

الفصل الثامن
"الجريمة الإلكترونية
والجهود الدولية للحد منها"

obeikandi.com

الفصل الثامن

"الجريمة الإلكترونية والجهود الدولية للحد منها"

الجريمة الإلكترونية :-

في البداية الجريمة " هي كل فعل أو نشاط يتم بطريقة غير مشرعة"، بمعنى كل نشاط مخالف للقوانين العرفية والوضعية المتعارف عليها والمعمول بها عبر مختلف دول العالم، هذا النشاط إذا ما استخدمت فيه وسائط تقنية علمية، أصبح الفعل جريمة إلكترونية، فالجريمة إلكترونية " هي كل سلوك غير مشروع أو غير أخلاقي أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها " كون التقنية فيها تكون إما وسيلة تستخدم في ارتكاب الفعل أو البيئة والوسط الذي يحدث فيه الجرم أو يكون الهدف أو الغاية لارتكاب الفعل المجرم، أي أن الوسيط يكون آلة تقنية كجهاز الحاسب الآلي، الذي يكون دوما وسيلة للفعل الإجرامي الإلكتروني دون إهمال بعض الأجهزة التقنية الأخرى كالجيل الثالث للهواتف المحمولة، ولا سيما مع الانتشار الواسع لاستخدامات الإنترنت الذي حوّل العالم إلى قرية صغيرة باعتباره وسيلة اتصالات عالمية تعتمد على البرامج المعلوماتية الحديثة في ضبط مختلف البيانات والمعطيات المعلوماتية الدقيقة.

فالجريمة الإلكترونية يمكن وصفها بأنها كل فعل يستهدف القضاء على استخدام التكنولوجيا الحديثة عبر الوسائط الإلكترونية، ومع غزو الإنترنت دول العالم أصبح من الصعوبة بمكان ضبط وكشف هذه الجرائم نظرا لكونها عابرة للحدود لا دين ولا وطن لها، وتتم بسرعة فائقة دون رقيب أو حسيب ودن رقابة من أي دولة مما ادي الي ارتكب كافة صور النشاط الإجرامي المتعارف عليها عبر الإنترنت حتي القتل والدليل عي ذلك الرجوع الي مؤلفنا الجريمة الإلكترونية ، كالسطو على برامج الحاسوب بغرض سرقة البيانات وقاعدة المعطيات المعلوماتية حتى السرية منها واستخدامها في التجسس، أو تلك المتعلقة بالقرصنة والسطو على الأموال إلى جانب ظهور ما اصطلح عليه بالإرهاب الإلكتروني وتهديد الأمن القومي للدول، وكذا جرائم

الآداب العامة والمساس بالأخلاق من خلال الإباحية الإلكترونية التي تجسدها المواقع الجنسية الإباحية، خاصة الموجهة منها للأطفال والمقدرة بأكثر من 1000 موقع يقدم مواد جنسية إباحية خاصة بالأطفال ما دون سن البلوغ، يتم فيها استخدام دعارة الأطفال والنساء، سواء بالعين أو قصر عن طريق تصويرهم مباشرة أو بالمحاكاة والتمثيل الرقمي للصورة باستعمال وسائل الترغيب والترهيب كالإغراء والتحذير أو التهديد.

كل النظريات والدراسات المنجزة تتفق حول نقطة أساسية، تتمثل في الغاية المادية البحتة التي يسعى إلى تحقيقها المجرم الإلكتروني، من سطو على الأموال، إلى الاعتداء على البيانات السرية وتدمير البرامج المعلوماتية لأية دولة لتهديدها في أمنها القومي وسلامة أراضيها ولعل أبرز مثال علي ذلك اقتحام موقع وزارة الدفاع الأمريكي، لتعود في صورة حديثة على شاكلة ما يعرف بإرهاب المستقبل الذي أصبح هاجسا حقيقيا يهدد سلامة وأمن المجتمع الدولي، عن طريق التهديد بتدمير أساليب واستراتيجية الدفاعات الأمنية والاقتصادية للدول وعوائدها المالية باستخدام الخطط التخريبية و الفيروسات لتدمير مختلف البرامج المعلوماتية وإتلاف مختلف البيانات الخاصة بتقنية الرقمية في حفظ وتخزين البرامج المعلوماتية لأية دولة ومهما كانت درجة سريتها، كما حدث مع فيروس ما يعرف بـ "دودة مورس"، كما اشرفنا في مؤلفنا الجريمة الإلكترونية أو فيروس "أوميغا" بإسرائيل بداية التسعينيات وكلف الدول خسائر مادية فادحة قدرت بملايير الدولارات. ففي سنة 2007 مثلا كانت تقع جريمة إلكترونية واحدة كل 03 ثواني، مع تسجيل 850 ألف حالة تخص التحرش بالأفراد، و 207 ألف حالة خاصة بالسطو وسرقة الأموال، تسبب ذلك في خسائر مادية بلغت 48 مليار دولار كل 03 دقائق. أما في الوطن العربي، فقد تم تسجيل خلال السنة نفسها 217 ألف قضية قرصنة وسطو بدولة الإمارات العربية المتحدة لوحدها، مع زيادة كبيرة خلال سنة 2008 بلغت 33 بالمائة.

ويتميز مرتكب جرائم الكمبيوتر بصفات خاصة تميزه عن غيره من مرتكبي الجرائم الواردة في قانون العقوبات، وذلك من حيث: صفات المجرم مرتكب جرائم الكمبيوتر: غالباً ما يتميز بالذكاء ولا يميل إلى استخدام القوة والعنف، كما يتميز بأنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عدااء سافر مع المجتمع الذي يحيط به - بل إنه إنسان متوافق معه.

أنواع المجرمين مرتكبي جرائم الكمبيوتر:

- 1- إما يكونوا مجرمين محترفين
 - 2- إما أن يكونوا من الهواة، ويطلق عليهم صغار نوابغ المعلوماتية.
- ### **الأسباب الدافعة لارتكاب جرائم الكمبيوتر**
- 1- الولع في جمع المعلومات وتعلمها .
 - 2- حب المغامرة والإثارة.
 - 3- الدوافع الشخصية: فغالباً ما يرتكب المبرمج جرائم الكمبيوتر نتيجة إحساسه بالقوة والذات، وبقدرته على اقتحام النظام، فيندفع تحت تأثير الرغبة القوية في تحقيق الذات.
 - 4- تحقيق مكاسب مالية.
 - 5- الفضول لدي الكثيرين .

صعوبة اكتشاف الدليل الرقمي

نظراً للخصائص المميزة التي تتسم بها الجريمة الإلكترونية 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 عائقاً حقيقياً أمام مهمة المحققين في التوصل إلى ضبط الدليل الرقمي للإثبات والإدانة للجناة، إلى جانب كونها تقع في بيئة افتراضية عابرة للحدود، حتى وصفت أحياناً 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، نظرا 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 تحدث في مصر مثلا وضحاياها في السعودية، فأى القانون يمكن تطبيقها في هذه الحالة، قانون مصر أم السعودية؟

هناك العديد من المشكلات والصعوبات العملية والإجرائية التي تظهر

عند ارتكاب أحد جرائم الإنترنت، ومن هذه المشكلات:

- 1- صعوبة إثبات وقوع الجريمة.
- 2- صعوبة تحديد المسؤول جنائياً عن الفعل الإجرامي.
- 3- صعوبة إلحاق العقوبة بالجاني المقيم في الخارج.
- 4- تنازع القوانين الجنائية من حيث المكان.
- 5- صعوبة التوصل إلى الجاني.
- 6- القصور في القوانين الجنائية القائمة.
- 7- افتراض العلم بقانون جميع دول العالم.

أهم صور الاعتداء الجنائي على المعلومات في الإنترنت

تتمثل أهم صور الاعتداء الجنائي في الجرائم الالكترونية التالي:

- 1- جرائم النصب والاحتيال عبر الإنترنت
- 2- جرائم سياسية عن طريق التجسس على الدول عبر الإنترنت، ومحاولة اختراق أنظمتها العسكرية.
- 3- جرائم التدمير والعبث بأنظمة الحاسب، وذلك عن طريق الدخول على الشبكة وتدمير برامج الحاسب، أو نشر مواقع تخريبية وفيروسات.
- 4- جرائم سرقة حقوق الملكية الفكرية عن طريق نسخ البرامج الأصلية

وتسويقها أو استخدامها دون إذن مسبق، مما يعرض الشركات المنتجة لهذه البرامج للكثير من الخسائر المالية.

5- الجرائم المتعلقة بإعادة إنتاج المعلومات المسجلة عبر الإنترنت بصورة غير مشروعة، أو تقليدها.

6- سرقة المعلومات بحسبها مجرد معلومات معنوية.

7- جرائم السب والقذف عبر الإنترنت

8- جرائم الاعتداء علي الحياة الخاصة للأفراد .

قسم بعض الباحثين في مجال المعلومات قرصنة الفضاء الإلكتروني إلى نوعين رئيسين:

الأول: وهم ما يطلق عليهم الهاكرز Hackers(16)، وجلهم يستهدف بالأساس إلحاق الأذى بالمحتويات التي تضمنتها الذاكرات والدوائر الإلكترونية في شبكات الحواسيب، سواء الخاصة بالمؤسسات والشركات أو الأفراد، لمجرد إثبات أنهم قادرون على هذا، لذلك فهم ينظرون إلى أنفسهم على أنهم أبطال أذكى، بينما يعتبرهم الآخرون مخربين خبثاء.

الثاني: وهم لصوص ومافيا السرقات الإلكترونية عبر الإنترنت، وهدفهم الرئيس هو سرقة أموال أو بيانات أو أسرار، تضمنها شبكات الحاسب بعينها، وذلك باستخدام تقنيات خاصة بالاختراقات المعلوماتية Computer Breaches.

وتتسم هذه النوعية من الجرائم الإلكترونية بسهولة ارتكابها، ما لم تكن ثمة احتياطات وتقنيات مضادة قوية تقف سداً منيعاً أمامها، وأيضاً بسهولة إخفاء معالمها.

ومن أشهر طرق الاختراق التي يستخدمها القرصنة واللصوص:

9- طريقة بث الفيروسات، وهي الطريقة المفضلة لدى القرصنة بوجه خاص، قد اشتهرت بعض الفيروسات في هذه الطريقة منها: فيروس (حصان طروادة)، وفيروس (الحب) ، وفيروس (المصيدة)، وفيروس (سيركام)،

وفيروس (كليز)، وغير ذلك من الفيروسات.

10- طريقة سرقة الشرائح: وهي من أكثر الطرق تداولاً بين لصوص الإنترنت.

الحل في ظل القوانين السارية :-

إزاء انتشار الجرائم الإلكترونية كظاهرة عالمية، كان من الضروري البحث في كيفية إيجاد حلول فعالة واتخاذ تدابير وقائية منها وردعية لوقف الزحف الخطير لهذه الكوارث التقنية التي باتت تهدد اقتصاديات أمن واستقرار الدول بعد تطور الجريمة الإلكترونية من إطارها الكلاسيكي المعروف إلى التقنية العلمية الحديثة لتصبح تجارة إلكترونية رائجة وهو ما اصطلح عليه بالاقتصاد الرقمي، وهو ما تفسره نسبة الشكاوى الرسمية التي اعتمدها المركز العالمي لشكاوى الانترنت والتي كلفت سنة، 2000 خسارة مادية فادحة قدرت بـ 12 بليون دولار جراء النتائج التدميرية التي تسببت فيها فيروسات إتلاف برامج المعلوماتية. وقد قدرت مجمل الشكاوى الرسمية التي قدمها الضحايا للمركز بـ 275284 شكوى وفي مصر خصص وزير الداخلية رقم " 108 " للتبليغ عن جرائم الانترنت 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 دورياً كل شهر إن تطلب الأمر ذلك، مع تكثيف برامج الرقابة على نوادي ومقاهي الانترنت، والعمل على ترصد وحجب المواقع الإباحية كما هو الحال بالعربية السعودية وتونس، مع اعتماد برامج خاصة مضادة للفيروسات التدميرية واستعمالها بشكل مستمر.

التعاون الدولي للحد من الجرائم الإلكترونية

أمام الفراغات التشريعية التي أصبحت عبء علي كاهل الدول بعد انتشار الجرائم الإلكترونية، خاصة مع استخدام الإنترنت "الشبكة العنكبوتية WWW" 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 الإلكتروني، 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 نظرا لطابعها العالمي،

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

وتعتبر السعودية أول دولة عربية سنّت قوانين خاصة بمكافحة الجريمة الإلكترونية، تلتها الإمارات العربية المتحدة ثم عمان، غير أنها قوانين غير فعالة نظرا لطابعها المحلي من جهة، والثغرات القانونية الموجودة بها، لذا أصبح من الضروري الدعوة للعمل على سن قانون دولي فعال شامل يكون مبنيا 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 الإلكترونية، 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 المشرع 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 كافٍ، حيث لازالت معظم القوانين الموجودة لا تتماشى وحجم الكوارث المرتكبة يوميا، لذا من الواجب من الآن، إعادة النظر في المنظومة القانونية الخاصة وإدراج قوانين جديدة للتصدي لظاهرة تنامي الجريمة الإلكترونية في أبعادها المختلفة.

فجرائم الإنترنت تخطت تفجيرات 11 سبتمبر" .. هكذا هي نظرة العالم الآن إلى شبكة الإنترنت بعد أن أصبح الدخول إليها مخاطرة غير محسوبة العواقب حيث انتشر الهاكرز على جناباته منتظرين الانقراض 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 الإنترنت.

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 للملاحقة ومقاضاة المجرمين، وستتسق 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 أيضا منح يور وبول مبلغ 300 ألف يوروو لتتشي جهازًا لتجميع تقارير الإجمام وإصدار تحذيرات حول الأخطار المحدقة.

و دعم الاجتماع الوزاري إستراتيجية مكافحة الجريمة الالكترونية التي ستشي فرق تحقيق تعمل عبر الحدود و ترخص 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 لأطفال".

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 إلكترونيًا لتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة على الانترنت، ويعتمد على مفهوم أن تنهض جهة مفردة بذلك التتبع، ما يمكن المعنيين من الرجوع إليها ومتابعتها بسهولة.

ووصف 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، وفقاً للبيان الصحفي
لـ"الاتحاد الدولي للاتصالات.

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

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

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

أول دولة عربية تصدر قانون جرائم الإنترنت

سبقت المملكة العربية السعودية نظيراتها من الدول العربية في إصدار
قانوناً جديداً لمكافحة جرائم المعلوماتية التي تشمل التهديد والابتزاز والتشهير
بالآخرين في مواقع الإنترنت وإنشاء مواقع الإنترنت الإرهابية.

ونقلت وكالة الأنباء الكويتية عن مصدر مسؤول بوزارة الداخلية
السعودية قوله أن نظام مكافحة جرائم المعلوماتية قد أصبح الآن قيد التطبيق
بعد صدور موافقة مجلس الوزراء عليه، معتبراً النظام إطاراً قانونياً مهماً جداً
في تعريف وتحديد الجرائم المعلوماتية والحد منها ومواجهتها بعد أن أصبحت
تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات الإنسانية.

وأوضح المصدر أن النظام الجديد يشمل 16 مادة تتضمن عقوبات
صارمة ضد مرتكبي هذه الجرائم تتراوح بين سنة و10 سنوات سجنًا وغرامات
مالية تصل إلى خمسة ملايين ريال سعودي، مضيفاً أن النظام تضمن تعريفات

المصطلحات والمسميات الواردة في النظام مثل "الشخص" و"النظام المعلوماتي" و"الشبكة المعلوماتية" و"البيانات والجريمة المعلوماتية الى جانب أهداف النظام بالحد من هذه الجرائم والعقوبات المقررة لكل منها.

وحددت مواد النظام الأخرى الجرائم المعلوماتية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة من الجرائم المعلوماتية واختصاصات كل من "هيئة الاتصالات وتقنية المعلومات" و"هيئة التحقيق والادعاء العام" في المساندة اللازمة للأجهزة الأمنية لتحقيق أهداف وغايات هذا النظام.

ويهدف النظام الجديد إلى حماية المجتمع من جرائم المعلوماتية والحد منها والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية المصلحة العامة والأخلاق والآداب العامة وحماية الاقتصاد الوطني

وتعانى السعودية في الفترة الأخيرة من محاولات اختراق مواقع الإنترنت، وكان آخرها يوم الثلاثاء الماضي، عندما تعرض أحد المواقع التعليمية الحكومية بالسعودية لاختراق استمر عدة ساعات كتب خلالها من قام بالاختراق ورمز لنفسه بالرمز (0) عبارات ينصح من خلالها مشرفي الموقع على الاهتمام بالموقع وحمايته وعدم استخدام برامج تصميم مجانية.

وتأخر كثيراً مشرفي موقع إدارة التربية والتعليم بمنطقة تبوك وهو الموقع الذي تم اختراقه في صيانة الموقع وحل مشكلة الاختراق حيث ظل فترة طويلة ورسالة الاختراق ظاهرة على واجهته.

الجدير بالذكر أن كثيراً من المواقع الحكومية قد تعرضت مؤخراً للاختراق إما بداعي التطفل أو لوجود كثير من الخلافات بين الجهة الحكومية ومن يقف خلف هذا الاختراق خاصة في المواقع التعليمية الحكومية مما اضطر مسؤولي وزارة التربية والتعليم السعودية و مؤخراً لنفي اختراق موقعه الخاص بشؤون المعلمين

وفيما يتعلق بإصدار قانون متخصص فى جرائم الإنترنت فكانت السويد هي من لها سبق على مستوى العالم فى سن مثل هذه التشريعات، ففي عام 1973 صدر قانون البيانات السويدي الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى تضمنه فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها .

وبدأت السعودية فى التفكير فى تطبيق قانون الحبس فى جرائم الإنترنت فى العام الماضي وبالتحديد فى شهر مارس عندما أعلنت السلطات هناك أنها ستفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال لجرائم القرصنة المرتبطة بالإنترنت وإساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح.

وقالت الحكومة حينها إنها وافقت على مشروع قانون بخصوص جرائم تكنولوجيا المعلومات كان مجلس الشورى السعودي قد اقترحه العام الماضي بموجبه توقع العقوبة على الدخول غير المشروع إلى موقع الكتروني أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع أو إغائه أو إتلافه أو تعديله.

كما يجرم مشروع القانون "المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف المحمولة المزودة بكاميرا أو ما فى حكمها بقصد التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة. وعارضت هيئة الأمر بالمعروف والنهي عن المنكر فى السعودية الهواتف ذات الكاميرات، وحظرت السعودية بيع هذه الأجهزة لعدة أشهر عام 2004. (26) لكن تلك القيود فشلت فى وقف انتشار أحدث الصيحات التكنولوجية فى البلد الذي يقطنه 24 مليون نسمة غالبيتهم من صغار السن ويتمتعون بمعدلات دخول فردية مرتفعة.

وتفرض السعودية رقابة شديدة على استخدام الانترنت من خلال تعقب المستخدمين وحظر المواقع الجنسية وبعض المواقع ذات المحتوى السياسي. شهد العالم تطورا نوعيا مسارعا في مجال التقنية الرقمية، يمكن اعتباره، ثورة رقمية أدت إلى ميلاد عالم افتراضي، لا يقل أهمية عن العالم المادي بما فيه من أحداث ووقائع، وقد نجم عن ذلك انفجار معرفي تطلب وسيلة جديدة لتبادل المعلومات وتسهيل المعاملات فأصبح التعامل الإلكتروني نمطا جديدا للحياة، تستطيع البشرية الاستغناء عنه فضلا عن كونه إنجازا تقنيا باهرا، حيث أن الوضع الراهن كشف عن الاستخدام المتزايد لهذه التقنية عن طريق الشبكة العالمية المعروفة بالإنترنت، مما ترك أثرا واضحا على كافة مناحي الحياة الاقتصادية، الاجتماعية والثقافية وحتى الأمنية، مع الاستحداث الملحوظة لجملة من القيم والعلاقات.

ثمة فجوة عميقة لدى أغلب الدول بين هذا التطور التقني الحاصل لديها من جهة وبين التشريع المواكب له، فبرزت معه ظاهرة الجريمة التي تتخذ من الحاسوب هدفا لها أو وسيلة لتحقيق أهدافها أو كونه البيئة والوسط الأمثل لتنفيذ هذه الأعمال الإجرامية التي شكّلت تحديا حقيقيا ومعضلة أمام القانون الجنائي التقليدي الذي لا يحوي في مفرداته عبارة الجريمة الإلكترونية ككيان مستقل بذاته خاصة أمام مبدأ الشرعية الجنائية، القاضي بأن "لا جريمة ولا عقاب إلا بنص" (27)، ومبدأ عدم القياس والتفسير الضيق لنصوص القانون الجنائي، وما يتطلب ذلك من إجراءات وقواعد نوعية تعتمد بالأخص على الجانب التقني المميز لإثبات الجريمة وضبط الدليل الرقمي الذي تتم بموجبه الإدانة.

"الأحدث" ومن خلال حضورها فعاليات الملتقى الدولي الأول حول التنظيم القانوني للانترنت والجريمة الإلكترونية والذي نظّمته مؤخرا كلية الحقوق والعلوم السياسية بجامعة زيان عاشور بالجلفة .

محاولات للحد من تلك الجرائم

وفى نفس السياق وللحد من الخطر القادم عبر الشبكات، تسارع الدول 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 أيضاً 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 وتحديث 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 والنوية".

وفي السعودية، تفرض الحكومة عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال فيما يعادل 133 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 الى موقع الكتروني لتغيير تصميم هذا الموقع أو إغائه 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 " .

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 :

بروتوكول مصري لمكافحة جرائم الإنترنت

وقعت الجمعية المصرية لمكافحة جرائم الإنترنت بروتوكول تعاون مع كلية الحقوق جامعة عين شمس بهدف تثقيف وتدريب طلبة وخريجي كليات الحقوق و الآداب والإعلام والسياحة والآثار والتجارة والحاسبات والمتخصصين ، والسادة القضاة وأعضاء النيابة العامة والسادة المحامين والعاملين في القطاعات القانونية في المؤسسات وتأهيل وإكساب المتدربين المهارات القانونية والعملية والفنية الخاصة بارتباط المعلوماتية والاتصالات بتخصصاتهم ومدى تأثير استخدام تكنولوجيا المعلومات في انجاز مهام أعمالهم والتعريف بماهية التعامل مع الإشكاليات القانونية في حقل المعاملات الالكترونية حول موضوعات تشمل كيفية إثبات الشخصية ، كيفية التوقيع الالكتروني ، أنظمة الدفع النقدي الرقمي ، المال الرقمي أو الالكتروني ، سرية وأمن المعلومات من مخاطر إجرام التقنية العالية ، خصوصية العميل ، المسؤولية عن الأخطاء والمخاطر ، حجية المراسلات الالكترونية ، التعاقدات المصرفية الالكترونية ، مسائل الملكية الفكرية لبرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة

بها ، علاقات وتعاقبات البنك مع الجهات المزودة للتقنية أو المورد لخدماتها أو مع المواقع الحليفة ، مشاريع الاندماج والمشاركة والتعاون المعلوماتي والجريمة الالكترونية وماهية التنظيم القانوني للعالم الافتراضي بأقسامه من المعاملات القانونية الرقمية وعقود التجارة الإلكترونية وحماية الملكية الفكرية عبر الإنترنت والتعريف بأنماط وأشكال الجرائم عبر الإنترنت وماهية الدليل الرقمي وحججته في الإثبات وعرض أحدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم.

ان كان ما أوردته عبارة عن دراسة بحثية صغيرة لكن لا بد أن نعرف ان الجريمة الإلكترونية جريمة ذات أبعاد دولية تخضع لمبدأ تنازع القوانين . هذا بالإضافة الي القصور التشريعي لدي الكثير من الدول للحد من تلك الجرائم هذا ما سطره قلمي فإن كان صواب فمن الله وان كان يعتريه الخطأ فمني ومن الشيطان والله ورسوله منه براء .