التجريم

لا يصعب على من كان مؤهلاً من رجال الفقه والقانون اكتشاف تجريم كل سلوك منحرف مهما كانت الوسيلة المستخدمة دقيقة وخفيفة، وعليه فإن المطلوب من المجتمع الإسلامي لمواجهة جميع الجرائم الواقعة أو المتوقعة عن طريق التجريم النصي، فلا بد أولاً من تكوين باحثين مجتهدين متخصصين يجمعون بين الأسس والمنطلقات بما فيها من مصادر ومقاصد وقواعد وثوابت وبين المعرفة الواسعة لمقتضيات العصر وعلومه ووسائله، لتكون لديهم خبرة تراكمية تستوعب ما مضى وتحيط بما يطرأ ويستجد حتى تكون على أهبة الاستعداد لحل المشكلات ومواجهة المعضلات.

فإن الإسلام قد أوجب الاجتهاد وإعداد المجتهدين، فالاجتهاد «فرض كفاية والأمة كلها ملزمة بإعداد وتكوين من يكفي للقيام باكتشاف واستنباط ما تحتاجه الأمة في المجالات كافة ومنها ما نحن بصدده من تجريم ما طرأ من انحرافات في الاستخدام غير المشروع للتقنية الرقمية فإن الاجتهاد هو البحث العلمي المتواصل ببذل الجهد واستفراغ الوسع للوصول إلى الحلول المطلوبة والمرء إن بذل جهده واستفرغ وسعه ووصل إلى حكم غلب على ظنه أنه الحق فقد برئت ذمته ويكون مأجوراً غير مأزور أصاب أم أخطأ لقوله ﷺ: «إذا حكم الحاكم فاجتهد فأصاب فله أجران وإذا حكم فأخطأ فله أجر واحد» لأن الاجتهاد في الشريعة الإسلامية ليس ميلاً شخصياً أو نفوراً ذاتياً، وإنما هو نظر مبني على منهج علمي ينتهي المرء بمراعاته والاعتماد عليه إلى ما يراه صواباً وهذا المنهج يتكون من المصادر النقلية وأهمها على الاطلاق كتاب الله تعالى وسنة نبيه ﷺ والمصادر العقلية ومنها الاجماع والقياس وهما مصدران يرجعان بطريق غير مباشر إلى الكتاب والسنّة ثم المصادر العقلية الأخري مثل المصالح المرسلة والعرف ومبدأ سد الذرائع والاستقراء وغير ذلك.

وقد وجدنا أن جميع المصادر النقلية والعقلية قد دلت على تجريم الاعتداء على حقوق الآخرين بعامة، وفيما يتصل بمعطيات وتقنيات الحاسب الآلي بخاصة، ففي نصوص الكتاب والسنة ما يدل على تحريم كل اعتداء على الناس في أنفسهم وأموالهم وأعراضهم وسائر حقوقهم مما يصلح أن يكون حقاً مشروعاً، ونهت عن كل إفساد في الأرض قلّ أو كثر، خفياً كان أو ظهر ومما يدل على ذلك من القرآن الكريم قوله تعالى: ﴿ ... وَتَعَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَىٰ وَلَا تَعَاوَنُوا عَلَى الْإِثْمِ وَالْعُدْوَانِ ... ﴾ [المائدة : ٢] وقوله تعالى: ﴿ قُلْ إِنَّمَا حَرَّمَ رَبِّيَ الْفَوَاحِشَ مَا ظَهَرَ مِنْهَا وَمَا بَطَنَ وَالْإِثْمَ وَالْبَغْيَ بِغَيْرِ الْحَقِّ ... ﴾ [الأعراف : ٣٣] وقوله تعالى: ﴿ إِنَّ اللَّهَ يَأْمُرُ بِالْعَدْلِ وَالْإِحْسَانِ وَإِيتَاءِ ذِي الْقُرْبَىٰ وَيَنْهَىٰ عَنِ الْفَحْشَاءِ وَالْمُنكَرِ وَالْبَغْيِ .. ﴾ [النحل : ٩٠] ونهيه سبحانه عن الظلم كما في قوله: ﴿ إِنَّمَا السَّبِيلُ عَلَى الَّذِينَ يَظْلِمُونَ النَّاسَ وَيَبْغُونَ فِي الْأَرْضِ بِغَيْرِ الْحَقِّ أُولَٰئِكَ لَهُمْ عَذَابٌ أَلِيمٌ ﴾ [الشورى : ٤٢] وقوله تعالى ناهياً عن التعرض لمال الغير: ﴿ يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُم بَيْنَكُم بِالْبَاطِلِ إِلَّا أَن تَكُونَ تِجَارَةً عَن تَرَاضٍ مِّنكُمْ .. ﴾ [النساء : ٢٩] ونختم هذه المجموعة من الآيات الكريمة بنهيه سبحانه وتعالى عن الفساد في الأرض بعامة، قال تعالى: ﴿ وَلَا تُفْسِدُوا فِي الْأَرْضِ بَعْدَ إِصْلَاحِهَا ... ﴾ [الأعراف : ٥٦] وقوله تعالى: ﴿ ... وَلَا تَبْغِ الْفَسَادَ فِي الْأَرْضِ إِنَّ اللَّهَ لَا يُحِبُّ الْمُفْسِدِينَ ﴾ [القصص : ٧٧].

فمن تأمل هذه الآيات وتدبر ألفاظ الظلم والفساد والإثم والفحشاء والمنكر والبغي والعدوان وأكل أموال الناس بالباطل، فلا يبقى في ذهنه شك في تجريم جميع أنواع السلوك المنحرف ومنها ما يتصل بالجرائم الرقمية وفي السنّة الشريفة ما لا يحصى من النصوص التي تحرم وتجرم جميع أنواع السلوك غير السوي ومنها جرائم الحاسب الآلي والإنترنت كما في قوله : «لا ضرر ولا ضرار»، وقوله ﷺ: «... كل المسلم على المسلم حرام دمه وماله وعرضه».

مواجهة التشريع الجنائي الإسلامي للجرائم الرقمية بالعقاب:

إن الأساس الذي تقوم عليه العقوبات في الشريعة الإسلامية يتمثل في حماية الجماعة وصيانة نظامها ودفع الشرور والاثام والأضرار والأخطار والمفاسد عنها من جهة ومن جهة ثانية إصلاح الأفراد وتهذيبهم ورعاية حقوقهم وحمايتهم من أنفسهم ومن بعضهم بعضا واستنقاذهم من الجهالة وإرشادهم من الضلالة وكفهم عن المعاصي وبعثهم على الطاعة.

وحتى يكون الأساس متيناً لا ينهار وقوياً لا ينثني يجب أن تكون العقوبة بحيث تمنع الكافة عن الجريمة قبل وقوعها وبعد وقوعها تزجر الفاعل وتمنعه من العود فهي موانع قبل الفعل وزواجر بعده، والعقوبة غير مرغوبة لذاتها وإنما المطلوب هو الظفر بما يترتب عليها من جلب المصالح ودفع المفاسد، وعليه فإن العقوبات في الشريعة الإسلامية رحمة وليست انتقاماً وتشفياً لأنها في مجملها إحسان للجميع بمن فيهم الجاني نفسه، إذ هي ترمي إلى إصلاحه ورد اعتباره وإعادة دمجه في المجتمع.

ولما كانت الجرائم الرقمية أو جرائم الحاسب الآلي والإنترنت معظمها جرائم تعزيرية فإن عقوباتها تفويضية أي غير مقدرة من الشارع الأعلى والعقوبات التفويضية هي مجموعة جزاءات أقرها الشارع وفوض أمر تقديرها للاجتهاد الفقهي أو القضائي لتتلاءم مع الجريمة وآثارها وتطورها وتنوعها وظروفها وتتلاءم أيضاً مع المجرم وخطره وسلوكه ونوعيته وهي تقبل الزيادة والنقصان والشدة واللين والشفاعة والعفو في جملتها ويجوز إثبات موجبها بجميع الطرق ومنها القرائن القديمة والحديثة، وهي تهدف في الغالب الأعم إلى العلاج والإصلاح والتأديب، ولذلك فلا يبلغ بها الاستئصال كالقتل والقطع في الأعم الأغلب وهي كثيرة ليست محصورة في نوع أو صنف من العقوبات وتبدأ بأخف العقوبات إلى أشدها أي من الوعظ والإرشاد إلى الإعدام وبينهما عقوبات كثيرة غير محصورة ومنها عقوبة التوبيخ واللوم والهجر والتشهير والتهديد، والحرمان والعزل والإزالة، والعقوبات المالية كالمصادرة، والغرامة، وعقوبة النفي، والتغريب، والسجن، والحبس، والجلد وغير ذلك وأقصاها الإعدام.

وقد ذهب اتجاه في الفقه الإسلامي إلى معارضة إدراج عقوبة الإعدام ضمن العقوبات التعزيرية لأنها تستهدف الإصلاح والعلاج غالباً، وأجاز اتجاه آخر التعزير بالقتل على أن يكون في أضيق نطاق وعند الضرورة القصوى كدفع مفسدة عامة أو تعذر إصلاح الجاني، وإذا تقرر استثناء جواز التعزير بالقتل فإنه لا ينبغي التوسع فيه ولا يترك أمره للاجتهاد القضائي وإنما يختص بتقديره الاجتهاد الفقهي التشريعي والقضاء تابع في تطبيقه للاجتهاد التشريعي.

وعليه، فإن كل جريمة تقع على الحاسب الآلي أو بواسطته فلا بد من رفعها إلى القضاء، لأن هذه الأفعال مشمولة بالتجريم في المصادر والمقاصد والقواعد والقضاء مفوض في تقدير العقوبة المناسبة منعاً لكل فراغ قانوني يستغله المفسدون، وسداً لكل ثغرة يفلت منها المجرمون.

فقد دلت الآيات والأحاديث على تجريم جميع صور الأذى مهما كانت الوسيلة المستعملة في ذلك سواء كانت مما عرف قديماً أم لم تعرف إلا حالياً أو ستعرف في مستقبل الزمان.

ولو فرضنا أن المجتهد سواء كان فقيهاً أو قاضياً لم يجد في المصادر ما يفيد تجريم تلك الأفعال فإن المقاصد العامة للشريعة والتي دل الاستقرار بوجوب حفظها من جانب الوجود بإيجادها وتنميتها ومن جانب العدم بتجريم الأفعال التي تزيلها أو تخربها أو تعطلها وتلك المقاصد أو المصالح تشمل حفظ الدين والنفس والعقل والنسل والمال وهي بتفريعاتها تتضمن قطعاً ما يتصل بجرائم الحاسب الآلي والإنترنت.

كما أن القواعد العامة التي قامت الأدلة على ثبوتها واعتبارها تقضي تجريم السلوك المنحرف الذي يكون الحاسب الآلي محلاً له أو يكون الحاسب ذاته وسيلة لنتائج ضارة وآثمة ومن تلك القواعد «لا ضرر ولا ضرار» و«الضرر يزال» و«الضرر يدفع بقدر الإمكان» و«درء المفاسد مقدم على جلب المصالح».

ومما تقدم نجد أن تجريم ما يتصل بالسلوك السيء الناتج عن استخدام الحاسب الآلي أمر مقطوع به وعليه فلم يبق بعد ثبوت التجريم إلا مواجهة تلك الجرائم بعقوبات رادعة.

وفضلاً عن ذلك فإن نظر القضاء في هذه الجرائم يعد تمهيداً ضرورياً للتعرف على تلك الأفعال وتكوين خبرة تراكمية عنها فيكون ذلك كله مما يمهد للتفويض الفقهي التشريعي حتى يصدرها في قوانين ملزمة، لأن القضاء تابع في الأصل للتفويض التشريعي متى وجد فإن فقد النص طلبه من المصادر والمقاصد والقواعد، فإن التشريع الإسلامي يتميز بكثرة مصادره وقواعده وشموله ومرونته وصلاحيته لكل زمان ومكان واستيعابه لجميع الأعراف وسعته لنظر العقول وسبقه للعصور وتقريره لمبدأ التفريد العقابي عندما فوض تقدير العقوبات في جميع الجرائم التعزيرية وهي تمثل تقريباً ٩٥٪ من التشريع الجنائي فإن العقوبات التعزيرية كالعلاج والعلاج لا يوصف قبل الكشف والفحص فإن من يقدر عقوبات محددة لجرائم مختلفة بزمانها ومكانها وظروف الجاني والمجني عليه كمن يصف دواء واحداً لجميع الأمراض أو يفصل مقاساً واحداً لجميع الأحجام والأجسام.

نظام مكافحة الجرائم المعلوماتية

المملكة العربية السعودية حسمت الأمر حين أصدرت نظام مكافحة جرائم المعلوماتية التي تمت الموافقة عليه بجلسة مجلس الوزراء رقم ٧٩ في ١٤٢٨/٣/٧هـ وقد تضمن النظام تجريم التنصت والدخول غير المشروع للمواقع للتهديد والابتزاز والدخول إلى المواقع بغية تغيير مضامينها أو شغلها أو تعديلها أو إتلافها أو التشهير بالآخرين وإلحاق الضرر بهم عن طريق وسائل تقنيات المعلوماتية المختلفة، أو الاستيلاء بطريق غير مشروع على مال منقول أو الوصول بطريق غير مشروع إلى بيانات بنكية أو ائتمانية وقد شمل التجريم أيضاً الدخول غير المشروع للمواقع بهدف إلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو تغييرها ومثلها في التجريم إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة أو تسريبها أو إتلافها ونحوهما.

وجرّم النظام كذلك كل ما من شأنه إلحاق الضرر بالنظام العام وكل ما يفضي إلى الاتجار بالجنس البشري أو إنشاء ما يتصل بالشبكات الإباحية وأنشطة القمار أو الاتجار بالمخدرات وترويجها أو إنشاء موقع للمنظمات الإرهابية وكل ما من شأنه تسهيل الحصول على بيانات عن الأمن الداخلي.

وقد تضمن النظام عقوبات مناسبة للجريمة المرتكبة أخفها عقوبة لا تزيد على سنة ولا تزيد على ٥٠٠ ريال أو إحداهما وأشدها وأعلاها عقوبة لا تزيد على عشر سنوات وغرامة لا تزيد على خمسة ملايين ريال أو إحداهما وبين النظام أيضاً حكم الشريك في الجريمة المعلوماتية والمحرض عليها وبين الظروف المشددة والظروف المخففة وأجاز المصادرة للأجهزة والبرامج المستخدمة في ارتكاب الجريمة وبين النظام جهة التحقيق والادعاء وحصرها في هيئة التحقيق والادعاء العام ولصعوبة إثبات جرائم المعلومات وخفائها والحاجة في ذلك إلى الخبرات العالية في المجال أوصى هيئة الاتصالات وتقنية المعلومات حسب الاختصاص بتقديم الدعم والمساندة الفنية للجهات الأمنية في جميع مراحل ضبط هذه الجريمة والتحقيق فيها والمحاكمة عليها.

الجرائم المعلوماتية والاتفاقات الدولية

حول عالمية جرائم المعلوماتية وتخطيها الحدود الجغرافية للدول وتعقد مجرياتها القضائية وحول هذا المحور كان لنا هذا الحوار مع **سعادة الأستاذ محمد بن عبدالعزيز المهيزع مدير عام إدارة المستشارين بوزارة العدل** فأوضح أن جرائم تقنية المعلومات ظهرت مع ظهور هذه التقنية وانتشارها الكبير في جميع مناحي الحياة وكان لا بد من التصدي لهذه الجرائم لخطورتها ومساسها بكافة أوجه حياة الناس المختلفة الاقتصادية

❖ المهيزع:

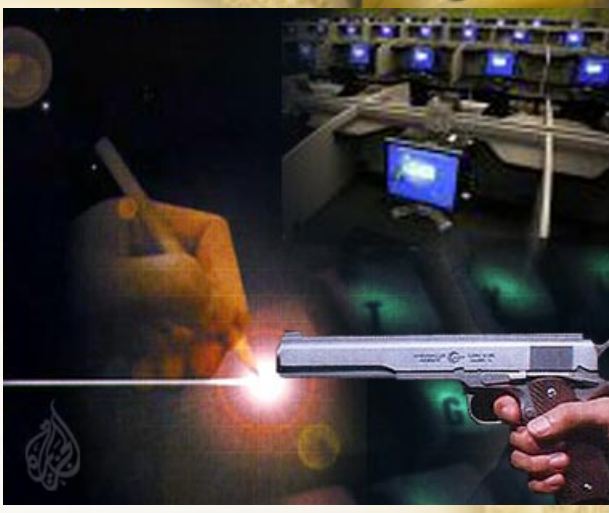
• نظام مكافحة جرائم المعلوماتية يسعى إلى تحقيق التوازن بين مصلحة المجتمع في الاستفادة من تقنية العصر ومصلحة الفرد في حماية حقوق استخدامها

• الاتفاقيات الدولية تساهم في مدّ ولاية الدولة القضائية لتشمل مرتكبي الجرائم خارج حدود الدولة التي وقعت فيها آثار الجريمة

• ضرورة إعلان العقوبة لتحقق الردع والحد منها

والاجتماعية وغيرها، ولذلك أصدرت العديد من الدول قوانين تجرم تلك الأفعال الإجرامية التي تستخدم تقنية المعلومات، ومن تلك الدول المملكة العربية السعودية التي أصدرت نظام مكافحة جرائم المعلوماتية، الذي يسعى إلى تحقيق توازن ضروري بين مصلحة المجتمع في الاستعانة بالتقنية الحديثة ومصلحة الإنسان في حماية حياته الخاصة والحفاظ على أسراره، والمساعدة على تحقيق النظام المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، كما يهدف إلى حماية المصلحة العامة والأخلاق والآداب العامة وكذلك حماية الاقتصاد الوطني، وتضمن النظام تجريم لعدد من الأفعال وأوقع عليها العقوبات الرادعة التي تصل إلى عشر سنوات سجن وغرامة تصل إلى خمسة ملايين ريال.

وتظل هذه العقوبات غير فاعلة ما لم تصل إلى القضاء المختص ويتم إيقاع العقوبة فعلاً على مرتكبي تلك الأفعال، ومن ثم إعلان تلك العقوبات على الملا من خلال وسائل الإعلام المختلفة ليدرك الجميع أن هذه الأفعال مجرمة وأن العقوبة عليها تطبق فعلاً على مرتكبيها، لكي يتحقق الردع الخاص والعام المقصود من العقوبات الجنائية.



جرائم غير وطنية

وتجدر الإشارة إلى أن جرائم تقنية المعلومات من الجرائم ذات الطابع غير الوطني بمعنى أن الجريمة قد تقع في دولة وتكون آثارها في دولة أخرى أو قد تقع الجريمة من أكثر من شخص في أكثر من دولة، وبالتالي فإن المكافحة الفعالة لهذه الجرائم لا يتحقق فقط بالتجريم المحلي لها، وإنما يتعين أن يكون هناك تجريم دولي لهذه الأفعال من خلال اتفاقية دولية، وكذلك يتعين عقد اتفاقيات ثنائية بين الدول لهذا الغرض، ولكي يتحقق الغرض من الاتفاقيات يتعين على الدولة أن تمد ولايتها القضائية لكي تشمل من يرتكب جرائم تقنية المعلومات خارج حدود الدولة التي وقعت فيها آثار الجريمة.

وإذا ما ارتكبت الجريمة من قبل جماعة إجرامية منظمة فإن ذلك معالج باتفاقية مكافحة الجرائم المنظمة غير الوطنية والتي صادقت عليها المملكة العربية السعودية وقد نصت في المادة (١٥) منها المتعلقة «بالولاية القضائية» على ما يلي: «١ - تعتمد كل دولة طرف ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الأفعال المجرمة بمقتضى المواد ٥، ٦، و٨، ٢٣ من هذه الاتفاقية في الحالات التالية:

أ - عندما يرتكب الجرم في إقليم تلك الدولة الطرف.

ب - أو عندما يرتكب الجرم على متن سفينة ترفع علم تلك الدولة الطرف أو طائرة مسجلة بموجب قوانين تلك الدولة وقت ارتكاب الجرم.

٢ - رهناً بأحكام المادة ٤ من هذه الاتفاقية، يجوز للدولة الطرف أن تؤكد أيضاً سريان ولايتها القضائية على أي جرم من هذا القبيل في الحالات التالية:

أ - عندما يرتكب الجرم ضد أحد مواطني تلك الدولة الطرف.

ب - عندما يرتكب الجرم أحد مواطني تلك الدولة الطرف أو شخص عديم الجنسية يوجد مكان إقامته المعتاد في إقليمها.

ج - أو عندما يكون الجرم:

١ - واحداً من الأفعال المجرمة وفقاً للفقرة (١) من المادة (٥) من هذه الاتفاقية، ويرتكب خارج إقليمها بهدف ارتكاب جريمة خطيرة داخل إقليمها.

٢ - واحداً من الأفعال المجرمة وفقاً للفقرة (١) ٢ من المادة (٦) من هذه الاتفاقية، ويرتكب خارج إقليمها بهدف ارتكاب فعل مجرم وفقاً للفقرة (١) أ، ١، أو ٢، أو (ب)، ١، من المادة (٦) من هذه الاتفاقية داخل إقليمها.

٣ - لأغراض الفقرة ١٠ من المادة ١٦ من هذه الاتفاقية تعتمد كل دولة طرف ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المشمولة بهذه الاتفاقية، عندما يكون الجاني المزعوم موجوداً في إقليمها ولا تقوم بتسليم ذلك الشخص بحجة وحيدة هي كونه أحد رعاياها.

٤ - تعتمد أيضاً كل دولة طرف ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المشمولة بهذه الاتفاقية عندما يكون الجاني المزعوم موجوداً في إقليمها ولا تقوم بتسليمه.

٥ - إذا أبلغت الدولة الطرف التي تمارس ولايتها القضائية بمقتضى الفقرة ١ أو ٢ من هذه المادة، أو علمت بطريقة أخرى، أن دولة واحدة أو أكثر من الدول الأطراف الأخرى تجري تحقيقاً أو تقوم بملاحقة قضائية أو تتخذ إجراء قضائياً بشأن السلوك ذاته، تتشاور السلطات المختصة في هذه الدول الأطراف أن تتشاور فيما بينها، حسب الاقتضاء، بهدف تنسيق ما تتخذه من تدابير.

٦ - دون المساس بقواعد القانون الدولي العام، لا تحول هذه الاتفاقية دون ممارسة أي ولاية قضائية جنائية تؤكد الدولة الطرف سريانها وفقاً لقانونها الداخلي».

ومن المهم الإشارة في هذا المقام إلى أن هذه التقنية قد لاقت اهتماماً كبيراً ومتزايداً من صغار السن من الشباب، وقد يقومون بأفعال تعتبر جرائم في هذا المجال دون إدراك لذلك، وبالتالي فإن التوعية من أهم الأمور في هذا الجانب ووسائل التوعية معروفة ومتوفرة هذه الأيام بحمد الله.

الاعتداء على الأموال رقمياً

السحب والإيداع والدخول إلى مواقع البنوك وإجراء التعاملات المالية عبر الإنترنت جعلت المجرمين تسيل لعابهم في استغلال هذه الوسائل للسرقة والتزوير والاختلاس.. حول هذا الجانب من ندوتنا شاركنا **الأستاذ فهد بن إبراهيم المفرج مدير**

❖ المشرح :

• مؤسسة النقد عقدت دورات لمنسوبي الأجهزة الأمنية وتعريف القضاة بأنواع الجرائم المصرفية والإلكترونية

• مشروع جديد لنظام مكافحة جرائم تقنية المعلومات بين دول مجلس التعاون لدول الخليج العربية

إدارة الإشراف البنكي بمؤسسة النقد العربي السعودي فأبان أن الاعتداء على الأموال المتداولة إلكترونياً سواء في إطار التجارة الإلكترونية أو من خلال العمليات المصرفية(سحب وإيداع) عبر أجهزة الصرف الآلي والدخول إلى مواقع البنوك بغرض الاختلاس فهناك الكثير من الوسائل والطرق التي يتبعها بعض ضعاف النفوس تتعلق باختراق حسابات الآخرين من خلال عمليات السرقة المباشرة للبطاقات أو من خلال الخطف بغرض الابتزاز، أو الدخول إلى حسابات البعض بعد الحصول على الأرقام السرية، كما أن هناك بعض العصابات التي تعرض المساعدة عند أجهزة الصراف الآلي لغرض استغلال كبار السن والأميين، ومن هذه الجرائم أيضاً استخدام مواقع مشابهة لمواقع البنوك على شبكة الإنترنت بهدف استدراج العملاء إلى استخدامها وبالتالي تتمكن هذه العصابات من سحب أموال عملاء البنوك، وقد تستخدم بعض العصابات (قارئات) شرائح إلكترونية توضع في أجهزة الصرف الآلي لتسجيل معلومات البطاقات ومن خلال أجهزة تصوير مثبتة في مواقع مخفية يمكن الحصول على الأرقام السرية، وهناك الكثير من القصص التي حدثت محلياً أو على مستوى العالم، ولا يخفى عليكم فالسباق مستمر بين التقنية وما يتوصل له المجرمون، وكذلك أساليب مكافحة جرائم المعلوماتية أو الحد منها.

وقد استغل بعض ضعاف النفوس في السنوات الماضية قصور العامة في فهم هذه الخدمات وخطورتها، إلا أنه بصدور نظام مكافحة جرائم المعلوماتية وتفعيله من الجهات الأمنية تكون المملكة قد دخلت مرحلة جديدة من العمل بتشريعات المعلوماتية، فكان له إيجابيات عديدة منها المساعدة في تحقيق الأمن المعلوماتي، ونشر الاستخدامات الإيجابية للتقنية، وكذلك حماية الاقتصاد الوطني من خلال المواد التي تعاقب كل من يلحق الضرر بشبكات المعلومات التي أصبحت جزءاً لا يتجزء من العمل اليومي للحكومة والجمهور، وهذا النظام يشكل لبنة أساسية من تشريعات المعلوماتية، وسوف يساعد على نشر الاستخدامات الإيجابية للتقنية ونشرها بين أفراد المجتمع، وكذلك حفظ وحماية الحقوق المترتبة على الاستخدام المشروع للحاسبات الالية وشبكات المعلومات وأجهزة الجوال وكل الوسائل التقنية المختلفة.

جهود مؤسسة النقد

أنشأت المؤسسة وحدة لمتابعة الاختلاس والاختلاس والاحتيال المالي الإلكتروني، ومن بين مهامها معالجة الجرائم الإلكترونية التي تتعلق بأنشطة البنوك إلى جانب السعي للحصول على أحدث التقنيات والأجهزة التي من شأنها الحد من تلك الجرائم، كما أن هناك وحدة لأمن المعلومات للتصدي لمحاولات الاختلاس ولتأمين مواقع البنوك على شبكة الإنترنت من خلال التنسيق مع هيئة الاتصالات وتقنية المعلومات.

والمؤسسة تنسق مع البنوك بخصوص توعية العامة وعملاء البنوك بصفة خاصة وكذلك هناك لجنة مصرفية مختصة بمكافحة الجرائم المالية تعقد اجتماعات دورية كل شهرين كما قامت المؤسسة بعقد دورات لمنسوبي الأجهزة الأمنية والتحقيق وكذلك القضاة للتعريف بأنواع الجرائم المصرفية ومنها الجرائم الإلكترونية.

وننوه أن هناك دراسة مشروع نظام لمكافحة جرائم تقنية المعلومات بدول مجلس التعاون لدول الخليج العربية، حيث تعرف جرائم تقنية المعلومات بأنها كل استخدام للشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية أو الحصول بقصد على أموال الغير دون وجه حق، ويتضمن مشروع النظام نحو (٣٩) مادة.

الإضرار بالآخرين

وعن استخدام هذه الوسائل الحديثة في التقنية في السب والتشهير والإضرار بالآخرين استضفنا في هذا الجانب **فضيلة الدكتور عبدالرحمن بن عبدالله السند - أستاذ الفقه المساعد بالمعهد العالي للقضاء** والذي له اهتمام بالجوانب الشرعية والفقهية في التقنية الإلكترونية، فأوضح أن القذف هو: الرمي بالزنا، وزاد الشافعية: في معرض التعبير.

وعرفه المالكية: بأنه رمي مكلف حراً مسلماً بنفي نسب عن أب أو جد أو بزنا.

أما السب فهو الشتم، وهو كل كلام قبيح، كقول إنسان لآخر:

يا أحمق، وعلى هذا فالسب أعم من القذف، وقد يطلق السب ويراد به القذف، ويطلق القذف ويراد به السب إذا ذكر كل منهما منفرداً، أما إذا ذكرا معاً فلا يدل أحدهما على الآخر.

وعند التغاير يكون المراد بالقذف ما يوجب الحد، وبالسب ما يوجب التعزير، والسب محرم في دين الله عزَّ وجلَّ، فيحرم سب المسلم من غير سبب شرعي يجيز ذلك، بل صرح كثير من الفقهاء بأنه كبيرة من كبائر الذنوب، فقد قال النبي ﷺ: «سباب المسلم فسوق».

أما من سب الله عزَّ وجلَّ، أو سب النبي ﷺ، أو سب الدين والملة فهو كافر خارج من الملة.

وكذلك فإن قذف المحصن والمحصنة حرام، وهو من كبائر الذنوب.

والقذف على ثلاثة أضرب: صريح، وكناية، وتعريض، فاللفظ الذي يقصد به القذف إذا لم يحتمل غيره فهو الصريح، فإن فهم منه القذف بوضعه فهو كناية وإلا فهو تعريض، واتفق الفقهاء على أن القذف بصريح الزنا يوجب الحد بشروطه، وأما الكناية فإن أنكر القذف صدق بيمينه وعليه التعزير للإيذاء.

وأما التعريض بالقذف فقد اختلف الفقهاء في وجوب الحد به، ليس هنا مجال التفصيل فيه،

القذف والسب الإلكتروني

إن جرائم القذف السب من أكثر الجرائم التي تقع من طريق الإنترنت فنجد بعض المتعاملين بشبكة المعلومات العالمية يستسهل الرمي بالقذف والسب للآخرين وذلك راجع إلى عدة أسباب منها:

١ - أن غالب من يرتكب ذلك يختفي وراء أسماء وهمية فيأمن بذلك العقوبة في زعمه.

- أن المتعاملين بالإنترنت لا تحدهم حدود جغرافية، فتجد القاذف أو السابّ من بلد والمقذوف من بلد آخر، الأمر الذي يأمن معه من الملاحقة القضائية والنظامية.

على أن القذف والسب عبر الإنترنت خطير جداً، لأن الذين يطالعون الإنترنت عدد كبير من الناس، فهو مشاع ومتاح للناس كافة، ما يتضرر به المقذوف أو الذي وقع عليه السب أكثر مما لو وقع ذلك في عدد قليل من الناس، لذلك فإن بيان الحكم الشرعي لهذه المسألة وتوعية الناس بها وبخطورة هذا الأمر مما يدعو إلى كف الناس عن الوقوع فيها، والانزلاق في هذا المزلق الخطير، فإن الله عزَّ وجلَّ يقول: ﴿وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْ يَأْتُوا بِأَرْبَعَةِ شُهَدَاءَ

❖ السند:

• جرائم السب والقذف من أكثر الجرائم الإلكترونية العالمية
• جمع المعلومات عن الجريمة المعلوماتية والبحث عن مرتكبيها يأتي عن طريق الأساليب النظامية والجهات ذات العلاقة

❖ زمزمي:

• مرحلة المحاكمة هي النهاية الطبيعية للفصل في الجرائم الإلكترونية

فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَةً وَلَا تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُولَئِكَ هُمُ الْفَاسِقُونَ ۝ إِلَّا الَّذِينَ تَابُوا مِنْ بَعْدِ ذَٰلِكَ وَأَصْلَحُوا فَإِنَّ اللَّهَ غَفُورٌ رَحِيمٌ﴾ [النور: ٤ - ٥] فدلَّ ذلك على خطورة القذف، وما أعده الله عزَّ وجل لمن ارتكب هذه الجريمة من عقوبات شديدة تهز قلب المسلم، ويعلم معها شناعة هذا الفعل وقبحه.

وقد يتم القذف أو السب عبر البريد الإلكتروني للمقذوف أو المسبوب فيتم إرسال هذه الرسالة إلى الشخص وحده، وقد ترسل إلى عدة أشخاص فيعظم بذلك الجرم، ويشتد الأذى على من وقع عليه القذف أو السب لانتشاره بين هذا العدد من الناس.

وفي أي حال، فإن الذي ينظر في واقع الإنترنت هذه الأيام ولا سيما في الساحات ومواقع الحوار والنقاش، يجد جرأة كثير من المشتركين على السب والقذف الذي يأنف منه المسلم، ويخشى عقوبته، مما يستلزم أن بين للناس خطورة هذا الأمر، وحكمه الشرعي، فكم تضرر أناس، واتهمت أسر وهتكت أسرار عبر هذه الساحات ومواقع الحوار والنقاش، ولا حول ولا قوة إلا بالله.

أنواع الجرائم الإلكترونية

الشبكة الإلكترونية (الإنترنت) أفرزت عدة أنواع من الجرائم قد لا تختلف عن الجرائم الأخرى في المسميات لكن الاختلاف في الوسائل فعن أنواع تلك الجرائم كان لنا في هذه الندوة مشاركة من **المحامي والمستشار القانوني الدكتور إبراهيم بن أحمد**

زمزمي وقد حدد الجرائم التي يمكن ارتكابها عن طريق الشبكة الإلكترونية بنوعين الأول جرائم الحدود والثاني جرائم التعزير.

أولاً: جرائم الحدود:

وهي خمسة أنواع:

١ - جرائم الدين، كالردة والبغي والقذف والحرابة (قطع الطريق).

فجريمة الردة بالرغم من كبر جرمها، لم تدرج ضمن الجرائم التي وردت بنظام مكافحة جرائم المعلومات السعودي.

وجريمة البغي متصور ارتكابها عن طريق الشبكات، وقد تضمنها نظام مكافحة الجرائم المعلوماتية، ومع ذلك فقد أفرد لها عقوبة تعزيرية، حيث تنص المادة (١/٦) منه على أن: «يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

- إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي».

وكل ما هناك أنه شدد هذا العقاب إذا اندرجت تلك الجريمة ضمن الجرائم التي ترتكب ضد الدولة، حيث تنص المادة السابعة على أن «يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

٢ - الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني».

وبالنسبة لجريمة القذف، فعقوبتها الجلد والحرمان من الشهادة.

ولفظ القذف أو الرمي، يطلق على كل ما ينسب للغير بالباطل، ويسبب له أذى سواء في ماله أو سمعته وشرفه، ولا عبرة في فعل الإسناد بالوسيلة التي يتبعها الجاني في التعبير عن إلصاقه عبارات القذف.

وتلك الجريمة وردت بنظام مكافحة الجريمة المعلوماتية، حيث تنص المادة (٤/٣) على ما يلي: «يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها».

وبالنسبة لجريمة الحرابة «الإفساد في الأرض» فعقوبتها النفي والقطع والقتل والصلب.

وهذه الجريمة يتصور ارتكابها أيضاً عن طريق الشبكات الإلكترونية، لأن الأفعال المؤثمة التي وردت بها وإن كانت مادية وتستلزم تلاقي الأطراف وهما الجاني قاطع الطريق والمجنى عليه الضحية، إلا أنه وعملاً بالقياس يتصور ارتكاب جريمة السرقة عن طريق الشبكات باعتبارها سرقة منفعة، وكذلك إخافة الناس عن طريق نشر ما يتسبب في إخافتهم ورعبهم عن طريق بث الإشاعات القابلة للتصديق.

ولعل من الضروري وضع نص عام واضح يقرر الآتي: «أن تطبيق هذا النظام لا يخل بتوقيع أي عقاب آخر شرعي أو تعزيري مقرر لأية جريمة من الجرائم التي لم ترد بهذا النظام» بدلاً من المادة (١٢) الحالية التي تنص على ما يلي: «لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة ما يتعلق بحقوق الملكية الفكرية، والاتفاقات الدولية ذات الصلة التي تكون المملكة طرفاً فيها».

٢ - جرائم النفس:

وتشمل القتل العمد والجرح العمد وعقوبتها القصاص، والجرائم على ما دون النفس عمداً كإتلاف الأطراف عمداً وعقوبتها القصاص أو الدية.

وهنا يثار التساؤل عن مدى ارتكاب جرائم القتل والجرح العمدي وغير العمدي عن طريق الشبكات الإلكترونية، وسبب ذلك أن الوسائل المعنوية ومن أمثلتها في جريمة القتل، إلقاء نبأ مفجع على شخص مريض بالقلب، يرى غالبية علماء الجريمة صلاحيتها لحدوث جريمة القتل متى ثبت توافر قصد القتل لدى الجاني ورابطة السببية بين هذا الفعل ووفاة المجني عليه.

٣ - جرائم النسل:

وصورها الزنا والاعتداء على العرض وعقوبتها الرجم أو الجلد أو التغريب.

ولا يمنع من توقيع العقاب الوارد بالمادة (٢/٦، ٣) من نظام مكافحة الجرائم المعلوماتية، حيث تجرم «إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس البشري، أو تسهيل التعامل به، أو إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها» على اعتبار أن تلك الأفعال دعوى وإعلان

عن الفجور، أو ممارسة البغاء.

٤ - جرائم العقل:

فقد حثّ الله تعالى على ضرورة احتفاظ الإنسان بعقله في مواضع كثيرة، وبالطبع فإن شرب الخمر غير متصور عبر الشبكات الإلكترونية، ولكن الدعوة والإعلان عنها متصور، وهذا ما تمت مراعاته في المادة (٤/٦) من نظام مكافحة الجرائم المعلوماتية، والتي تقرر تجريم: «إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل به.

٥ - جرائم المال «السرقة»:

وعقوبتها قطع اليد دون تمييز بين الرجل والمرأة وقد عالج النظام جرائم السرقة في نص المادة (٤) بأن يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١ - الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

٢ - الوصول -دون مسوغ نظام صحيح- إلى بيانات بنكية أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات».

ثانياً: جرائم التعزير:

وهي تشمل بقية الجرائم التي وردت في نظام مكافحة الجرائم المعلوماتية:

١ - جريمة التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو التقاطه أو اعتراضه (م ١/٣).

٢ - الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً (م ٢/٣).

٣ - الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه (م ٣/٣).

٤ - الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها (م ١/٥).

٥ - إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها، أو إتلافها، أو تعديلها (م ٢/٥).

٦ - إعاقة الوصول إلى الخدمة أو تشويشه أو تعطيلها بأي وسيلة كانت (م ٣/٥).

٧ - إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي (م ١/٦).

٨ - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس البشري، أو تسهيل التعامل به (م ٢/٦).

إجراءات الجرائم المرتبطة بالشبكات الإلكترونية

هذه الإجراءات تشمل ثلاثة مراحل حددها نظام الإجراءات الجزائية، وهي:

أولاً: مرحلة الاستدلال:

جمع المعلومات عن الجريمة، والبحث عن مرتكبها عن طريق الأساليب النظامية والجهات المسؤولة ذات العلاقة.

ثانياً: مرحلة التحقيق والاتهام:

وتتولاها سلطة التحقيق والادعاء العام، حيث تنص المادة (١٥) من نظام مكافحة الجريمة المعلوماتية على أن: «تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام».

وتتخذ العديد من الإجراءات مثل: التكليف بالحضور، وأمر الضبط والاحضار، والوضع تحت المراقبة، والقبض على المتهم مؤقتاً في حالة تلبس، وأوامر التوقيف الاحتياطي، ومصادرة المضبوطات.

ثالثاً: مرحلة المحاكمة:

وهي النهاية الطبيعية للفصل في الجرائم التي ترتكب عن طريق الشبكات الإلكترونية، وأمام ظاهرة تنامي تلك الجرائم، بسبب السرعة الفائقة التي تتيحها هذه الشبكات لارتكاب

❖ الزهراني:

• أمن وحماية المعلومات هاجس يقلق المسؤولين

• يوجد عدد من التحديات التي تواجه مشروع مكافحة الجرائم المعلوماتية

الجرائم، كان لا بد من تحديد القضاء المختص بنظر هذه الجرائم.

أمن المعلومات

في هذا العصر المتسارع والمتقارب جغرافياً بسبب التواصل التقني وفي عصر التطور الإلكتروني وقيام حكومات إلكترونية وتبدل نمط الحياة أصبح من الضروري الحفاظ على المعلومات والتفكير بأساليب أمنها، وفي هذا الجانب أدلى **الدكتور صالح بن غرم الله الزهراني وكيل كلية علوم الحاسب والمعلومات بجامعة الإمام محمد بن سعود الإسلامية**، وبين أن أمن وحماية المعلومات هاجس يقلق جميع العاملين والمسؤولين عن تقنية المعلومات في جميع المؤسسات والمنظمات العامة والخاصة وفي بداية الأمر عندما كان الاعتماد على مركزية الحاسبات في عدم وجود ربط خارجي مع الجهات الأخرى كان المسؤولون عن التقنية يسعون إلى حماية المعلومات من التلف بالنسخ الاحتياطية والتأكيد على العاملين باستخدام الأرقام السرية وغيرها، ومع اتصال المنظمات مع غيرها من المنظمات المتشابهة الأخرى أضحى الاعتماد علي نظم المعلومات في جميع قطاعات الدولة الحساسة كالتقنية والعسكرية والمالية أمر في غاية الأهمية، ونتيجة لذلك أصبحت مهمة أمن المعلومات ضرورة مهمة لجميع المنظمات وأصبحت قضية أمن المعلومات قضية وطنية وجزء أساسي من الأمن الوطني، واليوم مع ازدياد الاهتمام بالتقنية أصبح الاهتمام بقضايا أمن المعلومات وما يترتب عليها من القضايا الشائكة سواء ما يتعلق بالمعلومة نفسها ومدى صحتها أو ما يتعلق بالقضاة والمختصين في الفقه والقانون والمعلوماتية أمر ضروري، وفي حقيقة الأمر أصبحت الدولة في حاجة ماسة لتشريعات جنائية لمكافحة ومعاقبة مرتكبي جرائم الحاسب وفي هذه الحالة فإن المشرع يجد نفسه أمام عدد من التحديات منها:

- صعوبة الاستدلال وجمع الأدلة الجنائية لتأكد من الجريمة ومدى شرعية الأدلة.
- تنازع الاختصاص بين القضاة ورجال الأمن ورجال الفقه والقانون الجنائي والمختصين في مجال الحاسوب.
- التغير السريع وتطور مهارات مجرمي تقنية المعلومات واستيعابهم للتقنية والثغرات القانونية والفنية أكثر من المشرع وقدرتهم.

التهديد من الداخل والخارج

وتهديد أمن المعلومات وإن لم يكن ذلك التهديد مقصود في بعض الأوقات ولكن في النهاية هو أمر يستحق الاهتمام والتخطيط والمتابعة والحفاظ على سرية المعلومات وعموماً فالتهديد الأمني يأتي من جهتين هما:

أ - تهديد داخلي: ويقصد به التهديد والاعتداء من العاملين داخل المنظمة، حيث يقوم بعض الموظفين إما بإساءة استخدام صلاحياتهم أو إساءة استخدام الموارد المتاحة لديهم في أمور تضر بالمنظمة مثل أن يقوم مدخل البيانات بإدخال معلومات خاطئة ولك أن تتصور عندما يضيف مدخل البيانات في قسم الرواتب رقماً واحداً عمداً؟ ماذا سيحدث لميزانية المنظمة؟ وكم من الوقت يحتاج مدير النظام ليعرف موقع الخطأ؟ ويقوم بتصحيحه وعموماً يمكن تصنيف التهديد الداخلي إلى:

- أخطاء بشرية: ويحدث نتيجة الأخطاء في إدخال البيانات أو تصميم النظام أو تجميع البيانات أو من خلال إعطاء الصلاحيات لدخول المعلومات.
- أخطاء بيئية: مثل تصميم مواقع الحاسب في أماكن غير مناسبة تجعلها عرضة للكوارث الطبيعية كالسيول والحريق وانقطاع الكهرباء، وعموماً فقد أثبتت الدراسات الميدانية بأن ٨٥٪ من مشكلات أمن المعلومات تأتي من داخل المنظمة وليس من الخارج.

ب - تهديد خارجي: والمقصود به أن تتعرض المنظمة ومعلوماتها لتهديد من خارج حدود المنظمة من خلال الفيروسات والقرصنة الإلكترونية والتجسس ومحاولة جهات خارجية سواء منافسين أو مخربين لقصد الحصول على المعلومات الخاصة بالمنظمة، وهذا التهديد زاد حدة وكثرة خطره بعد انتشار شبكات الحاسب وأصبحت جرائم الحاسب لا تعترف بالحدود الجغرافية والأماكن والأزمنة وأصبح طفل صغير في قرية نائية في شرق الصين يهدد منظمة أفريقية بشقاوته ومعرفته في مجال الحاسب.

إن جميع المنظمات اليوم أصبحت في خطر كبير وأصبحت أكثر حاجة إلى نشر الوعي بين العاملين وتبني سياسة أمنية قوية لحماية ممتلكاتها، وفي حقيقة الأمر قد ساهمت شركات

أمن المعلومات في إنتاج خطط وبرامج قوية وتقنيات متقدمة كالكابلات المدفونة في الأرض لكشف المتطفلين وفحص الطرود المفخخة واستخدام التصوير الحراري، لكشف الغرباء، ولكن يبقى أن التوعية بأهمية أمن المعلومات ووضع سياسة أمنية واضحة من أهم مهام المنظمات التي تسعى إلى الحفاظ على أمن معلوماتها كإحدي الموارد التي يجب أن تحافظ عليها.

وخلاصة الأمر كم أتمنى أن تتم الاستفادة من القضاة والعلماء بعد أن تشرح لهم الطرق التقنية التي يتبعها مجرمي الحاسب لتنفيذ جرائمهم وتطبيق قوانينهم في القياس والاجتهاد في القضاء الإسلامي علي الواقع المعاصر، كما أتمنى الاستفادة من المفكرين ومشرعي القوانين والمختصين في مجال الحاسب لصياغة ووضع قوانين متفقة مع تقنية التبادل الإلكتروني ومتفقة أيضاً مع القوانين والتشريعات والنظام الاجتماعي بالمملكة.

التوصيات

- ضرورة تفعيل العقوبات الرادعة التي حددتها الأنظمة المختصة.
- توعية المجتمع وتثقيفه وتعريفه بالوسائل والطرق التي يستخدمها مجرمي المعلوماتية لتجنب الوقوع في حبائلهم.
- إنشاء جهة عدلية متخصصة ومؤهلة للتعامل مع جرائم المعلوماتية.
- ضرورة أن تؤخذ بالحسبان الضوابط الشرعية عند طرح أخلاقيات التداول والتعامل مع «الإنترنت».
- ينبغي لأجهزة العدالة الجنائية إنشاء موقعاً لأرشفة البيانات للرجوع إليها
- يمكن لأجهزة العدالة أن تستعين بشركة أو أكثر متخصصة في تقنية الحاسوب كشفاً للجريمة الإلكترونية
- سرعة تفعيل مواد نظام مكافحة جرائم المعلوماتية
- لما كانت الجرائم المعلوماتية بهذه الخطورة فإن خطورتها تتعدى مكان ارتكابها فهي جريمة عابرة للحدود والقارات فهي إذن جريمة دولية وطالما أنها كذلك فإن من الواجب على الدول المختلفة أن تقوم بإبرام اتفاقيات وعقد معاهدات لهذا لمواجهة شاملة لمثل هذه الجرائم حتى يمكن ملاحقة مجرمي المعلومات والحد من خطورتهم في أي مكان على الأرض.
- على وزراء الداخلية والعدل في الدول العربية وغيرها القيام بإقامة دورات تدريبية فيما يتصل بجرائم الحاسب الآلي والإنترنت للمحققين والقضاة والأجهزة الأمنية حتى يتمكنوا من القيام بدورهم في التصدي للجريمة المعلوماتية ومن الممكن إيجاد شرطة متخصصة وجهة ادعاء متخصصة في هذه الجرائم فإن خطرها قد تعدى المعقول.
- تشديد العقوبات بما يتناسب مع خطورة الجريمة المعلوماتية وقد تصل في بعض الأحيان إلى الإعدام تحقيقاً للردع العام والخاص ومقاومة دوافعها.
- العمل لدى الدول التي لا تعمل بالشريعة الإسلامية بنظرية التفويض القضائي المقررة في الشريعة الإسلامية عندما تتأخر الجهات المختصة في إصدار قوانين للجرائم ثم المستخدمة.

كي لا يتمكن مجرموا المعلوماتية من استغلال الفراغ القانوني قبل صدور القوانين التي تجرم تلك الأفعال فيفلتوا من العقاب ويجدون الوقت الكافي لتطوير أساليبهم ونشر فسادهم وإلحاق ضرر أكبر بالأفراد والمجتمع.

- إضافة مادة إلى نظام مكافحة جرائم المعلوماتية بالنص التالي: «تختص محاكم المملكة بمعاقبة مرتكبي الجرائم الواردة في هذا النظام، حتي ولو وقعت الجريمة في الخارج إذا كانت موجهة ضد أحد المواطنين، أو إذا امتدت آثار الجريمة إلى داخل إقليم المملكة العربية السعودية.
- عقد اتفاقية خليجية لمكافحة جرائم المعلوماتية.
- عقد اتفاقيات ثنائية بين المملكة وأكبر عدد ممكن من الدول في مجال مكافحة جرائم المعلوماتية.
- تطبيق نظام مكافحة جرائم المعلوماتية يجب أن لا يخل بتوقيع أي عقاب شرعي آخر مقر لأي جريمة بهذا النظام.
- جميع المؤسسات اليوم أصبحت في خطر كبير وهي أكثر حاجة إلى نشر الوعي بين العاملين.
- ينبغي وضع سياسة أمنية واضحة لتجنب تنازع الاختصاص بين الجهات الأمنية.