الوجيز في
جرائم الإنترنت



تأليف

سهيل محمد العزام

دراسات عليا في القانون

الوجيز في جرائم الإنترنت

المملكة الأردنية الهاشمية
رقم الإيداع لدى دائرة المكتبة الوطنية
(٢٠٠٩/٦/٢٣٦١)

٣٤٣,٠٩٤٤
العزام، سهيل محمد
الوجيز في جرائم الإنترنت/ سهيل محمد العزام.إربد: المؤلف، ٢٠٠٩
( )ص
ر. أ. : (٢٠٠٩/٦/٢٣٦١)
الواصفات: /الجرائم الحاسوبية// الإنترنت/ أمن المعلومات// القرصنة/

*أعدت دائرة المكتبة الوطنية بيانات الفهرسة والتصنيف الأولية
* يتحمل المؤلف كامل المسؤولية القانونية عن محتوى مصنفه ولا يعبر هذا المصنف عن رأي دائرة المكتبة الوطنية أو أي جهة حكومية أخرى

الوجيز في جرائم الإنترنت

تأليف

سهيل محمد العزام

دراسات عليا في القانون

الطبعة الأولى

٢٠٠٩

الفصل الأول
التعريف بالإنترنت واستخداماته

نعرف أولاً الإنترنت وتطور فكرته وتقنياته، ثم نعرض لاستخدامات الإنترنت والفوائد العظيمة والجوانب الإيجابية له وذلك في مبحثين كما يلي[1]:

المبحث الأول: التعريف بالإنترنت.

المبحث الثاني: استخدامات الإنترنت في حياتنا.

المبحث الأول
التعريف بالإنترنت

الإنترنت كفكرة ولدت في وزارة الدفاع الأمريكية، وتم تطبيقه كتجربة داخل الولايات المتحدة بمعرفة الهيئات العلمية المتخصصة عام ١٩٦٩.

وكانت الفكرة في البداية، تقوم على ربط الحواسيب الآلية ببعضها البعض في مراكز البحث، وفي كل منطقة، وفي كل مدينة على حده، إلى أن قامت مؤسسة العلوم القومية "N S F" بشراء حواسيب آلية عملاقة Super computer وتزويد مراكز الحاسب الآلي العملاق بها، ثم توزيعها على كل مناطق الولايات المتحدة الأمريكية حتى تعمل – إقليمياً – مع بعضها البعض في شكل شبكة قومية، وفي كل هذه المراحل

---

(1) أ. د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية مصر، ٢٠٠٧ ص ٢٥- ٣٥.

كانت شبكة الإنترنت مخصصة لأغراض البحث العلمي، وتتعامل مع مراكز البحث ومع الجامعات، وتيسر العلماء الاستفادة من إمكاناتها في القيام بالعمليات الرياضية المعقدة، والتي تعجز الحاسبات الآلية الصغيرة عن القيام بها.

وعندما استقرت الشبكة على مدى أكثر من عشرين عاماً على هذا النمط، ظهرت الحاجة الماسة إلى استخدام نفس الشبكات لأغراض تجارية يستفيد منها الأفراد والمؤسسات والشركات، ورغم عدم ارتياح "NSF" وبعض المشتغلين بالشبكات الرسمية لهذا التطور، إلا أن الشركات استطاعت من خلال نفوذها داخل الحكومة الفيدرالية ودوائر الحكومة الأمريكية أن تفتح المجال للاستخدام التجاري للشبكة محلياً وعالمياً، ولذلك يمكن القول أن الشبكة بدأت بشكل تجاري عام ١٩٩٣.

ولذلك تعرف الإنترنت بأنها – توصيلات تعاونية- لعدد من شبكات الحاسبات الآلية، وهي مكونة من كلمتين هما INTERNET CONNECTION أو NET WORK ، وهذا يعني أن مئات الشبكات المربوطة مع بعضها البعض – مكونة من حواسيب آلية مختلفة وكذلك تكنولوجيا مختلفة – ثم توصيلها ببعضها البعض بطريقة بسيطة وسهلة بحيث تبدو وكأنها قطعة واحدة أو نظام واحد دون إحساس أي من الأطراف بأنه يختلف فنياً عن الخر [١]

---

(١) د/ علي محمد شمو، التكنولوجيا الحديثة والاتصال الدولي والإنترنت، الشركة السعودية للأبحاث والنشر، جدة، بدون تاريخ، ص ٢٣٢ وما بعدها.

فالإنترنت عبارة عن حاسب آلي يتحدث إلى حاسب آلي أخر يرتبطان بواسطة – سلك التليفون العادي، أو أي فرع آخر من الكوابل، وإذا كانت الحواسيب موجودة في أماكن بعيدة ومتفرقة فيمكن استخدام الأقمار الصناعية للربط بينها ليتحقق بذلك الاتصال الدولي عبر الإنترنت، وحتى في داخل الدولة ذاتها تعتمد شبكة الإنترنت على الوصلات الوسيطة بين نقطتين، وهكذا كانت بداية إنترنت في وزارة الدفاع الأمريكية.

والإنترنت لا يملكها أحد، ولا يسيطر عليها أحد، إنما هي ملكية تعاونية للبشرية وللجميع بقدر إسهامهم فيها. وقد كانت خدمات شبكة الإنترنت في البداية مجانية وبغير مقابل، وكانت قاصرة على الاستخدامات العلمية والبحثية، وليس لها الصفة التجارية.

وفي الوقت الحالي تقوم شركات تجارية بإدارة شبكة إنترنت على أسس تجارية، لذلك فمن الضرري أن يدفع المشترك مبلغاً من المال مقابل استخدامه للمعلومات، وكذلك لتطوير الشبكة نفسها والمحافظة على تطورها وتحسين استخدامها، وذلك بالطبع إضافة إلى ما يدفعه المشترك في شبكة المعلومات مقابل استخدامه لبرامجها والاستفادة من المعلومات التي تبيعها للمستهلك مقابل إنتاجها وما بذلك من جهد للحصول عليها مع تحقيق الربح المعقول [1].

([1]) د/ إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت، بحث مقدم لمؤتمر القانون والكومبيوتر والإنترنت، جامعة الإمارات في الفترة من ١٣ مايو ٢٠٠٠ ك، ص٣.

وشبكة الإنترنت أو كما يطلق عليها الشبكة العالمية الإلكترونية أو شبكة الشبكات أو الشبكة العنكبوتية، تقدم للفرد والمجتمع كل ما تقدمه وسائل المعرفة السابقة مجتمعة، بل وتقدم – وذلك هو الأهم – المعلومات التي قد تمنعها السلطة ممثلة في الدولة أو الدين أو العلم أو الرقيب المتمثل في المدرسة أو المعلم أو الوالدين، كما تقدم هذه الشبكة معلومات لنا، لم تكن لتصلنا بسبب عوامل جغرافية أو سياسية أو اجتماعية.

كذلك قد يعجب الكثيرون حينما يعلمون أنه لا توجد إدارة مركزية للإنترنت، وهي شبكة وصفها البعض بأنها فوضي تعاونية، ذلك أن كل شبكة مشتركة في الإنترنت لها قواعدها الخاصة والهيكل التنظيمي لإدارتها، ولكن لا يمكن الاتصال بين الشبكات إلا إذا كان هناك تعاون بينهما، ولذلك تجد أن هناك الكثير من اللجان ومجموعات العمل، التي تمثل فيها كل شركات المعلومات، وهي في اجتماعات مستمرة من أجل الوصول إلى وضع الأسس والضمانات التي تكفل تحسين الأداء في الشبكة العالمة وتطوير أسلوب التشغيل والاتفاق على المصطلحات والمستجدات التكنولوجية التي تطرأ من حيث لآخر.

ومن المشكلات القانونية التي تثيرها شبكة الإنترنت، هي القانون الواجب التطبيق في شأن جرائم الإنترنت، وجوهر المشكلة أن الجريمة عبر الشبكة لا تعرف الحدود الجغرافية فالجاني قد يكون في دولة أوروبية ومحل الجريمة في آسيا أو في دولة أفريقية كما في حالة اختراق الشبكات بقصد التجسس المعلوماتي أو التجسس الذي يهدد الأمن القومي أو سرقة النقود

بطريق الإنترنت، كما أن بعض هذه الأفعال قد يكون مجرماً في بلد الجاني دون بلاد أخرى ومنها الدولة التي وقعت فيها الجريمة أو العكس، ولذلك فجرائم الإنترنت بصفة عامة تتطلب التعاون الدولي لمكافحتها.

والسؤال: هل للإنترنت أثر إيجابي في حياة البشرية؟ هذا ما نبحثه حالاً.

المبحث الثاني
استخدامات الإنترنت

تقدم شبكة الإنترنت خدمات جليلة لكل المستخدمين يمكن إجمالها في الآتي:

١- البريد الإليكتروني مع كل أنحاء العالم.

٢- الحصول على الرسائل العلمية والكتب والمعلومات الخاصة بالعلوم وملخصاتها، والتي قد لا تتوافر في المكتبات العامة.

٣- مشاهدة الأحداث العالمية فور وقوعاً وتفاصيلها بصورة أفضل من تلك التي تبث عبر الإذاعة والتلفزيون والصحف.

٤- مشاهدة الأفلام والأحداث الرياضية والعلمية والثقافية.

٥- قراءة الصحف اليومية والمجلات الأسبوعية.

٦- التعاقد على شراء السلع بصورة فورية عبر الشبكة والتجارة الإلكترونية.

٧- متابعة أسواق الأموال والأسهم والسندات.

٨- إنشاء نوادي صحافة من خلال الشبكة.

٩- نشر ثقافات الشعوب والدول على نحو يزيل الخطأ واللبس الثابت عن بعض الشعوب والطوائف والأديان.

١٠- نشر التراث والآداب والفنون والآثار.

١١- الدعاية التجارية والسياحية.

١٢- نقل التكنولوجيا من دولة إلى أخرى.

١٣- اتباع سياسة التعليم عن بعد.

١٤- الرد على المعلومات الخاطئة التي وجدت طريقها إلى الشبكة

١٥- الاستفادة من بعض التصميمات الهندسية في العمارة والصناعة.

١٦- أية معلومات أخرى مفيدة قد يعبر عليها الإنسان حال تصفحه لشبكة الإنترنت.

ونعرض بصورة موجزة لبعض الاستخدامات الشائعة لشبكة الإنترنت كما يلي:

أولا: البريد الإلكتروني:

والبريد الإليكتروني عبارة عن رسالة عادية – لكن بطريقة إليكترونية – يكتبها شخص، بطريقة عادية جداً على جهاز الحاسب الآلي الخاص به، وذلك بعد أن يفتح الصفحة الخاصة ببريده الإليكتروني، والتي لها رقم

سري، واسم المستخدم، ولا يمكن لغيره الدخول إليه، وبعد أن يتم الكتابة يقوم بالضغط على أمر معين في الصفحة وهو (Send) أي أرسل وفي حالة نجاح وصول الرسالة للعنوان المطلوب على جهاز حاسب آلي آخر يظهر له علامة (OK.) بما يفيد تمام إرسال الرسالة. وإذا كان هناك خطأ ما في إرسالها يظهر للمرسل، رسالة موجزة، تشير إلى موضوع الخطأ ويتولى هو تصحيحه ثم يعيد إرسالها مرة أخرى.

وهذه الرسالة يستوي أن ترسل إلى شخص مقيم في ذات المدينة أو الدولة أو دولة أخرى وفي لحظات معدودة، وتتوافر فيها عوامل الأمان والسرية ولا يمكن اختراق البريد الإلكتروني لشخص إلا بمعرفة كلمة السر الخاصة به، أو بناء على طرق فنية معقدة لا يجيدها سوى جهابذة المخترقين لشبكات الحاسب الآلي، ولذلك فهو وسيلة آمنة وسريعة ورخيصة التكلفة مقارنة بغيرها من وسائل التراسل.

ويلحق بوظيفة – البريد الإلكتروني – لدى الإنترنت ما يسمى بالقوائم البريدية، ويقصد بالقائمة البريدية Mailing list نظام إدارة وتصميم الرسائل والوثائق على مجموعة من الأشخاص المشتركين في القائمة، عبر البريد الإلكتروني، وتغطي القوائم مواضيع ومجالات شتى، وتتناول كل قائمة عادة، موضوعاً محدداً، فإذا كنت تريد متابعة آخر أخبار السباحة – مثلاً – يمكنك الاشتراك بإحدى القوائم المتخصصة في هذه الرياضة، وتصلك تباعاً النشرات الخاصة بها، كذلك لو كنت مغرماً

بالحيوانات أو بقضايا الثقافة أو الفنون أو الآداب فكل منها له القائمة الخاصة به، وهي مجانية ونادراً ما تجد قائمة تفرض بعض الرسوم .

وحتى يمكن لمستخدم الإنترنت الاشتراك في إحدى قوائم البريد الإلكيترونين فلابد أن يكون له صفحة وموقع في البريد الإلكتروني ذاته حتى تتم مراسلته على ذلك العنوان.

والقوائم البريدية نوعان أحدهم القوائم ذات الاتجاه الواحد والأخرى ذات الاتجاهين، وفي القائمة ذات الاتجاه الواحد يقتصر دور المستخدم على تلقي الرسائل والصادرة من مدير القائمة من خلال البريد الإليكتروني ولا يمكن للمستخدم تصميم وثيقة أو رسالة على بقية المشتركين في القائمة، بل حتى لا يمكن معرفة اسم مشترك آخر أو عنوان البريد الإلكتروني الخاص به.

أما في القوائم ذات الاتجاهين، فغن كل رسالة أو وثيقة يرسلها أحد المشتركين إلى العنوان الخاص بالقائمة إلى كافة المشتركين الآخرين، وذلك بالإضافة إلى الرسائل التي تصدر عن مدير القائمة ذاته .

ثانيا: مقاهي الإنترنت:

هي ليست مقاهي بالمعنى الحرفي لكلمة – مقهى – لكنها مشروعات تجارية – تعتمد الإنترنت كوسيلة وهدف – وتهدف إلى الربح، تجمع بين خدمة المقهى التقليدي حيث يمكن الحصول على مشروب، وخدمة الإبحار في شبكة الإنترنت.

ولمقاهي الإنترنت وجوهاً إيجابية عديدة منها أنها تسهم في نشر الوعي بمنافع شبكة الإنترنت، وتساعد في الحصول على المعلومات المتوفرة في مئات الألوف من مواقع الشبكة والمتاحة لمستخدمي الشبكة، كما أنها تقوم بدور المنفق لتجربة – الاتصال بشبكة الإنترنت – قبل الاشتراك فيها من قبل المستخدم أو الباحث – الموسمي – أو ذو الاهتمام المحدود.

وتنتشر مقاهي الإنترنت يوماً بعد يوم، ويؤمها العديد من العاملين في قطاع تكنولوجيا المعلومات، وأصدقاؤهم للاستراحة والحوار، كما في أي مقهى تقليدي، لكن مع خلاف بسيط، وهو أن هؤلاء الأصدقاء على مقربة من الكومبيوتر والذي يعطي هؤلاء الإحساس بقدراتهم على تملك المعلومات متى أرادوا، وإمكانية الوصول إليها بسهولة.

كذلك فقد أصبحت هذه المقاهي منتدى يرتاده الطلبة والشباب للتسلية واختيار البرامج الجديدة، والتي لم تصل للأسواق وتوزع تجارياً بعد، حيث تتنوع الوفود القارئة لهذه المقاهي، وكلهم من المهتمين والمتطلعين لن يكونوا من جيل الإنترنت، وكذلك الباحثين الأمر الذي حول هذه المقاهي إلى أبحاث ومراكز تعليمية للتدريب على إنترنت واستخداماتها.

ثالثا: منتديات الحوار والدردشة على شبكة إنترنت:

تشغل – الدردشة – عبر إنترنت مساحة كبيرة من حزمة البيانات التي يتم تبادلها بين مستخدمي هذه الشبكة العالمية، بل إن كثيراً من المستخدمين لا يرون في إنترنت إلا وسيلة للوصول إلى الآخرين، عن طريق وسائل

الاتصال العديدة التي توفرها مثل البريد الإلكتروني والمنتديات وبرامج التراسل الفوري ومواقع الدردشة، وعلى الرغم من أن الأخيرة وسيلة اتصال إلا أنها الدافع الرئيسي لأكثر من ٢٥٪ من المستخدمين لهذه الشبكة.

ومن مزايا الدردشة عبر الإنترنت، أنها نوع من الاتصال بين الناس، يقتصر على تبادل النصوص بين المتحاورين، ولذلك فهو نوع من الحوار الفكري البحت، بعيداً عن أية مؤثرات أخرى كالعرق أو الجنسية أو اللون أو الصوت، ويرى كثيرون أن هذا التواصل بين الناس – عبر غرف الدردشة – سيغير طريقة اتصال الناس مع بعضها البعض في دول العالم المختلفة حيث – يسمح بالتبادل الفكري الذي بدوره سيؤدي لتطور الفكر البشري بصورة أسرع عما قبل.

وهناك نظم كثيرة للدردشة من خلال شبكة إنترنت، لكن هناك نظام يسمى – بدالة إنترنت للدردشة internet relay chat ، ويعبر عن اختصاره بـ (I R C) وقد ابتكره الفنلندي – جاركو أبويكارين – عام ١٩٨٨، لكنه لم ينطلق إلا إبان حرب الخليج الثانية عام ١٩٩١.

وبالإضافة لنظام الدردشة على شبكة الإنترنت، هناك منتديات الحوار عن طريق المجموعات الإخبارية، وهي منتشرة في الوقت الحاضر من خلال المنتديات والمساحات الإليكترونية العربية، وهي توفر منبراص حراً للحوار، الأمر الذي يجعلها تجذب الرواد يوماً بعد يوم، وتجد فيها الأفكار

الغثة والأخرى الثمينة وتجد كذلك الرؤى السياسية والثقافية والدينية والأدبية والتي تمثل كل التيارات.

وقد تسللت بعض العبارات غير المهذبة في الآونة الأخيرة إلى منتديات الحوار المذكورة، ووجد العاملون أنفسهم – فجأة في وضع محرج – فأما أن يضعوا رقابة على ما يكتب في المنتدى ويحذفون ما لا يعجبهم منه، ومن ثم يفقد المنتدى سحره وجابيته، أو يتركوه حراً ويتقبلون النقد والاتهامات التي ستوجه إلى هذه المنتديات .

رابعا: كشف الجرائم وتعقب المجرمين والقبض عليهم:

في مبادرة جريئة للشرطة البريطانية أنشأت وحدة بوليسية تسمي- الوحدة الوطنية لمكافحة جرائم التكنولوجيا المتطورة – وهذه الوحدة هدفها تعقب مرتكب جرائم عبر الإنترنت، وقد اعترض عليها من قبل جماعات الدفاع عن الحقوق المدنية، لكن يبقى أثرها كتطبيق هام لاستخدامات الإنترنت الإيجابية [1].

وتأتي هذه المبادرة وغيرها في ظل نقاش بين المختصين موضوعه مدى جدوى الأساليب العلمية والإليكترونية الجديدة، ومنها الإنترنت في رفع الكفاءة اللازمة لمواجهة الجريمة. لكن ينبغي العلم كذلك أن التقدم التكنولوجي سوف يفتح أمام المجرمين مجالات جديدة للجريمة، فعمليات السرقة والاحتيال في الوقت الحالي تتم بطريق الإنترنت، وهي في تنامي

---

(1) د. عبد الفتاح بيومي حجازي مصدر سابق ص ٣٦، ٣٩.

وتطور مستمر على نحو يزيد صعوبة ملاحقة مرتكبي هذه الجريمة، ومع ذلك فإن مواجهة جرائم الإنترنت بأسلوب علمي يتعين أن يأخذ نصيبه في تطبيقات الإنترنت.

وقد أمكن بالفعل عن طريق الإنترنت القبض على من المتهمين – في بريطانيا – أثاروا شغباً، ووضعت صورهم على شبكة الإنترنت، وطلب من المواطنين مساعدة الشرطة في التعرف عليهم، وتلفت الشرطة بلاغات في شأن المشتبه فيهم، وأمكن عن طريق هذه البلاغات القبض على هؤلاء المتهمين.

وفي الولايات المتحدة الأمريكية، تمكن رجل من مساعدة الشرطة بطريق الإنترنت في القبض على أحد الأشخاص الذي اختطف زوجته واغتضبها، حيث حصل على مواصفات ذلك الشخص الذي اختطف زوجته واغتصبها، حيث حصل على مواصفات ذلك الشخص من زوجته، ودخل في حوارات عن طريق – غرف الدردشة – مع أشخاص لهم ذات الاهتمامات إلى أن اشتبه في أحدهم واستدرجه بالحديث واعترف الأخير بالواقعة على سبيل الدردشة، حيث قدمت التسجيلات للشرطة وبعد ذلك تم القبض عليه ومحاكمته.

وفي مصر كان هناك تعبير شائع يعرفه رجال البحث الجنائي وهو – الكعب الدائر – وهو عبارة عن رحلة عذاب إجبارية يقوم بها المذنبون بعد قضاء مدة العقوبة، وذلك لزيارة كل مديريات الأمن وأقسام الشرطة لمعرفة ما إن كان عليهم أحكاماً أم لا، ولكن في الوقت الحالي يتم التسجيل

الجنائي بطريق الحاسب الآلي في وزارة الداخلية، ويتم الكشف عن هذه السوابق في ثوان معدودة من أي حاسب آلي مرتبط بشبكة وزارة الداخلية، ويتم التسجيل بالصوت والصورة، ولذلك لا تنطلي محاولات تغيير ملامح الجاني على الحاسب الآلي، لأنه يكفي الحصول على بصمة العين أو الصوت حتى يتم حسم الموقف [1].

ويلاحظ لمستخدمي الإنترنت أن هناك نداءات توجهها بعض قنوات المعلومات أحياناً للمساعدة في القبض على المجرمين الذي يطلبهم البوليس الدولي Interpol، كما يمكن الإبلاغ عن الأشخاص بطريق الحاسب الآلي دون الانتقال إلى قسم الشرطة طالما أن الرقم الكودي للحاسب الآلي الذي صدر عنه البلاغ موجود على شبكة الإنترنت .

خامسا: المساعدة في كشف سرقة الأبحاث العلمية:

في الماضي القريب جداً استعان طلبة الجامعات والباحثون بشبكة الإنترنت لشراء وبيع وتوزيع ونسخ أوراق الأبحاث العلمية المطلوبة، وفي الوقت الحالي يستخدم أساتذة الجامعة، مواقع الشبكة للبحث عن الأوراق العلمية المسروقة، ويستخدم أعضاء هيئة التدريس في الكليات، مواقع الويب المخصصة للندوات والبريد الإلكتروني ومنتديات النقاش والمكتبات للحصول على ملاحظات تتعلق بوسائل اكتشاف عليمات غش الطلبة وسرقة الأبحاث العلمية، وهناك ملاحظة هامة بالنسبة للبحث عن الأبحاث العلمية – باللغة العربية – والتي تمت سرقتها، وذلك لأن ترجمة

(1) د. جميل عبد الباقي، الإنترنت والقانون الجنائي، مرجع سابق، ص ٢٤.

الورقة من الإنجليزية إلى العربية يجعل البحث عن الورقة الأصلية في إنترنت عملية معقدة واستهلاكاً للوقت، ويفضل أن تنطلق عملية البحث عن الغش من خلال المصطلحات الإنجليزية الواردة ضمن الورثيقة أو من جمل قصيرة .

وباختصار يمكن القول أن الأبحاث العلمية المسروقة حتى ولو من فترة زمنية طويلة يمكن اكتشاف سرقتها طالما أنه قد تم توثيقها في أي موقع على شبكة الإنترنت.

سادسا: العمليات الجراحية والفحص الطبي بطريقة الإنترنت:

يمكن للمرضى الحصول على الخدمة الطبية من خلال شبكة الإنترنت، فقد أنشأت الحكومة البريطانية موقعاً، يمكن للمرضى من خلاله الاتصال بممرضين ووصف الأعراض المرضية لهؤلاء الذين يمكنهم أن يقرروا ما لئن كانت الحالة المرضية بسيطة وسوف تشفى ذاتياً أم يتطلب الأمر عناية طبية خاصة، ورغم تحفظ البعض على هذه الخدمة، بدعوى أنها قد تمد المريض بمعلومات خاطئة، إلا أنها وسيلة ناجحة سيماً في حالات الطوارئ .

كذلك فقد يستعين الجراحون بشبكة الإنترنت عند إجراء العمليات الجراحية الدقيقة، وذلك عن طريق تصويرها بكاميرات فيديو لعرضها في ذات اللحظة على فريق من الأطباء في مختلف أنحاء العالم لأخذ رأيهم العلمي أثناء العملية الجراحية .

سابعا: التجارة الإلكترونية:

الإنترنت وسيةل من وسائل التجارة الإليكترونية، وهو ليس كل الوسائل الإليكترونية العديدة والمتاحة كالتليفون والفاكس والتلكس وغيره من سبل الاتصال بين المتعاقدين في نطاق البيع والشراء وغيرها من نظم تبادل السلع والخدمات، لكن الإنترنت أهم هذه الوسائل بالصوت والصورة رغم تباعدهما آلاف الأميال، والاتفاق على التفصيلات الدقيقة، بعد إبداء الإيجاب ثم القبول بطريق الإنترنت ثم إبرام العقد، والتوقيع عليه بطريق – التوقيع الإلكتروني – دون حاجة لاجتماع المتعاقدين في مكان واحد، ويتم إبرام العقد بالطبع، بعد أن يكون البائع أو المورد أو مقدم الخدمة قد أعلن عنها بطريقة واضحة وكافية على شبكة الإنترنت، وأن يكون الطرف الآخر قد اطلع على هذا الإعلان وحصل على الإيضاحات والتفسيرات المطلوبة بشأن السلعة أو الخدمة المعروضة، وكل هذه مراحل سابقة لإبرام العقد، ويمكن للمشتري أو المستورد أن يسدد قيمة بضاعته عن طريق الدفع – بواسطة شبكة الإنترنت – ويكفيه في ذلك رقم حسابه البنكي ورقم بطاقة الائتمان الخاصة به [1].

وبالطبع فإن التجارية الإلكترونية بطريق الإنترنت لا تخلو من مخاطر تتمثل في إمكانية سرقة الأموال أو البيانات المتداولة فيها بطريق الإنترنت،

---

(1) ر اجع في ذلك مؤلف: "النظام القانوني لحماية التجارة الإلكترونية" في مجلدين – الكتاب الأول: "نظام التجارة الإليكترونية وحمايتها مدنياً" – دار الفكر الجامعي، الإسكندرية، عام ٢٠٠٢، ص ٥ وما بعدها، ط أولى، الكتاب الثاني: الحماية لنظام التجارية الإليكترونية – دار الفكر الجامعي – الإسكندرية، عام ٢٠٠٢، ط أولى، ص١ وما بعدها – وطبعة ثانية لدى دار الكتب القانونية – ٢٠٠٧.

ومع ذلك فإن التشريعات المقارنة تسعى لتجريم هذه الأفعال حفاظاً على نمو وازدهار التجارة الإليكترونية بطريق الإنترنت .

أخيراً يلاحظ أن المظاهر الإيجابية لاستخدام الإنترنت عديدة ومتنوعة وتنمو يوماً بعد يوم في مجال التجارة أو الإدارة والأعمال، كذلك التعليم والصحة والطب على نحو أدى لظهور ما يسمى – بالحكومة الإلكترونية – . ومع ذلك فإن استعمال شبكة الإنترنت وإن كان لا يمكن التخلف عنه، إلا أن هناك خبرات ضارة، ومظاهر غير صحية قد يستمدها الأطفال والأحداث والمراهقين من هذه الشبكة العالمية، وهو ما نعرض له في الباب الأخير من هذا المؤلف .

الفصل الثاني
جرائم الإنترنت

تمهيد وتقسيم:

منذ قديم الأزل والجريمة جزء لا يتجزأ من سلوك الإنسان في المجتمع، حيث ندرة الموارد وحاجة هذا الأخير وأطماعه التي ليس لها حدود، تجعل من تضارب المصالح والتناحر عليها سمة يتميز بها كل مجتمع بصرف النظر عن درجة ثقافته وتقدمه الاقتصادي والعلمي. وعلى الرغم من الجهود الحثيثة التي تبذلها كل دولة لمقاومة الظاهرة الإجرامية، إلا أن الإحصائيات تشير دوماً إلى زيادة نسبة الإجراءم في الغالبية العظمى من دول العالم، وخصوصاً في القرن الأخير، الذي شهد ثورة معلوماتية من نمط مميز، وما أفرزته تلك الأخيرة من جرائم مستحدثة [1] لم يسبق أن عرفها العالم، تتميز عن تلك التقليدية بحداثتها من حيث الأساليب والأدوات المستعملة في تنفيذها وكذا في أسلوب ذلك التنفيذ [2].

---

(1) يقصد بالجرائم المستحدثة: أنماط من الجرائم التي لم يألفها المجتمع في السابق، من حيث أسلوب ارتكابها ونوع الجناة فيها وحجمها. أو هي الجرائم المخطط لها والتي يستعين المجرمون عند تنفيذها بمعطيات العلم الحديث، مثل: جرائم الإرهاب والمخدرات وجرائم الحاسب الآلي والإنترنت. أو هي تلك الجرائم التي يشترط لاستخدامها التقنية الحديثة من أجل تسهيل تنفيذها وإخفاء معالمها. اللواء. د/ محمد الأمين البشري: التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، ٢٠٠٤، ص ٨- ٩.

ومن هذه الجرائم المستحدثة جرائم التقنية العالية [1]، خاصة تلك المرتبطة بالإنترنت. والجريمة بالمفهوم الاجتماعي هي كل فعل أو امتناع يتعارض مع القيم والأفكار التي استقرت في كيان الجماعة [2].

أما قانوناً فهي سلوك إنساني غير مشروع صادر عن إرادة إجرامية، يفرض له القانون جزاءً جنائياً [3].

ويشترط لقيام الجريمة قانوناً ركنان:

ركن مادي: يتمثل في سلوك إرادي يترتب عنه نتيجة إجرامية وتربط بينهما رابطة سببية مادية.

وركن معنوي: يتمثل في الحالة النفسية التي أتى بها الجاني ذلك الفعل المكون للجريمة.

ولما كانت جرائم الإنترنت والتي هي محور دراستنا في هذا المبحث من الجرائم المستحدثة فقد جعلت رجال القانون يتساءلون عن طبيعتها وصفاتها ووسائل مكافحتها. أي أنها طرحت إشكالات قانونية جمة منها: ١- ماهية هذه الجرائم وما الفرق بينها وبين ما يلتبس بها من

---

(١) تضم الجرائم المستحدثة: الجريمة المنظمة، وجرائم التقنية العالية، وجرائم الإرهاب وجرائم غسل الأموال، وحوادث الطيران المدني.
وتعتبر جرائم التقنية العالية High – Technology Crimes نتائج طبيعية لبيئة التقنية العالية - High Technology Environment التي يعيش فيها، والذي يشكل الحاسب الآلي أساسها. أنظر اللواء. د/ محمد الأمين البشري، المرجع السابق، ص٤ وص ٨٥.

(٢) نبيلة هبة هدوال، الجوانب الإجرائية في مرحلة جمع الاستدلالات، دار الفكر إلى ص الاسكندرية ٢٠٠٦ ص ٢١- ٢٦.

مصطلحات؟ ٢- وما هي أنواعها؟ .. وكان لزاماً علينا التطرق إلى الإجابة عن هذه الأسئلة، لعلها تكون طريقاً لفهم هذا النوع من الجرائم، وذلك في المطلبين التاليين:

المطلب الأول: ماهية جرائم الإنترنت.

المطلب الثاني: أنواع جرائم الإنترنت.

المطلب الأول
ماهية جرائم الإنترنت

- إذا كانت الثورة المعلوماتية التي شهدها العالم في الألفية الأخيرة قد ساهمت في تسهيل الحياة البشرية وتطورها في جميع المجالات وخصوصاً مع ظهور الإنترنت، الطريق السريع للمعلومات، وما يقدمه من خدمات عديدة، وما يتميز به من سهولة الاستخدام من الكافة ومن العالمية، أي عدم اعترافه بوجود الحدود الجغرافية والسياسية، إلا أنه لسوء حظه لم ينج من يد المجرمين، خاصة من هؤلاء الذين يمتلكون أدوات المعرفة، إذ أصبح يشكل أداة لارتكاب جرائمهم أو محلاً لها، وهذا ما أدى إلى ظهور نوع مميز وجديد من أنواع الإجرام المهدد لمصالح المجتمعات والدول سواء المتقدمة منها أم النامية، وسواءً على المستوى الوطني أم الدولي.

ولما كان هذا الأخير من المواضيع الحديثة والخطيرة التي تشغل اهتمامات رجال القانون مشرعين أم قضاة أم رجال ضبط، وتجعلهم في أحيان كثيرة عاجزين عن مواجهتها وفهم طبيعتها، كان من الواجب علينا

أن نخصص هذا المطلب لإزالة الغموض الذي ينتابهم وللإجابة عن الأسئلة التي تشغلهم، وذلك من خلال التطرق إلى بعض النقاط الجوهرية التي يمكن حصرها فيما يلي:

١- تعريف جرائم الإنترنت.

٢- خصائصها.

٣. أركانها.

٤- الفرق بينها وبين جريمة الحاسوب.

الفرع الأول: تعريف جرائم الإنترنت

- لتعريف الجريمة وتحديد أركانها وخصائصها أهمية خاصة بالنسبة للمحققين ورجال الضبط الذين يسعون دائماً لإثبات أركان وعناصر الجريمة حسبما يحددها القانون، وإلى إيجاد العلاقة بين تلك الأركان والشخص المتهم بتنفيذها.

ولما كانت جرائم الإنترنت من جرائم التقنية العالية، أي من الجرائم المستحدثة، وكانت التشريعات العقابية قاصرة عن تناولها ' فإن كثيراً من المحققين ورجال الضبط في كثير من الدول يواجهون صعوبات أثناء التصدي لتلك الجرائم. فما المقصود بجرائم الإنترنت؟

أولا: التعريفات الفقهية لجرائم الإنترنت: تعد مسألة تعريف جرائم الإنترنت من المسائل الشائكة التي تقف كحجر عائق أمام رجال القانون، إذ أنه وحتى الان يصعب وضع تعريف عام وشامل له.

ولكن وبالرغم من ذلك حاول البعض تحديد المقصود من تلك الجرائم، فالبعض من الفقه عرفها بأنها: "هي كل الجرائم التي ترتكب بالاستخدام غير المشروع أو الاحتيالي للشبكات المعلوماتية وهي تضم:

- المساس بنظم المعلوماتية أو المعطيات المعلوماتية.
- إرسال حثالة البريد الإلكتروني .(Spam)
- الاعتداء على حرمة الحياة الخاصة والمعطيات الشخصية.
- الاحتمال باستخدام بطاقة الائتمان.
- العنصرية أو النازية أو التصرفات المعادية.
- تبييض الأموال.
- تنظيم مواقع للاستغلال الجنسي للأطفال ومواقع الدعارة وكذا مواقع الإرهاب"

والبعض الآخر يعرفها بأنها: "مجموعة الجرائم الجنائية التي ترتكب عبر شبكة الإنترنت" أو بأنها: "مجموعة الجرائم الجنائية التي تركتب عبر شبكة الإنترنت والتي تمثل ثلاثة أنواع مختلفة من الجرائم هي: ١- جرائم المحتوى، ٢- المساس بالملكية الفكرية، ٣- الجرائم المعلوماتية"، "كما تعرف بأنها: "تلك الأعمال غير المشروعة التي تكون شبكة الإنترنت، أو أحد تطبيقاتها إما وسيلة لها أو ضحية مستهدفة من قبل الفاعل أو الفاعلين"، أو بأنها: "مجموعة الأفعال والأعمال غير القانونية والتي تتم عبر شبكة الإنرتنت أو تبث عبر محتوياتها"، أو بأنها: "جميع الأفعال

المخالفة للقانون والشريعة والتي تبث ترتكب بواسطة الحاسب الآلي من خلال شبكة الإنترنت"، أو: "كل ما يمكن ارتكابه من أفعال غير مشروعة يعترف قانون الإنترنت بكونها جرائم"، أو بأنها: "تلك الجرائم التي لا تعرف الحدود الجغرافية Crime transborder والتي يتم ارتكابها بأداة هي الحاسب الآلي Computer عن طريق شبكة الإنترنت، وبواسطة شخص على دراية فائقة بهما" [1]، أو بأنها: "كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها"، أو هي: "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب. وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في البيئة الإليكترونية"، أو هي: جميع الأفعال المخالفة للشريعة الإسلامية، وأنظمة المملكة العربية السعودية المرتكبة بواسطة الحاسب الآلي من خلال شبكة الإنترنت ويشمل ذلك: الجرائم الجنسية والممارسات غير الأخلاقية وجرائم الاختراقات والجرائم المالية وجرائم إنشاء أو ارتياد المواقع المعادية وجرائم القرصنة".

ثانيا: النقد الموجه للتعريفات الفقهية السابقة:

وبعد استعراضنا التي قيلت في جرائم الإنترنت، فإنه وكما سبق ذكره في البداية لا يوجد أي من تلك التعريفات التي حددت المقصود من هذه الجرائم بصورة جامعة مانعة، لكونها متقاربة من بعضها البعض، واقتصرت على اعتبار تلك الجرائم قائمة في حالة واحدة، هي الحالة التي

---

(1) نبيلة هبة هدوال مصدر سابق ص ٢٧- ٣٢.

تستخدم فيها الإنترنت كوسيلة لارتكاب الجريمة، متناسية في ذلك أنها من الممكن أن تكون محلاً لتلك الأفعال غير المشروعة، كما هو الشأن في حالة إرسال القنبلة المعلوماتية (Bombe informatique).

هذا من جهة، ومن جهة أخرى نجد أن من تلك التعريفات من قصرها على الأفعال المخالفة للشريعة الإسلامية ولأنظمة دولة معينة. في حين كان من اللازم عليها عدم حصرها في تلك الأفعال، وذلك لكون جرائم الإنترنت ظاهرة عالمية تعاني منها جميع الدول العربية والأجنبية، المتقدمة والنامية. فهي كما سنرى، جريمة يمكن أن تكون وطنية كما يمكن أن تكون دولية.

هذا من ناحية، ومن ناحية ثانية فإننا نعرف أن الدول المتقدمة أو بالأحرى الدول الأجنبية تعترف بالقانون الوضعي في تنظيم وتسيير أمورها، ولا تعترف بالشريعة الإسلامية كمصدر من مصادر القانون. ولذلك كان من الواجب عدم حصرها في الجرائم المخالفة للشريعة الإسلامية.

أما بالنسبة للتعريف الذي تبناه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، فبالرغم من كونه من أفضل التعريفات التي تناولت ظاهرة الإجرام المعلوماتي بصورة عامة، إلا أنه لم يعرف جرائم الإنترنت فقط، فقد اشتمل على جرائم الحاسب الآلي وكذا الجرائم التي ترتكب عبر الشبكات سواء المحلية أم الممتدة كالإنترنت.

هذا من جهة، ومن جهة أخرى نجد أن التعريف الذي اعتبر جرائم الإنترنت هي: "كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها"، قد تضمن مصطلح "نظم الحاسب الآلي" والذي يضم كما سبق ذكره في الهامش مكونات الحاسب الآلي وشبكاته المحلية او الممتدة وكذا الأشخاص الذين تتحقق من خلالهم تلك الوظيفة.

ولذلك كان من الواجب وكما هو متفق عليه في لغة القانون استخدام مصطلحات دقيقة تعبر عن تلك الجرائم، والاقتصار على عبارة نظم الحاسب الآلي بما أنها تضم الشبكات.

ولهذا نرى أنه يمكننا تعريف جرائم الإنترنت بأنها: "تلك الجرائم العابرة للحدود والتي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص على دراية فائقة بها".

ثالثا: نشأة وظهور جرائم الإنترنت:

ولقد ظهرت جرائم الإنترنت في حقل جرائم التقنية العالية في نهاية الثمانينيات، وكان ذلك من خلال جرائم العدوان الفيروسي وبالأخص جريمة دودة موريس المؤرخة واقعتها في نوفمبر ١٩٨٨.

ولقد أطلق مصطلح جرائم الإنترنت في مؤتمر جرائم الإنترنت المنعقد في أستراليا في الفترة من ١٦- ١٧/ ٢/ ١٩٩٨[1].

---

(1) ويقابل هذا المصطلح في اللغة الإنجليزية: Cyber crime . أو Internet crime. وفي اللغة الفرنسية Cybercriminalite أو Cyberdelinquance أو La criminalite informatique sur I, Internet.

وتجدر الإشارة إلى أن الكثير من الباحثين يستخدمون مصطلحات غير دقيقة للتعبير عن جرائم الإنترنت. إذ نجد البعض يستخدم مصطلح "الإجرام المعلوماتي" (La criminalite informatique)، أو يستخدم مصطلح "جرائم التكنولوجيا المتقدمة" (La criminalite de haute technologie)، أو مصطلح "الغش المعلوماتي". في حين أنه يجب استخدام المصطلح الدقيق والمتماشي مع طبيعة تلك الجرائم وهو "جرائم الإنترنت". ذلك لأن "الإجرام المعلوماتي" وإن كان يقصد التعبير عن الجرائم الواقعة عن طريق جهاز الكمبيوتر، إلا أن هذا لا يعني من جهة أخرى أن الاعتداء على المعلومة يتحقق دائماً باستخدام الكمبيوتر وخصوصاً باستخدام الإنترنت، ذلك لأن الوسائل التقليدية هي دائماً ما تكون أداة لارتكاب تلك الجريمة، وبالتالي فالجريمة المعلوماتية قد تكون أشمل من جرائم الإنترنت وذات الشأن بالنسبة "للغش المعلوماتي" وكذا "جرائم التكنولوجيا المتقدمة".

ولقد لاحظ مؤتمر القانون والإنترنت المنعقد في لشبونة/ البرتغال في ٢٦/ ١/ ٢٠٠١ أنه يجب عدم الالتفات إلى مثل هذه المصطلحات غير الدقيقة، واعتماد مصطلح "Cyber crime" دون غيره للتعبير عن جرائم الإنترنت،مع الأخذ بالاعتبار التمييز بين الجرائم التي يمكن ارتكابها عبر الإنترنت وتلك التي لا يمكن ارتكابها عبر تلك الأخيرة.

رابعا: الدراسات التي أجريت حول جرائم الإنترنت:

وبالرغم من أن هذه الظاهرة حديثة، إلا أنها اجتاحت العالم بأكمله وأصبحت تهدد مصالح دوله في جميع المجالات الاقتصادية والاجتماعية، وهذا ما أثبتته بعض الإحصائيات والدراسات.

ففي أحدث التقارير السنوية لمركز شكاوي احتيال الإنترنت (IFFC) الأمريكي، أظهر التحليل الشامل الشكاوي التي قدمت للمركز، أن عدد الشكاوي التي تلقاها ذلك الأخير قد تضاعفت سنة ٢٠٠٢، لتصل إلى ٤٨٢٥٢ شكوى مقارنة بتلك التي سجلت سنة ٢٠٠١، وقد بلغت الخسائر المتصلة بتلك الجرائم ٥٤ مليون دولار على غرار سنة ٢٠٠١ حيث بلغت ١٧ مليون دولار وسنة ٢٠٠٠ ٤،٦ مليون دولار.

وتجدر الإشارة إلى أن هذه الحالات التي تم الإبلاغ عنها وأن كانت تتعلق فقط بجريمة الاحتيال عبر الإنترنت والتي هي واحدة من أنماط جرائم الإنترنت، إلا أنها لا تعكس الأرقام الحقيقية لذلك الهاجس الذي يؤرق دول العالم، إذ أن الكثير من تلك الجرائم ترتكب وتظل في طي الكتمان، وهذا ما يعبر عنه علماء الإجرام "بالرقم الأسود" أو "الرقم المخفي" "Le chiffre noire".

وإلى جانب ذلك فقد أجريت عدة دراسات عن هذا النمط الحديث من الجرائم منها، تلك الدراسة التي أجرتها منظمة Software Alliance Business في الشرق الأوسط، والتي تبين من خلالها وجود تباين بين دول تلك المنطقة في حجم الخسائر، حيث تراوحت بين ٣ ملايين دولار أمريكي

في المملكة العربية السعودية والإمارات العربية المتحدة، ومليـون وأربعمائـة ألف دولار أمريكي في لبنان.

وفي دراسة أخرى أجرتها هيئة الأمم المتحدة، اتضح أن ٢٤- ٤٢٪ من منظمات القطاع الخاص والعام كانت ضحية لتلك الجرائم.

أما في الولايات المتحدة الأمريكية، فقد قدرت أضرار جرائم الإنترنـت والحاسب الآلي بحـوالي ٥ مليـارات دولار سـنوياً. كمـا قـدرت المباحـث الفدرالية الأمريكية (F. B. I) أن تكلفة جريمة الحاسـب الآلـي والإنترنـت الواحـدة حـوالي ٦٠٠ ألـف دولار سـنوياً مقابـل مبلـغ سـتة آلاف دولار تكلفة جرائم السرقة بالإكرام.

وبينـت دراسـة أخـرى أجريـت مـن قبـل منظمـة The Computer Security Institute عـام ١٩٩٩، أن خـسائر ١٦٣ شـركة أمريكيـة مـن الجرائم المتعلقة بالحاسب الآلي والإنترنت قد بلغت أكثـر مـن مئـة وثلاثـة وعشرين مليون دولار أمريكي. في حـين أظهـر المسح الـذي أجـري عـام ٢٠٠٠ ارتفاع عدد الشركات المتضررة من تلـك الجـرائم حيـث وصـل إلى ٢٧٣ شركة بلغ مجموع خسائرها أكثـر مـن مـائتين وسـتة وخمـسين مليـون دولار.

ولعل ما ساعد جرائم الإنترنت على ترتيـب تلـك الخـسائر، الـصفات والمميزات التي تتميز وتنفرد بها عن غيرها مـن الجـرائم لا سـيماً التقليديـة منها. فيا ترى ما هي خصائص هذه الجريمة؟

الفرع الثاني: خصائص جرائم الإنترنت

- جرائم الإنترنت كما سبق ذكره، "هي تلك الجرائم العابرة للحدود والتي تقع إما على شبكة الإنترنت أو بواسطتها من قبل شخص على دراية فائقة بها".

- باستقراننا لهذا التعريف تتضح لنا الخصائي التي تتميز بها جرائم الإنترنت، والتي يمكن حصرها فيما يلي:

أولا: الحاسب الآلي هو أداة ارتكاب جرائم الإنترنت:

تعتبر هذه الخاصية من أهم الخصائص التي تميز جرائم الإنترنت عن غيرها من الجرائم الأخرى لا سيماً التقليدية، ذلك لأن شبكة الإنترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة، ولذلك فإن ارتباطها بالحاسب الآلي هو أمر لا مفر منه، باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي، وإن كنا اليوم نعاصر إمكانية استعمال الإنترنت عبر الهاتف الخلوي.

ويقصد بالحاسب الآلي، ووفقاً للموسوعة الشاملة لمصطلحات الحاسب الإلكتروني: "كل جهاز إلكتروني، يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال (data imput) أو إخراج معلومات (Information output)، وإجراء عمليات حسابية أو منطقية. وهو يقوم بالكتابة على أجهزة الإخراج (output devices) أو التخزين. والبيانات يتم إدخالها بواسطة مشغل الحاسب (operator) عن طريق

وحدات الإدخال أو استرجاعها من وحدة المعالجة المركزية. وبعد معالجة البيانات، تتم كتابتها على أجهزة الإخراج "[1].

وهو يتكون من كيانين: كيان مادي (Hard ware) وكيان معنوي (Software). يضم أولهما الأجهزة المادية المختلفة والتي تشمل وحدات الإدخال وكذا الإخراج ووحدات التشغيل المركزية. أما الكيان الثاني، فيشتمل على البرمجيات الجاهزة والبيانات والمعلومات المنطقية.

ثانيا: الجرائم ترتكب عبر شبكة الإنترنت أو عليها:

تعد شبكة الإنترنت الحقل الذي تقع فيه جرائم الإنترنت، وذلك لأنها تمثل حلقة الوصل بين كافة الأهداف المحتملة لذلك الجرائم، كالبنوك والشركات الصناعية وغيرها من الأهداف التي تكون غالباً الضحية لها، إلا أنه وبالرغم من كونها، الوسيلة لارتكاب جرائم الإنترنت إلى جانب الحالسب الآلي، فإنها كذلك لم تنج من يد المجرمين، لأنها هي الأخرى قد تكون محلاً للاعتداءات.

ثالثا: مرتكب جرائم الإنترنت هو شخص ذو خبرة فائقة في مجال الحوسبة:

تتطلب جرائم الإنترنت على غرار الجرائم التقليدية حرفية فنية عالية سواءً عند ارتكابها أو عند العمل على عدم اكتشافها من الشخص الذي

([1]) نبيلة هبه هدوال، مصدر سابقاً ص ٣٧- ٤٤.

يرتكبها. أي يجب أن يكون ذلك الشخص خبيراً بالقدر اللازم والكافي بأمور الحوسبة والإنترنت.

ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي، وأن الشرطة تبحث أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب هذا النوع من الجرائم.

رابعا: جريمة الإنترنت جريمة عابرة للحدود الدولية:

لقد سبق وأن ذكرنا أن شبكة الإنترنت لها طابع دولي، إذ أنها لا تعترف بتلك الحدود القائمة بين الدول سواءً الجغرافية أو السياسية، وهاذ ما أدى إلى اعتبار جرائم الإنترنت من الجرائم الدولية وكذا من الجرائم ذات البعد الدولي. وتأخذ جرائم الإنترنت بعداً دولياً، من حيث إمكانية أن يكون العمل الإجرامي عبر الإنترنت من طبيعة عالمية، وذلك حينما ترتكب داخل دولة، إلا أنها تمتد إلى خارج إقليم تلك الأخيرة، مما يعني خضوعها لأكثر من قانون جنائي كما هو الشأن في جرائم المخدرات والإرهاب والتجسس الاقتصادي وغسل الأموال. كما أنها قد تأخذ ذلك البعد في الحالة التي يعترف فيها المشرع الدولي بأن العدوان يمكن أن تقوم به دولة ولو في صيغة تأييد. مثلما قامت به عصابات الكيان الصهيوني من دعوة لاجتماع الهكرة في مؤتمر عالمي في شهر ماي/ مايو سنة ٢٠٠٠ في فلسطين المحتلة.

وتعتبر جريمة الإنترنت جريمة دولية في الحالة التي يكون أحد أطرافها شخصاً دولياً، كما حدث في التجسس الذي قامت به الولايات المتحدة، إذ

استخدمت الأسلحة المعلوماتية الفتاكة وذلك عن طريق انتهاك أنظمة حاسوب أعدائها أثناء القصف الجوي للحلف الأطلنطي Nato في كوسوفو.

وتجدر الإشارة إلى أنه يمكن أن تكون جريمة الإنترنت في مقابل ذلك جريمة وطنية، إذ أن لها أثراً إقليمياً، من حيث أن حجم الأثر المكاني يحتويها كأي جريمة ثانية، لكونها ينبغي أن تبدأ في نطاق إقليمي معين، ومن ثم ينعقد الاختصاص للتشريع الجنائي لذلك الإقليم.

خامسا: صعوبة إثبات جرائم الإنترنت:

تعتبر هذه الخاصية من أهم الخصائص المميزة لجرائم الإنترنت عن غيرها من الجرائم وخصوصاً تلك التقليدية. نظراً لكونها ترتكب بواسطة أو على الإنترنت، ومن قبل شخص ذي دراية فائقة بها، وما ينجم عن ذلك من سهولة إخفاء معالم الجريمة والتخلص من آثارها، وبالتالي صعوبة التحقيق فيها وتتبع مرتكبيها والقبض عليهم على غرار الجريمة التقليدية. وإلى جانب الأسباب السابقة، فإنه تعود صعوبة إثبات جرائم الإنترنت إلى:

١- صعوبة الاحتفاظ الفني بآثارها إن وجدت.

٢- الحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها، وهذا ما يعرقل عمل المحقق الذي تعود التعامل مع الجرائم التقليدية.

٣- أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها. فهؤلاء يعتمدون على التخفي عبر دروب افنترنت تحت قناع فني.

٤- أنها تعتمد على قمة الذكاء والمهارة في ارتكابها.

٥- يلعب البعد الزمني (اختلاف المواقيت بين الدول) والمكاني (إمكانية تنفيذ الجريمة عن بعد) والقانوني (أي قانون يطبق دوراً مهما في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم،

الفرع الثالث: أركان جريمة الإنترنت

- لا تختلف جريمة الإنترنت عن أي جريمة أخرى، إذ أنها تتطلب لتحققها الأركان المتفق على ضوررة توفرها في أي جريمة لكي تتواجد على أرض الواقع، فبالإضافة إلى ضرورة تواجد الشرط المبدئي في كل جريمة أي النص الشر عن المجرم أو الصفة غير المشروعة، فإنه لابد من وجود الركنين الذين تتألف منهما كل جريمة وهما: الركان المادي والركن المعنوي.

أولا: النص المجرم أو الصفة غير المشروعة في جرائم الإنترنت:

النص الشرعي هو نص التجريم الذي يضفي على الفعل أو الامتناع الصفة غير المشروعة. وقد اختلف الفقه ولا زال حول طبيعته، فهناك من يعتبره ركناً في الجريمة إلى جانب الركن المادي والمعنوي، وهناك من يعتبره صفة غير مشروعة تقترن بالسلوك فتجعله مجرماً ومعاقباً عليه. ويتجسد

هذا النص من خلال مبدأ شهير هو "مبدأ لا جريمة ولا عقوبة ولا تدبير أمن إلا بقانون". أي ما يعرف بمبدأ شرعية الجرائم والعقوبات.

وهو مبدأ ذو طابع عالمي، إلا أن الدول اعتادات على الاعتراف به في النطاق المحلي لا غير. والإشكال المطروح هنا هو: ما محل جريمة الإنترنت من مبدأ شرعية الجرائم والعقوبات؟، وما مدى التقاء هذا المبدأ مع ظاهرة جرائم الإنترنت العابرة للحدود؟، وهل تنتمي جرائم الإنترنت إلى قانون الإنترنت أم انها مشتقة من التجديد الذي يخترق بالضرورة أحد فروع القانون المتعددة وهو فرع القانون الجنائي؟.

- لقد أثار الفقه المعاصر موضوعاً على جانب كبير من الأهمية يتعلق بتفاعل نظم التقنية الحديثة مع القانون الجنائي وتأثير ذلك على مبدأ الشرعية لا سيماً حال انعدام وجود نصوص قانونية تحكم مظاهر التعامل مع تلك التقنية.

وتعتبر جرائم الإنترنت التي أفرزتها تقنية الإنترنت، أحد التحديات الكبرى والتي تقف أمام تطبيقات القانون الجنائي، والذي يكون في كثير من الأحيان محلاً لقصور بين في تنظيم تلك الجرائم المستحدثة وهذا ما يسهل للكثير من المجرمين ارتكابها والإفلات من العقاب.

ولعل القوانين الأمريكية والفرنسية والإنجليزية أحسن مثال على ذلك، فكم من الانتهاكات حدثت عبر الإنترنت ونتيجة لعدم وجود نصوص تجرم وتعاقب، أفلت الجناة من العقاب، ولكن هذا لا يعني أن مبدأ شرعية الجرائم والعقوبات لا وجود له فيما يخص جرائم الإنترنت. فلو قلنا ذلك،

فإننا ننفي وجود تلك الجرائم في حد ذاتها، إذ وبالرغم من حداثتها واعتمادها على التقنية، ولا سيماً في إطار تهديدها للألفية الثالثة، فإن التشريعات المقارنة قد تصدى لهذه الأخيرة بتجريمه لصور الاعتداء الناجمة عن المعالجة الآلية للبيانات والتي تنطبق بلا شك على صور الاعتداء على شبكة الإنترنت، حيث أصدر نصوصاً قانونية عدة تكفل الحماية الجنائية للحاسب الآلي وشبكاته وخصوصاً الإنترنت. فعلى سبيل المثال: نجد أن المشرع الفرنسي قد جرم في المادة ٣٢٣- ١ إلى المادة ٣٢٣- ٧ من قانون العقوبات الجديد لسنة ٢٠٠٣ صور الاعتداء الناجمة عن المعالجة الآلية للبيانات، مما يسمح بانطباقه على الأفعال التي تقع على الإنترنت (كمحل للاعتداء) أو بواسطته (كوسيلة للاعتداء).

وفي نفس السياق نجد المشرع الأمريكي قد أصدر العديد من القواعد القانونية لمواجهة الجرائم المرتكبة عبر الإنترنت ومنها "قانون آداب الاتصالات عام ١٩٩٦"، والذي جرم من خلاله أفعال القذف والسب عبر شبكة الإنترنت، وكذا أفعال التعرض للأخلاق والآداب العامة عبر تلك الشبكة، كما كفل الحماية الجنائية للأطفال ضد الاستغلال الجنسي لهم بقانون عام ١٩٩٨ المعروف بـ "قانون حماية الأطفال على الخط". وفي إطار حماية حرمة الحياة الخاصة من الاعتداء عليها، أصدر المشرع الأمريكي "قانون الخصوصية عام ١٩٧٤" وقانون "خصوصية الاتصالات الإلكترونية عام ١٩٩٨". كما قام بإصدار "قانون منع القرصنة الإلكترونية عام ١٩٩٧".

وقد سار المشرع الإنجليزي على نفس المنوال، فبادر إلى مواجهة المشكلات القانونية الناجمة عن تطور تقنيات المعلوماتية، وذلك بإفراده حماية خاصة للأطفال من الاستغلال الجنسي بقانون "حماية الطفل لعام ١٩٧٨".

أما على مستوى الدول العربية، فإنه وحتى هذا التاريخ، لم تقم أغلبية تلك الدول بسن قوانين خاصة بجرائم الإنترنت، ما عدا البعض منها، كمصر مثلاً، والتي تناولتها في "قانون الاتصالات لعام ٢٠٠٢" وكذا من خلال قوانين "حماية [١].

الملكية الفكرية لسنة ٢٠٠٢". وذات الشأن بالنسبة للجزائر إذ نجدها قد خصصت قسماً خاصاً بتجريم ومعاقبة المساس بأنظمة المعالجة الآلية المعطيات وذلك في المواد من ٣٩٤ مكرر إلى المادة ٣٩٤ مكرر ٧ من قانون العقوبات الجزائري المتمم والمعدل.

ثانيا: الركن المادي:

لقد سبق وأن انتهينا آنفاً، إلى أن الجريمة تتألف من ركنين أساسيين، ركن مادي وركن معنوي. فأما الركن المادي فهو يتمثل في سلوك إرادي تترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سببية مادية، ففيما يتمثل هذا الركن في جرائم الإنترنت؟

---

(١) لمزيد من التفاصيل أنظر د/ مدحت رمضان: الحماية الجنائية لموقع الإنترنت ومحتوياته، مجلة التشريع، العدد الثاني، السنة (١)، يوليه ٢٠٠٥، ص ٤١ وما بعدها.

- باستقراننا للتعريف السابق للركن المادي، نستنتج أنه يتكون من سلوك إرادي، ونتيجة إجرامية، ورابطة سببية.

والركن المادي في جرائم الإنترنت يتكون من العناصر السابقة أي:

أ- سلوك إجرامي:

يعتبر السلوك المادي عبر الإنترنت محلاً لجملة من التساؤلات لا سيماً فيما يتعلق ببدايته أو الشروع في ارتكاب الجريمة، وهو يختلف عما هو الحال في العالم المادي، ذلك لأن ارتكاب الجريمة عبر الإنترنت تحتاج بالضرورة إلى منطق تقني. أي أنها تتم عبر الإنترنت أو باستخدام المعالجة الآلية للبيانات، كما أنها تحتاج إلى ممارسة نشاط تقني محدد يتمثل في استخدام الحاسوب والإنترنت.

ومن أمثلة السلوك المادي في الجريمة عبر الإنترنت: المصرفي الذي ينوي سرقة مبالغ من المصرف الذي يعمل فيه باستخدام الإنترنت، وذلك بممارسة نشاط التعامل مع الحاسوب والولوج إلى الإنترنت، ثم الدخول على شبكة المصرف عبر مزودات مجهولة يمكن الاستعانة من خلالها ببرمجيات اختراق موضوعة على مواقع هكرة يتم تجديدها باستمرار.

ففي هذا المثال فإن المصرفي المذكور يمارس النشاط المادي للاختلاس عن طريق الحاسوب والإنترنت.

ب- النتيجة الإجرامية:

يعد هذا العنصر أحد عناصر الركن المادي في الجريمة إلى جوار السلوك الإجرامي وعلاقة السببية. وتثير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة من أهمها: تحديد هل جريمة الإنترنت هي جريمة مرتكبة سلوكاً ونتيجة في العالم الافتراضي أم أن هناك امتداداً للنتيجة ليتحقق منتهاها في العالم المادي؟.

ج- علاقة السببية:

هي العنصر الثاني من العناصر التي يتكون منها الركن المادي في الجريمة، ويجب لقيام جريمة الإنترنت، أن تكون هناك رابطة مادية ما بين السلوك المادي والنتيجة الإجرامية المتحققة. فمثلاً: يجب لتحقق جريمة انتهاك الحق في الخصوصية عبر الإنترنت أن يكون هناك دخول على الإنترنت باستخدام حاسوب عامل والقيام باختراق الخوادم المختلفة في مسارها، ثم بعد ذلك التعدي على خصوصية موقع ما. وكذلك يمكن اعتبار علاقة السببية قائمة بمجرد ثبوت الضرر في مجرد البث. وهذا ما قررته محكمة استئناف مقاطعة British Colombia الكندية في إحدى أحكامها.

إن كل جريمة تحدث باستخدام الإنترنت إنما تحدث كلها أو بعضها حسب الأحوال في العالم الافتراضي. وإذا كان النشاط المادي يحدث كله في العالم الافتراضي وكذا العلاقة السببية، فإن النتيجة الإجرامية لها كيان

منفصل، لكونها تحدث بشكل انقسامي ما بين حدوثها في العالم المادي جزئياً أو كلياً، ومن أهم الآثار المترتبة عنها أنها تؤثر على قواعد الاختصاص في الدول. فمثلاً في الولايات المتحدة الأمريكية، جعلت نتيجة الإجرامية القضاء الأمريكي (ولاية Tenneessee) في قضية توماس يعترف باختصاص القضاء لمجرد تحقق النتيجة في الولاية المذكورة وبغض النظر إذا ما كانت كاليفورنيا تجرم مثل هذه الأفعال.

هذا وتجدر الإشارة إلى أن جرائم الإنترنت تنتشر فيها فكرة النتيجة المحتملة، وذلك راجع إلى طبيعة النشاط التقني الذي قد يترتب عليه نتائج عدة. فمثلاً: من يقصد القرصنة ويتحقق معها انتشار فيروسات، فإن ذلك يعتبر نتيجة محتملة لذلك العمل. ويلاحظ أن المشرع الأمريكي قد توسع في فكرة النتيجة المحتملة لتشمل الجريمة التي ليس فيها ضحية على الإطلاق، أي الحالة التي لا يكون للضحية وجود مادي وإنما رقمي فقط، [وهو ما يقرره في القسم ١٨ (.see use ٢٤٢٢b)]، وجسدت هذه الحالة في قضية U S A V. Roots أمام القضاء الأمريكي، والتي حسم فيها موضوع التوسع في الاحتمال.

ثالثا: الركن المعنوي في جرائم الإنترنت:

ويطلق عليه الركن الأدبي أو الشخصي، وهو المسلك الذهني أو النفسي للجاني.

والركن المعنوي في جرائم الإنترنت له ثلاث صور:

أ- العمد:

- لما كانت جرائم الإنترنت من جرائم التقنية العالية، التي تتطلب المعرفة والتعليم التخصصي من قبل من يمارس هذا النوع من وسائل الاتصال، فإنه كان من المتصور غالباً عدم وقوعها إلا في صورة واحدة هي صورة العمد. أي أن مرتكب تلك الجريمة قد خطط ودبر لارتكابها سواءً من أجل الحصول على المعلومة أو لاختراق شبكة حاسوب آخر. فمثلاً: جريمة القذف والسرقة تتطلب من الفاعل إرادة ارتكاب السلوك وتحقيق النتيجة، وقد يكون القصد الجنائي هنا عاماً أو خاصاً.

- وتجدر الإشارة إلى أن القضاء الأمريكي يقع في حيرة تقرير مدى إمكانية امتداد البحث في الركن المعنوي، وتحديداً العمد إلى الجرائم الأخرى ذات الامتداد بالجريمة الأولى في جرائم الإنترنت، والمتمثلة في جريمة الاختراق. إذ أن المخترق قد يرتكب الجريمة لمجرد الاختراق، وفي هذه الحالة نكون أمام جريمة عمدية في صورة قصد عام. إلا أنه وفي أغلب الأحيان، يتعدى ذلك إلى أكثر من مجرد الاختراق كما لو كان غرضه بعيداً عن ذلك كالتعديل أو الإلغاء أو التعدي على الحق في الخصوصية.

وفي هذا نجد اتجاه في القضاء المقارن يعتبر أن الجريمة الثانية هي جريمة موضوعية لا تحتاج لركن معنوي؛ ولقد برزت الفكرة أول مرة في قضية الولايات المتحدة الأمريكية ضد موريس، والذي أسس دفاعه على انتفاء الركن المعنوي وبالتالي العمد لديه، ولقد امتد هذا الأخير إلى الاستئناف، حيث وضعت المحكمة هذا الجدل في الصيغة الاستفهامية التالية: "هل يلزم

أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول، بحيث تثبت نية المتهم في الولوج إلى حاسب فيدرالي، ثم يلزم إثبات نية المتهم في تحدي حظر استخدام نظام المعلومات في الحاسوب. وبالتالي تحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح".

ولقد ذهبت المحكمة في ردها على هذا إلى التأكيد على التفسير اللغوي لتشريع ١٩٨٤ وتعديله في عام ١٩٨٦، وهذا ما جعلها تؤكد على أن الركن المعنوي الواجب توفره في جريمة موريس إنما يتأسس على العمد والذي يتحقق بالإرادة في جريمة الولوج.

- أما القضاء الفرنسي، فعلى غرار مثيله الأمريكي، نجد أن منطق سوء النية يكتسح النصوص التي تطبق بشأن جرائم الإنترنت مثلما هوت مقرر في المادة ١٥ و ٢٢٦ عقوبات فرنسي جديد، حيث يشترط سوء النية حين وجود عدوان على البريد الإلكتروني.

ب- القصد المتعدي:

يمكن أن يتوافر القصد المتعدي في جرائم الإنترنت، ومثال ذلك: الحالة التي يكون فيها الولوج بقصد اللهو في حركة أو مسار القطارات، فيخرج الأمر عن السيطرة ويتم تدمير بيانات تحريك القطارات عبر الحاسوب، وبالتالي تحدث كارثة تكون نتيجتها خسائر مادية وبشرية كبيرة. أو كمن يرسل فيروساً عبر البريد الإلكتروني إلى أحد الأفراد بقصد الانتقام منه، دون أن يكون على دراية بالوسيط الخادم ومدى إمكانية حدوث انتشار الفيروس في ذلك الأخير. فيتسبب في اجتياح الفيروس في كل حاسوب

مرتبط بذلك الخادم. فهنا قصد الشخص قد تجاوز ما كان يهدف إلى تحقيقه.

ج. الخطأ غير العمدي:

للخطأ مكانه في تطورات الركن المعنوي في جرائم الإنترنت، إذ أن هناك بعض الجرائم تتم نتيجة لخطأ لم يكن مقصوداً. كتدمير أجهزة المؤسسة نتيجة إفراط من قبل الموظف المسؤول الذي استخدم جهاز الحاسب العائد لها بعمليات لحسابه الخاص معتمداً على مهاراته في تجنب متاعب الفيروسات. أو كاستخدام القرص المرن في أجهزة هذه المؤسسة ونقل فيروسات لها مما ينجم عن تدميرها بشكل جزئي أو كلي.

وتجدر الإشارة إلى أن المشرع الأمريكي يتجه إلى إضفاء الطابع الخطئي على الجريمة الثانية التي تتجاوز جريمة الدخول العمدي إلى نظام حاسوب عامل لدى هيئة فيدرالية أو مالية.

الفرع الرابع: الفرق بين جريمة الإنترنت وجريمة الحاسب الآلي.

- لقد سبق وأن ذكرنا أن الإنترنت تلك التقنية الحديثة تتميز بمجموعة من الخصائص، من أهمها ارتباطها بالحاسب الآلي، إذ يعتبر ذلك الأخير النافذة التي تطل بها على العالم. ولقد أدى ذلك الارتباط إلى اعتبار عدد كبير من الفقه أن جريمة الإنترنت هي نفسها جريمة الحاسب الآلي. إلا أننا نرى أن هناك اختلافاً كبيراً بينهما، فما هو هذا الاختلاف؟.

أولا: أوجه التشابه:

- تختلف جريمة الإنترنت عن جريمة الحاسب الآلي في عدة نقاط، إلا أنه وقبل التطرق إلى هذا الاختلاف، فإنه من الواجب علينا الإشارة إلى أوجه الشبه المشتركة بين هاتين الجريمتين:

أ- لعل وجه الشبه الذي يربط جريمة الإنترنت بجريمة الحاسب الآلي، أن كلاهما من الجرائم الخطيرة.

ب- أن كلا منهما يعتبر جريمة تقنية، ففي كلتيهما تستعمل التقنية لارتكابها.

ج- أن كلاً منهما يحتاج لارتكابه شخصياً ذا دراية فائقة بهما.

د- أن كلاً منهما يشترك في أداة ارتكاب تلك الجرائم وهي "الحاسب الآلي".

هـ- بالإضافة إلى ذلك فإنهما يشتركان كذلك في صعوبة اكتشافهما وإثباتهما.

ثانيا: أوجه الاختلاف:

وفي مقابل ذلك، فهما يختلفان في النقاط التالية:

أ- تعرف جريمة الحاسب الآلي: "بأنها جريمة تقع بواسطة الحاسب الآلي أو على مكوناته المادية والمعنوية". أما جرائم الإنترنت فهي:

"تلك الجرائم العابرة للحدود والتي ترتكب بواسطة الإنترنت أو عليها من شخص ذا دراية فائقة بها".

باستقرائنا للتعريفين السابقين يتضح لنا: أن جريمة الحاسب (سواءً: أكان وسيلة أم ضحية) يمكن أن تتم دون الحاجة إلى الارتباط بشبكة الإنترنت، مثل توظيف الحاسبات وملحقاتها في جرائم التزوير والتزييف أو سرقة المعلومات وتدميرها. أما جريمة الإنترنت فشرطها الرئيسي وجود جهاز حاسب متصل بالإنترنت لإتمام أركانها.

٢- تاريخياً أرجع الفقه الجنائي ظهور جرائم الحاسوب إلى العام ١٩٦٠. أما جرائم الإنترنت فيرجعها إلى العام الذي أفاق فيه العالم على دودة موريس أي عام ١٩٨٨، والتي كانت السبب في تعديل التشريع الفيدرالي الأمريكي.

٣- مجرم الإنترنت ومجرم الحاسب الآلي: مجرم الإنترنت المتميز هو الهاكر والذي يتخذ الشكل الخبيث له في مصطلح كراكر (Cracker). في حين أن مجرم الحاسب الآلي هو القرصان مرتكب جرائم العدوان على حقوق الملكية الأدبية والفكرية عامة وجرائم استخدام التقنية للسيطرة على استخدام الحاسوب خاصة كاختراق كلمات العبور لملفات مشفرة مخزنة في الحاسوب. ويطلق على الهاكر في الدراسات العربية مصطلح القرصان أو المخترق.

ويختلف مجرم الإنترنت عن مجرم الحاسب الآلي في كونه مجرماً لا يتمتع بمدارك علمية أو تخصصية ذات طابع أكاديمي، وإنما هو يملك تقنية

الإنترنت دون حاجة لأن يكون دارساً لها، ولعل أحسن مثال عن ذلك الأطفال الذين يرتكبون تلك الجرائم وهم في سن مبكرة.

ويرتبط سلوك مجرم الإنترنت بظاهرة الاختراق على عكس مجرم الحاسب الآلي والذي يرتبط بالقرصنة.

٤- الإنترنت يحكمه قانون الإنترنت على عكس الحاسوب الذي يحكمه قانون الحاسوب.

٥- اختلاف فيروس الإنترنت كجريمة تقنية عن فيروس الحاسب الآلي، ذلك لأن فيروس الحاسب برز لأول مرة سنة ١٩٧٤ في شركة " Xerox" على عكس فيروس الإنترنت الذي ظهر سنة ١٩٨٨.

هذا من جهة، ومن جهة أخرى يتميز فيروس الإنترنت بأنه سريع الانتشار طالما أن الشبكة تعمل وحتى لو أغلق أحد الحواسيب أو الشبكات أو الخوادم أضف إلى ذلك أن مهام ذلك الأخير تتجاوز عملية التخريب؛ إذ يمكن استخدامه في الاختلاس المعلوماتي. ومثال ذلك ما كشف عنه التطور الفيروسي عن وجود دودة يطلب عليها .Badtrans١٣٣١٢ @ mm ، تلعب دور المختلس المعلوماتي الذي يختلس النظام المعلوماتي وما يحويه من معلومات مخزنة. بينما فيروس الحاسوب فيكمن في الحاسوب المصاب به ولا ينتقل إلى حواسيب أخرى إلا عند انتقال ملف أو برمجية من الحاسوب المصاب إلى الحاسوب غير المصاب. أضف إلى ذلك فإن فيروس الإنترنت لا يلزمه تدخل إنساني للانتشار على عكس فيروس الحاسوب.

المطلب الثاني

أنواع جرائم الإنترنت

- لقد انتهينا سابقاً، أن جرائم الإنترنت هي تلك الجرائم العابرة للحدود والتي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص ذا دراية فائقة بها.

باستقراننا للتعريف السابق، يتضح لنا أن هناك نوعين من جرائم الإنترنت: النوع (١): حينما تكون شبكة الإنترنت هدف الجريمة وغايتها، وهذا ما يسمى بـ: "الإجرام المعلوماتي على الإنترنت". والنوع الثاني: حينما تكون شبكة الإنترنتقد استخدمت كوسيلة في ارتكاب الجريمة، وهذا ما يسمى "بالإجرام غير المعلوماتي في شبكة الإنترنت".

وفيما يلي تفصيل ذلك:

الفرع الأول: الإجرام المعلوماتي على شبكة الإنترنت:

ويشتمل هذا النوع من الإجرام على الجرائم التالية:

أولا: الاعتداءات المنطقية:

أ- جرائم مهاجمة الشبكة بالفيروسات والبريد الإلكتروني التطفلي :

تعتبر هذه الجرائم من أخطر الجرائم التي تهدد الحواسيب وشبكة الإنترنت، وتلحق بها خسائر مادية بعشرات الملايين من الدولارات [١].

([١]) نبيلة هبة هدوال، مصدر سابق ص ٥٧- ٦٤.

والفيروس هو برنامج حاسوب يهدف إلى إحداث أكبر ضرر بنظام الحاسوب، وله القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتياً. ويقوم الفيروس بالانتشار بين برامج الحاسوب المختلفة وبين مواقع مختلفة في الذاكرة.

ومن النتائج التي تترتب على هذا الفيروس، تعديل البرامج والتنقل بواسطتها إلى برامج أخرى، نسخ أوامر بدلاً عن أوامر البرنامج، إلحاق أضرار بالغة بالبرامج، تقليل سرعة الحاسب.

ومن أخطر الفيروسات المنتشرة عبر شبكة الإنترنت، فيروس Nimada ، والفيروس المدمر الذي تشهده الحاسبات والشبكات في أيامنا هذه، فيروس Mytob. U. @mm ٣٢W. أو Mytob. x ٣٢W. ، وفيروس RtA.

وتصنف ضمن الفيروسات:

١ـ الدودة المعلوماتية: (**Ver informatique**)

وهي برامج معلوماتية صغيرة، قائمة بذاتها وغير معتمدة على غيرها وضعت بهدف تدمير وإعاقة وتشويش الشبكات، أو بغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم على شبكة الإنترنت أو لإلحاق الضرر بهم أو بالمتصلين بهم.

وتتميز هذه الدودة بسرعة الانتشار وفي نفس الوقت يصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة، ومن أشهر

أمثلتها: الدودة التي اخترعها روبرت موريس، والمسماة بدودة الحب، وكذلك دودة ميلسيا وأنا كارنيكافو.

٢ـ القنبلة المعلوماتية: (**Bombe informatique**)

وتعرف كذلك بالشفرة المعيقة أو القنبلة الموقوتة، وهي عبارة عن برنامج يعد من قبل مصمم للنظام المعلوماتي يبثه بداخله،وتكون الغاية منه جعله ينطلق أو يعمل بعد فترة محددة على استعمال النظام المعلوماتي بهدف تعطيله، كأن يتوقف عن العمل ويلصق رسالة أو صورة أو إشعار ... أو تدمير أو محو البيانات التي يحتويها.

وتجدر الإشارة إلى أنها أكثر ما تبرز في الحملات الإعلانية للبرمجيات وكذا في البرمجيات المؤجرة [١].

٣ـ الفخ أو الخبيئة: (**Trappe**):

وهو منفذ يجهز مسبقاً في نظام معلوماتي من قبل مصممه، من أجل إنزال برامج خاصة من شأنها أن تعيق سير عمل هذا النظام، وأن تدخل إليه عناصر إعاقة لتطبيقاته.

٤ـ حصان طراودة: (**Cheval de Troite**):

تعد هذه العملية الطريقة الغالبة في الاحتيال والتخريب بواسطة الحاسب الآلي، وهي تمثل تغطية أوامر الحاسب الآلي لتمكينه من الإتيان

---

(١) نبيلة هبة هدوال، مصدر سابق ص ٥٧- ٦٤.

بوظائف غير مصرح له بها مع ترك البرنامج على حاله للاستثمار في تحقيق أهدافه.

ومن أبرز الأمثلة المعروفة بحصان طروادة، مبرمج يعرف باسم (Bak orifice) الذي يصفه أحد خبراء الحاسوب الأمريكان بأنه: "... يمكنه أن يدمر الكاميرا التي تملكها، ويمكنه أن يفتح جهاز الميكروفون الخاص بك. ويمكنه أن ينسخ ملفاتك وأن ينقل كل ما يراه ويسمعه ويقرأه ويعيد إرساله".

ب- القناة المخفية: (Canal Cache):

وهو نوع خطر من الاعتداءات، يقوم على مبدأ تهريب المعلومات عبر خرق سياسة الأمن والحماية المعتمدة في الأنظمة المعلوماتية، وهي هي ذلك تتطلب ذكاءً فائقاً من المعتدي.

ج- انتحال شخصية الفرد أو شخصية الموقع:

ويعني ذلك انتحال صلة من له الحق في الدخول إلى نظام معلوماتي معين، وذلك باستغلال بياناته كعنوانه أو تاريخ ميلاده أو رقم ضمانه الاجتماعي استغلالاً سيئاً، من أجل الحصول على بطاقات الائتمان أو رخص القيادة أو بهدف تشويه سمعة صاحب الموقع.

هذا فيما يخص انتحال الشخصية الفرد، أما فيما يخص انتحال شخصية الموقع، فهي تعني أنه بإمكان بعض الأشخاص الدخول على الموقع بغرض حجبه أو تغييره، ووضع الموقع الخاص به، وهذا ما يحدث غالباً في المواقع

السياسية أو الدينية، ومن ذلك ما نجده في المواقع الفلسطينية والمواقع الإسرائيلية، فكثيراً ما يدخل الفلسطينيون على المواقع الإسرائيلية يقومون بإلغاء الصفحة الرئيسية ويضعون بدلاً منها العلم الفلسطيني والعكس صحيح.

وفي إطار الجريمتين السابقتين هناك جريمة من نفس النوع وهي جريمة معاودة إرسال.

إشارات سبق أن استخدمها مستعمل مرخص له بالدخول إلى هذا النظام، وتم تسجيلها بشكل خفي بدون علمه.

ثانيا: الاعتداءات المادية:

وتعتبر هذه الأخيرة النوع الثاني من الجرائم التي تكون شبكة الإنترنت محلاً لها، ومن أبرزها:

١ـ الاعتراض المتعمد للبيانات:

ويقصد به رصد إشارات إلكترومغناطيسية في الأنظمة المعلوماتية وتحليلها، بهدف استرجاع المعلومات المفهومة أو المقروءة منها.

بـ التشويش:

وبهدف هذا النوع من الاعتداء، إلى إعاقة المستوى التشغيلي للأنظمة المعلوماتية وجعلها عاجزة عن العمل.

ج- الاكتساح والتفخيخ:

ويقصد بالاعتداء الأول منهما إرسال حزمة من المعلومات إلى الشبكة للتوصل إلى تحديد أي من هذه المعلومات هي الصحيحة، أما الاعتداء الثاني فيقصد به إدخال وظائف خفية في مرحلة تصميم أو تصنيع أو نقل أو صيانة النظام المعلوماتي.

الفرع الثاني: الإجرام غير المعلوماتي في شبكة الإنترنت

- وهو النوع الثاني من جرائم الإنترنت، يحدث حينما تستخدم الإنترنت كوسيلة لارتكابها، ويشمل هذا النوع من الإجرام جرائم عديدة مثل الجرائم الجنسية، والممارسات غير الأخلاقية وجرائم الاختراقات والجرائم المالية وجرائم إنشاء وارتياد المواقع المعادية وجرائم القرصنة والجرائم المنظمة وجريمة غسل الأموال والمخدرات ... الخ.

ولقد ارتأينا تقسيم هذه الجرائم إلى:

جرائم الاعتداء على حرمة الحياة الخاصة عبر الإنترنت:

جرائم تقع على الأموال:

والتي تشمل السرقة والنصب عبر الإنترنت وكذا جريمة غسل الأموال عبر الإنترنت وجريمة ترويج المخدرات عبر الإنترنت.

جرائم الاعتداء على حقوق الملكية الفكرية.

جرائم الاعتداء على أمن الدولة، وخصوصا الإرهاب الإلكتروني.

أولا: جرائم الاعتداء على الأشخاص:

إن التوافق بين السياسة الجنائية وحق الأفراد في سلامة أبدانهم من كل أذى يحيط بهم مطلب أساسي ومشروع لمواجهة الإجرام التقني المستحدث الناتج عن استخدام شبكة الإنترنت والتي يلجأ إليها المجرم المعلوماتي لتنفيذ رغباته الإجرامية في بيئة لا يحكمها قانون، فلقد أتاحت الثورة المعلوماتية لهذا المجرم تسخير الفضاء الكوني لتحقيق أغلب صور الاعتداء على الأشخاص من جنح بسيطة إلى جنايات كبرى إما كفاعل أصلي أو كفاعل معنوي وبأبسط الأساليب من خلال التلاعب ببرامج أو برمجة البيانات عن بعد بالضغط على زر واحد، ومن أهم الاعتداءات على الأشخاص عبر الإنترنت: جرائم الأخلاق وجرائم الاعتداء على حرمة الحياة الخاصة.

١ـ جرائم الأخلاق:

لقد احتلت مشكلة الأخلاق عبر الإنترنت حيزاً كبيراً في بحوث الفقه المقارن، وذلك لاختلاف الأخلاقيات من شعب لآخر، وجرائم الأخلاق وفقاً للتصنيف المصلحي في قانون العقوبات هي تلك النوعية من الجرائم التي تتضمن العدوان على القيم الأخلاقية المتعارف عليها في النظم الاجتماعية والاقتصادية[1]، وهي مجرمة في جميع تشريعات العالم مع

(1) نبيلة هبة هدوال، مصدر سابق ص ٥٧- ٦٤.

اختلاف الأخلاقيات في تلك الأخيرة، فمثلاً في مصر نجد قانون العقوبات فيها يرصد الجرائم الأخلاقية في البابين الرابع والسابع من الكتاب الثالث، وكذلك قانون العقوبات الجزائري، إذ يتناولها في الأقسام الخامس والسادس والسابع من المواد ٢٦٩ إلى ٣٤٢ عقوبات.

وتجدر الإشارة إلى أن العلنية شرط مهم في الجرائم الأخلاقية، وهذا ما نجده متحققاً في تلك الجرائم الواقعة عبر الإنترنت، ومن أهم هذه الجرائم:

١ـ جرائم القذف والسب والتشهير عبر الإنترنت:

تعد جرائم القذف والسب والتشهير من أكثر الجرائم شيوعاً في نطاق شبكة الإنترنت، وإن كانت تلك الأخيرة جرائم تقليدية، إلا أنها ونظراً لوقوعها بواسطة شبكة الإنترنت فإنها تصنف ضمن الجرائم المستحدثة. وتعاقب معظم التشريعات العقابية على هذه الجريمة، ومنها القانون الجزائري في مادته ٢٩٧ و ٢٩٦ عقوبات، وكذا القانون المصري في المادة ٣٠٢، ٣٠٦، ٣٠٨ عقوبات، كما تجرم التشريعات العقابية المقارنة تلك الجريمة ومنها قانون العقوبات الإيطالي في المواد ٥٩٤- ٥٩٥، والقانون الأمريكي في النص: ٢٢٣ 47sec .

وتتنوع صور القذف والسب عبر شبكة الإنترنت بتنوع الغرض من استخدامها:

فقد يكون القذف والسب وجاهياً. ومثالها ما يحدث من خلال مجموعات الأخبار، وخاصة في الحالة التي يتبادل فيها الجاني والمجني عليه

الرسائل أو في الحالة التي يكون كلاهما في صدد تعليق ومشاركة على موضوع معين.

وقد يكون كتابة وهذا ما نجده غالباً في غرف المحادثات والدردشة (chat , rooms) وقد يكون غيابياً كما هو الشأن في مجموعات الأخبار، عندما يترك المستخدم عنوان بريده الإلكتروني على تلك المجموعات ليتسنى له استقبال الرسائل حول موضوع ما ولمعرفة أخبار موضوع يشغل اهتمامه، وقد يكون بواسطة المطبوعات أي بواسطة الجرائد والصحف اليومية أو الموقوتة عبر شبكة الإنترنت، وهذا ما نجده بكثرة في البريد الإلكتروني وشبكة الويب.

وغالباً ما يرتكب السب والقذف عبر شبكة الإنترنت من خلال إسناد مادة كتابية أو صوتية أو فيديوية صوتية تسئ إلى أحد الأشخاص ومن شأنها أن تنال من شرفه أو كرامته أو تعرضه إلى بعض الناس واحتقارهم، ويشترط في هذه الجريمة أن تكون علنية.

هذا فيما يخص السب والقذف، أما بالنسبة للتشهير فهو الآخر نوع من أنواع القذف وهو عبارة عن تشويه أو تهديد لسمعة شخص ما بهدف التقليل من قدر ذلك الأخير في نظر المجتمع والناس أياً كانت نوعية هذه العلاقة أو لابتزازه وبالتالي رضوخه، ويشترط في جريمة التشهير: ١) غياب المجني عليه أي عدم حضوره الواقعة، ٢) أن ترتكب أمام عدة أشخاص أو في الصحف أو في وثيقة عمومية، أضف إلى ذلك تشترط بعض القوانين فيه

الكتابة[1]. وهي ترتكب عبر الإنترنت بإنشاء مواقع خصيصاً لذلك (create location).

ومن أمثلة جرائم التشهير عبر الإنترنت: الحادثة التي تمكنت فيها المباحث المصرية من ضبط شخص٢ بتهمة نشر معلومات كاذبة على الإنترنت للتشهير بعائلة مسؤول وابنته (١٧ عاماً)، وذلك بعد رفض والدها خطبته لها، حيث قام المهندس المتهم بتصميم موقع إلكتروني بهدف التشهير بهذه الفتاة وعائلتها. كما أن هناك حادثة أخرى مشهورة جرى تداولها بين مستخدمي الإنترنت في بداية دخول الخدمة في منطقة الخليج، حيث قام شخص في دولة خليجية بإنشاء موقع على شبكة الإنترنت نشر فيه صورة لفتاة وهي عارية مع صديقها، وكان قد حصل على تلك الصور بعد التسلل إلى جهاز الحاسب الآلي الخاص بتلك الفتاة ونسخ منه تلك الصور، ولما حاول ابتزازها جنسياً بتلك الصور ورفضت، قام بإنشاء ذلك الموقع ونشر فيه تلك الصور مما أدى بالفتاة إلى الانتحار بعد ما سببه لها من فضيحة بين أهلها. كما وقعت حادثة تشهير أخرى من قبل من أسموا أنفسهم "الأمجاد هكرز" حيث أصدروا بيان نشر على الإنترنت بواسطة البريد الإلكتروني أوضحوا فيه قيام شخص بالتطاول في أحد المنتديات بالسب والقذف على شيخ الإسلام "ابن تيمية" وغيره من رموز الفكر الإسلامي الذين يلتف حولهم المسلمون لمعرفة أمور دينهم ودنياهم، وقد استطاع هؤلاء اختراق البريد الإلكتروني لهذا الشخص ومن ثم تم نشر

---

(١) كالقانون الأمريكي، أنظر د/ عرم محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص ٤٦٩.

صوره وكشف أسراره في موقعهم على الإنترنت لتجرؤه على ما ارتكب في حق رموز الإسلام.

٢ـ جرائم الاستغلال الجنسي للأطفال:

لقد وفرت شبكة الإنترنت – أكثر الوسائل فعالية وجاذبية – لصناعة ونشر الإباحية الجنسية، إذ أنها جعلت تلك الأخيرة بشتى وسائل عرضها من صور وفيديو وحوارات – سواءً أكانت مسجلة أم مباشرة – في متناول الجميع كباراً وصغاراً، ذكوراً وإناثاً. وهذا ما أثبتته عدة تقارير ودراسات منها التقرير الذي نشرته شبكة CNN الإخبارية بتاريخ ١٥/ ٣/ ٢٠٠٣ على موقعها عبر شبكة الإنترنت CNN. Com بعنوان "سهولة الوصول إلى الملفات الإباحية". وكذا الدراسة التي أجريت من قبل BBC عام ١٩٩١.

وتعد الإباحة الجنسية جريمة معاقب عليها في معظم بلدان العالم، وخاصة العربية، وهي تندرج تحت جريمة اسمها: "إتيان الأعمال الفاضحة علنية والتحريض على ممارستها"، ولعل أخطر صور تلك الجريمة المنتشرة عبر الإنترنت، هي جريمة استغلال الأطفال جنسياً. إذ أصبحت تلك الفئة عرضة ومحلاً للعديد من الجرائم الجنسية، وذلك بتصويرها بأوضاع جنسية مخلة بالآداب وذلك إما بصور حقيقية أو مفترضة (مزيفة).

ولقد برزت الأخطار المحتملة ضد الأطفال عبر شبكة الإنترنت نتيجة ثلاثة مخاوف رئيسية هي:

١- سهولة وصول الأطفال إلى مواقع خليعة رئيسية تنظم دعارة الأطفال عبر شبكة الإنترنت.

٢- الإنترنت هي المكان المناسب لبيع منتجات منتجي دعارة الأطفال.

٣- وجود أشخاص خطرين ومنجذبين نحو الأطفال على شبكة الإنترنت، والذين يشحرون ضحاياهم إلى لقاءات حقيقية في الحياة مكن خلال تخاطب البريد أو غرف التخاطب أو من خلال المراسلة عبر البريد الإلكتروني.

ولقد جرمت عدة تشريعات جريمة استغلال الأطفال جنسياً ومنها قانون العقوبات الفرنسي الجديد، وخاصة بعد انضمام فرنسا ومصادقتها لاتفاقية الأمم المتحدة لحقوق الطفل عام ١٩٨٩. وذات الشأن بالنسبة للقانون الإنجليزي، إذ أنه صدر في بريطانيا قانون حماية الطفل عام ١٩٧٨ وكذا التعديل الذي أضافه الأمر الخاص بالعدالة الجنائية والنظام العام لسنة ١٩٩٤. أما بالنسبة للقانون الأمريكي فقد جرم تلك الأفعال في التعديل التشريعي للقانون الاتحادي لعام ١٩٩٩.

أما بالنسبة للتشريعات العربية فنجد منها "قانون الطفل المصري رقم ١٢/ ١٩٩٦ "وكذا قانون العقوبات الاتحادي في دولة الإمارات العربية المتحدة.

وبالإضافة إلى ذلك فقد جرم المشرع المصري مجموعة من الأفعال تسمى بجرائم البغاء في قانون "مكافحة الدعارة رقم ١٠/ ١٩٦١".

وذات الشأن بالنسبة للقانون الأردني، إذ بين الجرائم الماسة بالأطفال في الفصل الثاني من الباب السادس من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، وهي الجرائم التي تمس الأسرة في المواد ٢١٨ إلى ٢١٩. كما أورد نصوصاً تجرم أفعالاً إذا كان الاعتداء فيها متعلقاً بالعرض والاغتصاب أو الإغواء في الفصلين الأول والثاني من الباب السابع من قانون العقوبات. أما القانون الجزائري فقد جرم ذلك في قانون العقوبات لعام ١٩٦٦ في الفصل الثاني من الباب الثاني في الأقسام (١) و(٦) و(٧).

ومن الجرائم التي تتعلق بالآداب العامة وتمثل خطورة على الأحداث وتمت بالفعل عن طريق الإنترنت:

١- في عام ١٩٥٥ وجهت الشرطة البريطانية أول اتهام لاستخدام الإنترنت في تبادل المواد الإباحية. وفي بعض الدول تم ضبط عصابات تستخدم الأطفال في إجراء مكالمات حية تتناول موضوعات جنسية فاضحة مع مستخدمين لشبكة الإنترنت.

ب- جرائم الاعتداء على حرمة الحياة الخاصة:

حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية في مختلف تشريعات الدول المتقدمة، لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معاً.

والحق في الخصوصية هو أحد الحقوق اللصيقة التي تثبت للإنسان والتي غالباً ما يصعب حصر جوانبها المختلفة، والتمييز بحدود واضحة بين ما يعد من الحياة الخاصة للإنسان وما بعد من الحياة العامة له.

ولقد لعبت الثورة المعلوماتية وما نتج عنها من تطرو تكنولوجي دوراً بارزاً في تأثيراتها على الحق في الخصوصية، بأطوار وأشكال مختلفة، إذ أصبحت تلك الأخيرة تعرف ببنوك المعلومات. ولكنها وفي الوقت نفسه أصبحت مهددة بالعديد من الانتهاكات والاعتداءات، ولا سيماً مع ظهور الطريق السريع للمعلومات، وهذا ما جعل رجال القانون في مواجهة مباشرة مع تحديات عصر التكنولوجيا المتطورة، وذلك بسعيهم لوضع قوانين تتماشى مع ذلك التطور.

وتقوم جرائم الاعتداء على حرمة الحياة الخاصة عبر الإنترنت على مبدأ التمركز في موقع معين داخل شبكة الإنترنت والعمل على تسجيل وحفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية، وتعتبر البيانات الإسمية محلاً لتلك الاعتداءات. ووسيلة هذه الاعتداءات "مبرجات الحواسيب" والتي هي عبارة عن "جسيمات تنصب على الويب"، وهي تستخدم من قبل الشركات الإلكترونية لتعقب المستهلكين من خلال الإنترنت، ويتم الحماية منها عن طريق برامج رصد متطورة تسمى "بالكعكات".

ومن جرائم الاعتداء على حرمة الحياة الخاصة عبر الإنترنت.

- جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص: وهذا ما نص عليه المشرع الفرنسي في المادة ٢٢٦- ١٦ من قانون العقوبات الفرنسي الجديد.

- جريمة التسجيل غير المشروع للبيانات الإسمية: وهي الأخرى نص عليها المشرع الفرنسي في المادة ٢٢٦- ١٧ إلى ١٩ من قانون العقوبات الفرنسي الجديد.

- جريمة الحفظ غير المشروع للبيانات الإسمية: والمنصوص عليها في المادة (٢٢٦- ٢٠) من نفس القانون.

ثانيا: الجرائم المالية:

لم تقتصر أساليب إساءة استخدام الثورة التقنية على الاعتداء على الأشخاص، بل تعدتها لتطال الذمة المالية للغير.

وفي نطاق شبكة الإنترنت يعد الحاسب الآلي أداة سلبية لارتكاب الجريمة ضد الفرد، إذ تستخدم الحواسيب المرتبطة بشبكة الإنترنت كوسيلة لتنفيذ الجرائم والاعتداء على أموال الغير والتي اتخذت صوراً مستحدثة، وهذا ما دفع رجال القانون إلى الدعوة إلى فرض الحماية الجنائية من مخاطر استخدام شبكة الإنترنت.

وتنقسم الجرائم المالية التي تتم عبر شبكة الإنترنت إلى:

- جرائم السرقة والنصب أو الاحتيال.

- جرائم التجارة الإلكترونية.

- جرائم غسل الأموال والمخدرات.

أ- جرائم غسل الأموال:

مع نهاية القرن العشرين برزت ظاهرة غسل الأموال عبر الإنترنت لتشكل معضلة كبيرة للنظم القانونية المعاصرة، ولعل السبب الرئيسي في استجلاء هذه الظاهرة هي المدفوعات الافتراضية (Cyber- payment).

وغسل الأموال هو عبارة عن معالجة لمصدر الدخل الأول أو الأساسي غير المشروع (الناجم عن جريمة) بالقيام بمجموعة تحركات اقتصادية مشروعة تؤدي إلى طبع الأموال غير المشروع المصدر بطابع المشروعية وبطريقة لا يمكن بمقتضاها التعرف على المصدر الأصلي (غير المشروع).

ويعتبر غسل الأموال من الصور الحديثة للجرائم الاقتصادية التي كثر الحديث عنها في الآونة الأخيرة. وهو ظاهرة ترتبط بالجريمة المنظمة وعلى الأخص بجرائم الاتجار بالمخدرات والإرهاب وتهريب الأسلحة والرقيق الأبيض والغش والتزييف والفساد السياسي والمالي، كما تتصل بالبنوك والمؤسسات المالية الأخرى لما توفره عملياتها من قنوات تستخدم في غسل الأموال غير النظيفة.

وهي بذلك ظاهرة إجرامية ومشكلة عالمية، وهذا ما أدى بالعديد من الدول إلى تجريمها ومكافحتها وذلك من خلال وضع تشريعات خاصة بها.

وكما سبق ذكره أعلاه، فإن هذه الظاهرة الإجرامية قد تطورت مع ظهور شبكة الإنترنت، واجتاحت العالم بأكمله، ذلك لكون تلك الشبكة

تمثل الوسيلة الفعالة والمسهلة لعمليات تبييض الأموال، وهذا ما جعل الأمر أكثر صعوبة بالنسبة للجهات المعنية في متابعتها للمتعاملين عبر الشبكة وتحديد هويتهم أو جمع أية معلومات عنهم، ويرجع السبب في ذلك إلى:

- أن شروط التعامل عبر الشبكة الدولية لا تتطلب إجراءات معقدة، إنما فقط تدوين الاسم ورقم بطاقة الائتمان الخاصة بالمتعامل.

- أضف إلى ذلك فإن النقود الإلكترونية قد مكنت المتعاملين من تحويل مبالغ طائلة من دولة إلى أخرى بسهولة ودون مخاطر.

بـ جرائم المخدرات:

إلى جانب الجرائم السابق ذكرها والتي ترتكب عبر شبكة الإنترنت، هناك جريمة أخرى أكثر خطورة تهدد جميع فئات المجتمع هي جرائم المخدرات، إذ أضحت الإنترنت قناة اتصالية ممتازة ومجالاً رحباً للتعامل غير المشروع لمستهلكي المخدرات والمؤثرات العقلية بشكل أكثر أمناً للمروج والمدمن أو المعتمد على المخدرات والمؤثرات العقلية بشكل أكثر أمناً للمروج والمدمن أو المعتمد على المخدرات والمؤثرات العقلية، وهذا ما أدى إلى قيام عدة منظمات غير مشروعة تستخدم الإنترنت كوسيلة للترويج غير المشروع للمخدرات والمثرات العقلية سواءً على المستوى المحلي أو الإقليمي أو الدولي. بل أكثر من ذلك أصبحت هناك مواقع تبين وتشرح التدريب على زراعة المخدرات وطرائق وعمليات تحويلها خطوة

بخطوة وكذلك كيفية التعاطي لأول مرة والجرعات والمدة بين الجرعة والأخرى.

وهذا ما نجده في أحد المواقع الإنجليزية، والتي ينشر فيها الاتجار غير المشروع بالمخدرات والمؤثرات العقلية عبر الإنترنت مثل الاتجار بـ Cannabios seeds and derivatives وكذا بعقار ethylemedioxyme thamphamine MDMA والمعروف في التداول باسم ecstasy وكذا الكوكايين والهيروين.

وتجدر الإشارة إلى أن أكثر الدول التي تنتشر فيها حركة الاتجار بالمخدرات والمؤثرات العقلية عبر الإنترنت هي هولندا وسويسرا.

ولقد جرمت الدول هذه الأفعال وأوردت عليها عقوبات ومنها: مشروع قانون تعديل قانون المخدرات والمؤثرات العقلية لسنة ١٩٩٠ بما يتوافق ونظم تقنية المعلومات.

ج- الجرائم المتعلقة بالتجارة الإلكترونية:

إن التجارة الإلكترونية هي خدمة من الخدمات التي تقدمها شبكة الشبكات، إلا أنها وبالرغم من ذلك قد واجهت مصاعب ومعوقات قانونية جعلتها عرضة للاعتداءات الإجرامية، ومن أبرز تلك الجرائم:

١- الجرائم المتعلقة بتداول البيانات الخاصة بالتجارة الإلكترونية والمتمثلة في جريمة التعامل في البيانات بدون ترخيص، وجريمة انتهاك سرية وخصوصية البيانات، وجريمة التصريح عمداً بمعطيات خاطئة.

٢- والجرائم المتعلقة بمضمون عملية التجارة الإلكترونية والمتمثلة في جرائم الاعتداء على التوقيع الإلكتروني وجريمة استغلال ضعف أو جهل المتعامل في البيع الإلكتروني وجريمة التهريب الضريبي[١].

د- جرائم السرقة والنصب أو الاحتيال عبر الإنترنت:

بعد هذا النوع من الجرائم واسع الانتشار عبر الإنترنت، وذلك بسبب مجهولية المصدر بالنسبة إلى مستخدمي هذه الشبكة، فضلاً على عدم توفر سبل الحماية الكافية للحد من تلك الجرائم.

ولعل أشهر صور النصب والاحتيال والسرقة عبر الإنترنت هي صورة النصب ببطاقات الائتمان، والذي يكون إما من حاملها الشرعي أو من الغير.

وإن من بين الوسائل المستخدمة في تلك الجرائم عبر الإنترنت هي وسيلة البريد الإلكتروني، إذ يستعمل لإرسال ما يسمى بالقائمة القذرة وكذا عبر مزودات الإنترنت.

وإضافة إلى الجرائم السابقة فإنه يرتكب عبر شبكة الإنترنت جرائم الاعتداء على الملكية الفكرية وذلك عن طريق العدوان على حقوق النسخ وكذا عن طريق العدوان على برمجيات الحاسوب وكذا العدوان على براءات الاختراع، ولقد جرمت عدة قوانين هذه الاعتداءات ومنها القانون المصري لحق المؤلف.

---

(١) لمزيد من التفاصيل أنظر د/ هدى حامد قشقوش: الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ٣٦، وما بعدها.

هذا من جهة، ومن جهة أخرى ظهرت وخصوصاً في الآونة الأخيرة ظاهرة الإرهاب الإلكتروني عبر الإنترنت، مما جعل المشكلة مستعصية. ومن أمثلة ذلك ما حصل في مصر في الآونة الأخيرة وبالضبط في حادثة الأزهر، عندما اهتزت مصر على انفجار قنبلة وضعها طالب في كلية الهندسة والذي حصل على معلومات عن كيفية صنع القنبلة من خلال الإنترنت.

آلية ارتكاب الجرائم عبر الإنترنت:

إن الجرائم المرتكبة عبر الإنترنت تقوم أساساً على التلاعب بالبيانات والمعلومات والبرامج فيما عدا بعض الحالات[1]، ويتم ذلك بالقيام بالمعالجة الآلية للبيانات. بمحوها أو تعديلها أو تشويهها أو إلغائها أو تحويل مجراها. ولعل الصورة الغالبة لتحقيق غاية المجرم المعلوماتي في نطاق شبكة الإنترنت تتمثل في فعل الدخول غير المشروع unauthorized access إلى النظام المعلوماتي informatice System أو البقاء فيه بدون إذن – وهو ما يعاقب عليه في التشريعات المتقدمة – ومن ثم قيام الجاني بارتكاب فعله الذي يكون مجرماً بنصوص عقابية، أو لا يكون كذلك.

ويخلو التشريعان العقابيان الأردني والمصري- حتى لحظة إعداد الدراسة- من أية نصوص تجرم أوتخطر فعل الدخول غير المشروع إلى

(1) محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة عمان ٢٠٠٤ ص ١٩٢.

النظام المعلوماتي أو البقاء فيه بدون إذن؛ سواء كان هذا الفعل بقصد ارتكاب أية جريمة أم لا.

وحتى نعرض بصورة واضحة لآلية ارتكاب الجريمة عبر الإنترنت، ارتأينا عرض صورة هذه الجريمة في التشريع الفدرالي الأمريكي، والتشريع الإنجليزي، والتشريع الفرنسي باعتبارها إحدى التشريعات التي جرمت إساءة استخدام الحاسب الآلي وشبكاته العامة أو الخاصة.

أولا. جريمة الدخول غير المشروع إلى أنظمة المعلوماتية في التشريع الأمريكي:

كفل المشرع الأمريكي حماية الأنظمة المعلوماتية من أن تكون محلاً للاعتداء أو وسيلة له بتشريعات متعاقبة، توجها بإصدار قانون الاحتيال وإساءة استخدام الكمبيوتر (C F A A) عام ١٩٩٦.

وحظر المشرع الفدرالي فعل الدخول غير المشروع إلى النظام المعلوماتي في (١٠٣٠) من ذات القانون، وهي متجهة بشكل كبير إلى حماية الحكومة الفدرالية، بالإضافة إلى الأموال وكمبيوترات المؤسسات الطبية.

وتعاقب المادة ١٨ . S. c .u. s ١٠٣٠a)) كل من:

١-يدخل عمداً إلى جهاز حاسوب بدون تصريح، أو يتجاوز التصريح الممنوح له ويحصل بأية وسيلة على معلومات تقررت من قبل حكومة الولايات المتحدة بناء على أمر تنفيذي أو تشريع برلماني يتطلب الحماية ضد الإفشاء غير المخول له لأسباب تتعلق بالدفاع الوطني أو العلاقات

الأجنبية، أو أية معلومات محظورة كما هي مبينة في الفقرة (y) من المادة (١١) من قانون الطاقة الذرية لسنة ١٩٥٤، إذا توافر الاعتقاد بأن هذه المعلومات التي تم الوصول إليها يمكن استعمالها لإيذاء الولايات المتحدة الأمريكية، أو بنقلها عمداً لفائدة أية دولة أجنبية، أو يسلم أو ينقل أو يتسبب في نقلها أو تسليمها لأي شخص غير مخول بتلقيها، أو أن يحتفظ عن قصد بذات الشيء أو يخفق في تسليمه إلى مأمور أو موظف الولايات المتحدة المخول باستلامها أو تلقيها.

٢- يصل عمداً إلى حاسوب بدون ترخيص، أو يتجاوز الترخيص الممنوح له بقصد الحصول على:

أ) معلومات واردة في سجل مالي لمؤسسة مالية أو لمصدر البطاقة كما هو مبين في المادة ١٦٠٢ (N) من الفصل ١٥، أو أن تكون المعلومات مشتمل عليها في ملف وكالة مستهلك يرفع تقريراً عن مستهلكين.

ب) معلومات من أي مؤسسة أو وكالة تابعة للولايات المتحدة.

جـ) معلومات من أي حاسوب محمي، إذا تعلق بمحتوى اتصالات خارجية أو بين الولايات.

٣- يصل عمداً بدون ترخيص لأي حاسوب غير عام يخص إحدى إدارات أو وكالات الولايات المتحدة، إذا كان مخصصاً بشكل وحيد لاستعمال حكومة الولايات المتحدة، أو في حالة إذا لم يكن الحاسوب

مخصصاً بشكل وحيد لاستعمال حكومة الولايات المتحدة، أو في حالة إذا لم يكن الحاسوب مخصصاً بشكل وحيد لهذا الاستعمال وكان قد استعمل من قبل أو لأجل حكومة الولايات المتحدة الأمريكية، وكان ذلك التصرف مؤثراً على ذلك الاستعمال من قبل أو لأجل حكومة الولايات المتحدة.

٤- يصل عن معرفة وبقصد الغش إلى حاسوب محمي، بدون ترخيص أو بتجاوز الترخيص الممنوح له وبأية وسيلة تسهل نية الغش ويحصل على أي شيء ذا قيمة، ما لم يكن موضوع الغش والشيء المتحصل عليه يتوقف فقط على استخدام الحاسوب، وأن قيمة هذا الاستخدام لا تزيد عن (٥٠٠٠) دولار خلال فترة سنة واحدة.

٥- كل من:

(أ) يسبب عن معرفة بث برنامج أو معلومات أو شيفرة (رمز) أو أمر ويسبب ضرراً عن قصد كنتيجة لهذا التصرف، وبدون ترخيص لكمبيوتر محمي.

(ب) يصل متعمداً لكمبيوتر محمي بدون ترخيص وكنتيجة لهذا التصرف يسبب ضرراً نتيجة إهمال.

(جـ) يصل متعمداً لكمبيوتر محمي –بدون تفويض – وكنتيجة لهذا السلوك يسبب ضرراً.

٦- كل من يسلب باحتيال عن قصد ومعرفة، تجارة أو مقايضة (كما هي مبينة في المادة ١٠٢٩) في أي كلمة سر أو معلومات مشابهة يمكن من خلالها الوصول للكمبيوتر بدون تفويض إذا:

أ- كانت تلك التجارة غير المشروعة أو المقايضة تؤثر على التجارة الخارجية أو التجارة بين الولايات.

ب- كان هذا الكمبيوتر مستعملاً من قبل أو لأجل حكومة الولايات المتحدة.

٧- كل من يقصد ابتزاز أية نقود أو شيء آخر ذا قيمة من أي شخص أو شركة أو جمعية أو مؤسسة تربوية أو مؤسسة مالية أو هيئة حكومية أو أي كيان قانوني آخر. وكذلك نقل أو بث أي اتصال في التجارة الخارجية أو التجارة بين الدول؛ بحيث يكون مستعملاً أي تهديد من شأنه أن يسبب ضرراً لكمبيوتر محمي. وقد أفرد المشرع الأمريكي عقوبات مشددة للجرائم المشار إليها والشروع في ارتكابها، تتراوح ما بين الغرامة أو الحبس حتى عشر سنوات أو بكلتا العقوبتين معاً.

وقد انتقد هذا القانون؛ لانظوائه على الكثير من الغموض والقصور؛ بحيث يمكن للمجرمين تلافي تطبيق القانون عليهم باستخدام حاسبات وشبكات من خارج الولايات المتحدة، والدخول إلى أنظمة الحاسبات داخل الولايات والاعتداء عليها، أو استخدام هذه الأنظمة ذاتها عن بعد للاعتداء على حاسبات تقع في دول أخرى.

ثانياً- جريمة الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه دون صلاحية في التشريع الإنجليزي:

كفل المشرع الإنجليزي حماية البيانات المخزنة في الحواسيب من الاعتداء عليها، أو إساءة استخدامها، بإصداره لقانون إساءة استخدام الكمبيوتر عام ١٩٩٠ computer Misuse A C T.

وتتعلق المادة الأولى من القانون – المشار إليه – بتجريم فعل الدخول غير المشروع إلى النظام المعلوماتي إذا قصد الجاني تدبير الدخول إلى أي برنامج أو بيانات موضوعة في أي كمبيوتر، مع جعله يؤدي أية وظيفة لتحقيق الدخول.

وكذلك يعاقب المشرع على أي دخول يقصد به تدبير غير مشروع؛ إذا توافر للجاني العلم بعدم مشروعية الدخول وقت تغييره لوظيفة الكمبيوتر، أو إذا اتجهت نيته للاعتداء على تفاصيل أي برنامج أو بيانات في أي كمبيوتر محدد أو غير محدد.

وتتعلق المادة الثانية من ذات القانون بتجريم فعل الدخول غير المشروع لارتكاب أية جريمة يعاقب عليها النص، أو لتسهيل ارتكاب الجريمة، سواء للجاني نفسه أو لأي شخص آخر.

أما المادة الثالثة، فتعاقب على الغاية من فعل الدخول إذا تعمد الجاني تعديل modification محتوى أي كمبيوتر. فيعاقب على إتلاف عمل

الكمبيوتر، أو إعاقة الدخول لأي برنامج أو بيانات موضوعة في أي كمبيوتر، أو إتلاف عمل أي برنامج أو صحة أي بيانات.

وكذلك يعاقب الجاني متى اتجهت نيته بصورة مباشرة إلى أي كمبيوتر شخصي، أو أي برنامج خاص أو بيانات من نوع خاص أو أي تعديل من نوع خاص، متى توافرت لديه المعرفة السابقة والمتمثلة بأي تعديل يقصده الجاني كي يتسبب بفعله غير المشروع.

ثالثا: جريمة الدخول غير المشروع أو البقاء دون صلاحية داخل النظام المعلوماتي في التشريع الفرنسي.

تناول المشرع الفرنسي مجموعة من الجرائم التي تقع على أنظمة معالجة البيانات في المواد من (٣/ ٣٢٣)- (١/ ٣٢٣).

وتتعلق المادة (١/ ٣٢٣) بتجريم الدخول غير المشروع إلى النظام المعلوماتي، أو البقاء فيه بطريقة غير مشروعة؛ حيث نص المشرع على أن:

"الدخول أو البقاء – بطريق الغش- داخل كل أو جزء من نظام المعالجة الآلية للمعطيات، يعاقب عليه بالحبس لمدة سنة، وغرامة مقدارها (١٠٠,٠٠٠) فرنك. فإذا نجم عن هذا الدخول محو أو تعديل في المعطيات المختزنة فيه، أو إتلاف تشغيل هذا النظام، تكون العقوبة: الحبس لمدة سنتين، وغرامة مقدارها (٢٠٠,٠٠٠) فرنك".

ومن استعراض النصوص التشريعية الخاصة بجريمة الدخول إلى النظام المعلوماتي أو البقاء فيه في القانون الأمريكي والإنجليزي والفرنسي، نجد أن

هنالك فرقاً بين فعل الدخول غير المشروع من ناحية، وبين البقاء دون صلاحية من ناحية أخرى؛ إذ أن البقاء داخل النظام المعلوماتي قد يكون نتيجة دخول مشروع أو نتيجة خطأ أثناء التجوال في النظام المعلوماتي، وهما في كلا الحالتين يقضيان ضرورة توافر القصد الجنائي.

وبعد فعل الدخول غير المشروع إلى النظام المعلوماتي من الجرائم الوقتية، ولا يلزم توافر صفة خاصة في مرتكبيها، أو الغاية من ارتكابها، حيث يستوي أن يكون الفاعل من الخبراء أو من الأفراد العاديين، ويستوي كذلك أن يكون الدخول بهدف ارتكاب فعل غير مشروع أو لمجرد التسلية وحب الاستطلاع.

وأيضاً تعد من قبيل الجرائم الشكلية، التي يكتمل شكلها القانوني بمجرد تحقق السلوك الإجرامي، دون تطلب عنصر آخر في الركن المادي للجريمة.

ويتحقق فعل البقاء بمجرد التواجد المعنوي أو الإلكتروني داخل نظام المعالجة الآلية للمعلومات بدون إذن أو تصريح بذلك، بما يؤدي إلى اختلاس وقت النظام، متخذاً بذلك صورة الجريمة المستمرة.

وكذلك تتحقق الجريمة سواء كان الدخول إلى النظام المعلوماتي بطريق الخطأ أو الصدفة، أو تم الدخول والبقاء في النظام بشكل مشروع، ولكن تجاوز الفاعل الوقت المحدد والمسموح به، أو الغرض الأساسي المصرح به للدخول خلافاً لإرادة صاحب الشأن المسيطر على هذا النظام.

ولكن هل يشترط لقيام جريمة الدخول غير المشروع أن يكون النظام المعلوماتي محمياً بتجهيزات أمنية إلكترونية تمتع الوصول إلى النظام كجدران النار Fiar wall أو ضرورة توافر كلمة مرور passwords أو وجود جهاز إنذار لمنع الدخول غير المشروع؟

ذهب الرأي الغالب – وهو ما نؤيده – إلى عدم ضرورة وجود نظام أمني إلكتروني لكي تقوم الجريمة، وطبقاً لهذا الرأي فإن نظام الأمن لا يكون له إلا دوراً واحداً، وهو إثبات سوء نية من قام بانتهاك النظام والدخول بطريقة غير مشروعة، ولكن القصد الجنائي يمكن إثباته بطريقة أخرى. ويستند أنصار هذا الرأي إلى المبادئ المستقرة في القانون الجنائي بعدم جواز تقييد النص المطلق أو تخصيص النص العام، طالما لم ينص المشرع على ذلك. فعدم ذكر شرط الحماية الفنية تعني أن المشرع أراد استبعاد هذا الشرط صراحة.

ويرى البعض الآخر من الفقه[1]، ضرورة وجود نظام أمني لتجريم فعل الدخول إلى النظام المعلوماتي، إذ يقتضي المنطق والعدالة توافر مثل هذا الشرط. فوجود نظام حماية يمكن اعتباره التزاماً مفروضاً بنص القانون على كل من يقوم بإدارة نظام معلوماتي؛ ومن ثم يفترض أن تقع الجريمة على نظام لا يجوز سوى لأشخاص محددة الدخول إليه.

(1) GROZE (H). ety. Bismuth, droit de L,informatique, La responsabilite penale neede L,informatique, no ١٠.

وقد ثار تساؤل بين الفقه فيما إذا كان فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن يشكل تعداداً مادياً للجرائم أم إنه يشكل جريمة واحدة؟

فذهب البعض إلى القول بأننا أمام جريمة واحدة، نظراً لأن الجاني أراد بالدخول غير المشروع البقاء داخل النظام.

وذهب البعض الآخر إلى تحقق الاجتماع المادي للجرائم بين جريمتي الدخول غير المشروع إلى النظام المعلوماتي والبقاء فيه مدة من الوقت. ولكن ثار الخلاف فيما بينهم حول تحديد الفترة التي تنتهي فيها جريمة الدخول لتبدأ بعدها جريمة البقاء غير المشروع.

الفصل الثالث

الطبيعة القانونية لجرائم الحاسوب والإنترنت

تختلف جريمة الإنترنت عن الجريمة التقليدية التي تتسم بطابع خاص هو أنها جرائم عبارة للحدود فهي تتم داخل الدولة ويكون تأثيرها منحصراً في تلك الدولة وإنما تلك الجرائم تركتب عبر عدد من الدول لتتم في دولة أخرى وتكون آثارها ممتدة لتصل إلى عدد غير محدود من الدول. كما أن هذه الجريمة وفي جميع الأحوال يكون الحاسب الآلي هو أداة ارتكاب الجريمة وأن مرتكبها هو شخص ذو خبرة فائقة في مجال الحاسب الآلي ومحل هذه الجريمة هو دائماً المعطيات إما بذاتها أو بما تمثله.

تقوم جرائم الحاسوب وترتكز على المحاور التالية [1]:

١. أن الاعتداء على الكيانات المالية للحاسوب يخرج عن نطاق جرائم الحاسوب: لأن هذه الكيانات المادية محل صالح لتطبيق نصوص التجريم التقليدية الناظمة للجرائم الواقعة على الأموال.

٢. أن محل جرائم الحاسوب هو دائماً المعطيات "أما بذاتها أو بما تمثله، وقد تكون هذه المعطيات مخزنة داخل النظام أو على أحد وسائط التخزين أو تكون في طور النقل والتبادل ضمن وسائل الاتصال المدمجة مع نظام الحوسبة.

---

(١) د. علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، اليازوري، عمان ٢٠٠٩ ص ٣٥، ٤٢.

٣. أن المصلحة محل الحماية في ميدان "جرائم الحاسوب" وهي الحق في المعلومات ككيان معنوي ذو قيمة اقتصادية عالية.

وعليه ظاهرة "جرائم الحاسوب" يمكن تعريفها وفق التحديد المتقدم بأنها: "الأفعال غير المشروعة المرتبطة بنظم الحواسيب، أما تعريف جريمة الحاسوب فإنها "سلوك غير مشروع معاقب عليه قانوناً صادر عن إرادة جرميه لمعطيات الحاسوب"، فالسلوك شامل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك ضمير مشروع باعتبار أن المشروعية تنفي عن الفعل الصفة الجرمية، ومعاقب عليه قانوناً لأن أسباغ الصفة الإجرامية لا يتحقق في ميدان التشريع العقابي إلا بإرادة المشرع ومن خلال النص على ذلك، حتى ولو كان السلوك مخالفاً للأخلاق[١].

ومحل جريمة الحاسوب هو دائماً المعطيات بدلالتها الواسعة (البيانات المدخلة والمخرجة والمخزنة والبرامج على أنواعها)، وأما الحاسوب فهو النظام التقني بمفهومه القائم على المزاوجة بين تقنيات الحوسبة والاتصالات أو ما يعرف "بالتقنية العالية".

ونظراً لحداثة عهد اللجوء إلى الحاسب الآلي خصوصاً في الدول النامية ومنها الأردن وجدت المشاكل القانونية بوجه عام وتلك تدخل تحت طائلة قانون العقوبات بشكل خاص ذلك أنه لا يوجد في الأردن تشريع يضع الحلول لتلك المشاكل فضلاً عن أنها لم تطرح على القضاء ليقول فيها

---

(١) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول ٢٠٠٤، ط٣، من ١- ٣ مايو ٢٠٠٠م.

كلمته، ومما يزيد الأمر تعقيداً أن الفقه القانوني الأردني لم يتناولها بالشرح والتحليل بشكل مسبق إذ أن الفقه يجري جاهداً وراء الاكتشافات العلمية الحديثة محاولاً وضع الحلول القانونية اللازمة لما ينشأ عنها من ظواهر إجرامية بعد أن تنشأ وتستقر ويتكشف عن استخدامها الكثير من الظواهر الإجرامية الأمر الذي يضفي أهمية بالغة على هذا الموضوع.

إن التنوع في الجرائم الناشئة عن استخدام الإنترنت يجعل التمييز قائماً بين جرائم الحاسوب وبين جرائم الإنترنت فليست كل جريمة ناشئة عن استخدام الإنترنت تعد بالضرورة من جرائم الإنترنت بل إن هناك من الجرائم ما يمكن وصفه بالجرائم التي كانت وسيلتها الإنترنت ويقضي مثل هذا الأمر تجريم الوسيلة في حين أنها بالطبيعة مشروعة.

وتعرف الوسيلة بأنها الطريقة التي يتم استخدامها من قبل مرتكب الجريمة لمباشرة السلوك المادي أو النشاط الإجرامي ولا تعد الوسيلة نشاطاً مادياً وإنما يقرر القانون لزوم وجودها لكي يمكن إحداث تطابق بين النموذج الإجرامي وبين الواقعة ومن ثم استحقاق العقاب والإلزام بأن يعترف القانون بالوسيلة للقول بلزوم توافرها، وقرار المشرع بلزوم توافر وسيلة معينة يعني في القانون إضافة ظرف مشدد أو جعل العقوبة مشددة أو يجعل من اللازم اتخاذ تدابير معينة حيال مرتكب الجريمة.

والإنترنت لا يمكن أن يكون وسيلة إلى ارتكاب جرائم كونها بالأصل من الأنشطة المشروعة ذلك أن الإنترنت لا يمكن حيازته واستخدامه بشكل ذاتي فهي ليست شيء ملموس وإنما سلوك تقني بالضرورة يحتاج لوسائل

أخرى للقول بتوافرها. حيث تحتاج إلى الحاسوب ومكوناته على أن تكون مجموع الحواسيب متصلة فيما بينها مكونة شبكة ثم شبكات ثم ربط ذلك بحركة الاتصالات ونظم المعلومات يخلق بالنهاية بيئة معلوماتية كاملة حتى يمكن القول بتوافر الإنترنت، فالإنترنت ليست بيئة غير مشروعة أصلاً إنما يمكن ارتكاب أعمال إجرامية فيها أو من خلالها أو عبرها.

أركان جريمة الإنترنت:

يتطلب المشرع للقول بقيام جريمة ما توافر الركن المادي والركن المعنوي لها، أما الركن المادي فيتكون من عناصره الثلاثة السلوك المادي والنتيجة الإجرامية والعلاقة السببية ما بينهما، أما الركن المعنوي بعنصريه العلم والإرادة.

الركن المادي في جرائم الإنترنت:

السلوك الإجرامي: إن ارتكاب الجريمة عبر الإنترنت يحتاج إلى منطق تقني يتمثل بسلوك مادي إيجابي مما يجعل الجريمة عبر الإنترنت ذات طابع موحد فهي تباشر من حيث السلوك أو النشاط المادي فيها بوصفه أحد عناصر الركن المادي يضاف إلى فلسفة الركن المادي فيها، تدارك هذا الأمر المشرع المقارن حين النص على جرائم يمكن أن ترتكب عبر الحاسوب ففي مثل هذه النصوص نجد المشرع يقرر صراحة عبارة" . . . إذا ارتكبت الجريمة باستخدام الحاسوب ..." أو عبارة "... باستخدام المعالجة الآلية

للبيانات..." ويكون بهذه الحالات المشرع مدركاً للقيمة الموحدة للشروع في ارتكاب جريمة عبر الإنترنت أو باستخدام الحاسوب المرتبط بالإنترنت.

ضرورة استخدام الآلة وسيطاً لارتكابها مما يجعل جرائم الإنترنت خاصة والحاسوب عامة من نوعية جرائم الوسيلة، وهذا الأمر غير مقبول لمشروعية هذا الوسيط المستخدم لارتكاب الجريمة وهو هنا الحاسوب أو الشبكة أو الخادم ... وهذه أدوات مشروعة بحسب الأصل.

من اللازم استخدام الحاسوب لكي يمكن ارتكاب الجريمة التي ترتبط بإمكانية استخدام ومدى تمتع الشخص بالتقنية الكافية في هذا الشأن لارتكاب الجريمة، وأن كل من الحاسوب والإنترنت يدخلان في طائلة المشروعية لا يمكن أن تقوم أي من الجرائم التي أشار إليها المشرع سوى باستخدامها وهذا يجعل مسألة استخدام الحاسوب والإنترنت جزءاً من النشاط المادي في الجرائم الناشئة عن استخدام أي من الحاسوب والإنترنت.

مما تقدم نرى أن النشاط المادي يبنى على العلاقة التقنية بين مرتكب جريمة الإنترنت وبين الآلة وفي كيفية تحديد حدوث السلوك الإجرامي باستخدام الإنترنت والحاسوب وجد المشرع الأمريكي أن استخدام الإنترنت ليس له هدف في ذاته فلا يستخدم الإنترنت لمجرد الاستخدام وإنما هو تحقق فوائد عظيمة في الوقت الذي يمكن أن تكون مهداً لارتكاب الجريمة أيضاً لذلك لم يمانع في تحديد طرائق السلوك الإجرامي بشكل

تفصيلي لكي يمكن القول بقيام النشاط الإجرامي بما يجعل هذا النص ينطبق مع مراعاة تحقيق النتيجة المشار إليها.

العلاقة السببية ما بين السلوك الإجرامي والنتيجة: وهي إسناد ماديات إلى مصدرها بشكل تسلسلي وهي من طبيعة مادية كأصل عام، فالعلاقة السببية هي علاقة مادية وليست علاقة قانونية والمشرع يعترف بها قانوناص صراحة أو ضمناً ولا يحيلها إلى الوصف القانوني بحيث تبرز كما لو كانت صلاحية في الإنسان لإحداث أمر ما فهي ليست مجرد علاقة أو رابطة زمنية لكونها عنصر رئيسي في الركن المادي للجريمة. والمبدأ العام الذي يحكم علاقة السببية أن الإنسان لا يسأل إلا عن النتائج التي يكون لنشاطه دخلاً في إحداثها فاستحقاق العقاب في القانون الجنائي رهن دائماً بقيام الرابطة السببية بين نشاط الجاني وبين الواقعة الإجرامية التي تستوجب العقاب وذلك في معنى علاقة السبب بالنتيجة أو عللة بالمعلوم لأنه ما دام الجاني يعاقب على النتيجة التي أدى إليها فعله فإنه ينبغي لمسائلته أن تكون هناك رابطة بين ماديات الفعل وبين النتيجة الإجرامية.

ففي جريمة انتهاك الحق في الخصوصية عبر الإنترنت يجب أن يكون هناك دخول على الإنترنت باستخدام حاسوب عامل والقيام باختراق الخوادم المختلفة في مسارها ثم بعد ذلك التعدي على خصوصية موضع ما أو أن يقوم بإعداد موقع ما ثم بعد ذلك يبث عليه في إحدى صفحاته صور ذات خصوصية لأشخاص مشهورين... الخ.

وتكون علاقة السببية قائمة بمجرد ثبوت الضرر في مجرد البث حيث؛ لأن علاقة السببية في الجريمة المتعلقة بحيازة صور دعارة الأطفال في حاسوب مضيف تتحقق بقيام رابطة بين العمل على إيجاد وحيازة هذه الصور في الحاسوب والإنترنت وبين الترويج أو العرض أو التداول ... الخ، والذي يحقق ضرراً مباشراً بالأطفال والقاصرين لكون ذلك يؤدي إلى انتهاك حقوق الأطفال المقررة. وكذلك القيام بإعداد الحاسوب وتهيئة الالتقاط مثل هذه الصور أو إعداد قرص صلب خاص بهذه الصور أو الأفلام وكذلك القيام بتخصيص برمجيات في القرص الصلب الخاص لكي يكون معد لعرضها. فكل هذه الأفعال يجب لكي تتم أن تقوم علاقة سببية بين مباشرة النشاط المادي فيها وبين النتيجة المقررة هنا التي تبرز في ظهور النتيجة حال كونها كاملة أو الشروع في ارتكابها شرط الخيبة أو وقف ارتكابها بسبب لا دخل لإرادة الجاني فيه.

النتيجة الإجرامية:

وتعني النتيجة الإجرامية ذلك التغيير الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي والذي يعتد به القانون فيجعله عنصر من العناصر المكونة لجريمة معينة فلا تقع الجريمة تامة إلا بتوافره مع بقية العناصر الأخرى. فالنتيجة الإجرامية هي إحدى عناصر الركن المادي في الجريمة.

تثير النتيجة الإجرامية في جرائم الإنترنت مشاكل متعددة حيث مسألة مكان وزمان تحقق النتيجة الإجرامية، فهل تعد هذه الجريمة مرتكبة سلوكاً ونتيجة في العالم الافتراضي أو أن هناك امتداداً أو أن هناك امتداداً للنتيجة

لكي يتحقق منتهاها في العالم المادي بينما يتحقق أولها في العالم الافتراضي ومن ثم يكون هناك امتداد في النتيجة من العالم الافتراضي إلى المادي؟ مع الأخذ في الاعتبار أن هناك من الجرائم التي يكون لها وجود سواء عبر الإنترنت أم بمعنى أكثر وضوحاً هي من ضمن جرائم التقنية التي لا يمتد أثرها إلى العالم المادي ويشمل ذلك بالطبع صعوبة اكتشافها وإقامة الدليل على ارتكابها ويتجه الفقه المقارن إلى محاولة إرساء رؤية الإفساد أو الإعاقة لكي تكون المحصلة في العمل الإجرامي ومن ثم فإن النهج هنا ينطلق نحو الاعتداء بالضرر في تقدير قيام المسئولية الجنائية حيث ينبغي وفقاً لهذه النظرية الأخذ في الاعتبار ضرورة أن تكون كل علاقة وهمية على تعطيل الخدمات التي يقدمها الحاسوب للمستخدم الشرعي، كل ذلك يؤدي بالضرورة إلى الاهتمام بالنتيجة الإجرامية على حساب النشاط المادي للجريمة من حيث كونه الخلاصة النهائية التي ما تحرك المشرع المقارن إلا بسببها.

ويواجه تحديد الخطر أو الضرر بوصفه نتيجة إجرامية عبر الإنترنت العديد من المشاكل كالمتعلقة بجرائم العدوان الفيروسي إذ تثير هذه النوعية من الجرائم مشكلة تحديد الضرر أو الخطر وهي من الصعوبات التي تواجه الفكر القانوني المعاصر في هذا المجال خاصة إذا كان المشرع يتطلب تحقق نتيجة معينة، أما أثر النتيجة الإجرامية ذا البعد الدولي سواء في شكل امتداد الضرر أو الخطر إلى ما يتجاوز الحدود الإقليمية التي وضع فيها

السلوك وبعض النتيجة ويأخذ هذا الامتداد شكل العدوان المحدد على مصلحة قائمة ومشروعة في دولة أو دول متعددة.

إن البحث في العلاقة بين النشاط وبين النتيجة الإجرامية يجعل منطق بناء النتيجة الإجرامية في جرائم الإنترنت من الصعوبة بمكان، ذلك أنه كيف يمكننا القول أن النشاط الإجرامي المرتكب عبر الإنترنت أدى بالضرورة إلى النتيجة المقررة في الجرائم التي يتطلب فيها المشرع حدوث نتيجة معينة فالمنطق هنا يسعى بنا إلى التأكيد على أن الجريمة عبر الإنترنت ككل مح لجدل إذ أن التغيير الحادث في العالم المادي والمؤدي إلى التقرير بوجود جريمة يظل جزاءاً منه إن لم يكن كله قد حدث في العالم الافتراضي ومن ثم يلزم الحال هنا التعرض لتأثير منطق العالم الافتراضي في العالم المادي لكي يمكن أن تتعرف على نوعية هذا التأثير الذي اعترف فيه المشرع المقارن.

إن كل جريمة تحدث باستخدام الإنترنت إنما تحدث كلها أو بعضها حسب الأحوال في العالم الافتراضي وإذا كان النشاط المادي يحدث كله في العالم الافتراضي بما يستتبع ذلك علاقة السببية كذلك فإن النتيجة الإجرامية لها كان منفصلاً هنا حيث أنها تلك الجزئية التي تحدث بشكل انقسامي ما بين حدوثها في العالم المادي جزئياً أم كلياً، وذلك أم استفهامي يقودنا حتماً إلى التقرير بالاهتمام بالنتيجة التي قررها المشرع تحديداً في نموذجه الإجرامي دون تمام التي تحدث تقنياً، فإذا تطلب المشرع القتل في جريمة اختراق قواعد بيانات المستشفيات مثلاً بقصد ارتكاب جريمة قتل

فإن تمام النتيجة تقنياً هو اكتمال تغيير بيانات الدواء ويلزم هنا لكي يمكن القول بتمام الجريمة على وفق تطلب النموذج القانوني للجريمة أن يتم إعطاء المريض الدواء الخاطئ فعلاً فإذا لم يتم إعطاء المريض الدواء الخاطئ فإن الجريمة مادياً تضل في حالة شروع شكلي ومن الناحية العملية فإن النتيجة الإجرامية التي يتم ارتكاب نشاط إجرامي ما عبر الإنترنت بقصد الوصول إليها من الصعوبة بمكان إثبات القصد الإجرامي فيها توصلا إلى تحديد تسمية معينة للجريمة وذلك من الأمور التي تجعل الإثبات هنا قاصراً على التوصل إلى تحديدها بالدقة المتطلبة فقد يكتفي في مثل الجريمة السالفة بالاستعاضة عن جريمة الشروع بالقتل بجريمة تغيير أو تعديل بيانات إسمية أو العدوان على بيانات مرضية بما يشكل في النهاية عدوان على الحق في الخصوصية. سوف تظل مشكلة النتيجة الإجرامية في الجرائم الناشئة عن استخدام الإنترنت محلاً لجدل قانوني يجب أن يتم التطرق إليه من منطق التزاوج بين العالم المادي ونظيره الافتراضي بحيث يكون بناء معدلات الجريمة حين هيكلة ركنها المادي بالأخذ في الاعتبار هذا التزاوج.

الركن المعنوي في جرائم الإنترنت:

ويعني الجاني أو المجرم تحديداً فالركن المعنوي هو المسلك الذهني والنفسي للجاني باعتباره محور القانون الجنائي ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسئولية الجنائية من إسناد وإذناب مع إقرار حق الدولة في العقاب الذي يبنى على هذه المقومات، ويعرف الركن المعنوي بأنه العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها وهذه

العلاقة هي محل الإذناب في معنى استحقاق العقاب ومن ثم يوجه إليها لوم القانون وعقابه. واجهت جرائم الحاسوب والإنترنت مشكلات تتعلق بمدى تطلب القصد الجنائي فيها وبشكل يمكن أن يحقق غرض المشرع في هيكلة الإدانة.

إن تفهم موقف الركن المعنوي في جرائم الإنترنت يعد من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص العقابية التي يلزم تطبيقها إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع لذلك فإن اتجاه القضاء المقارن في تطلب العمد بالنسبة لجريمة الولوج فقط يعد من الموضوعات المنتقدة هنا، فالتمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام يعد تمييزاً دقيقاً.

لم يستقر القضاء الأمريكي على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الإنترنت من حيث تحديد ما إذا كانت تتطلب قصداً عام أم خاص فنجده لا يمانع في تطلب قصد جنائي خاص في جريمة التهديد إلا أنه يقرر من جديد أنه يستكفي بالقصد العام عن ذات الجريمة كما هو الشأن في جريمة التهديد بالبريد الإلكتروني وعبر المجموعات الإخبارية. والقصد العام فيها يتم استجلاء معالمه من النظرة الموضوعية إلى السلوك الشخصي من مجموعة الظروف المحيطة بالجريمة بما في ذلك فحص الحالة العقلية لمرتكب الجريمة.

أما القضاء الفرنسي فإن منطق سوء النية يكتسح النصوص إلى تطبق بشأن الإنترنت حتى أنه يخال أن هذه الجرائم لا يمكن أن تدخل حيز التطبيق ما لم يتوافر سوء النية في منطق القصد الخاص وإرادة الإضرار حيث اشترط قانون العقوبات الفرنسي سوء النية حين وجود عدوان على البريد الإلكتروني، كما ألزم تقنين البريد والاتصالات وزير الاتصالات الفرنسي بالسهر على مبدأ احترام سرة الاتصالات فالشرط الأساسي لتطبيق هذه النص مع الإلتزام بضرورة توافر سوء النية هو وجود عدوان على الحق في خصوصية الاتصالات بما يستدعي ذلك أن يكون هناك وسيلة اتصال تتمتع بهذه الخصوصية أولاً ومن ذلك البريد الإلكتروني حيث يعد من وسائل الاتصال الخاصة والتي تتطلب بالضرورة حماية قوية.

الفصل الرابع
الجوانب القانونية للإنترنت

بدأت التكنولوجيا تغزو كافة مناحي الحياة، اقتصادياً وطبياً وتعليمياً، وبدأت معظم دول العالم تعج بمراكز المعلومات والتي تسوق تجارة مستحدثة قوامها مجموعة من المعلومات الأمر الذي يدفع الأفراد للاستغناء عن كثير من التقليديات مثل الصحيفة اليومية والمجلات كما بدأنا نستغني عن النقود السائلة.

الوسيلة الحديثة قوامها استغلال شبكات متصلة حول المعمورة، تجعل من السهل جداً غزو هذه المواقع والاطلاع عليها من خلال استغلال الاتصالات عبر الأقمار الصناعية (Telecommunication parsotellite) ونقل الأخبار عبر الأثير. فأصبحت تشكل من العالم قرية صغيرة حيث بدأ التعاقد من مواطن بعيدة جداً دون أن يرتب ذلك إخلال بالأصول التقليدية للعقد.

إلا أن ذلك لا يمنع من وجوب توفر ترسانة خاصة من القوانين المنظمة لمثل هذه الأمور المستجدة [1].

شبكة المعلومات أو ما اصطلح على تسميتها بالإنترنت، ثورة علمية كبيرة استغلت بمجالين الخير والشر. فالخير لأهله والشر مجال بحثنا نتناول

([1]) أسامة أحمد المناعة وآخرون، جرائم الحاسب الآلي والإنترنت، دار وائل عمان ص ٢٠٠١ ص ٢٠٩- ٢١٥.

به جريمة الإنترنت والتي تتميز أنها عابر للدول غالباً، فيكون الفاعل بعيداً عن موطن الجريمة الأمر الذي يستوجب تحديد القانون الواجب التطبيق من حيث مكان وزمان ارتكابها، ويسوي الأمر أن نعرض لأهم الجرائم المتصور ارتكابها عبر هذه التقنية في مطلبين: المطلب الأول: الاختصاص القضائي.

المطلب الثاني: جرائم الإنترنت.

المطلب الأول: الاختصاص القضائي

هذا الوجه المشرق للإنترنت لم يمنع فئة أخرى شريرة أن تسيء استعمالها لغايات غير ودية، بهدف ارتكاب مجموعة من الجرائم تكون شبكة المعلومات وسيلة أو أداة لارتكابها وأداة لتصديرها، فلا تستغرب ارتكاب جرائم الانتحار وتجارة المخدرات وغيرها.

ولما تمتاز به هذه الجريمة من خصائص أهمها السرعة في ارتكابها والسرية الكبيرة من جهة، واتساع مسرح الجريمة من جهة أخرى، فالفاعل قد يكون في أقصى المعمورة، والنتيجة الجرمية تقابلها بالشق الآخر منها. فما هو القضاء صاحب الولاية؟ وما هو زمان ارتكابها؟.

إن ما يثير الأشكال في هذا المجال، أن الجريمة ليست موحدة عبر العالم ككل، فهناك من الدول لا تجرم مثل هذه الاعتداءات مما يجعلها مرتعاً لارتكابها اصطلح على تسميتها الجنة الرقمية، فمن هي المحكمة المختصة،

هل هي مكان إدخال البيانات؟ أم استخراجها؟ لقد انقسم الفقه في ذلك إلى ثلاث اتجاهات:

الاتجاه الأول:

ويرى أن أولى المحاكم بالاختصاص. محاكم دولة تحميل البيانات فهي مكان ارتكاب الجريمة، وهذا يساعد أكثر على جمع البيانات والأدلة – بالإضافة إلى أنه مكان واحد بعكس الاستقبال الذي يكون من دول عديدة. ويساعد في ذلك أن بنك المعلومات محل التحميل أكثر ثباتاً.

لكن يؤخذ على هذا الاتجاه عدة مآخذ أبرزها. أن بعض هذه الأفعال قد لا تجرم لدى دولة التحميل، مما يعود بنا إلى الجنة الرقمية. مما يساعد الفاعل بالتهرب من العقاب. بالإضافة إلى أن تحمي البيانات في إقليم أحد الدول قد يكون بشكل عارض، أثنار المرور بقطار أو باخرة ونحوهما.

الاتجاه الثاني:

يرى إعطاء الاختصاص لمكان النتيجة الجرمية، لتعدد دولة التحميل مما يعقد الاختصاص لأكثر من دولة، ويسبب ضياع المسئولية، كذلك إذا كانت دولة التحميل لا تعاقب على مثل هذه الأفعال، إلا أن هذا الاتجاه لم يسلم من النقد فيؤخذ عليه أنه لم يراع مصلحة المتهم بجره إلى أماكن بعيدة المحاكمة. مما يزيد في تكاليف التقاضي ويطيل في أمد الخصومة (١).

---

(١) د. عوض، محمد، مشكلات السياسة الجنائية المعاصرة من جرائم نظم المعلومات، بحث مقدم في المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣.

الاتجاه الثالث:

يرى أن الاختصاص ينعقد لمكان المعتدى عليه، فهو المكان الذي تتحقق به النتيجة الجرمية ومحدد بشخص المعتدى عليه. وهو أكثر تحديداً من موطن التحميل. فيجنب المتهم تكاليف باهظة لإجراءات المحاكمة كون المتهم بريء حتى تثبت إدانته.

في ظل القانون الأردني:

لم يتبن المشرع الأردني قواعد قانونية خاصة تعالج الاعتداء على النظم المستحدثة في مجال تكنولوجيا المعلومات وشيكاتها. الأمر الذي يستوجب بنا تطبيق القواعد العامة قدر الإمكان للمدى الذي يتفق وطبيعة الجريمة المستحدثة.

فمتى تعتبر الجريمة مرتكبة؟ وما هي المحكمة المختصة؟

وفقاً للقانون الأردني سار المشروع مع الاتجاه الذي يعتد بالفعل الجرمي دون النظر إلى النتيجة. فبمجرد القيام بالأفعال الجرمية كاملة فإن الجريمة تصبح تامة، دون النظر لوقت النتيجة، وعليه تتم جريمة إفشاء الأسرار بمجرد نشر المعلومة دون الانتظار لحين تحقق النتيجة.

ومن ناحية أخرى فقد استعرض المشرع الأردني في الفصل الثاني من الباب الأول في الكتاب الأول من قانون العقوبات الاختصاص المكاني للقضاء الأردني.

- من حيث الصلاحية الإقليمية والتي تعطي الاختصاص للقضاء الأردني على كل الجرائم المرتكبة في الأردن، بغض النظر عن طبيعة الجريمة – جرائم أموال أو أشخاص أو جريمة معلوماتية – وبغض النظر عن جنسية الفاعل، وبالتالي، إذا ارتكب جريمة الإنترنت في الأردن فإن القضاء الأردني يكون مختصاً بنظر هذه القضايا باعتبارها دول التحميل، فإذا ما ارتكب أحد الأفعال أو العناصر التي تؤلف مثل هذه الجرائم فينعقد الاختصاص للقضاء الوطني (م ٧/ ٢) عقوبات.

- كما تناول المشرع الصلاحية الذاتية لبعض الجرائم التي تمس أمن البلد، فينعقد الاختصاص للقضاء الأردني بغض النظر عن جنسية الفاعل، شريطة أن تكون مرتكبة من خارج الأردن. فإذا نشرت معلومات عبر الإنترنت تمس بأمن الأردن واستقراره ينعقد الاختصاص للقضاء الوطني.

- وتعقب القانون الأردني المواطن الأردني الذي يرتكب الجريمة خارج الأردن إذا ما كانت من نوع الجناية أو الجنحة، وإن فقد جنسيته بعد ارتكابها. وينطبق هذا على الموطنين الأردنيين في الخارج وفق أحكام المادة ١٠ من قانون العقوبات.

- ولمنع التهرب من العقاب يحاكم أمام القضاء الوطني كل أجنبي ارتكب خارج الأردن جناية أو جنحة يعاقب عليها في الأردن ما لم يكن قد طلب استرداده أو قبل.

ومن خلال مجموعة الأحكام العامة السابقة الذكر نرى أنها قابلة للتطبيق على مجموعة من الجرائم المرتكبة باستغلال شبكات المعلومات

(الإنترنت) كون المشرع لم يفرق بين أنواع الجرائم، وسواء كان الأردن بلد التحميل فيتم المعاقبة وفق قواعد الاختصاص الإقليمي، أو تم ارتكابها خارج الأردن من وطنيين فيتصدى لها قواعد الاختصاص الشخصي، وترك الأمر في المعاقبة إذا كان مرتكب الجريمة المعلوماتية خارج الأردن أجنبياً ضمن قواعد الاختصاص العالمي.

المطلب الثاني: جرائم الإنترنت

وضعت تقنية الإنترنت بيد المجرمين وسائل جديدة لتهديد وانتهاك حقوق وحريات الأفراد، سواء تعلق ذلك بالاعتداء على الحياة الخاصة أو بإفشاء الأسرار أو الاطلاع عليها، أو الاحتفاظ بنسخة منها بصورة غير مشروعة.

كما ظهرت للسطح أنواع وصور جرمية مستحدثة لجرائم اختراق نظم المعلومات أو الحيلولة دون استخدام صاحب النظام المعلوماتي لنظامه وغيرها، سندرس هذه الجرائم وفقاً للترتيب التالي:

الفرع الأول: حماية الحياة الخاصة في زمن الحاسب الآلي.

الفرع الثاني: جريمة اختراق نظم الاتصالات بطريقة غير مشروعة.

الفرع الثالث: جريمة عدم الخروج من النظام المعلوماتي حال كون الدخول صدفة.

الفرع الرابع: جريمة الحيلولة دون استخدام صاحب النظام المعلوماتي لنظامه والدخول إليه.

الفرع الخامس: جريمة الحصول على منفعة حاسب آلي دون حق.

الفرع السادس: جريمة إتلاف البيانات المعلوماتية.

الفرع السابع: جريمة الاعتراض على الرسائل المنقولة عبر شبكات الاتصال.

الفرع الأول: حماية الحياة الخاصة للأفراد في زمن الحاسب الآلي:

عنت التشريعات القانونية على مختلف أنواعها، وفي الغالبية العظمى من الدول بالحياة الخاصة للأفراد داخل المجتمع، وكفلت لها الحماية اللازمة ضد اختراق حرمتها وكشف مستورها.

من ذلك كفالة الدستور الأردني للحرية الشخصية في المادة السابعة بقوله "الحرية الشخصية مصونة" كما حفظ الدستور الأردني للمساكن حرمتها فحرم دخولها إلا في الأحوال وبالكيفية المبينة في القانون، حيث جاء في المادة العاشرة منه للمساكن حرمة فلا يجوز دخولها إلا في الأحوال المبينة في القانون، وبالكيفية المنصوص عليها فيه"، هذا بالإضافة إلى صيانة المراسلات البرقية والبريدية والهاتفية وكفالة حرية الرأي والتعبير.

حماية الحياة الخاصة للأفراد تجد جوهرها في حق الأفراد في أن يكون لهم مأمن لإيداع أسرارهم الخاصة، وحقهم في إبقائها طي الكتمان فلا يعلم بها غيرهم، ولا تمتد لها يد العابثين فيساء استخدامها، هذه الأسرار الخاصة ظلت حيناً من الزمن حبيسة القرطاس حتى انفجار ثورة التكنولوجيا، وظهور الحاسب الآلي وتطوره إلى الحد الذي أصبح معه

يملك القدرة على الاحتفاظ بكميات هائلة من المعلومات والبيانات وإلى ما لا نهاية، وفق أسس وبرامج تعد لهذه الغاية.

ولعل هذه الثورة الهائلة للتكنولوجيا ونظم المعلومات لم توقظ عند العديدين من رجال القانون من فقهاء ومشرعين المخاوف من المخاطر الجمة التي يمكن أن تلحق حياة الأفراد الخاصة على أساس أن الحاسب الآلي لم يكن سوى وسيلة جديدة لحفظ الأسرار الخاصة، وبالتالي فلا حاجة لنصوص قانونية جديدة للحماية إذ تكفي النصوص التقليدية.

غير أن الأمر ليس بهذه البساطة، ذلك أن ظهور الحاسب الآلي لم يكن مجرد وسيلة جديدة للحفظ والتخزين، بل كانت تقنية حديثة جلبت معها بالإضافة إلى المميزات العالية للحفظ والتخزين مخاطر كبيرة على حياة الأفراد وخصوصياتهم وأسرارهم، إذا أعطت هذه التكنولوجيا فرصة للإطلاع على أسرار الأفراد الخاصة المخزنة في الحاسب الآلي بسهولة وبسرعة فائقة، فضلاً عن إمكانية نسخها بوقت يكاد لا يلحظ، ناهيك عن إمكانية اختراقها والاطلاع عليها من مسافات شاسعة عن طريق أجهزة الاتصالات البعدية من خلال النهايات الطرفية للشبكة مع ظهور ما يسمى بـ (الإنترنت).

لذا، فمن الواجب البدء سريعاً في رصد مختلف أنماط السلوكيات الخطورة على حياة الأفراد الخاصة والتي صاحبت ثورة التكنولوجيا وتحديد أوجه الحماية اللازمة، وقبل ذلك لابد أن نحدد مفهوم السر وطبيعته وأشكاله، وجوانب الخطورة الكامنة والجهات التي تظهر منها.

البند الأول: مفهوم السر ضمن الحياة الخاصة للأفراد:

يعرف الفقه القانوني السر في هذا الخصوص بأنه "واقعة أو صفلة ينحصر نطاق العلم بها في عدد محدود من الناس، إذا كانت ثمة مصلحة يعترف بها القانون لشخص أو لأكثر في أن يظل العلم بها محصوراً في ذلك النطاق"[1].

من هذا المفهوم الدقيق للسر نستبعد كافة الوقائع التي لا تمتع بحماية القانون كأسرار خاصة، وتلك الوقائع التي يوجب القانون ضرورة العلم بها من قبل جهة ما، من ذلك عدم كتمان الجريمة لمن يعلم بها، وكذلك واجب الطبيب المعالج في الإبلاغ عن أي مريض معد أو غريب يكشف عنه.

بهذا المعنى يكون السر متعلقاً بمعلومة عن الحياة الخاصة للفرد، يحرص على أن تبقى في حدود هو فقط، أو في حدود علم المقربين له تحديداً، لا خلاف فيما إذا كانت هذه المعلومة تتعلق بحالة الشخص الصحية كمرض ألم به، أو عجز أصابه، أو معلومة متعلقة بوضعه المالي، ومركزه التجاري كمعاناته من ضائقة مالية، أو قرب دنوه من الإفلاس، أو معلومة ذات صلة بشخصية الفرد كأوصافه الجسمانية، أو مكان سكنه أو عمله، أو معلومة ذات صلة بانتماءاته السياسية أو الحزبية أو النقابية، أو أفكاره الفلسفية أو الاجتماعية أو الاقتصادية، أو معلومة تتعلق بقضية له أمام المحاكم، أو حكم أو سابقة قضائية، وغيرها مما لا يمكن حصره هنا من

---

(1) لمزيد من التفاصيل أنظر د/ هدى حامد قشقوش: الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ٣٦، وما بعدها.

معلومات كتابية، أو صور ونماذج ورسوم، سواء أكانت من واقع الحياة، أو من بناة فكر صاحبها.

المهم في الأمر لاعتبار المعلومة سراً يستحق الحماية أن تكون ذات صلة بالفرد يمكن أن تؤثر عليه مادياً أو معنوياً، وأن يكون حريصاً على إبقائها على الكتمان، بعيدة عن علم الغير.

هذه المعلومات السرية يمكن أن تكون موجودة على جهاز الحاسب الآلي الخاص العائد للفرد، سواء أكان الحاسب الآلي موجوداً في البيت، أو في مكان العمل الخاص، هذا الحاسب الآلي قد يوجد منفرداً، وقد يكون مربوطاً بشبكة اتصالات محلية أو عالمية، كما يمكن أن تكون هذه المعلومات السرية لدى جهات أخرى يرتبط معها الفرد بعلاقة ما، كعيادة طبيب يعالجه، أو مكتب محاماة يتولى شؤونه القانونية، كما يمكن أن تكون هذه المعلومات لدى جهات حكومية كوزارة أو مؤسسة من ذلك دائرة الأحوال المدنية.

بالنظر إلى أماكن تواجد المعلومات السرية يمكن أن ترد جهة الخطورة المتعلقة بها إلى ناحيتين:

١- الاطلاع على المعلومة السرية بصورة مباشرة: ويكون ذلك من الشخص الذي يشرف على تلك المعلومات من حيث تصنيفها وتبويبها وتخزينها ومعالجتها آلياً وكتمانها، سواء أكان هو القائم بالفعل شخصياً، أو مشتركاً مع غيره، أو ساهم بحدوث ذلك بطريقة غير مباشرة بإهماله تدابير وإجراءات الحفظ والحماية.

٢- الاطلاع على المعلومة السرية بصورة غير مباشرة: ويكون ذلك باستخدام تقنية الاتصالات المعلوماتية الحديثة المعتمدة على أجهزة الاتصالات البعدية في كل الفروض التي يكون الحاسب الآلي حاوي المعلومات السرية مربوطاً بالتوازي مع شبكة اتصالات متاحة كحاسبات آلية أخرى سواء على ؟؟؟ ص٢١٧ المحلي أو العالمي.

البند الثاني: صور السلوكيات التي تشكل خطورة على سرية المعلومات:

تتمثل صور الاعتداء على الحياة الخاصة للأفراد وسرية معولماتهم بصورة أساسية في أربعة أنماط، نبحث تالياً هذه الأنماط من خلال تجسيد السلوك في الواقع، ثم بيان أوجه التحريم المتاحة.

أولا: الاطلاع المجرد:

يتحدد المظهر الأول من مظاهر الاعتداء على الحياة الخاصة للأفراح وانتهاك حرمة أسرارهم الخاصة المخزنة على الحاسب الآلي بالاطلاع المجر على تلك الأسرار بما تتضمنه من بيانات ومعلومات:

أ- تجسيد السلوك في الواقع:

بداية يجب أن نعرف أن محل الاطلاع هنا هو معلومات شخصية وخاصة يريد صاحبها إبقاءها سرية، وبالتالي لا يتحقق هذا السلوك في جميع الفروض التي يكون الاطلاع فيها مباحاً للكافة.

أما صورة هذا السلوك هنا فتحدد بواقعة الاطلاع التام الكلي أو الجزئي على تلك الأسرار الخاصة، بحيث يقوم اليقين بالعلم بها لدى

الفاعل وفهمها، فإذا كانت الأسرار بلغة لا يفهمها الفاعل، أو لا يحسن تحليلها، لم يتحقق الاطلاع كما لا يتحقق الاطلاع إلى بتكامل الصورة وترابط أجزائها، فإذا لم يكن ما أطلع عليه الفاعل سوى جزئيات غير مترابطة وغير ذات معنى مفيد لم يتحقق الاطلاع أيضاً.

هذا الاطلاع يجب أن يكون في ذاته غير مشروع، وأن يتم من شخص لا يملك قانوناً ترخيصاً بالولوج إلى تلك المعلومات والبيانات الخاصة، ولذا لا يتصور وقوع هذا الفعل من الشخص المكلف بتخزين وحفظ الأسرار الخاصة، أو تصنيفها أو إجراء أية معالجة آلية بها.

كما يشترط لتحقيق فعل الاطلاع هنا – بحدود هذه الصورة – أن يكون الاطلاع مجرداً، أي أن يكون قصد الفاعل مجرد الاطلاع على تلك المعلومات السرية، ومجرد العلم الشخصي فقط، فإن تعدت نيته إلى استغلال تلك المعلومات في أغراض غير مشروعة خرجنا من هذه الصورة إلى صور أخرى قد تشكل واقعة الإفشاء، أو التهديد أو الابتزاز وهو ما سنتحدث عنه فيما بعد.

أما وسيلة الاطلاع على تلك المعلومات السرية فيمكن ردها إلى طريقة مباشرة وأخرى غير مباشرة، أما الطريقة المباشرة فتتمثل بالولوج إلى المعلومات السرية بواسطة الحاسب الآلي حاوي المعلومات ذاته، وذلك باقتحام الفاعل لمكان تواجد الحاسب الآلي واستغلاله لذلك، أما الطريقة غير المباشرة فتتمثل باختراقات عن بعد لأنظمة الاتصال المعلوماتية بمعونة أجهزة تحليل الشيفرات، وفي بيئة تمهد لها تقنية (الإنترنت)، بحيث تحقق

هذه التقنية فرصة لعمل تلك الاختراقات عن بعد، وفرصة للتجول داخل أنظمة المعلومات والاطلاع على ما يريد الفاعل الاطلاع عليه منها.

بـ أوجه التجريم المتاحة:

بينا فيما سبق أحد السلوكيات التي تمثل بنظرنا اعتداء على الحياة الخاصة الأفراد وبالذات انتهاك حرمة السرية الخاصة بهم، وهنا نبحث في مدى تجريم مثل هذه السلوكيات في القانون المقارن وفي القانون الأردني.

القانون المقارن:

القوانين الجزائية المقارنة لم تجرم هذا السلوك المتعلق بمجرد الاطلاع على المعلومات الخاصة السرية – بيد أن القانون الفرنسي وتحديداً في المادة (٢٢٦/ ١٧) من قانون العقوبات الجديد ١٩٩٤ – نص على معاقبة كل من أجرى أولاً طلب إجراء معالجة آلية للمعلومات الإسمية دون أن يأخذ كل الاحتياطات الكافية والمجدية لضمان أمن هذه المعلومات، وعلى وجه الخصوص لمنع تشويهها أو إتلافها أو الوصول إليها من شخص غير مصرح له بذلك.

صحيح أن هذا النص يجرم عدم اتخاذ الاحتياطات الكافية والمجدية لمنع ذلك، لكن لا يمكن أن يبنى عليه إمكانية تجريم الشخص الذي أطلع على المعلومات السرية ذاتها.

القانون الأردني:

الاطلاع المجرد على المعلومات الخاصة السرية وفق التشريع الجزائي الأردني غير مجرم، استناداً لقاعدة "لا جريمة ولا عقوبة إلا بنص" إذ لم نجد نصاً يعاقب على مثل هذا السلوك سواء بشكل صريح أو ضمني.

ولعل غياب قاعدة التجريم سواء في القانوني المقارن أو في القانون الجزائي الأردني يعود إلى عدم تحقق ضرر جراء هذا السلوك، ومع ذلك فإننا نرى أن هذا السلوك المتمثل بمجرد الاطلاع يمكن أن يجد علة التجريم في انتهاك حرمة الحياة الخاصة للأفراد المحمية بالدستور والقوانين، تماماً كما جرم المشرع خرق حرمة المنازل وأوجب لها عقوبة حتى عند عدم تحقق ضرر، إذ الحماية ضد انتهاك الخصوصية الفردية والتي تتحقق بمجرد الدخول إلى المنزل، أو الولوج إلى نظم المعلومات المعالجة آلياً[1].

ثانيا: الاطلاع بقصد الإفشاء:

أ- تجسيد السلوك في الواقع:

في هذه الصورة من صور الاعتداء على الحياة الخاصة للأفراد لا يكون اطلاع الفاعل على الأسرار الخاصة المخزنة على الحاسب الآلي مجرداً، وإنما لتحقيق غرض وهدف آخر هو إفشاء تلك الأسرار بما تتضمنه من معلومات وبيانات شخصية.

([1]) أسامة المناعة، مصدر سابق ص ٢٠٤- ٢٢٩.

يتم هذا السلوك إما من الشخص المتاح له بحكم عمله الاطلاع على المعلومات والبيانات الخاصة السرية كموظف في دائرة الأحوال المدنية، أو عامل أو مستخدم لدى عيادة طبيعة أو مستشفى أو محكمة، كما يمكن أن يحدث هذا السلوك من شخص أجنبي يتوسل بخبرته ودرايته بأنظمة المعلومات لتحقيق اختراقات واتصالات بعدية أو مباشرة مع الحاسب الآلي الموجودة عليه تلك الأسرار الخاصة، بحيث يتمكن من الاطلاع على تلك الأسرار الخاصة وإفشائها.

أما فعل الإفشاء بذاته فيمكن أن يكون موجهاً لشخص معين، أو أشخاص معينين، يبغي الفاعل إخبارهم، كما يمكن أن يكون إفشاء السر بصورة مفتوحة عامة، بحيث يستطيع الجميع العلم به، كنشر به، كنشر الأسرار في محلات عامة أو مفتوحة للجمهور أو أماكن معرضة للأنظار.

كما ينظر إلى الحاسب الآلي كوسيلة فعالة في خرق وتحديد حرمة حياة الأفراد الخاصة، والاطلاع على أسرارهم، يمكن أن يشكل الحاسب الآلي وسيلة أكثر فعالية في نشر وإفشاء الأسرار الخاصة للأفراد بشمولية وتوسيع كبير، وبسرعة وكفاءة عالية، وذلك باستخدام قنوات الاتصال المتعددة التي تتيحها أنظمة الاتصالات المعلوماتية الحديثة مع ظهور (الإنترنت) وبشكل خاص خدمة البريد الإليكتروني الذي يوفر سرعة فائقة في نقل المعلومة في إرجاء المعمورة كلها. بالإضافة إلى إمكانية بناء المواقع الخاصة، ووضع الإعلانات والإشارات ضمن عناوين إليكترونية خاصة يمكن الجميع الوصول إليها، والاطلاع على ما فيها من معلومات.

ب- إمكانية التجريم المتاحة:

لا يخفي على الكثير منا مدى الأضرار المادية أو المعنوية التي يمكن أن تلحق صاحب الأسرار الخاصة إذا ما أقدم الغير على إفشائها، ناهيك عن إمكانية المنفعة التي يمكن أن يحققها الفاعل جراء ذلك، الأمر الذي دفع المشرع الجزئي نحو التصدي لمثل هذه السلوكيات الضارة بنصوص تجريم رادعة، نبحث المسألة في القانون المقارن ثم نتلوها بموقف مشرعنا الجزائي الأردني.

١- القانون المقارن:

القانون الفرنسي:

يعتبر القانوني الفرنسي أكثر القوانين الدولية تطوراً في هذا المجال، حيث ورد في نص المادة (٢٦٦/ ٢٢) من قانون العقوبات ١٩٩٤ معاقبة كل من كان قد استقبل بمناسبة تخزين المعلومات أو تصنيفها معلومات سرية خاصة ذات اعتبار لأصحابها ومن شأن إفشائها إلحاق ضرر بهم، وقام بنقل تلك المعلومات السرية الخاصة إلى من لا حق له بالاطلاع عليها، كما عاقبت المادة ذاتها الشخص المكلف إذ نتج الإفشاء عن إهمال أو تقصير منه ولكن بعقوبة مخففة".

كما عاقبت المادة (٣٢٣/ ١) من ذات القانون بالسجن وبالغرامة (١٠٠،٠٠٠) فرنك كل من أجرى أي نشر أو فضح أو تزوير في كل أو جزء من النظام المعالج آلياً.

القانون الأميركي:

تبصرت الولايات المتحدة منذ البداية لخطر ثورة المعلومات على الحياة الخاصة للأفراد فأصدرت قانون سنة ١٩٧٤ متعلقاً بهذا الشأن، جاء في مادته رقم (٥٥٢/ أ) أنه لا يجوز لأية جهة أن تفشي أي معلومات يتضمنها نظام للمعلومات بأي وسيلة من الوسائل لأي شخص أو لأية جهة أخرى ما لم يكن ذلك بناء على طلب كتابي بموافقة صاحب الشأن الذي تتعلق به المعلومات. مع إيراد استثناء يتعلق بالمصلحة العامة أو بناء على أمر المحكمة.

كما جاء في قانون العقوبات لولاية فلوريدا النص على معاقبة كل ولوج بسوء نية في نظام أو شبكة معلوماتية بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير، أو كل من أدخل معلومات مصطنعة بغرض تحسين أو إساءة سمعة الغير.

أما في قانون العقوبات المصري فإن النصوص التقليدية تقف عاجزة عن استيعاب سلوكيات الإفشاء والنقل للأسرار والتي أتت بها التقنية الحديثة لأنظمة المعلومات ذلك أن المادة (٣٠٩) والمادة (٣٠٩) مكرر من قانون العقوبات تتحدث عن استراق السمع أو تسجيل ما يسمع من محادثات، والتقاط أوة نقل صورة شخص في وضع خاص بأي جهاز من الأجهزة، كما تتحدث المادة (٣٠٩) مكرر عن معاقبة كل من أذاع أو سهل إذاعة أو استعمل ولو في علانية تسجيلاً أو مستنداً متحصل عليه بإحدى الطرق المبينة في المادة (٣٠٩) أو كان ذلك بغير رضا صاحب الشأن.

من هنا يبدو وجه القصور في النصوص، إذ تتحدث عن صور أو صوت فقط في حين لا تقف خصوصية حياة الأفراد عند هذه المفردات بل تمتد إلى غيرها من محررات مكتوبة أو مسجلة بأية وسيلة، وخصوصاً أنظمة المعالجة الآلية للمعلومات، الأمر الذي يدفع في النهاية الحاجة نحو تعديل وتطوير النصوص.

٢ـ القانون الأردني:

نظم قانون العقوبات الأردني موضوع إفشاء الأسرار في المواد (٣٥٥-٣٥٧) ضمن الفصل الثاني من الباب الثامن المعنون بالجنايات والجنح التي تقع على الإنسان. وبتصفح تلك النصوص نلحظ أنها تعالج بالمقام الأول إفشاء الأسرار الرسمية من قبل الموظف الحاصل عليها بحكم عمله، كما تعالج مسألة الاحتفاظ بوثائق سرية أو رسومات أو مخططات أو نماذج أو نسخ عنها دون حق ودون مقتضى قانوني.

والسؤال الذي يغرض نفسه هنا، هل تكفي هذه النصوص في ظل ثورة المعلومات؟

في اعتقادنا أن نص المادة (٣٥٥) عقوبات نص قاصر يضيق من دائرة التجريم، ولا يستوعب بحال السلوكيات الجديدة لخرق نظم المعلومات وإفشاء الأسرار، وذلك أن النص يشترط للتجريم أن يكون الحصول على معلومات سرية رسمية، وأن يتم هذا الحصول من الفاعل بحكم وظيفته أو مركزه الرسمي، أو بمعرض قيامه بمهمته، وبالتالي، ووفقاً لهذا التحديد لا يشمل نطاق التجريم الحصول على معلومات تشكل أسراراً غير رسمية،

أو الحصول على أسرار رسمية من شخص لا تقتضي وظيفته العلم بها، ومن باب أولى لا يشمل نطاق التجريم كافة أشكال الاختراقات غير المشروعة لأنظمة المعالجة الآلية للمعلومات من أشخاص لا تقتضي أعمالهم الاطلاع على الأسرار الخاصة للأفراد، ومع أن وسيلة الحصول على السر ليست بذات جدوى في التجريم، علاوة على أن التجريم في النص السابق يقتصر فقط على الأسرار التي يباح لبعض الموظفين أو أصحاب المهن الاطلاع عليها، ثم يفشونها بغير وجه مشروع، من ذلك الأطباء والمحامين الذي تتحصل لديهم أسرار ذات علاقة بحياة الأفراد الخاصة.

لذلك كله، لابد من مواكبة النصوص وتطورها بحيث تجرم بشكل صريح وواضح كافة أشكال الإفشاء والنقل غير المصرح به قانوناً لمعلومات سرية ذات علاقة بالحياة الخاصة للأفراد أياً كانت نوعية المعلومات وأياً كانت صور الإفشاء وأشكاله، وبغض النظر عنه طريق الحصول على تلك الأسرار الخاصة.

ثالثا: أو الابتزاز: أ. تجسيد السلوك في الواقع:

يتمثل التهديد بالاستغلال غير المشروع للأسرار الشخصية أحد أهم مظاهر الاعتداء على الحياة الخاصة للأفراد، حيث يستغل الفاعل ما يتحصل عليه من معلومات ذات طابع سري وذات علاقة بالحياة الخاصة للأفراد في تحقيق منافع مادية أو معنوية وذلك بتهديد صاحب الأسرار بإفشائها أو فضح أمرها في حال عدم تحقيق مطالبة.

لتحقق فعل التهديد لابد أن تكون للفاعل القدرة على القيام بما هدد به والذي يتعلق بإفشاء سر يعود للمهدد بحرص على ألا يطلع عليه أحد. ويمتلك الفاعل هذه القدرة باطلاعه التام على المعلومات السرية بأية وسيلة كانت، وأن يكون لديه الوسيلة اللازمة لتحقيق فعل الإفشاء مستقبلاً. فإن كانت المعلومات التي بحوزة الفاعل غير سرية ومباحة للجميع، أو لا يحرص صاحبها على إبقائها سراً، فإن فعل التهديد لا يتم، كما لا يتم التهديد إذا لم يكن لدى الفاعل القدرة على إفشاء ما تحصل عليه من معلومات سرية نتيجة لعدم تكامل الصورة لديه، أو عدم قدرته على تحليل رموز المعلومات.

يتحقق فعل التهديد بالقول الموجه مباشرة أو بطريق غير مباشر لصاحب المعلومات السرية الخاصة، كما يتحقق فعل التهديد بالكتابة بأي صورة كانت ومن ذلك الرسائل الإليكترونية عبر (الإنترنت).

ويشترط كذلك لتحقق فعل التهديد بالإضافة لما سبق أن يحدث إفشاء تلك المعلومات السرية الخاصة الرهبة لدى صاحبها من خلال ما يتضمن الإفشاء من أضرار مادية أو معنوية تلحق صاحبها ككون المعلومات السرية ذات علاقة بمرض يعانيه المهدد من شأن إفشائه إلحاق ضرر معنوي به، أو تعطيل تجارته.

وأخيراً، يشترط لتمام فعل التهديد بالصورة المبحوثة هنا أن يكون الغرض الحصول على منفعة غير مشروعة، كالحصول على وظيفة لا يستحقها، أو مبلغ من المال. فإن كان القصد حصول الفاعل على منفعة

مشروعة كاستيفاء دين له في ذمة المهدد فلا يقع فعل التهديد، وإن أمكن تصور أنماط أخرى يعاقب عليها القانون الجزائي كجريمة استيفاء الحق بالذات.

أ- إمكانية التجريم المتاحة:

لا شك في مدى خطورة التهديد كفعل غير مشروع على الحياة الخاصة للأفراد وعلى أسرارهم الشخصية، الأمر الذي يستوجب تجريم هذا الفعل بنصوص واضحة ودقيقة.

١- القانون المقارن:

القانون المصري: ورد في قانون العقوبات المصري في المادة (٣٠٩) مكرر (أ) أنه يعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم الحصول عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عن عمل.

وبتفسير عبارة "بإحدى الطرق المشار إليها" الواردة في النص نجدها تنصرف إلى ما سبق أن ورد في المادة (٣٠٩) عقوبات مصري، وهذه الطرق هي تحديداً استراق السمع أو تسجيل أو نقل المحادثات، والتقاط أو نقل صورة شخص في مكان خاص وهي طرق قاصرة كما بينا فيما مضى لا تشمل كافة جوانب الحياة الخاصة للفرد، خصوصاً المعلومات الخاصة الموجودة على شكل كتابات ورقية أو آلية.

لذلك فإن تعديل نص المادة (٣٠٩) عقوبات يعطي النص المبحوث هنا، وهو نص المادة (٣٠٩) مكرر (أ) من ذات القانون، معناة وكفايته ليشمل تجريم كافة صنوفاً التهديد بالحصول على منفعة غير مشروعة استناداً لأية معلومات أو بيانات سرية ذات علاقة بالحياة الخاصة للأفراد، وبأية وسيلة كانت.

٢ـ القانون الأردني:

نظم قانون العقوبات الأردني التهديد كجريمة في الفصل الثاني من الباب الثامن تحت عنوان في الجنايات والجنح التي تقع على الإنسان، ما يهمنا هنا هو نص المادة (٣٥٤) والذي جاء فيه "كل تهديد آخر بإنزال ضرر غير محق، إذ حصل بالقول أو بإحدى الوسائل المذكورة في المادة (٧٣) وكان من شأنها التأثير في نفس المجني عليه تأثيراً شديداً يعاقب عليه بناء على الشكوى بالحبس حتى أسبوع أو بغرامة لا تتجاوز الخمسة دنانير".

المقصود بكل تهديداً آخر الوارد في النص السابق كل صنوف التهديد غير إشهار سلاح ناري أو التوعد بجناية أو جنحة بالقول أو بالكتابة، وهذا المعنى يمكن معه إدراج التهديد بإفشاء سر خاص متعلق بالمجني عليه دون إذن منه مما يلحق به ضرراً مادياً أو معنوياً، بحيث يشمل نطاق التجريم كافة أفعال التهديد التي تتم باستخدام تقنية الاتصالات البعدية وفقاً لأشكال العلانية الواردة في المادة (٧٣) ومنها الكتابة والرسوم والأفلام

التي توزع على أكثر من شخص ... بالإضافة إلى التهديد بالقول مباشرة لصاحب المعلومات السرية.

هذا وإن كنا قد طوعنا النص السابق ليشمل في نطاقه أعمال التهديد بإفشاء سر خاص استناداً للفظ النص الذي يقول "كل تهديد آخر بإنزال ضرر غير محق.." إلا أننا نرى في العقوبة التي يستحقها الفاعل تواضعاً لا يجوز أن يستمر خصوصاً مع النظر إلى خطورة فعل التهديد، وأثره على المجني عليه الأمر الذي نتطلع من خلاله نحو تشديد العقوبة بحق الجاني.

رابعا: الاحتفاظ بنسخة أ. تجسيد السلوك في الواقع:

لا تقتصر مظاهر الاعتداء على الحياة الخاصة للأفراد في ظل نظم المعلوماتية على مجرد الاطلاع أو الإفشاء أو التهديد بإفشاء تلك المعلومات السرية الخاصة، بل يمكن أن يأتي هذا الاعتداء بصورة الاحتفاظ بنسخة لتلك المعلومات السرية الخاصة. والاحتفاظ بنسخة يمكن أن يكون بفعل الشخص المكلف بتصنيف وتخزين والاحتفاظ بالمعلومات السرية، كما يمكن أن يكون بفعل شخص آخر يتوسل بنظم الاتصالات الحديثة لاختراق شبكة الحاسوب والاطلاع على المعلومات السرية الخاصة وأخذ نسخة عنها، وكل ذلك يتم بسهولة وسرعة فائقة، ومن أماكن بعيدة في الغالب.

تكمن الخطورة في هذا الفعل في إمكانية استخدام تلك المعلومات السرية الخاصة في المستقبل لتحقيق أغراض غير مشروعة كتهديد أو ابتزاز

صاحبها، كما يمكن أن تكون عرضة للضياع أو الاطلاع عليها من قبل الغير، لهذا كله تبرز علة التجريم على مثل هذه الأفعال الضارة.

ب- أوجه التجريم المتاحة:

القانون المقارن:

القانون الفرنسي:

ورد في قانون العقوبات الفرنسي الجديد ١٩٩٤ ما يشير إلى تجريم كافة أفعال التخريب والاحتفاظ بالمعلومات الخاصة السرية دون موافقة صاحب الشأن حيث ورد في نص المادة (٢٢٦/ ١٩) إلى أنه "يعاقب بالحبس خمس سنوات وغرامة مليوني فرنك فرنسي على تخزين معلومات إسمية في ذاكرة الآلة دون موافقة صريحة من صاحب الشأن متى كانت هذه المعلومات تظهر بصورة مباشرة أو غير مباشرة الأصول العرقية أو الآراء السياسية أو الفلسفية أو الدينية أو الانتماءات النقابية أو الأخلاق الشخصية، وذلك في غير الأحوال الواردة في القانون وينطبق ذلك على المعلومات الإسمية المتعلقة بالجرائم والعقوبات والتدابير المحكوم بها" [١].

كما عاقب قانون العقوبات الفرنسي كل جمع لمعلومات إسمية بطريق التدليس أو الخديعة أو أي طريق غير مشروع..." (٢٢٦/ ١٨).

---

(١) أسامة المناعة، مصدر سابق ص ٢٣٠ – ٢٣٥.

٢ـ القانون الأردني:

لم يعالج قانون العقوبات الأردني هذه المسألة كشأن كافة المسائل المستحدثة المتعلقة بخصوصية نظم المعلومات، غير أنه وإن ورد في نص الفقرة الثانية من المادة (٣٥٥) ما يفيد معاقبة كل من كان يقوم بوظيفة رسمية أو خدمة حكومية واستبقى بحيازته وثائق سرية أو رسوماً أو مخططات أو نماذج أو نسخاً عنها دون أن يكون له حق الاحتفاظ بها، أو دون أن تقتضي ذلك طبيعة عمله، فإن في هذا قصور جلي إذ لا تشمل العقوبة سوى من يقوم بوظيفة رسمية أو خدمة حكومية وبالتالي يخرج من نطاق التجريم كافة العاملين في غير القطاع الحكومي كموظفين الشركات والمهن الحرة حتى ولو لم يكن الاحتفاظ بتلك النسخ من طبيعة عملهم، كما يخرج من نطاق التجريم- وهذا المهم- كافة أشكال الاختراقات غير المشروعة لنظم المعلومات المعالجة آلياً والاحتفاظ بنسخ آلية لتلك المعلومات، المر الذي يدفعنا إلى الدعوة إلى سد الفراغ التشريعي القاضي بتجريم هذه الأفعال طالما لا يملك الشخص الحق بالاحتفاظ بالمعلومات السرية إطلاقاً أو خلال مدة معينة، مهما كانت طريقة الحصول على تلك المعلومات ومهما كانت طريقة الحصول على النسخ والاحتفاظ بها.

الفرع الثاني: جريمة اختراق نظم الاتصالات المعلوماتية بطريقة غير مشروعة:

يتمثل الركن المادي في هذه الجريمة بالدخول غير المشروع لأنظمة المعلومات المعالجة آلياً والعائدة للغير بدون وجه حق، ويقصد بالدخول

هنا ليس المعنى المادي المألوف وإنما استخدام الحاسب الآلي كنظام اتصال لتحقيق الولوج وفقاً لتكنولوجيا الاتصال الحديث التي تتيح إمكانية للاتصال من أي نهاية طرفية للشبكة ويتم هذا الدخول باستخدام طرق متعددة منها كلمة السر، البطاقات الممغنطة الخاصة، حيازة جهاز معين يتيح مثل هذا الولوج.

يبدو أن عملية الدخول هنا تتم بصورة غير مشروع، وهو وجه التجريم في الفعل، إذ يلج الفاعل في نظام الاتصال دون أن يكون له حق الولوج ويتوسل بذلك بالحصول على كلمة السر بطريقة غير مشروعة، أو تجريب أرقام..، أو بالاستعانة بأجهزة إليكترومغناطيسية أو صوتية أو ميكانيكية.

هذا السلوك غير المشروع يمكن أن يرتكبه أحد العاملين في الأنظمة أو الجهات المالكة للأنظمة أو المعلومات والذي لا تسمح له طبيعة عمله بالولوج إلى تلك المعلومات وإحداث اتصال مع النظام، كما قد ترتكب من أشخاص خارج المؤسسة بمساعدة أو دون مساعدة أحد من الداخل، كما يمكن – وهذا الأظهر – أن يكون الاختراق عن بعد باستغلال تقنية (الإنترنت) التي توفر قدرة للاتصال وتحقيق الاختراقات اللازمة للأنظمة المعلوماتية، وهو الأمر الذي جلب معه المخاطر الجمة، سواء في سهولة تحقيق الفعل أو في صعوبة ضبط الجناة.

هذه الخطورة أيقظت المشرعين في الدول المتقدمة ودفعت نحو وضع نصوص قانونية كفيلة بتجريم الفعل بدقة، من ذلك نص المادة (٣٢٣/ ١)

من قانون العقوبات الفرنسي الجديد ١٩٩٤ والتي عاقبت على الدخول بطريق الغش في اتصال مع نظام لمعالجة المعلومات آلياً كله أو بعضه.

كما عاقبت المادة (٢١) في القانون السويدي الخاص بالبيانات الشخصية الصادر سنة ١٩٧٣ كل من ولج بوسائل غير مشروعة في سجل "حقوق معلومات" مخصص للمعالجة الآلية للبيانات، أو كل من أتلف أو محا ...."

أما في الأردن فلا يزال هذا الفعل مغيباً عن بال المشرع إذ لم نجد نصاً في التشريع الأردني يمكن أن يصلح نموذجاً لتجريم الفعل، وهو أمر يوجب علينا دعوة مشرعنا نحو سن التشريع الكافي لمعالجة هذا السلوك، وغيره ذي العلاقة بثورة المعلومات. وقد تم التأكيد على خطورة هذا السلوك وضرورة التصدي للجريمة بنصوص واضحة في المشروع الصادر عن لجنة الوزراء الأردنية سنة ١٩٨٩، وكذلك التوصيات الصادرة عن منظمة التعاون والتنمية الاقتصادية (OECD) تحت عنوان التوصل غير المرخص بما في ذلك التغلب على الإجراءات أو التدابير الأمنية.

الفرع الثالث: جريمة عدم الخروج من النظام المعلوماتي حال كون الدخول صدفة:

هذه الجريمة تعالج حالات الإبقاء على الاتصال مع النظام المعلوماتي الخاص بالغير رغم عدم مشروعية الدخول أصلاً والحال هنا أن الدخول لم يتم بإرادة الفاعل بل كان بمحض الصدفة، ولذا فلا قصد جرمي للفاعل في الدخول وإجراء اتصال مع النظام المعلوماتي.

لكن الركن المادي لهذه الجريمة يتمثل في عدم الخروج الفوري لحظة تحقق الاتصال والعلم بأنه لا حق ولا سند يجيز إجراء الاتصال أو الإبقاء عليه.

ولهذا يبدأ الركن المادي للجريمة منذ إدراك الفاعل حقيقة الاتصال الحاصل ورفضه الخروج والبقاء ضمن النظام المعلوماتي، وهذا يعني أن هذه الجريمة عملية.

عاقب المشرع الفرنسي على هذه الجريمة في ذات المادة السابقة وهي المادة (٣٢٣/ ١) إذ جرمت الإبقاء بطريق الغش على الاتصال غير المقصود أصلاً بالنظام المعلوماتي كله أو بعضه، وقررت عقوبة الحبس من شهرين إلى سنة، والغرامة من ألفين إلى خمسين ألف فرنك فرنسي.

هذا ولم نجد نصاً يوصلنا إلى ذات النتيجة في التشريع الأردني الأمر الذي يوجب على المشرع القيام بجهود حثيثة نحو تجريم الفعل وسن العقوبة المناسبة.

الفرع الرابع: جريمة الحيلولة دون استخدام صاحب النظام المعلوماتي لنظامه والدخول إليه:

يتمثل الركن المادي في هذه الجريمة في إقدام الفاعل على تصرف يؤدي إلى منع صاحب النظام المعلوماتي من حقه في الولوج إلى نظامه واستغلاله وفقاً لما يرى، ويتوسل الفاعل هنا لتحقيق هدفه هذا بإجراء عمليات اتصال متكررة تهدف إلى خرق شبكة التحكم بالنظام المعلوماتي ذاته

بوسائل فنية خاصة والوصول إلى تعديل شيفرات الدخول ككلمة السر ونحوها، أو تبديل صفة المستخدم، وشخصه، ونحوها.

هذا وقد جرمت مثل هذه الأفعال في بعض الدول المتقدمة نذكر منها تحديداً كندا، إذ ورد في المادة (٤٣٠/ ١- ١) وفي الفقرة الرابعة منها أنه "يعاقب كل شخص يقترف أذى عن قصد ... جـ. يعترض سبيل، يقاطع أو يدخل مع شخص في الاستخدام القانوني أو يحجب الوصول للبيانات عن شخص مخول له بالوصول إليها".

ولا نص مماثل في التشريع الأردني على الإطلاق.

الفرع الخامس: جريمة الحصول على منفعة حاسب آلي دون حق:

مهدت تقنية (الإنترنت) للأفراد داخل المجتمع الحصول على كثير من الخدمات الخاصة والتجارية وفي مختلف نواحي الحياة مقابل بدل معقول يدفع لشركات متخصصة تأخذ على عاتقها مهمة خدمة الأفراد وتوفير الخدمة المطلوبة لهم، من ذلك خدمة الإعلانات التجارية، وخدمة التصفح والدخول إلى كثير من المواقع العلمية والفنية والاقتصادية.

لكن اليد المساهمة والعقل الذكي لم يقف عند هذا الحد، بل هداه طمعه نحو إيجاد طرق متعددة للحصول على تلك الخدمات وغيرها بصورة غير مشروعة، ودون وجه حق.

وهذا السلوك استناداً لما يظهره من خطورة جرمية على المجتمع، ورغبة في منع إلحاق الضرر بمؤسسات المجتمع وبقاء أدائها لمهامها وخدماتها لهذا كله يجب أن يجد هذا السلوك غير المشروع طريقة نحو التجريم من المشرع.

وبالنظر إلى طبيعة عمل (الإنترنت) واعتمادها بالأساس على خطوط الهاتف العادية يمكن لنا أن نتصور إمكانية تجريم السلوك السابق وفقاً لذات النصوص التي تجرم كافة أفعال سرقة المكالمات الهاتفية الواردة في قانون مصلحة الهاتف، أو إيجاد التشريع والنص الملائم والحديث المنسجم مع ثورة المعلومات.

في كندا استجاب المشرع لهذه النداءات واعتمد الأسلوب الثاني لسن نصوص جزئية تجرم أفعال الحصول على خدمات دون حق من حاسب آلي حيث نص المادة (٣٤٢/ ١) من قانون العقوبات الكندي على أنه: ١. كل شخص يمارس بالتحايل والخداع وبدون وجه حق: أ. يحصل بصورة مباشرة أو غير مباشرة على خدمة حاسب آلي...

الفرع السادس: جريمة إتلاف البيانات المعلوماتية:

سبق وأن بحثنا جريمة إتلاف البيانات المعلوماتية في الجزء الخاص بالجرائم الواقعة على الحاسب الآلي باعتبار البيانات أحد العناصر المعنوية للحاسب الآلي، لن نبحثها هنا منعاً للتكرار مكتفين بما سبق بيانه، غير أن (الإنترنت) كتقنية اتصالات معقدة وواسعة مهدت وأعطت الفرصة الكبيرة للمجرمين لتحقيق أفعال إتلاف البيانات المعلوماتية عن بعد

باستخدام برامج معدة لهذه الغاية من ذلك (الفيروسات) متعددة الأسماء والأشكال والصفات كأحصنة طروادة والقنابل الموقوتة وغيرها.

الفرع السابع: جريمة الاعتراض على الرسائل المنقولة عبر شبكات الاتصال: [1].

يتمثل الركن المادي في هذه الجريمة بقيام الفاعل بالتدخل غير المشروع بالاتصالات التي تتم غير شبكات الاتصال سواء اتخذ هذا التدخل صفة اعتراض الرسائل المنقولة أو إعاقتها أو تحويرها أو شطب محتوياتها.

كما قد يتخذ الفعل هنا سلوك التشويش على الموجات المخصصة لاتصال الغير عن طريق إساءة استخدام الموجبات الكهرومغناطيسية بحيث يعطل بأية صورة الوظيفة التي يؤديها الحاسب الآلي. أو إجراء تدخل واتصال دون وجه حق.

جرم هذا السلوك في عدد من الدول المتقدمة بنصوص واضحة من ذلك مثلاً، قانون العقوبات الكندي الذي جاء في مادته (٤٣٠/ ١) معاقبة كل شخص يقترف عن قصضد أذى باعتراض سبيل أو مقاطعة أو تدخل مع أي شخص في الاستخدام القانوني للبيانات.

كما عاقبت المادة (٣٤٢/ ١) من ذات القانون كل شخص يتوسل بوسائط إليكترومغناطيسية أو صوتية أو ميكانيكية أو أي أداة أخرى لوقف

---

(1) لمزيد من التفاصيل أنظر د/ هدى حامد قشقوش: الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ٣٦، وما بعدها.

أو اعتراض سبيل أو التسبب باعتراض – بصورة مباشرة أو غير مباشرة – أي وظيفة لنظام حاسب آلي.

أما في التشريع الجزائي الأردني فإن قانون العقوبات يأتي خلواً من أي نص ملائم لتجريم هذه الواقعة فالمواد (٣٥٦، ٣٥٧) تتحدث عن سلوكيات مادية تتعلق بالاطلاع على رسائل مغلقة أو كشف محادثة هاتفية أو إتلاف رسالة أو برقية، ومع ذلك فحسناً فعل مشرعنا إذ تنبه لهذا الأمر فسارع في قانون الاتصالات الأردني رقم (١٣) لسنة ١٩٩٥) إلى تجريم مثل هذه الأفعال في المادتين (٧٦، ٨٠).

فقد نصت المادة (٧٦) على أنه "كل من اعترض أو أعاق أو صور أو شطب محتويات رسالة بواسطة شبكة الاتصال أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على ٢٠٠ دينار أو بكلتا العقوبتين".

ونصت المادة (٨٠) على أنه: "كل من قام متعمداً باعتراض موجات مخصصة للغير أو بالتشويش عليها أو باستخدام موجات كهرومغناطيسية بدون ترخيص يعاقب بالحبس مدة لا تزيد عن ستة أشهر أو بغرامة لا تقل عن ٥٢٠ دينار ولا تزيد عن ٢٠٠٠ دينار أو بكلتا العقوبتين".

في نص المادة (٧٦) عاقب المشرع كافة أعمال الاعتراض أو الإعاقة أو المحو أو الشطب الواقعة على الرسائل الإلكترونية وبأية وسيلة كانت، كما عاقب على التشجيع على ارتكاب مثل تلك الأعمال سواء بتوفير الأجهزة اللازمة، أو تقديم الخبرة الفنية الأساسية ونحو ذلك، وقد كانت العقوبة

لمثل هذه الأفعال هي الحبس من شهر إلى ستة أشهر والغرامة بما لا يزيد عن مائتي دينار أو بكلتا العقوبتين، كما نتمنى أن يشمل المشرع مصادر كافة الأجهزة المستخدمة في إطار العقوبة.

أما المادة (٨٠) فقد عالجت أفعالاً اعتراض الموجات العائدة للغير أو التشويش عليها أو أي استخدام للوحات الكهرومغناطيسية دون ترخيص وأفردت عقوبة للفاعل هي الحبس مدة لا تزيد عن ستة أشهر، وبالغرامة بين (٥٠- ٢٠٠) دينار أو بكلتا العقوبتين.

الفصل الخامس
التحديات والممارسات العملية في مجال

مكافحة جرائم المعلوماتية والإنترنت وأفضل الحلول المطروحة

ثمة تحديات جهة تواجه الجهود المبذولة لمكافحة جرائم المعلوماتية سواء على الصعيد الوطني أو الدولي، وسوف نبحث في هذا الإطار ماهية هذه التحديات وأمثلة عملية عليها وأفضل الممارسات والحلول في مواجهتها [1].

المبحث الأول
التحديات التقنية والإجرائية لمكافحة

جرائم المعلوماتية والإنترنت

تواجه جهود مكافحة جرائم المعلوماتية والإنترنت تحديات ومشكلات جمة تغاير في جوانب كثيرة التحديات والمشكلات التي ترتبط بالجرائم العادية انطلاقاً من الطبيعة الخاصة لجرائم المعلوماتية، والتي امتدت إلى شبكة الإنترنت بعد أن كانت تقتصر على الكمبيوتر وأنظمته [2]. وسوف نبحث فيما يلي في مجموعة من التحديات المذكورة.

---

(1) أ. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي، ط١ ٢٠٠٧ ص ٤٥- ٥٥.

(2) لمزيد من التفاصيل أنظر د/ هدى حامد قشقوش: الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ٣٦، وما بعدها.

المطلب الأول

التحديات المرتبطة بالبحث عن أدلة الجريمة

والتفتيش وإجراءات الضبط

سبق لنا أن ذكرنا أن هذا النوع من الجرائم لا يترك أي أثر مادي في مسرح الجريمة. فضلاص عن أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة.

أما بالنسبة لإجراءات التفتيش ففي هذا النمط من الجرائم يتم عادة على شبكات المعلومات، وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة، وهذا هو الوضع الغالب في ظل شيوع الشبكات الداخلية على مستوى الشركات أو المؤسسات والشبكات المحلية والإقليمية والدولية على مستوى الدول.

ويعتبر امتداد نطاق التفتيش إلى نظم غير النظام محل الاشتباه محل تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

وبالنسبة لإجراءات الضبط فإن عملية الضبط لا يتوقف على تحريز جهاز الكمبيوتر فقد يمتد من ناحية ضبط المكونات المادية إلى مختلف أجزاء النظام التي تزداد يوماً بعد يوم، والأهم أن الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه، وأي أدوات دفع إلكترونية وأي أشياء ذات طبيعة معنوية معرضة

بسهولة التغيير والاتلاف، وهذه الحقائق تثير مشكلات متعددة، منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز إضافة إلى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه – وإن كان المشتبه به – عندما تتعدى أنشطة الضبط إلى كل محتويات النظام التي تضم عادة معلومات وبيانات قد يحرص على سريتها أو أن تكون محل حماية بحكم القانون أو لطبيعتها أو تعلقها بجهات أخرى .

المطلب الثاني

التحديات المرتبطة بأدلة الإدانة والاختصاص

بالنظر في الجريمة

تعتبر أدلة الإدانة ذات نوعية مختلفة، فهي معنوية الطبيعة كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ، وقد أثارت وتثير أمام القضاء مشكلات جمة من حيث مدى قبولها وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبات التقليدية.

أما بالنسبة للاختصاص بالنظر في الجريمة فإنه، يلاحظ أن اختصاص القضاء بنظر الجرائم التي تتم عبر الإنترنت خاصة غسل الأموال أو أي من الجرائم التي تتم عبر الشبكة العنكبوتية والقانون المتعين تطبيقه على الفعل لا يحظى دائماص بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال ترتكب من قبل أشخاص من خارج الحدود أو أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من

داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية اختبار مدى ملاءمة قواعد الاختصاص والقانون الواجب التطبيق وما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات في حق الاختصاص القضائي. ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية [1].

إذن وربما يحسن في هذه المرحلة النظر عند تقويم هذه القضايا من زاوية أن ما نشاهده اليوم في مسرح الجريمة التقني ما هو إلا عبء جديد يضاف على كاهل مؤسسات الأمن والقضاء في أن معاً. في ظل الاتجاه العالمي بتحويل كثير من الأنظمة المالية إلى أنظمة الدفع الإلكتروني. وفي هذه المرحلة، يفضل أن تبدأ الأجهزة الأمنية الدولية المختصة في مكافحة جرائم الإنترنت والمعلوماتية عموماً في استخدام خطط وقائية عبر التخطيط الدقيق والفعال لمواجهة السلبيات الحالية والمحتملة. وكذلك توظيف إيجابيات شبكة الإنترنت والتعاون الدولي في مجال مكافحة الجريمة عبر مقاربة كل هذه التعديات وربطها بالبعد الإجرائي للجرائم التي تتم عبر الإنترنت.

---

(1) محمد الشوابكة، جرائم الحاسوب والإنترنت، المرجع السابق، ص١٢.

ولعل هذا ينطوي على تحديات ومشكلات جمة تتمثل تجلياتها في التالي:

- الحاجة إلى سرعة الكشف عن الجريمة وتعقبها خشية ضياع الدليل، بالإضافة إلى خصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم[1].

- مدى قانونية وحجية الأدلة للجرائم التي تتم عبر الإنترنت.

- مشكلات الاختصاص القضائي والقانون الواجب التطبيق.

- الحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود.

وهذه المشكلات كانت ولا تزال محل اهتمام على الصعيدين الوطني والدولي [2].

(١) أنظر نبيلة هدوال، المرجع السابق ذكره، ص ٢٢٨.
(٢) www. Moffed. com

المبحث الثاني
قضايا عملية في جرائم المعلوماتية

والإنترنت وسبل مكافحتها

يشهد استخدام شبكة الإنترنت كوسيط تجاري نمواً متسارعاً حيث بات مصطلح التجارة الإلكترونية في نظر الكثيرين مرادفاً للأرباح السهلة والوفيرة في ظل اقتصاد عالمي يتزايد اعتماده على شبكة الإنترنت بصورة متنامية.

ومع نمو التجارة يتزايد انتشار الجريمة على شبكة الإنترنت وتتنوع أشكالها بصورة مطردة بداية من سرقة بيانات الحسابات المصرفية وبطاقات الائتمان من قبل محترفي اختراق الشبكات (الهاكرز) وقيام عصابات غسل الأموال بإخفاء الأموال غير الشرعية عبر متاهة من الحسابات المصرفية على الشبكة العالمية.

وتتنوع أشكال الجرائم عبر الإنترنت ولكن يجمع بينها عنصر واحد هو الحاجة إلى عملة رقمية لتسهيل أنشطة التبادل التجاري (المشروع وغير المشروع) عبر أجهزة الكمبيوتر المتصلة بشبكة الإنترنت.

ومنذ البدايات الأولى للإنترنت ظهر العديد من البدائل للعملات الورقية التقليدية كأن آخرها ما بادرت إليه شركة أميريكية تسمى "أي جولد المحدودة" تقدم للمتسوقين وأصحاب الأنشطة التجارية بديلاً فريداً للمعاملات التجارية عبر الإنترنت. وتقدم "أي جولد" لعملائها عملة

رقمية تطلق عليها الذهب الإلكتروني ولا يحتاج فتح حساب لدى موقع الشركة إلا يضع نقرات على الماوس.

ويمكن للعملاء أن يستخدموا أسماء مزيفة لأنه لا توجد جهة تراقب أنشطة الشركة. وعن طريق بطاقة ائتمان أو تحويل إلكتروني يشتري العميل وحدات من الذهب الإلكتروني يمكن نقلها ببساطة لأي عميل آخر لديه حساب لدى الشركة وبالنسبة لمتلقى الأموال تتم عملية تحويل وحدات الذهب الإلكتروني إلى أموال تقليدية بنفس السهولة وأيضاً دون الحاجة للكشف عن هويته الحقيقية وتجتذب فكرة الذهب الإلكتروني الأشخاص الذين يفضلون الاستثمار في الذهب ويعتقدون أن الأموال يجب أن ترتبط به وتتباهى شركة "أي جولد" بأن عملتها الافتراضية مدعومة باحتياطي ذهبي مخزن في لندن ودبي. لكن الفكرة تجتذب أيضاً المجرمين الذين يريدون نقل الأموال بسرعة ودون أن يكتشفهم أحد وفي حين تخضع المصارف الأمريكية وشركات تحويل الأموال التقليدية مثل "وسترن يونيون" لالتزامات قانونية بمراقبة عملائها وإبلاغ السلطات عن أي تحويلات مريبة لا تواجه "أي جولد" هذه المشكلة فالشركة تمارس أنشطتها من ولاية فلوريدا الأميريكية لكنها مسجلة في جزيرة نيفس بالبحر الكاريبي حيث القوانين المالية متساهلة للغاية.

ويخشى المسؤولون الأمنيون ورجال القانون حول العالم من أن صناعة العملات الرقمية الناشئة تتحول بصورة متزايدة إلى ماكينة لغسل الأموال من قبل عصابات الإجرام حول العالم[1].

ويخشى المسؤولون الأمنيون ورجال القانون حول العالم من أن صناعة العملات الرقمية الناشئة تتحول بصورة متزايدة إلى ماكينة لغسل الأموال من قبل عصابات الإجرام حول العالم.

ففي ١٩ ديسمبر ٢٠٠٥ قام عملاء من مكتب التحقيقات الفيدرالي (أف. بي. بي) بتفتيش مقر شركة جولد اند سيلفر ريسرف (الشركة الأم لشركة "أي جولد") في مدينة ميلبورن بولاية فلوريدا الأميريكية ومنزل مؤسس الشركة دوجلاس أل جاكسون وقاموا بنسخ وثائق وملفات كمبيوتر لكن حتى الآن لم توجه أي اتهامات للشركة ورفض مكتب التحقيقات التعليق على حملة التفتيش كما نفي جاكسون أن تكون شركته متورطة في أي أنشطة مخالفة للقانون لكن عميل بارز لدى مكتب التحقيقات الفيدرالي أكد لمجلة بيزنس ويك أن تحريات يجريها المكتب وجدت أن "أي جولد" هي العنصر المشترك بين عشرات الأنشطة المخالفة للقانون عبر شبكة الإنترنت. وتتجاوز المخاطر المحتملة لهذا الاتجاه شركة "أي جولد" بمراحل.

---

(1) د. محمد البشري، التحقيق في جرائم الحاسب والإنترنت، بحث منشور في المجلة العربية للدراسات الأمنية، المجلد ١٥ العدد ٣٠، منشورات أكاديمية نايف للعلوم الأمنية، الرياض، نوفمبر ٢٠٠٠، ص ٣١٧.

ويؤكد محققون في هذه الجرائم أن عملات رقمية أخرى يتم استخدامها بنفس الطريقة لخدمة أغراض غير قانونية وتوجد دستة من هذه الخدمات على الأقل في مناطق مثل روسيا وبنما وتدعي ثمانية منها على الأقل بما في ذلك "أي جولد" أن سبائك ذهب حقيقية تغطي معاملاتها المالية ووفقاً لاتحاد العملات الرقمية العالمي فإن إجمالي قيمة التحويلات المالية التي تنفذها هذه الشركات يبلغ مليارات الدولارات سنوياً وتحقق "أي جولد" ومنافسوها أرباحاً من خلال تحصيل نسبة صغيرة من الرسوم على تلك التحويلات.

وتركز معظم تحريات الأجهزة الأمنية على عمليات غسل الأموال والاحتيال التي تتم عن طريق خدمة "أي جولد" وتؤكد مصادر أمنية أميريكية أن الخدمة يتزايد استخدامها في مواقع الإنترنت التي تقوم بأنشطة مخالفة للقانون مثل بيع معلومات الحسابات المصرفية وبطاقات الائتمان لكن الخطر الأعظم كما تشير هذه المصادر يتمثل في إمكانية استخدام الذهب الإلكتروني والعملات الرقمية الأخرى لتمويل الإرهاب وهي الدعوى التي ترفضها كل الشركات العاملة في هذه الصناعة الناشئة. ويشير محققون إلى التشابه في طريقة العمل بين خدمة "أي جولد" ونظام الحوالات الذي استخدمته تنظيمات إرهابية في منطقة الشرق الأوسط لنقل الأموال وتم بالفعل إغلاق العديد من هذه الشركات في أعقاب هجمات ١١ سبتمبر مما يجعل العملات الرقمية الخطوة المنطقية التالية[1].

(1) www .alriyadh. com

ونبتت فكرة "أي جولد" من بنات أفكار دوجلاس أل. جاكسون وهو مستثمر أمريكي يؤمن بقاعدة الصرف بالذهب حاول قبل عشر سنوات تأسيس نظام مالي خاص يقوم على قاعدة الذهب متصوراً أن بإمكانه إطلاق عملة ذهبية إلكترونية عالمية تكون مقبولة في كل مكان. هذه الرؤية لم تتحقق لكن شركة "آي جولد" نجحت في اجتذاب الكثيرين ممن يؤيدون قاعدة الصرف بالذهب وبين هؤلاء اندست أعداد كبيرة من المجرمين كما يقول مسؤولون من جهات أمنية أميريكية. ويبلغ عدد الحسابات المسجلة لدى شركة "آي جولد" ١ر٢ مليون حساب تمت من خلالها تحويلات بقيمة ١ر٥ مليار دولار في عام ٢٠٠٥ ويقول جاكسون أن إيرادات الشركة بلغت مليوني دولار في ٢٠٠٥ لكنه يرفض الإعلان عن حجم الأرباح.

وبدأت "آي جولد" أنشطتها في عام ١٩٩٦ في إطار موجة أكبر من شركات الدفع الإلكتروني التي عملت على تحويل الأموال الحقيقية إلى عملات افتراضية يمكن تحويلها عبر الإنترنت. لكن معظم هذه الشركات انهارت بسبب عدم رغبة المستهلكين في دفع رسوم إضافية فيما تطور بعضها مثل بايبال إلى خدمات لتحويل بطاقات الائتمان. وفي المقابل قامت "آي جولد" وحفنة من المنافسين مثل شركة جولدموني على مبدأ مختلف فقد أمن مؤسسوها بأن ربط سعر الصرف النقدي بقاعدة ذهبية سيقود إلى استقرار اقتصادي أكبر ويقلل مخاطر التضخم ووفرت الإنترنت لهؤلاء

الوصول بسهولة لعملاء يؤمنون بنفس الفكرة تماما كما لعبت دور سندوق التجارب لكل صاحب فكرة جديدة أخرى.

ويبرز جاكسون عدم قيام الشركة بمراقبة حسابات العملاء بأن "آي جولد" ليست مثل أي نظام آخر فهي غير ملزمة بالقوانين التي تنظم العمل في المؤسسات المالية والمصرفية التقليدية ويعترف المسؤولون الأميركيون بهذه الثغرة ويقول مارك راسك من شركة سوليوشنري لأمن الشبكات والرئيس السابق لوحدة مكافحة جرائم الكمبيوتر بوزارة العدل الأميريكية الأمر ليس كما لو أنها تخضع للرقابة التنظيمية لطرف آخر أنها لا تخضع لأي تنظيم. وتقول شبكة مكافحة الجرائم المالية التابعة لوزارة الخزانة الأمريكية أنها تعمل على سد تلك الثغرة ولكن حتى ذلك الحين يجب على الشركات مثل "آي جولد" أن تقوم طواعية بكل ما في وسعها لمنع استغلال خدماتها في أنشطة إجرامية.

المبحث الثالث

الحلول العلمية لمكافحة جرائم المعلوماتية والإنترنت

سوف نبحث في بعض الحلول العملية فيما يتعلق ببعض الإجراءات المتطلبة في هذا المجال وفيما يتعلق بضبط وتفتيش أنظمة الكمبيوتر وعمليات التفتيش التي تتم عبر شبكة الإنترنت.

المطلب الأول

الحلول العملية فيما يتعلق ببعض الإجراءات

المتطلبة في هذا المجال

- لابد من اتخاذ وسائل الحيطة والحذر في تعامل البنوك مع الأنشطة المصرفية التي تتم عبر الإنترنت نظراً لأن تركيز غاسلي الأموال يتم على هذه البنوك وبهذه الأساليب باعتبارها مرتعاً خصباً لتجارتهم خصوصاً إذا كانت الدول التي ترعى هذه البنوك أو التي في ضيافتها تعاني من عجز في النظام الرقابي العام للدولة.

- إصدار قوانين واضحة وصارمة تلزم جميع المصارف بوضع الخطوات العملية الضرورية لمنع غسل الأموال فيها خاصة تلك الأموال التي يتم التعامل بها عبر الإنترنت.

- ضرورة قيام المصارف بتدابير عملية من شأنها تكشف محاولات غسل الأموال فيها ومراقبة جميع التعاملات الإلكترونية.

- ضرورة قيام المصارف بإنشاء أجهزة أو إدارات تتولى مراقبة ومتابعة البلاغات التي تصلها عن أي عملية أو نشاط مشبوه. وبالتالي الإبلاغ عنها للجهات المختصة في الدولة خاصة إن كانت تلك العمليات المصرفية تتعلق بأنشطة تتم عبر الإنترنت.

- ضرورة تدريب العاملين في المباحث الجنائية على تفحص الأدلة الإلكترونية.

- ضرورة تدريب المحققين على القيام بالكشف عما تحتويه أجهزة الكمبيوتر من برامج مخزنة عند الضرورة مما ييسر عمليات التفتيش التي تتم على كمبيوتر المتهم.

- ضرورة الاستعانة بخبراء في الكمبيوتر والشبكات أثناء عمليات التقصي والتحقيق في الجرائم المعلوماتية والإنترنت[1].

المطلب الثاني

الحلول العملية فيما يتعلق بضبط وتفتيش أنظمة الكمبيوتر وعمليات التفتيش التي تتم عبر شبكة الإنترنت

إن الانتشار الكبير للإنترنت في الحياة العملية أظهر الحاجة في وضع الحلول القانونية للمشاكل الناتجة عن استخدام الإنترنت في ضوء القواعد العامة للقانون إضافة إلى أهمية توجيه نظر المشرع للتدخل لوضع قواعد خاصة لتنظيم استخدام الإنترنت في بعض المجالات الحيوية واستخلاص القواعد الرئيسية في هذا المجال والتي يمكن ببمشرع أن يستهدي بها إذا ما أراد يوماً تنظيم مجال أو أكثر من مجالات استخدام الإنترنت بقواعد خاصة كالإثبات وكذلك بيان الأحكام القانونية لاستخدام الإنترنت في بعض المجالات[2].

([1]) أ. محمد الألفي. المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت. المكتب المصري الحديث القاهرة. ٢٠٠٥، ص ٢٠٢.

([2]) أ. عبد الله عبد الكريم عبد الله، مصدر سابق ص ٥٦- ٦٠.

وعلى المشرع وضع بعض النقاط نصب نظره وهي الحماية المدنية لمواقع الإنترنت والإثبات والضوابط القانونية لاستخدام الإنترنت والتحديات التقنية وإرهاصات الجريمة المنظمة عبر الإنترنت وتفعيل قانون العقوبات. ومخاطر تقنية المعلومات وأمن المعلومات في الإنترنت. بالتالي فقد تعولمت الجريمة وظهرت أنماط جديدة منها وأصبحت الجريمة تنفذ عن بعد دون الحاجة إلى الفعل التقليدي فيما يتعلق بموضوع الجريمة.

ففي جريمة مثل غسل الأموال وتحويلها عبر الإنترنت وسرقة البنوك والحسابات التي لم تعد تتطلب السطو على البنك في موقفه الحقيقي في مكان معين، وإنما يمكن أن يكون ذلك إلكترونياً بتحويل أرصدة من الحسابات إلى حسابات أخرى في دول أخرى أي في موقع افتراضي معين.

وظهرت جرائم الحاسب والجرائم المرتبطة بالحاسب، وجرائم الملكية الفكرية وجرائم القرصنة عبر الإنترنت وانتهاك حقوق الملكية الفكرية. والنصب الإلكتروني عبر الإنترنت وكل هذه الأنماط شكلت تحدياً جديداً في وسائل الوقاية والمكافحة.

لذلك فالتدخل التشريعي الوطني والدولي مطلوب الدولي مطلوب بقوة في هذه المرحلة بشكل أكبر من أي وقت مضى في ظل سرعة اتلاف الدليل وطبيعة ما يثبت الجريمة ذاتها من الأدلة. وفي ظل الحاجة للتدخل السريع لضبط متعلقات الجريمة. وفي ظل ارتباط مادة الجريمة أو وسيلتها بأنظمة أطراف أخرى لا صلة لهم بها أو بشبكات ونظم معلومات خارج الحدود. فإن المكافحة الفاعلة قد تنطوي على إهدار لحقوق وحريات

الكثيرين والتفريط بضمانات المتهم وما توجبه قرينة البراءة المقررة له. وهذا التناقض لا مجال لفضه إلا بإقامة معيار تعكسه القواعد التشريعية، فالاستثناء على الحرية والقيد المقرر عليها يعدو مقبولاً في ضوء اعتبارات مصلحة المجتمع وأمنه متى ما توفر بحق هذا المبرر ومتى ما كان المعيار مدركاً أن الاستثناء لا يجوز التوسع فيه ويتعين تقييده بالقيد التشريعي الواضح الذي لا يتيح للسلطات استخدامه عبثاً بما منحها القانون من حقوق أو بما تفسره هي وفق رؤيتها لما قرره القانون لها من صلاحيات.

فالتفتيش بصورته التقليدية يتطلب مذكرة قضائية. أما في حالة اتصل ذلك بجريمة تتم عبر الإنترنت فلابد أن تشمل المذكرة القضائية ما مفاده جواز تفتيش أنظمة الكمبيوتر والقواعد التي ترعى التعامل عبر الإنترنت. وأما إجراء التفتيش دون مذكرة قضائية أو الحصول على بيانات من جهات ليست محلاً للاشتباه لتعلقها بالمشتبه بها. فإنها مسائل تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد وتوتجب مشروعية الدليل وسلامة مصدره، أو تبطل كل إجراء يتم خلافاً للقواعد الأصولية المتعلقة بالتفتيش والضبط المنصوص عليها في القانون.

لذلك يجب أن يتضمن إذن التفتيش الإجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت استخدام الأنظمة الآلية

لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات[1].

وتعتبر هذه المسائل محل قصور يحاول أن ينفد من خلالها الجناة عند عدم إجازة القانون هذا المسلك الاستثنائي وعلى نحو يجعل من الضرورة بمكان التمسك بضرورة عدم اللجوء إلى هذا السلوك لأن المشروعية الإجرائية توجب تحقيق أقصى ضمانات للمتهم تتفق ومقتضيات قرينة البراءة.

لذلك نجد أنه ونظراً لحداثة تلك الجرائم ولتنوعها وللطابع التقني الذي يستخدم في ارتكابها، تواجه السلطة القضائية والأجهزة الأمنية صعوبات عديدة في اكتشاف وملاحقة مرتكبيها [2].

ومن الثابت أنه لا يمكن إلزام أية جهة بتقديم أية بيانات بشأن الخدمات المقدمة للزبائن أو علاقتهم به. لأن هذه البيانات في الأصل سرية ولا يجوز إفشاؤها إلا وفق القانون، فإن الحاجة تعدو ماسة للتدخل التشريعي لإتاحة آلية الضبط المستعجل للنظم المشتبه بها مع أمر كف يد المشتبه به عن استخدام النظام فوراً بمجرد البدء بإجراءات التفتيش، إضافة إلى الحق في ضبط الأجهزة لإجراء التفتيش عليها في مقار التحقيق باستخدام التقنيات التي تتيح ذلك والتي قد لا تتوفر في مكان التفتيش، خاصة إذا ما علمنا أن تفتيش جزء صغيرة جداً من الذاكرة قد يحتاج

---

(1) قرار محكمة الجنايات اللبنانية منشور في مجلة العدل اللبنانية ٢٠٠٠ ص ٣٧٥.

(2) د. فتوح الشاذلي وعفيفي عفيفي، جرائم الكمبيوتر. منشورات الحلبي الحقوقية ٢٠٠٢ بيروت، ص ١٧.

ساعات، فكيف هو الحال وقد أصبحت ذاكرات الكمبيوترات قادرة على تخزين ملايين الملفات، إضافة إلى أن التفتيش الأولي قد لا يحل مشكلة الملفات المخبأة أو المحمية أو المشفرة.

لكن هذه الحلول في نطاق التفتيش تناقض القواعد المقررة قانوناً في حقل ضمانات المتهم وضمانات احترام حقوق الإنسان والحريات الفردية وفي مقدمتها الخصوصية. فمثل هذه الإجراءات قد تؤدي إلى كشف بيانات شخصية أو كشف أسرار العمل أو الوصول إلى ملفات يحرص أصحابها على سريتها أو تيح لهم القانون ذلك، وتعدو المسألة أكثر خطورة عندما يمتد التفتيش إلى نظم مرتبطة بالنظام موضوع الاشتباه، فتطال ملفات وبيانات جهات لا علاقة لها بالجريمة قد تكون خاضعة لسرية مهنية أو قواعد حماية سرية بيانات العملاء كما في حالة نظم الكمبيوتر الخاصة بمزودي الخدمات أو نظم كمبيوترات البنوك أو كمبيوترات مزودي خدمات الإنترنت أو الشركات التي تتعاطى البيع عبر الإنترنت [1].

(1) أنظر نبيلة هدوال، المرجع السابق ذكره، ص ٢٢٩ وما بعدها.

الفصل السادس

الإطار الإقليمي لمكافحة جرائم الإنترنت

تعتبر الجرائم المرتكبة عبر الإنترنت وجرائم المعلوماتية كما رأينا من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني والدولي. على حد سواء، والتي ينبغي مواجهتها بتشريعات حاسمة ومعاهدات دولية لمكافحتها وإنزال العقاب بمرتكبيها حيث تعد – وبحق – من أبرز إفرازات ثورة المعلوماتية وعصر العولمة [1].

وتتجلى أهمية دراسة الموضوع من عدة جوانب فقد تثير المعلوماتية وتجلياتها مشكلات قانونية عدة، إذ يساء استخدامها لارتكاب الجريمة عن بعد من جهة، أو تكون محلاً للاعتداء عليها من جهة أخرى، مما يثير مسألة تكييف الاعتداء وما إذا كان يشكل جريمة أم لا. وما يتبع ذلك من مشكلة الدليل والتحقيقات.

بالإضافة إلى ما تثيره من مشكلة تحديد الاختصاص القضائي والقانون الواجب التطبيق على الجرائم المرتكبة عبرها.

وعلاوة على ذلك فإن الإجراءات الجنائية المتبعة في نظام ملاحقة مرتكبي جرائم المعلوماتية تثير الكثير من المشكلات القانونية، بدءاً من مرحلة الاستدلال وجمع الأدلة، حتى صدور الحكم الجنائي، ولا سيماً في ما يتعلق بإثبات الجرائم المرتكبة عبر الإنترنت وصلاحية الدليل الرقمي

---

(1) عبد الله عبد الكريم عبد الله، مصدر سابق ص ٢٠٠٧م- ١٤٢.

للإثبات ومدى شرعية الأدلة المتحصلة بواسطة الإنترنت وقبولها لدى القاضي الجنائي.

وتبدو أهمية الموضوع بجلاء أيضاً من كون المعلومات تمثل قيماً اقتصادية، مما ينبغي معه وضع مبدأ الحق في المعلومات في نصابه، وذلك بتحقيق التوازن بين الاستخدام الحر للمعلومات، وبين الحقوق والحريات والمصلحة العامة، بحماية من تتعلق بهم المعلومات على نحو غير مشروع في ارتكاب جرائم الغش المعلوماتي وحماية حقوق الملكية الفكرية على شبكة الإنترنت[1].

ونظراً لتزايد المواقع التجارية على شبكة الإنترنت، وظهور ونمو التجارة الإلكترونية وقيام المنافسات غير المشروعة، فإن أهمية الدراسة تنبثق في ضرورة تنظيم هذه المواقع وتنظيم محتواها. وحماية المواقع الأصلية على الشبكة من التقليد أو المنافسة غير المشروعة، بالإضافة إلى حماية الإسم التجاري والعلامة التجارية، وتنظيم آلية الدفع الإلكتروني تجنباً لجرائم السرقة أو الاحتيال أو ما يعرف بالغش المعلوماتي، بما يؤدي إلى استقرار المعاملات والشعور بالثقة والأمان.

فإساءة استخدام هذه المواقع تؤثر سلباً من الناحية الاقتصادية على حجم التجارة الإلكترونية والمبادلات التجارية الإلكترونية، بما يؤدي إلى ضياع الحقوق وانتهاكها.

---

(1) أنظر نبيلة هدوال، المرجع السابق ذكره، ص ٢٢٩ وما بعدها.

وتجد العصابات الإرهابية شبكة الإنترنت خير وسيلة لنشر أفكارها والتشجيع على القيام بأعمال إرهابية.

فعلى المستوى القومي يجد المجرمون دوراً كثيرة في ممارسة إجرامهم، وستغلال شبكة الإنترنت في أنشطة إرهابية ووضع المعلومات التي تتناسب مع مصالحهم. حيث يؤثر ذلك على قانون العقوبات فيما يتضمنه من نصوص تتعلق بالجرائم الماسة بأمن الدولة والجرائم ذات الطبيعة السياسية والجرائم المتعلقة بالإرهاب وغسل الأموال عبر الإنترنت.

من هنا تبرز أهمية وجود منظمة عربية لمكافحة جرائم المعلوماتية والإنترنت لوضع قواعد تساعد في إبراز مدى كفاية النصوص الجنائية الحالية لمنع الجرائم المرتكبة عبر الإنترنت وردع مرتكبيها، أم يلزم تعدل هذه النصوص بما يتواءم مع التطور التقني للمعلوماتية، وكذلك إنشاء وعي قانوني ومهني لدى المشتغلين بهذا الموضوع وتبادل الخبرات معهم عبر الندوات والمؤتمرات وورش التدريب والعمل بما يساهم في تحقيق الأهداف المتوخاة من إنشاء هذه المنظمة.

المبحث الأول

القانون العربي الاسترشادي (النموذجي) لمكافحة

جرائم تقنية أنظمة المعلومات وما في حكمها

(قرار ٤١٧، د ٢١/ ٢٠٠٤م) [١].

اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة، والذي كان قد اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم ٤٩٥- د ١٩ – ٨/ ١٠/ ٢٠٠٣ ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين.

وسوف نعرف لأحكام هذا القانون الاسترشادي حسب مواده.

المطلب الأول

المفاهيم المتضمنة في هذا القانون

نصت المادة (١) على ما يلي:

في تطبيق أحكام هذا القانون يقصد بالكلمات والعبارات الآتية، المعاني الموضحة قرين كل منها:

❖ **البيانات:**

---

(١) Arabic – mjustice. dz.

كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي، كالأرقام والحروف والرموز وما إليها ..

❖ **البرنامج المعلوماتي:**

مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام الحاسب الآلي ومعدة لإنجاز مهمة ما.

❖ **النظام المعلوماتي:**

مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

❖ **الشبكة المعلوماتية:**

ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.

❖ **الموقع:**

مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

❖ **الالتقاط:**

مشاهدة البيانات أو المعلومات أو الحصول عليها.

المطلب الثاني
الإطار التجريمي والعقابي

نصت المادة (٢) على ما يلي:

مع عدم الإخلال بأية عقوبة أشد في قانون العقوبات (الجزاء) أو في أي قانون آخر، يعاقب على الأفعال المنصوص عليها في المواد التالية، بالعقوبات المقررة فيها.

أما المادة (٣) فقد نصت على ما يلي:

كل من دخل عمداً وبغير وجه حق موقعاً أو نظاماً معلوماتياً يعاقب بالحبس ... والغرامة .... أو بإحدى هاتين العقوبتين.

فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف او تغيير أو بإعادة نشر بيانات أو معلومات شخصية يكون الحد الأدنى لعقوبة الحبس .... ولعقوبة الغرامة .....

المادة (٤) نصت على التالي:

كل من ارتكب تزويراً في أحد المستندات المعالجة في نظام معلوماتي يعاقب بالحبس مدة لا تقل عن .... ويعاقب بذات العقوبة كل من استعمل المستند المزور مع علمه بالتزوير.

أما المادة (٥) فقد نصت على التالي:

إذا ارتكب الجاني أياً من الجرائم المنصوص عليها في المادة (٣) أثناء أو بسبب تأديته وظيفته، أو سهل ذلك للغير، يكون الحد الأدنى لعقوبة الحبس .... ولعقوبة الغرامة ...

فإذا توفر أي ظرف من الظروف المشددة المنصوص عليها في الفقرة الثانية من المادة المذكورة، يكون الحد الأدنى لعقوبة الحبس ..... ولعقوبة الغرامة .....

المادة (٦) نصت على ما يلي:

كل من أدخل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات يغرض ذلك ولم يتحقق غرضه يعاقب بالحبس .... والغرامة ... أو بإحدى هاتين العقوبتين. فإذا تحقق الغرض كان الحد الأدنى لعقوبة الحبس .... ولعقوبة الغرامة .....

نص المادة (٧) كما يلي:

كل من أعاق أو شوش أو عطل عمداً وبأية وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها الوصول إلى

الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات يعاقب بالحبس .... والغرامة ..... أو بإحدى هاتين العقوبتين.

نصت المادة (٨) على التالي:

كل من تنصت أم التقط أو اعترض بدون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، يعاقب بالحبس .... والغرامة ..... أو بإحدى هاتين العقوبتين.

المادة (٩) نصت على ما يلي:

كل من استعمل الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس ..... والغرامة ..... أو بإحدى هاتين العقوبتين.

إما المادة (١٠) فأتى نصها على الكل التالي:

كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجنى عليه. يعاقب بالحبس .... والغرامة ... أو بإحدى هاتين العقوبتين.

المادة (١١):

كل من استخدم الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في الوصول، بدون وجه إلى أرقام أو بيانات بطاقة ائتمانية وما في حكمها بقصد استخدامها في الحصول على بيانات الغير أو أمواله أو ما تتيحه من خدمات، يعاقب بالحبس ... والغرامة ... أو بإحدى هاتين العقوبتين.

المادة (١٢):

كل من انتفع، بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة المحاسب الآلي وما في حكمها بخدمات الاتصالات يعاقب بالحبس ..... والغرامة .....

المادة (١٣):

كل من أنتج أو أعد أو هيأ أو أرسل أو خزن عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها ما من شأنه المساس بالنظام العام أو الآداب العامة يعاقب بالحبس .... والغرامة ..... فإذا كان الفعل موجهاً إلى حدث يكون الحد الأدنى لعقوبة الحبس .... ولعقوبة الغرامة ....

المادة (١٤):

مع عدم الإخلال بالأحكام المقررة لحماية حقوق الملكية الفكرية، يعاقب كل من نشر أو نسخ عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها مصنفات فكرية أو أدبية أو أبحاث علمية أو ما في حكمها بدون وجه حق، بالحبس .... والغرامة ..... أو بإحدى هاتين العقوبتين. فإذا كان النشر أو النسخ بقصد التسويق أو الربح تكون العقوبة الحبس ....

المادة (١٥):

كل من دخل بدون وجه حق، في موقع خاص لشركة أو مؤسسة أو غيرها لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين.

المادة (١٦):

كل من اعتدى على أي من المبادئ أو القيم الدينية أو الأسرية أو حرمة الحياة الخاصة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، يعاقب بالحبس مدة لا تقل عن ...

المادة (١٧):

كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الاتجار في الجنس البشري أو تسهيل التعامل فيه يعاقب بالحبس ... والغرامة ...

المادة (١٨):

كل من كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، بقصد الاتجار أو الترويج أو التعاطي بالمخدرات أو المؤثرات العقلية وما في حكمها أو تسهيل التعامل فيها يعاقب بالحبس ... والغرامة .....

المادة (١٩):

كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه، أو قام باستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع، أو بتحويل الموارد أو الممتلكات، مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر موقعاً لارتكاب أي من هذه الأفعال، يعاقب بالسجن ...

المادة (٢٠):

كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لأي مجموعة تدعو لتسهيل وترويج برامج وأفكار مخالفة للنظام العام يعاقب بالحبس ..... وبالغرامة .....

المادة (٢١):

كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن .....

المادة (٢٢):

كل من دخل عمداً وبغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني يعاقب بالسجن ....

فإذا كان الدخول بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو بث أفكار تمس ذلك، يكون الحد الأدنى لعقوبة السجن .....

المادة (٢٣):

كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة الجرائم المنصوص عليها في هذا القانون ووقعت الجريمة بناء على التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة المقررة لها.

ويعاقب بنصف العقوبة المقررة للجرائم المنصوص عليها في المواد (١٦- ٢٢) ولو لم تقع الجريمة الأصلية.

المادة (٢٤):

يعاقب على الشروع في الجرائم المنصوص عليها في المواد (٣- ١٥) بنصف العقوبة المقررة لها ويعاقب على الشروع هي الجرائم المنصوص عليها في المواد (١٦- ٢٢) بذات العقوبة المقررة لها.

المادة (٢٥):

مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو المشروع الذي يكون محلاً لارتكاب أي من هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالكها، وذلك إغلاقاً كلياً أو للمدة التي تقدرها المحكمة [١].

(١) نقلاً عن أ. عبد الله عبد الكريم عبد الله مصدر سابق ص ١٤٧- ١٥٨.

المطلب الثالث

إطار تطبيق هذا القانون

المادة (٢٦):

تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه حتى ولو ارتكبت كلياً أو جزئياً خارج إقليم الدولة، متى أضرت بأحد مصالحها ويختص القضاء الوطني بنظر الدعاوي المترتبة عليها.

المادة (٢٧):

فضلاً عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه وفقاً لمواد (١٦- ٢٢).

المبحث الثاني

الإطار العربي المقترح كإطار مؤسسي لمكافحة جرائم المعلوماتية والإنترنت

(المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت)

سوف نبحث في هذا المجال في اقتراح نظام أساسي وداخلي لإنشاء المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت كي تكون إطاراً مؤسسياً هدفه مكافحة جرائم الإنترنت والمعلوماتية وإبرازها لمعالجة الآثار السلبية الناشئة عنها بجهد عربي موحد يوائم ويكمل الجهد الذي بذل في إبرام قانون عربي موحد لمكافحة الجرائم المعلوماتية.

المطلب الأول

النظام الأساسي المقترح لإنشاء المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت

المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت هي منظمة علمية ومهنية غير حكومية ذات طابع عربي واهتمامات قانونية واقتصادية معنية بتنظيم الأطر القانونية والإجرائية والمؤسسية لمكافحة الجرائم التي تتم عبر الإنترنت وكافة الجرائم المعلوماتية.

وتم الاتفاق على إنشاء منظمة عربية تحمل اسم المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت.

وتم وضع الإطار التنظيمي للمنظمة كما يلي:

(النظام الأساسي)

مادة (١)

تنشأ منظمة باسم "المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت" يكون مقرها الرئيس في دولة ..... وهي منظمة مهنية متخصصة لا تتوخى الربح ولا تتعاطى أية أنشطة سياسية.

مادة (٢)

تأسيس المنظمة

تم تأسيس المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت، منظمة علمية غير حكومية ذات استقلال مالي وإداري وتتخذ الطابع الإقليمي وذلك في المؤتمر الدولي الأول لمكافحة جرائم المعلوماتية والإنترنت المنعقد في "....." . وتعمل المنظمة بالتنسيق مع كافة المنظمات الإقليمية والدولية التي تساند المنظمة مادياً وتنظيمياً في جميع أنشطتها.

مادة (٣): مركز المنظمة:

دولة .....

مادة (٤): أهداف وأنشطة المنظمة

تهدف المنظمة وتستهدف تحقيق ما يلي:

١. نشر الوعي القانوني والمهني للتعريف بالجرائم الناشئة عن استخدام الإنترنت وجرائم المعلوماتية وتعزيز جهود وأساليب مكافحتها.

٢. إعداد الدراسات والبحوث حول سبل مكافحة جرائم المعلوماتية وكافة الجرائم التي تتم عبر أو باستخدام شبكة الإنترنت أو الحاسوب والعمل على تشجيع البحث العلمي في مجال دراسة الجرائم الناشئة عن استخدام الإنترنت.

٣. إعداد ومتابعة المحافل العلمية والأكاديمية وحضور المؤتمرات والندوات المتعلقة بالجرائم ضد المعلوماتية والجرائم الناشئة عن استخدام الإنترنت.

٤. إعداد قاعدة بيانات للجرائم ضد المعلوماتية والجرائم الناشئة عن استخدام الإنترنت.

٥. تقديم الاستشارة والدعم العلمي والمهني للمؤسسات والأفراد والحكومات وكل من له مصلحة في مكافحة الجرائم الناشئة عن استخدام الإنترنت.

٦. تنمية الكوادر البشرية في مجال مكافحة هذه الجرائم وتأهيل أعضاء المنظمة مهنياً لذلك ..

٧. إعداد الأطر القانونية والإجرائية والمؤسسية للمكافحة.

٨. المساهمة في رسم أطر وقائية وعقابية لمكافحة جرائم المعلوماتية والإنترنت.

٩. تشجيع وتنمية وتطوير تفاعل العمل غير الحكومي مع الأهداف الرامية لمكافحة جرائم المعلوماتية والإنترنت والمساهمة في وضع التصور الإقليمي لمكافحة جرائم المعلوماتية والإنترنت والتعاون مع الجهات الحكومية وغير الحكومية المحلية الإقليمية والدولية في هذا الإطار.

١٠. مكافحة كافة أشكال الجرائم التي تقع ضد المعلوماتية في كافة أشكالها (الأجهزة والبرامج والشبكات والمعلومات والبيانات والأموال ووسائل الاتصال والجرائم ضد السمعة والجرائم ضد الشخصية) والجرائم ضد الإنسانية والجرائم الموجهة للأمن القومي في كافة أشكالها وصورها.

وبالعموم مكافحة كافة الجرائم التي يكون الحاسب أو الإنترنت أداة من أدواتها أو هدفاً من أهدافها أو سطا لها.

١١. إعداد مراكز تدريب عربية في إطار مكافحة جرائم المعلوماتية والإنترنت، وعمل دورات تدريبية وورش عمل ومؤتمرات تعالج هذا الموضوع.

١٢. إصدار الكتب والنشرات المتعلقة بالمواضيع محل اهتمام المنظمة وإصدار مجلة تحمل اسم المنظمة دورياً.

ويجوز للجمعية العمومية إدخال التعديلات التي تتماشى وتطوير نشاط المنظمة.

مادة (٥): موارد المنظمة

١. اشتراكات الأعضاء.

٢. المنح والمساعدات.

٣. اشتراكات الأنشطة التي تقوم بها المنظمة كالدور الاستشاري والعلمي والقانوني والمهني وخطط العمل والمشروعات التي تضطلع بها المنظمة ..

٤. دعم المنظمات الدولية والإقليمية.

مادة (٥): تأليف المنظمة

الهيكلية: تتألف المنظمة من هيئتين: الهيئة الإدارية والهيئة العامة ويحدد تأليفهما بموجب أحكام النظام الداخلي، وتضم عدة لجان متخصصة تحدد أيضاً في الضمان الاجتماعي.

مادة (٦) الانتساب

١- الانضمام إلى عضوية المنظمة متاح لكافة القانونيين والاقتصاديين والمهنيين والممارسين لهذا المجال والمهتمين بأهداف المنظمة وتطلعاتها والذين يرغبون بالاستفادة من أنشطة وبرامج المنظمة والمشاركة فيها شرط استيفائهم معايير العضوية.

٢. تقبل الجمعية جميع الحاصلين على مؤهلات جامعية من كافة الأقطار العربية كأعضاء عامين كما تقبل الجمعية انضمام طلبة الجامعات والمدارس العليا كأعضاء منتسبين لحين حصولهم على المؤهل وبلوغهم سن الثامنة عشرة .....

٣. يجوز قبول عضوية مؤسسات أكاديمية وبحثية علمية كأشخاص معنوية.

٤. العضوية الشرفية التي يتم منحها بعد استيفاء الدراسات اللازمة في هذا الشأن. ويجوز منح العضوية الشرفية لكل من قدم خدمات جليلة للمنظمة.

مادة (٨): كيفية الانتساب

١. يتقدم من تتوفر فيه شروط العضوية بطلب يعلن فيه عن رغبته بالانضمام إلى المنظمة مرفقاً بالسجل العدلي وصورة عن الهوية الشخصية أو جواز السفر.

٢. تدرس الهيئة الإدارية الطلب والمستندات المرفقة وتتخذ القرار المناسب.

مادة (٩) الهيئة الإدارية

١- تتألف الهيئة الإدارية من ..... أعضاء. ويقوم المؤسسون بصلاحيات الهيئة الإدارية لمدة سنتان من تاريخ الترخيص للمنظمة.

٢- تنتخب الهيئة الإدارية من قبل الهيئة العامة بالاقتراع السري بشرط حضور أكثر من نصف أعضاء الهيئة العامة المسددين لاشتراكاتهم السنوية وتكون ولاية الهيئة الإدارية .....

ويدير جلسة الانتخاب هيئة من ثلاثة أعضاء من الهيئة العامة من غير

مادة (١٠) الهيئة العامة

تتألف الهيئة العامة من جميع الأعضاء النتسبين فعلياً وتتحدد صلاحياتها تفصيلاً في النظام الداخلي.

مادة (١١) الحل:

يمكن حل المنظمة بناء على طلب مقدم منها واستناداً إلى قرار من الهيئة العامة مقروناً بموافقة ٧٥٪ من مجموع أعضائها.

المطلب الثاني

النظام الداخلي المقترح للمنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت

يكون النظام الداخلي كما يلي:

الفصل الأول

الباب الأول

التأسيس، المقر، والأهداف

المادة ١- التأسيس

يسمى هذا النظام (النظام الداخلي للمنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت)، ويعمل به منذ تاريخ الترخيص بالعمل.

المادة ٢- المقر

تكون مدينة ..... المقر الرسمي للمنظمة، على أنه يحق للمنظمة فتح فروع لها في أية منطقة تراها مناسبة داخل أو خارج .....

الباب الثاني

رسالة المنظمة وأهدافها

حيث أن المنظمة جمعية/ هي منظمة علمية ومهنية غير حكومية ذات طابع عربي واهتمامات قانونية واقتصادية معنية بتنظيم الأطر القانونية والإجرائية والمؤسسية لمكافحة الجرائم التي تتم عبر الإنترنت وكافة الجرائم المعلوماتية.

تهدف المنظمة وتستهدف تحقيق ما يلي:

١. نشر الوعي القانوني والمهني للتعريف بالجرائم الناشئة عن استخدام الإنترنت وجرائم المعلوماتية وتعزيز جهود وأساليب مكافحتها.

٢. إعداد الدراسات والبحوث حول سبل مكافحة جرائم المعلوماتية وكافة الجرائم التي تتم عبر أو باستخدام شبكة الإنترنت أو الحاسوب والعمل على تشجيع البحث العلمي في مجال دراسة الجرائم الناشئة عن استخدام الإنترنت.

٣. إعداد ومتابعة المحافل العلمية والأكاديمية وحضور المؤتمرات والندوات المتعلقة بالجرائم ضد المعلوماتية والجرائم الناشئة عن استخدام الإنترنت.

٤. إعداد قاعدة بيانات للجرائم ضد المعلوماتية والجرائم الناشئة عن استخدام الإنترنت.

٥. تقديم الاستشارة والدعم العلمي والمهني للمؤسسات والأفراد والحكومات وكل من له مصلحة في مكافحة الجرائم الناشئة عن استخدام الإنترنت.

٦. تنمية الكوادر البشرية في مجال مكافحة هذه الجرائم وتأهيل أعضاء المنظمة مهنياً لذلك.

٧. إعداد الأطر القانونية والإجرائية والمؤسسية للمكافحة.

٨. المساهمة في رسم أطر وقائية وعقابية لمكافحة جرائم المعلوماتية والإنترنت.

٩. تشجيع وتنمية وتطوير تفاعل العمل غير الحكومي مع الأهداف الرامية لمكافحة جرائم المعلوماتية والإنترنت والمساهمة في وضع التصور الإقليمي لمكافحة جرائم المعلوماتية والإنترنت والتعاون مع الجهات الحكومية وغير الحكومية المحلية الإقليمية والدولية في هذا الإطار.

١٠. مكافحة كافة أشكال الجرائم التي تقع ضد المعوماتية في كافة أشكالها (الأجهزة والبرامج والشبكات والمعلومات والبيانات والأموال ووسائل الاتصال والجرائم ضد السمعة والجرائم ضد الشخصية) والجرائم ضد الإنسانية والجرائم الموجهة للأمن القومي في كافة أشكالها وصورها. وبالعموم مكافحة كافة الجرائم التي يكون الحاسب أو الإنترنت أداة من أدواتها أو هدفاً من أهدافها أو سطا لها.

١١. إعداد مراكز تدريب عربية في إطار مكافحة جرائم المعلوماتية والإنترنت، وعمل دورات تدريبية وورش عمل ومؤتمرات تعالج هذا الموضوع.

١٢. إصدار الكتب والنشرات المتعلقة بالمواضيع محل اهتمام المنظمة وإصدار مجلة تحمل اسم المنظمة دورياً.

الباب الثالث

عضوية المنظمة

المادة ٣- تحتفظ المنظمة بسجل خاص يحوي أسماء وعناوين الأعضاء، وأية معلومات أخرى تراها ضرورية لنجاح عملها.

المادة ٤-

١- الانضمام إلى عضوية المنظمة متاح لكافة القانونيين والاقتصاديين والمهنيين والممارسين لهذا المجال والمهتمين بأهداف المنظمة وتطلعاتها والذين يرغبون بالاستفادة من أنشطة وبرامج المنظمة والمشاركة فيها شرط استيفائهم معايير العضوية.

٢. تقبل الجمعية جميع الحاصلين على مؤهلات جامعية من كافة الأقطار العربية كأعضاء عامين كما تقبل الجمعية انضمام طلبة الجامعات والمدارس العليا كأعضاء منتسبين لحين حصولهم على المؤهل وبلوغهم سن الثامنة عشرة.

٣. يجوز قبول عضوية مؤسسات أكاديمية وبحثية علمية كأشخاص معنوية.

٤. العضوية الشرفية التي يتم منحها بعد استيفاء الدراسات اللازمة في هذا الشأن. ويجوز منح العضوية الشرفية لكل من قدم خدمات جليلة للمنظمة.

المادة ٥- رسوم العضوية

١. يحق لمجلس إدارة المنظمة رفع توصيه للهيئة العامها لعامة من أجل تحديد وتعديل رسوم العضويها لعضوي. إلغاء تحديد رسوم العضوية المستحقة للاتحاد كما يراه مناسباً من حين إلى آخر بحسب متطلبات العضوية، إلغاء – يحق لمجلس الإدارة تحديد رسوم مختلفة لفئات العضوية الثلاث – العضو الفعال. العضو المؤازر

٢. يجب أن تكون رسوم العضوية متساوية بين الأعضاء ضمن في فئة العضوية الواحدة.

٣. لا تستحق رسوم عضوية على لعضو الشرف.

٤. يراعي مجلس إدارة المنظمة، عند تحديده لرسوم العضوية، حاجات الاتحاد واحتياجات أعضائه.

٥. يحق لمجلس إدارة المنظمة تحديد رسوم خاصة لأية نشاطات أو خدمات يقدمها الاتحاد لكافة أعضائه.

٦. تبدأ العضوية في اليوم الأول من الشهر التالي لقبول مجلس إدارة الاتحاد للعضو ودفع العضو للرسوم: وتنتهي عضوية جميع الأعضاء بتاريخ ٣١ كانون أول من كل عام.

٧. يجب على كافة الأعضاء (الذين تستحق عليهما رسوم العضوية) تسديدها في موعد أقصاه ٣١ من شهر شباط من كل عام. في حالة تخلف العضو عن السداد بالموعد المذكور: فإن على مجلس إدارة المنظمة فرض غرامة تأخير تعادل ٢٥٪ من رسوم العضوية السنوية. إلا إذا تقدم العضو بعذر يقبله مجلس إدارة المنظمة يبين وجود ظروف طارئة وقاهرة منعته من تسديد ما استحق عليه وذلك لمرة واحدة فقط. لغايات هذه المادة، تعرف الظروف الطارئة بأنها تلك الظروف التي يعرفها القانون المدني بأنها ظروف معقولة ومقبولة لعدم تسديد ما استحق على الفرد.

المادة ٦- تنتهي عضوية أعضاء المنظمة في الحالات التالية:

١. حل الشخصية المعنوية وتصفيتها:

٢. الانسحاب:

٣. الوفاة لأعضاء الشرف والمؤازرينو والمؤازرين:

٤. بعد شهر على قرار من مجلس إدارة المنظمة بإنهاء العضوية دون تقديم طلب باستئنافها إلى مجلس إدارة المنظمة. وفي حال تقديم طلب الاستئناف يتم تعليق القرار إلى البت فيه.

المادة ٧- إنهاء العضوية

يحق لمجلس إدارة المنظمة – بالأغلبية البسيطة (٥٠٪ + ١) إنهاء عضوية عضو المنظمة للأسباب التالية:

١. إذا ألحق العضو ضرراً مالياً أو معنوياً كبيرين بالمنظمة.

٢. إذا تأخر العضو مدة ستة أشهر عن تسديد المستحقات المالية التي عليه للمنظمة، شريطة أن يكون مجلس المنظمة قد أخطره بذلك خطياً قبل موعد الإنهاء.

٢. إلغاء – إذا قصر العضو بالقيام بالتزامات العضوية:

المادة ٨- يحق لمجلس إدارة المنظمات – بالأغلبية البسيطة (٥٠٪ +١). إنهاء عضوية عضو المنظمة للأسباب التالية:

١. إذا ألحق العضو ضرراً مالياً او او معنوياً كبيرين بالمنظمة.

٢. إذا تأخر العضو مدة ستة أشهر عن تسديد المستحقات المالية التي عليه للمنظمة، شريطة أن يكون مجلس المنظمة قد أخطره بذلك خطياً قبل موعد الإنهاء.

٢. إلغاء – إذا قصر العضو بالقيام بالتزامات العضوية:

المادة ٨- يحق لمجلس إدارة المنظمة – بالأغلبية البسيطة (٥٠ +١)، تجميد عضوية عضو المنظمة للأسباب التالية:

١. إذا تأخر مدة شهرين عن تسديد المستحقات المالية التي عليه للمنظمة، شريطة أن يكون المدير العام قد أخطر ذلك العضو خطياً قبل موعد التجميد.

٢. إذا اختلت أي من شروط العضوية.

المادة ٩- إعادة العضوية يحق لمجلس إدارة المنظمة إعادة عضوية من جمدت عضويته أنهيت عضويته بسبب عدم دفع جميع الرسوم المستحقة عليه بشرط أن يدفع العضو جميع الرسوم المتراكمة مع الغرامة المستحقة عليها.

المادة ١٠- يجب على سكرتارية المنظمة تبليغ العضو خطياً بقرار مجلس الإدارة المتعلق بتجميد أو إنهاء أو إعادة العضوية.

الباب الرابع

الشؤون المالية للمنظمة

المادة ١١- موارد المنظمة

١. اشتراكات الأعضاء.

٢. المنح والمساعدات.

٣. اشتراكات الأنشطة التي تقوم بها المنظمة كالدور الاستشاري والعلمي والقانوني والمهني وخطط العمل والمشروعات التي تضطلع بها المنظمة ..

٤. دعم المنظمات الدولية والإقليمية

المادة ١٢- السنة المالية

تبدأ السنة المالية للمنظمة في الأول من شهر كانون الثاني وتنتهي في ٢١ من شهر كانون الأول من كل عام.

المادة ١٣ - المخولون بالتوقيع عن المنظمة من يقرره مجلس إدارة المنظمة لذلك.

المادة ١٤ – يجب أن تصرف أموال المنظمة لتحقيق أهدافه المنصوص عليها في هذا النظام فقط، ولا يجوز صرف أية أموال خلافاً لذلك.

الفصل الثاني

أولاً: الهيئة العامة

المادة ١٥ – الهيئة العامة هي صاحبة أعلى سلطة في المنظمة وهي تتكون من إلغاء مع جميع الأعضاء الفاعلين في المنظمة وسددو كامل رسوم العضوية المستحقة عليهم.

المادة ١٦- تعقد الهيئة العامة اجتماعات عادية وأخرى غير عادية.

الاجتماعات العادية.

المادة ١٧- تجتمع الهيئة العامة العادية مرة كل سنة على الأقل خلال مدة ٣ أشهر من انتهاء السنة المالية، وذلك في مقر المنظمة المكان والزمان الذي يحدده مجلس إدارة المنظمة.

المادة ١٨ – توجه الدعوة للهيئة العامة لأي اجتماع قبل تاريخ انعقاده بمدة لا تقل عن خمسة عشرة يوماً من تاريخ تسلم الدعوة ويذكر في إعلان الدعوة مكان وتاريخ وساعة الاجتماع والمواضيع التي سيجري بحثها. ترسل الدعوة بوساطة الفاكي و/ أو البريد الإلكتروني و/ أو بأية وسيلة أخرى يراها المجلس مناسبة على أن يتم التأكد من وصول الدعوة بشكل شخصي لجميع الأعضاء من قبل السكرتاريا.

المادة ١٩- النصاب

١. لا تعتبر الجلسة الأولى لاجتماع الهيئة العامة العادية وغير العادية قانونية ما لم يحضرها نصاب قانوني من الأعضاء يمثلون أكثر من نصف الأعضاء الفاعلين (٥٠ + ١). يجب أن لا يقل التمثيل عن ثلثي أعضاء المنظمة في الحالتين التاليتين:

* حل المنظمة أو تصفيتها.

* تعديل نظامها الداخلي.

٢. يجوز التوكيل لاجتماعات الهيئة العامة العادية وغير العادية للحضور والتصويت. (لغايات هذه المادة، يعرف التوكيل بأنه قيام عضو في المنظمة لمفوضين عنه بتوكيل غيره من الأعضاء أو مفوضيه بالتمثيل والتصويت في اجتماعات الهيئة العامة)

المادة ٢٠- في حالة عدم اكتمال النصاب القانوني لاجتماع الهيئة العامة العادية في جلسته الأولى، يقوم مجلس إدارة المنظمة.

بالدعوة اجتماع ثان خلال ١٤ يوماً من تاريخ الاجتماع الأول ويحدد الموعد الجديد خلال نفس الاجتماع على أن يبلغ بذلك جميع الأعضاء، ويعتبر الاجتماع الثاني قانونياً بمن حضره من الأعضاء.

المادة ٢١- يرأس رئيس مجلس إدارة المنظمة.

الاجتماعات حال غيابه يتولى نائب الرئيس ترأس ذلك الاجتماع. أما حال غياب الرئيس ونائب الرئيس، يقوم الأعضاء الحاضرين انتخاب من يتولى رئاسة وذلك الاجتماع.

المادة ٢٢- تعقد جميع اجتماعات الهيئة العامة بصورة علنية. إلغاء ما لم يتم الطلب من قبل ١٠ من الأعضاء الفاعلين لعقد الاجتماع واتخاذ القرارات بصورة سرية.

المادة ٢٣- من ضمن صلاحيات الهيئة العامة العادية الأمور التالية:

١. إقرار جدول الأعمال لاجتماعات الهيئة العامة:

٢. مناقشة التقرير السنوي المقدم من مجلس إدارة المنظمة حول إنحازاته العام المنصرم.

٣. تبني تقرير مدقق الحسابات.

٤. انتخاب أعضاء مجلس إدارة.

٥. الموافقة على تعيين مدقق الحسابات للسنة المالية الجديدة: على أن يكون من غير أعضاء. بحسب توصية مجلس الإدارة الذي يجب أن لا يكون من أعضاء.

٦. إلغاء مراجعة تقرير مجلس الإدارة عن نشاطات السنة المنصرمة، التعليق عليها وإعطاء تقرير عن أعضاء الاتحاد الجدد. مراجعة الخطة السنوية والميزانية للعام الجديد التي يتبناها مجلس الإدارة.

٧. أية أمور أخرى يراها مجلس إدارة الاتحاد ضرورية .

المادة ٢٤- يقتصر البحث في الاجتماع السنوي أو في أي اجتماع غير عادي على ما ورد في جدول الأعمال، إلا أنه يجوز للهيئة العامة تعديل جدول الأعمال بالأغلبية البسيطة (أعاد صياغة) في اجتماعات الهيئة العامة العادية وغير العادية، لا يجوز مناقشة أية مواضيع سوى تلك التي وردت في جدول الأعمال، إلا إذا قررت الهيئة العامة (بالأغلبية البسيطة) تعديل جدول أعمال ذلك الاجتماع.

الاجتماعات غير العادية

المادة ٢٥- (أ) تجتمع الهيئة العامة غير العادية بناء على دعوى من مجلس إدارة دارة مباشرة أو بناء على طلب خطي موقع من ١٥٪ من الأعضاء الفاعلين، على أنه يجب أن يتضمن الطلب المواضيع المطلوب مناقشتها في ذلك الاجتماع. موضوع الاجتماع بالطلبة.

المادة ٢٦- (ب) في حالة عدم اكتمال النصاب القانوني لاجتماعات الهيئة العامة غير العادية في جلسته الأولى، يقوم مجلس إدارة بالدعوة إلى اجتماع ثاني بعد ١٤ يوماً من تاريخ الاجتماع الأول، إذا لم يكتمل النصاب القانوني للاجتماع الثاني بحضور ما لا يقل عن ٤٠٪ من الأعضاء الفاعلين، فإنه يلغي ذلك الاجتماع مهما كانت الأسباب الداعية إليه.

المادة ٢٧- يجب على مجلس إدارة المنظمة دعوة الهيئة العامة غير العادية للاجتماع في مدة لا تتجاوز خمسة عشر يوماً من تاريخ تسلمه الطلب موضوع المادة ٣٣ أ أعلاه.

المادة ٢٨- تسري جميع الأحكام المواد هذا النظام على اجتماعات الهيئة العامة غير العادية المفروضة على الاجتماعات غير العادية.

ثانياً: مجلس إدارة المنظمة.

المادة ٢٩- يتولى إدارة المنظمة وتصريف شؤونها مجلس إدارة مكون من ..... أعضاء تنتخبهم الهيئة العامة بطريقة الانتخاب السري المباشر.

المادة ٣٠- لا يجوز أن يكون عضواً في مجلس الإدارة.

١. من لم يمض على عضويته في الهيئة العامة مدة سنة عدا مجلس إدارة الاتحاد الأول.

٢. من كان محكوماً عليه بجنحة أخلاقية أو السرقة أو الاحتيال أو إساءة الأمانة أو التزوير أو الإفلاس التقصيري أو الشهادة واليمين

الكاذبين إلغاء من كان يشترك في إدارة اتحاد مشابهة أو منافسة لأعمال الشركة.

المادة ٣١- يجتمع مجلس الإدارة خلال أسبوع من انتخابه من أجل توزيع المناصب الإدارية، بحيث يتم انتخاب نائب الرئيس، الأين العام والأمناء العامون المساعدون. أمين الصندوق.

المادة ٣٢- يتولى مجلس الإدارة القيام بجميع السلطات والصلاحيات التي تكفل إدارة المنظمة وسير العمل فيها وتصريف شؤونها، وفقاً لغاياتها.

المادة ٢٣ – يكون لمجلس الإدارة الصلاحيات التالية:

١. الدعوة للاجتماعات العادية وغير العادية للهيئة العامة.

٢. مناقشة وإقرار التقارير التنفيذية المعدة من قبل المدير التنفيذي.

٣. مناقشة وإقرار البرنامج السنوي والميزانية للسنة المالية الجديدة.

٤. مناقشة وإقرار التقارير المالية للسنة المالية المنصرمة.

٥. تحديد المصاريف المسموح بها لأعضاء مجلس الإدارة المتصلة بنشاطات عمل المنظمة.

٦. تعيين المدير التنفيذي وتحديد صلاحياته، وإنابة الصلاحيات اللازمة له من أجل ضمان تنفيذ هذه الأعمال المنوطة به.

٧. النظر بطلبات العضوية بقبول الطلب أو رفضه.

المادة ٢٤- يحق لمجلس الإدارة تعيين مدير عام يتولى الصلاحيات المعطاة إليه من قبل مجلس الإدارة.

المادة ٢٥- يحق لمجلس الإدارة تشكيل لجان فرعية تتولى صلاحيات محددة ووضع آليات ونطاق عمل من أجل ضمان تنفيذ الغايات الأساسية.

المادة ٢٦ – تتضمن صلاحيات الرئيس ما يلي:

١- رئاسة اجتماعات المجلس والهيئة العامة.

٢- تمثيل الاتحاد لدى السلطات الرسمية والقضائية والمؤسسات والأفراد، وله حق توقيع الوكالات والعقود باسم المنظمة وفقاً لما يقرره المجلس.

٣- الإشراف على كافة أعمال المنظمة واللجان المنبثقة عنها.

٤- تفويش بعض صلاحياته الإدارية لأي عضو من أعضاء المجلس.

يتولى نائب الرئيس كامل صلاحيات الرئيس حال غيابه.

المادة ٢٧

- تتضمن صلاحيات أمين الصندوق ما يلي:

١- تسلم المبالغ التي ترد إلى المنظمة بإيصالات مختومة بخاتم المنظمة موقعة منه.

٢- تنفيذ قرارات المجلس فيما يتعلق بمعاملات المنظمة المالية.

٣- حفظ السجلات والمستندات المالية في مركز المنظمة لتكون تحت طلب الجهات المختصة.

٤- إعداد الموازنة التقديرية لكل عام بإشراف الرئيس وتقديمها إلى المجلس لإقرارها.

٥- وضع بيان مالي في نهاية كل سنة عن واردات ونفقات المنظمة وتنظيم الميزانية الختامية عن ذلك العام وتصديقها من فاحص الحسابات المعين من قبل المنظمة.

المادة ٣٨ – يجتمع مجلس إدارة المنظمة بدعوة خطية من رئيسه أو بناءً على طلب ربع أعضائه، على الأقل، مرة كل ..... يوماً.

المادة ٣٩ – يرأس رئيس مجلس إدارة المنظمة الاجتماعات، وفي حال غيابه يتولى نائب الرئيس ترأس ذلك الاجتماع. أما في حالة غياب الرئيس ونائب الرئيس، يقوم الأعضاء الحاضرين بانتخاب من يتولى رئاسة ذلك الاجتماع.

المادة ٤٠- يجب حضور ما يزيد على نصف أعضاء مجلس إدارة المنظمة لتكون قراراته قانونية.

المادة ٤١- يعقد مجلس إدارة المنظمة اجتماعاته في مقر المنظمة و/ أو في الزمان والمكان التي يحددهما الإدارة.

المادة ٤٢- (أ) تدون مداولات وقرارات مجلس إدارة إدارة المنظمة في سجل خاص يدون فيه أسماء الأعضاء الحاضرين.

المادة ٤٣- (ب) جميع محاضر الجلسات يوقع عليها يجب على الرئيس رئيس وأعضاء مجلس إدارة المنظمة الذين حضروا تلك الجلسات التوقيع على جميع صفحات محضر الاجتماع مع بيان مخالفة العضو للقرار فوق توقيعه، حال حدوث ذلك. وعلى العضو المخالف أن يسجل سبب مخالفته خطياً فوق توقيعه ويجوز إعطاء صورة عن كل محضر موقع من الرئيس. إعادة صياغة لغوية.

المادة ٤٤ – يتخذ مجلس إدارة المنظمة قراراته بالأغلبية (٥٠٪ + ١) وفي حالة تساوي الأصوات، يكون للرئيس صوت مرجح.

المادة ٤٥- يحتفظ رئيس مجلس إدارة المنظمة بختم المنظمة في مكان أمين.

المادة ٤٨- يتولى مجلس الإدارة القيام بجميع السلطات والصلاحيات التي تكفل إدارة الاتحاد وسير العمل فيه وتصريف شؤونه وفقاً لغاياته.

المادة ٤٩- يقرر مجلس الإدارة مقدار الرواتب الشهرية لموظفي الاتحاد، إلا أنه لا يجوز أن يتقاضى أعضاء مجلس الإدارة أية رواتب عن أعماله في الاتحاد. إمكانية تقسيم البند إلى قسمين مستقلين ويكون لمجلس الإدارة الصلاحيات التالية:

١. الدعوة للاجتماعات العادية للهيئة العامة.

٢. مناقشة وإقرار التقارير التنفيذية المعدة من قبل المدير التنفيذي.

٣. إعداد البرنامج السنوي والميزانية للسنة المالية الجديدة.

٤. إعداد وإقرار التقارير المالية للسنة المالية المنصرمة.

٥. الدعوة للاجتماعات غير العادية للهيئة العامة.

٦. تحديد المصاريف المسموح بها لأعضاء مجلس الإدارة المتصلة بنشاطات عمل الاتحاد.

٧. تعيين المدير التنفيذي وتحديد صلاحياته وإنابة الصلاحيات اللازمة له من أجل ضمان تنفيذ هذه الأعمال المنوطة به.

٨. النظر بطلبات العضوية وإقراره أو رفضها حسب النظام الداخلي

ثالثاً: الانتخابات

المادة ٤٦- مدة دورة مجلس الإدارة المنتخب سنة كاملة.

المادة ٤٧- ينتخب رئيس مجلس الإدارة من قبل الهيئة العامة بالاقتراع السري من ضمن الأعضاء المنتخبين للمجلس.

المادة ٤٨- يحتفظ مجلس الإدارة بكافة نتائج الانتخابات.

المادة ٤٩- مع مراعاة ما ورد في هذا النظام، تسقط عضوية أي عضو من أعضاء مجلس الإدارة ويعتبر منصبه خالياً في إحدى الحالات:

١. إذا قدم استقالته الخطية إلى مجلس الإدارة بحيث تعتبر نافذة من تاريخ مصادقة المجلس عليها.

٢. إذا وجد أو أصبح معتوهاً أو مختل العقل.

٣. تسقط تلقائياً عضوية العضو المتغيب عن اجتماعات مجلس الإدارة إذا تغيب العضو عن ثلاثة اجتماعات متتالية بدون عذر.

٤. إذا ثبت لمجلس الإدارة قيام العضو بإفشاء أسرار المنظمة أو عدم محافظته على سمعتها أو مصلحتها أو محاولة الإضرار بها أو القيام بعمل منافس أو مشابه لأعمالها.

٥. إذا أدين بالسرقة أو الاحتيال أو إساءة الأمانة أو التزوير أو الشهادة واليمين الكاذبين.

المادة ٥٠- (أ) إذا شغر مكان عضو مجلس إدارة المنظمة لأي سبب من الأسباب فيخلفه العضو التالي في الترتيب بالاستناد إلى نتائج انتخابات مجلس إدارة المنظمة.

المادة ٥١- (ب) في حالة رفض العضو المستبدل دخول مجلس الإدارة، أو لأي سبب آخر لم يتمكن العضو من إشغال ذلك المنصب، فإنه يكون للعضو الذي يليه (بحسب نتائج الانتخابات)، الحق في شغر ذلك المكان.

المادة ٥٢- (ج) في حالة شغور منصب الرئيس يتولى نائب الرئيس صلاحياته على أن يتم عقد اجتماع هيئة عامة غير عادي خلال ٤٥ يوم لانتخاب جديد رئيس.

المادة ٥٣- (د) أما في حالة عدم وجود أي خلف لملئ الشاغر يتم عقد اجتماع هيئة عامة غير عادي خلال ٤٥ يوم لانتخاب لملء الشاغر.

الفصل الثالث: حل المنظمة

المادة ٥٤- تحل المنظمة بقرار من الهيئة العامة غير العادية بأغلبية ثلثي الأعضاء الأعضاء عبر بالتصويت المباشر.

المادة ٥٥- تؤول جميع ممتلكات المنظمة بعد التصفية إلى الجهة والمكان والطريقة التي تراها الهيئة العامة غير العادية مناسبة – شريطة أن لا يتعارض توزيع الممتلكات والأموال مع الغاية الرئيسية للمنظمة.

الفصل الرابع: مواد عامة

المادة ٥٦ – يكون للمنظمة الحق في الدخول والاشتراك والاندماج بأية منظمة أخرى إقليمية أو دولية أو مؤسسة مسجلة بالاستناد إلى القوانين والأنظمة العربية.

المادة ٥٧- يحق للمنظمة امتلاك العقارات وغيرها من الأموال المنقولة، ولها الحق في البيع والرهن والإجارة وغيرها من الأعمال كما يراه مجلس الإدارة مناسباً.

الفصل السابع

تجربة جمهورية مصر العربية في مكافحة جرائم الحاسبات و شبكات المعلومات

للحديث عن تجربة جمهورية مصر العربية في مجال مكافحة جرائم الإنترنت أو ما يطلق عليه الجرائم المعلوماتية لابد أن يكون بداية الحديث عن تلك القوانين التي لابد وأن تكون موجودة كأساس يتم بموجبه تحديد ماهية الأفعال التي تعتبر جرائم ففي كل الدول الحديثة المتقدمة تكنولوجيا وعلمياً وقانونياً يوجد قانون للعقوبات يحدد الجرائم التقليدية وأركانها كل أنه يوجد أيضاً قانون الإجراءات الجنائية وهو القانون الذي يقرر أساليب وسائل الإبلاغ عن الجريمة التقليدية والطرق المتبعة في التحري عن صحتها ومرتكبيها وجمع الاستدلالات عنها وضبطها والتحقيق فيها ثم أخيراً إحالة المتهم بارتكابها إلى المحاكمة حيث تتم إدانته ويلقي العقاب المنصوص عليه في القانون جزاء ما ارتكبت يداه أو يقضى ببراءته فيطلق سراحه [1].

كل ذلك يستلزم وجود الدليل المقبول لإدانة ذلك المتهم ومن القواعد الثابتة في قانون العقوبات في أي دولة

- أنه لا جريمة إلا بنص
- لا عقوبة إلا بقانون

([1]) خير محمد الجنبيهي وممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي، ووسائل مكافحتها ار الفكر الجامعي، ٢٠٠٤ ص ١٣١- ١٣٩.

- أن الشك يفسر لصالح المتهم

وعليه فبعض الجرائم قد تتم بالأسلوب التقليدي العادي غير الإلكتروني فتقه تحت طائلة نصوص القانون السارية في الدولة ويلقي المتهم عقابه على ما ارتكبت يداه.

أما جرائم الاعتداء على نظم وشبكات المعلومات وشبكات الاتصال والتي تقع بالشكل الإلكتروني غير التقليدي لا تتوافر لها حتى الآن نصوص قانونية سواء في قانون العقوبات أو في قانون الإجراءات الجنائية لتجريمها ولتقرر العقوبة المقررة على كل جريمة تتم بهذا الشكل غير التقليدي.

هذا من جهة ومن جهة أخرى فإن تلك الجرائم الإلكترونية تشمل في معظم الأحوال أفعالاً ضارة تقع على نظم المعلومات وشبكات الاتصال وهو ما يؤثر بالسلب على التجارة الإلكترونية أو أي أعمال إلكترونية أخرى نظراً لأن تلك الجرائم تكون أداة الجريمة فيها نظم الحاسبات والبرمجيات ومن ثم فإنه لكي تتوافر إمكانية تجرين تلك الأفعال ووضع العقاب على من يرتكبها لابد من توافر نصوص قانونية في قانون العقوبات وقانون الإجراءات الجنائية تجرم أفعال الاعتداء على نظم وشبكات المعلومات والحاسبات والاتصالات أي جرائم المجال الإلكتروني أو ما يطلق عليه جرائم الإنترنت او أي أفعال اعتداء على الأشخاص والأموال والتي تقع باستخدام وسائل إلكترونية بالإضافة إلى نصوص قانونية أخرى تبين ماهية الوسائل التي يتم استخدامها عند جمع

الاستدلالات عن تلك الجرائم وضبطها والكيفية البحث عن الأدلة الخاصة بها والحفاظ عليها والتحقيق في تلك الجرائم تمهيداً للقبض على مرتكبها لينال ما ارتكبت يداه من أفعال ضارة.

ويلزم قبل توافر تلك النصوص القانونية وجود الشرطة الفنية المدربة فنياً وتكنولوجيا على التعامل مع ذلك النوع من الجرائم التكنولوجية الحديثة فيلزم أن تكون أجهزة الشرطة مدربة فنياً بالقدر الكافي الذي يجعلها قادرة على ضبط تلك الجرائم والتعامل مع مرتكبيها وإيجاد الدليل الخاص بها والحفاظ عليه وليست أجهزة الشرطة فقط هي التي يجب أن تكون مؤهلة لذلك بل يجب أن يكون رجال النيابة العامة ورجال القضاء والسادة المحامين يجب أن يكونوا جميعاً مؤهلين للتعامل مع ذلك النوع من الجرائم الإلكترونية الحديثة هذا من جهة ومن جهة أخرى يلزم توافر الأجهزة الفنية لهم أيضاً ليستطيعوا القيام بما هو منوط بهم من واجبات لإمكانية التعامل معها فالتدريب الفني فقط لا يأتي بالنتائج المرجوة بل لابد من وجود الأجهزة الفنية التي تعينهم على القيام بمهامهم.

هذا ولما كانت الجرائم الإلكترونية التي تقع على نظم وشبكات الحاسبات والاتصالات في أحيان كثيرة جرائم عابرة للحدود CRIMES TRANS BORDER أي أن مرتكب الجريمة قد يستخدم حاسباً أو جهازاً أو شبكة اتصال في دولة وتقع الجريمة على حاسب أو نظام أو شبكة اتصال في دولة أخرى فإن الأمر يستلزم وجود اتفاقية دولية تنظم هذه المسائل بين الدول حتى تعدل قوانين العقوبات وقوانين الإجراءات الجنائية في كل منها

لتجريم تلك الأفعال – فلا يكون هناك أفعال معاقب عليها في دولة ما ولا يكون معاقب عليها في دولة أخرى وبالتالي تكون الفرصة سانحة أمام مرتكبي تلك الأفعال أن يفلتوا بفعلتهم باللجؤ إلى الدول التي لا تجرم تلك الأفعال – وذلك كي يتحقق التعاون الدولي بين الدول في تلك الجرائم فلا يفلت الجاني بفعلته علماً أن ذلك التنظيم موجود جزئياً من خلال ما يعرف بمعاهدة بودابست لمكافحة جرائم نظم وشبكات الاتصالات THE BUDAPEST CONVENTION ON CYBER CRIMES والتي لم تنضم مصر إليها حتى الآن.

وعليه ففي مجال عرضنا لتجربة جمهورية مصر العربية في مجال مكافحة جرائم الإنترنت سوف نعرض لعدة نقاط هي:-

١ – إصدار قانون حماية الملكية الفكرية.

٢ – تحديث القوانين السائدة إلى قوانين جديدة تجرم جرائم الإنترنت.

٣ – استحداث قوانين جديدة تقنن الاستخدامات الإلكترونية مثل قانون . التجارة الإلكترونية وقانون التوقيع الإلكتروني.

٥ – إنشاء إدارات جديدة بوزارة الداخلية تكون مسئولة عن تلك الجرائم.

٦ – تحقيق الأمن المعلوماتي للكيانات الاقتصادية.

١- إصدار قانون حماية الملكية الفكرية.

كانت جمهورية مصر العربية من أولى الدول العربية التي انضمت إلى كافة المعاهدات والاتفاقات الدولية التي كانت تعمل في مجال حماية حقوق الملكية الفكرية من القرصنة وتأسيساً على هذا الاهتمام فقط انضمت مصر إلى معاهدة برن وتريبس ومعاهدات الويبو وكان من نتيجة هذا الاهتمام أن أصدرت مصر قانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٣ والذي يوفر الحماية لمصنفات الحاسب الآلي لمدة خمسون عاماً من تاريخ وفاة المؤلف أو من تاريخ النشر.

أما عن الحقوق التي يتمتع بها المؤلف طبقاً لهذا القانون فقد نص القانون على تمتع المؤلف وحده بالحق في الترخيص أو عدم الترخيص لأي جهة باستغلال مصنفه سواء بالنسخ أو البيع أو التأجير أو الإعارة أو إتاحته عبر أجهزة الحاسب الآلي وشبكة الإنترنت وغيرها من شبكات المعلومات ووسائل الاستغلال.

ويحظر القانون الآتي: -

- أي نسخ كلي أو جزئي للبرامج أو الاقتباس منها إلا بعد الحصول ترخيص كتابي مسبق من المؤلف أو من الممثل القانوني له.

- إزالة أو تعطيل أو التغيب لأي حماية تقنية يستخدمها المؤلف كالتشفير

- أو غيره

- تقليد أو بيع أو عرض للتداول أو للإيجار في مصر مصنفاً منشوراً في الخارج أو تصديره.

- النشر عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصالات أو غيرها من شبكات والوسائل دون إذن كتابي مسبق من المؤلف.

- الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف العقوبات التي تقررت بموجب قانون حماية الملكية الفكرية:-

الجزاءات الجنائية:-

- يعاقب المعتدي بالحبس من شهر حتى ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف جنيه لكل برنامج أو بإحدى هاتين العقوبتين.

- بإغلاق المنشأة التي استغلها المقلدون أو شركاؤهم كما يجوز للمحكمة أن تقضي مدة لا تزيد على ستة أشهر.

- وفي حال معاودة المخالفة يصبح الحبس وجوبياص بحد أدنى ثلاث شهور مع غرامة مالية قد تصل إلى ٥٠ ألف جنيه ويصبج غلق المنشأة وجوبياً.

- وتتم في كل الأحوال مصادرة النسخ المقلدة والأدوات المستخدمة في الاعتداء.

- ينشر ملخص الحكم الصادر بالإدانة في جريمة يومية واحدة أو أكثر على نفقة المحكوم عليه.

الجزاءات المدنية:-

- يستحق المؤلف أو من يخلفه في حال الاعتداء على حق أو أكثر من حقوقه والحصول على تعويضات مدنية عما لحقه من أضرار أدبية – ومالية قد تصل إلى ملايين الجنيهات.

- يلزم القانون كل المحال التي تطرح للتداول بالبيع أو بالإيجار أو بالإعارة أو بالترخيص بالاستخدام مصنفات الحاسب الآلي أو قواعد البيانات بالحصول على ترخيص بذلك من وزارة الاتصالات والمعلومات ويعاقب على مخالفة هذه المادة بغرامة لا تقل عن خمسة آلاف و تزيد عن عشرين ألف جنيه مصري.

- يلزم القانون ناشرو وطابعو ومنتجو مصنفات الحاسب الآلي أو قواعد البيانات بإيداع نسخة من المصنف أو أكثر بما لا يجاوز العشرة ويعاقب على مخالفة هذه المادة بغرامة لا تقل عن ألف جنيه ولا تزيد عن ثلاثة عن كل مصنف.

٢- تحديث القوانين السائدة إلى قوانين جديدة تجرم جرائم الإنترنت

MODERNISATION THE REIGNING LAWS TO A NEW LAWS CRIMINALISING THE INTERNET CRIMES.

حتى الآن لم يتم استحداث أي قوانين جديدة في جمهورية مصر العربية تجاري التطور الحادث في نوعية الجرائم وطرق ارتكابها – فحتى الآن يتم إدراج تلك الجرائم الإلكترونية التي ترتكب عبر شبكة الإنترنت تحت نصوص القوانين القديمة ويتم تطبيق العقوبات القديمة عليها رغم أن تلك الجرائم تحتاج إلى غلظة العقوبة حتى تكون المحاولة جادة في الحد من ارتكاب تلك الجرائم – وكان يجب أن تكون تلك القوانين قد تم سنها منذ أن انتشرت خدمة الإنترنت في مصر على نطاق واسع لأن انتشارها على نطاق واسع سيؤدي بالطبع إلى زيادة الاحتمال باستخدامها استخداماً سيئاً في ارتكاب الجرائم الجديدة على المجتمع وبالتالي كان يجب أن تكون تلك القوانين جاهزة للتطبيق لا أن يتم التفكير في سنها بعد أن زاد ارتكاب تلك الجرائم بكافة أنواعها.

إلا أنه في نفس الوقت لابد من الإشارة إلى أن ارتكاب تلك الجرائم لا زال في مراحله الأولى رغم الانتشار السريع للإنترنت في مصر نظراً لطبيعة المصريين وما يحكمهم من عادات وتقاليد تحد كثيراً من أي نزعات إجرامية قد تكون موجودة في أي فئة من فئات البشر فالطبيعة السمحة وتقربهم من الدين والتزامهم بأوامره ونواهيه تعمل على الحد من نسبة ارتكاب الجرائم عنها في أي بلد من بلاد العالم منها يتاح لهم من وسائل ارتكابها.

وعملية تحديث القوانين لا تتم في جمهورية مصر العربية بالسرعة المطلوبة لتجارة التطور الحادث في التكنولوجيا ووسائل الاتصال وعمليات التجارة الإلكترونية وما إلى ذلك من تطور حاصل في كافة المعاملات التي

تتم باستخدام أحدث ما وصل إليه العالم من التكنولوجيا وسوف نعرض فيما يلي بعض من أهم القوانين التي لا يجب التأخر في عمليات التحديث الخاصة بها حتى لا نبتعد عن عمليات التطور التي تحدث يومياً ولكي لا تزداد الهوة التكنولوجية التي تعمل على زيادة الفارق فيما بين الدول المتقدمة والدول النامية.

ومن أهم القوانين التي تحتاج إلى تحديث :-

١- تلك القوانين التي تتعلق بمأموريات الشهر العقاري والتوثيق واللوائح الخاصة بها وأهمية تحديث تلك القوانين واللوائح لكي تتواءم مع العاملات الجديدة – المعاملات الإلكترونية- ومن نواحي التحديث التي يمكن طرحها أنه يمكن اعتماد مصلحة الشهر العقاري والتوثيق لتصبح هي الجهة المؤتمنة على حفظ الوثائق الإلكترونية واعتمادها – الطرف الثالث المحايد المودع لديه الوثيقة – أو يمكن إيجاد جهادت حكومية أخرى تتسم بالنزاهة والحيدة كهيئة البريد للقيام بتلك المهمة.

٢- تحديث القوانين المنظمة لهيئة سوق المال وكذلك القوانين المنظمة للبورصات واللوائح الخاصة بها وذلك لأمر هام حيث أنه من الضروري تحديث التعاملات التي تتم على الأسهم والسندات ليكون في الإمكان التعامل على الأسهم والسندات المصرية بالأساليب الإلكترونية الحديثة وبالتالي يمكن جذب رؤوس الأجنبية للاستثمار في مصر حيث أنه بدون

تحديث تلك القوانين وتقنين الأساليب الحديثة الإلكترونية ستتعاظم الفوارق التي تفرق بيننا وبين الدول الدول المتقدمة تكنولوجيا.

٣- نوع آخر من القوانين لابد من التعامل معه بمزيد من الأهمية لأنه يؤثر كثيراً مع رؤوس الأموال الأجنبية التي لابد من جذب الكم الأكبر منها إلى مصر فالتشريعات واللوائح الضريبية لابد من تحديثها ليكون في إمكانها العمل في عصر يتم التعامل التجاري فيه إلكترونياً دون أي يرى أي من أطرافه الطرف الآخر وعليه فلابد من تحديث تلك التشريعات التي تحكم المجال الضريبي في مصر ليجاري التطور الجاري في المجال التجاري الدولي وإلا فلن تتمكن الدولة من تحصيل ما تستحقه من حقوقها الضريبية على ما يتم من معاملات تجارية تتم إلكترونياً دون أن تكون الدولة قادرة على متابعتها وبالتالي تقف القوانين عاجزة عن أن تحصل حقوق الدولة.

٤- أما عن التشريعات الجمركية فالحال مع التشريعات الضريبية هو نفسه، الحال مع التشريعات الجمركية إذ أنه لابد من تحديث تلك التشريعات الجمركية، أيضاً وبالتوازي مع التحديث الذي يجب إتمامه مع التشريعات الضريبية بل ومع كافة التشريعات الأخرى التي يتم تحديثها فالتأخير في تحديث تلك التشريعات القديمة التي عفى عليها الزمن.

٥- لما كان لا يمكن الفصل بين التعاملات التجارية التي تتم داخل البلد الواحد وبين التعاملات التجارية التي تتم بين الدول كان من اللازم تحديث تلك القوانين الداخلية التي قد يرى البعض أنه لا فائدة كبيرة من

تحديثها وهو رأى خاطئ لأن التعاملات التجارية الداخلية هي امتداد طبيعي للمعاملات التجارية الخارجية وعليه فتحديث القوانين التي تستخدم في التعاملات في داخل مصر هو أمر ذو أهمية قصوى ومن تلك القوانين قانون المناقصات والمزيدات والتوريدات وأهمية ذلك التحديث ليكون هناك توافقاً وتلائماً بين تلك القوانين وطبيعة التجارة الإلكترونية.

٦- أما التشريعات الخاصة بحماية المستهلك في مجال التجاري الإلكترونية فهي من أهم التشريعات التي يجب أن تكون لها الأولوية في التحديث لأن تحديث القوانين في كافة المجالات هدفه الأول هو تقوية الاقتصاد الوطني وهدف تقوية الاقتصاد الوطني هو تحسين الحالة الاقتصادية للمستهلك لأنه الأساس في كل ذلك وبالتالي فإن القوانين التي تستهدف حماية المستهلك هي الأولى في أن تنال الأولوية في التحديث لا أن يتم إهدارها وإهمالها وإغفال دورها في حماية المستهلك [١].

٧- تعديل قانوني العقوبات والإجراءات الجنائية ليكون النص فيهما صريحاً على تجريم جرائم الإنترنت والحاسبات الآلية بدلاً من إدراج تلك الجرائم تحت النصوص القانونية القديمة وتحت مسمى الجرائم التقليدية القديمة لعدم وجود نصوص قانونية جديدة تنص صراحة وبوضوح على تجريمها.

فيكون هناك نصوص تنص صراحة على تجريم التشهير عبر الإنترنت ونصوص أخرى تجرم الاحتيال عبر الإنترنت وأيضاً أفعال الاعتداء على

---

(١) خير محمد الجنيني، مصدر سابق ص ١٣٩ – ١٤٥.

نظم وشبكات الحواسب المعلوماتية والاتصالات أو استخدام تلك الوسائل والتكنولوجيا الحديثة في الاعتداء على الأشخاص والأموال وكذلك الدولة والأفراد والهيئات أو الشركات والنصب والغش والاحتيال والقرصنة المعلوماتية وهكذا تكون هناك نصوص تنص صراحة على تجريم أي جرائم يمكن أن ترتكب عبر الإنترنت إلا أنه يجب أن تراعى أيضاً أن تكون تلك النصوص قد صيغت على أساس أن تستوعب أي تطوير قد يحدث في المستقبل – على الأقل القريب – في طرق ووسائل ارتكاب مثل تلك الجرائم.

كما أنه من المستحسن على النص صراحة على الأساليب التي يجب أن تتبع عند جمع الاستدلالات والتفتيش والتحقيق وضبط وحفظ الأدلة الجنائية في الجرائم المعلوماتية تحديداً للمسئولية الجنائية وحماية للتجارة الإلكترونية والمعاملات الإلكترونية.

هذا من جهة ومن جهة فلابد من من تنظيم الدورات التعليمية الكافية لرجال البحث القضائي وأعضاء النيابة العامة وأعضاء الهيئات القضائية وكذلك السادة المحامون لتدريبهم على الوسائل والأدوات الإلكترونية لفهما واستيعابها ليتمكنوا من القيام بما هو منوط بهم في أعمالهم على الوجه الأكمل دون أي تقصير.

٣ـ الإنضمام إلى المعاهدات والدولية التي تعمل على مكافحة جرائم والإنترنت.

كانت حكومة جمهورية مصر العربية على قناعة تامة ومنذ البداية على أن الانضمام إلى المعاهدات والاتفاقات الدولية هو من أهم الوسائل التي يجب الأخذ بها واتباعها في مجال مكافحة جرائم الإنترنت وعليه فلم تتوان مصر في الانضمام إلى كافة المعاهدات الدولية التي تم عقدها في هذا المجال وذلك إيماناً منها بأن الانضمام إلى الأسرة الدولية هو من أهم الوسائل التي يجب اتباعها في مجال مكافحة جرائم الإنترنت.

ويجب أن نربط بين التعاون الدولي في مكافحة جرائم المعلومات وما تقوم به مصر من خطوات هامة في هذا المجال فالتعاون الدولي الهام يتمثل في أوضح وأهم صورة في المعاهدات والاتفاقات الدولةي التي يتم عقدها سواء في مجال مكافحة جرائم الإنترنت وأيضاً في مجال حماية الملكية الفكرية وقد انضمت مصر إلى الاتفاقات الدولةي الخاصة بحماية حق الملكية الفكرية كما أنها أصدرت قانون حماية الملكية الفكرية الخاص بها والصادر برقم ٨٢ لسنة ٢٠٠٣ وقد كانت المعاهدات الدولية كمعاهدة برن ومعاهدة تريبس ومعاهدات الويبو هما الأساس الذي تم بناء عليهم سن هذا التشريع الذي تنضم به مصر إلى الأسرة الدولية في مجال حماية الملكية الفكرية.

ومن جهة أخرى فقد قامت مصر أيضاً بمسايرة الأسرة الدولية فيما تبنته هيئة الأمم المتحدة من إصدار قوانين خاصة بالتجارة الإلكترونية

والتوقيع الإلكتروني وقد تم ذلك أيضاً إيماناً من مصر بأن الانضمام إلى المجتمع الدولي فيه الخير والفائدة إلى جمهورية مصر العربية.

ومثال ذلك أيضاً انضمام مصر إلى كافة الاتفاقات العربية التي أقرها مجلس وزراء الداخلية العرب وكذلك مجلس وزراء الداخلية والعدل العرب وهي اتفاقات عربية تهدف إلى التعاون فيما بين الدول العربية في مجال مكافحة الجريمة المنظمة والاتجار في المخدرات والمؤثرات العقلية ومكافحة الإرهاب.

٤- استحداث قوانين جديدة تقنن الاستخدامات الإلكترونية مثل قانون التجارة الإلكترونية وقانون التوقيع الإلكتروني

تلعب التجارة الإلكترونية ELECTRONIC COMMERCE بصفة خاصة والتطور الهائل في تقنيات الاتصال والمعلومات بصفة عامة دوراً أقل ما يوصف بأنه هائل جداً في تطور الاقتصاد العالي بصفة عامة والاقتصاد الوطني بصفة خاصة فلا يمكن إنكار أن التجارة الإلكترونية عملت وبشلك كبير جداً على سرعة انتقال المعاملات ورؤوس الأموال وألغت ما كان يعوقها قديماً من الحواجز الجغرافية التي كانت تحد كثيراً من حركتها وكذلك قلة المعلومات التي كانت تعتبر في الماضي الحاجز الأكبر في عدم اجتياز اقتصاد الدول الدنامية في النفاذ إلى العالمية والحصول على نصيبه الطبيعي من حجم التجارة الدولية.

إلا أنه ومن جهة أخرى فإن التفاوت التكنولوجي فيما بين الدول المتقدمة والدول النامية قد يؤدي إلى عدم استفادة اقتصاد الدول النامية من

ذلك التقدم التكنولوجي الهائل الذي يعيشه العالم حالياً والمسمى التجارة الإلكترونية وعليه فصحيح أن الحواجز التي كانت تعوق الدول النامية قد زالت إلا أنه قد وجد مكانها حاجز آخر ألا وهو التقدم التكنولوجي الذي يعبر أسهل ولو جزئياً في إمكانية تجاوزه والعمل على التفوق فيه مع أهمية ملاحظة أن عدم قدرة الدول النامية على تجاوز مثل هذا الحاجز فسوف تزيد الهوة فيما بينها وبين الدول المتقدمة وأن يفيد عندئذ أي مجهود قد يبذل للعمل على تقليله.

هذا ويعد الإنترنت هو القوة الدافعة في انتشار التجارة الإلكترونية ELECTRONIC COMMERCE وبعد ما وفرته شبكة الإنترنت من سرعة قصوى في تناقل البيانات والأموال والوثائق في أقل من ثواني قليلة مهما كانت المسافة التي تفصل بين الأطراف فشبكة الإنترنت تعد هي الوسيلة الوحيدة في إبرام الصفقات في الكثير جداً من الصفقات في الوقت الحالي.

ورغم أن العديد من الدول النامية لم تستفيد حتى الآن من تلك التكنولوجيا المتطورة نظراً لعدم وجود البنية التحتية لخدمات الاتصالات الهاتفية إلا أن جمهورية مصر العربية ليست كذلك.

فجمهورية مصر العربية لديها بنية تحتية متكاملة جداً في مجال الاتصالات الهاتفية وهو ما جعلها تستفيد أقصى استفادة وجعل انتشار شبكة الإنترنت INTERNET يتضاعف سنوياً بل إنه قد يكون يتضاعف أكثر من مرة في العام الواحد.

ويتمثل ذلك في زيادة الخدمات الهاتفية في مصر خلال السنتين الأخيرتين بنسبة كبيرة لتصل عدد الخطوط الثابتة إلى ٦،٨ ملايين خط تليفوني بزيادة شهرية قدرها ٨٠٠٠٠ خط جديد كما زادت نسبة انتشار التليفون المحمول في مصر لتصل إلى ٥٪ سنوياً أي ٥،٣ ملايين مشترك وهذا يرجع إلى اهتمام الحكومية المصرية بتطوير البنية الأساسية للمعلومات والاتصالات الهاتفية فمنذ عام (١٩٨٥) اتخذ قرار لإنشاء البنية الأساسية للمعلومات الوطنية لتصبح الأساس لتطوير جميع القطاعات والصناعات بمشاركة القطاع العام مع القطاع الخاص، وخلال الفترة من ٨٥- ٩٥ تم إنشاء أكثر من ٦٠٠ مركز لدعم واتخاذ القرار في ٢٦ محافظة بهدف تطوير التجارة والحياة الاقتصادية والاجتماعية.

كما أن مصر تنظر إلى التجارة الإلكترونية ELECTRONIC COMMERCE كداعم أساسي للتجارة وخطط التقدم الاجتماعي والاقتصادي حيث تقدم التجارة الإلكترونية فرصاً لزيادة حجم التجارة وتنشيط الاستثمار وتسهيل الصفقات التجارية بالإضافة إلى أنها تتيح أسواقاً أكبر وأكثر تنوعاً وطرقاً تسويقية جديدة ويتوقع أن يصل حجم التجارة الإلكترونية إلى أكثر من تريليون دولار أميركي وهذه الزيادة في حجم التجارة تحمل في طبائعها مزايا كامنة للاقتصاد المصري إذا استطاع استخدامها جيداً وخاصة بالنسبة للمشروعات الصغيرة والمتوسطة والتي قبل استخدام التجارة الإلكترونية كانت تفتقر السبل لترويج منتجاتها بالخارج.

كما أنه من المعروف أن التجارة الإلكترونية لا تقتصر فقط على التجارة وإنما تمتد لتشمل قطاعاً كبيراً من الأعمال كالخدمات المالية كالتأمين والبنوك والتجارة والسياحة والترفيه والدعاية والتسويق والمعلومات والتعليم والتدريب والإعلام كالكتب الإلكترونية.

ولتكون التجارة الإلكترونية موجودة في بيئة صحيحة وليتم الاستفادة منها أقصى استفادة فقد قامت مصر باتخاذ عدد من الخطوات نوجزها فيما يلي:-

- وقد تم إصدار قانون يقنن التجارة الإلكترونية في مصر.
- وكذلك أصدرت قانون آخر لتقنين مسألة التوقيع الإلكتروني.
- تطوير البنية الأساسية للمعلومات بإنشاء العديد من مراكز المعلومات على مستوى الجمهورية.
- تنفيذ العديد من المشروعات التي تعتمد وبشكل أساسي على الصناعات ذات التكنولوجيا العالية لنقل تلك التكنولوجيا إلى داخل مصر.
- زيادة الوعي من جميع الجهات المعنية بالاستفادة من تلك التكنولوجيا المتقدمة والعمل على فتح منافذ للصناعات المصرية عبر تلك البوابة الإكترونية التي تختصر الكثير من الوقت والمسافات.

ورغم أن مصر قد خطت الكثير من الخطوات في مجال التجارة الإلكترونية وتنشيطها والاستفادة منها إلا أن الأمن هو من أكبر المشاكل التي تعرقل مثل هذه الخطوات.

فالحفاظ على السرية والخصوصية هو من أهم المشكلات التي تواجه التجارة الإلكترونية ليس في مصر فقط بل في العالم أجمع.

فلابد من التأكيد على السرية والخصوصية فيما يتعلق بالبيانات والمعلومات التي يتم تداولها على شبكة الإنترنت في مجال التجارة الإلكترونية ولابد من النص قانوناً على الحفاظ على تلك السرية إذا أردنا على الاستفادة.

ورغم أننا نطالب بالنص قانوناً على الحفاظ على السرية إلا أن تلك السرية يمكن أن تنتهك عبر الشبكة دون إمكانية التحقق من الهوية.

فعدم القدرة على التأكد من هوية المستخدم والتحقق من المعاملات من أكبر المشاكل التي تواجه التجارة الإلكترونية ويعتبر النقص في تحديد الهوية من الأسباب الرئيسية لتسهيل الاحتيال والخداع ويمكن أن يؤدي إلى جرائم عديدة لا يمكن ارتكابها في الأسواق التقليدية بنفس الطريقة فالاحتيال عن طريق كروت الائتمان يمكن أن يظهر عندما يطلب التجار دليلاً حقيقياً والذي لا يمكن أن يمتلكه إلا المالك الحقيقي.

كما أن النظام الورقي البنكي الحالي يعوق التجارة الإلكترونية ولا يوجد ما يعوق البنوك بشكل قانوني من استخدام الإنترنت ولكن بسبب

المخاوف المتعلقة بالأمن فإنهم لا يشعرون بالراحة من تبادل الصفقات والبيانات عبر الإنترنت لذلك فإن البنوك لا تقبل الدفع عبر الإنترنت ولا تبادل الصفقات حتى لو لم يكونوا ممنوعين بشكل رسمي من ذلك ويرجع الرفض السائد لدى البنوك المصرية في تسهيل الائتمان عبر الإنترنت والتبادل التجاري لنقص ضمان السرية والأمن بخصوص إجراء تلك العمليات كما أن أعمال البنوك المحدودة عبر الإنتنت كانت مقصودة ولكن إضافة إلى ذلك فقد تم التبليغ عن بعض عمليات الاحتيال التي تمت ولم يتم تحديد هوية مرتكبيها.

٥ـ إنشاء إدارات جديدة بوزارة الداخلية تكون مسئولة عن تلك الجرائم

أنشأت وزارة الداخلية في جمهورية مصر العربية إدارة جديدة تماماً في تكوينها ونوعية عملها جديدة في تكوينها لأنها تتكون من ضباط على أعلى درجة من التخصص والحرفية في تكنولوجيا الحاسبات وشبكة الإنترنت وجديدة في نوعية عملها على أساس أن عملها ليس ضبط المجرمين التقليدين الذين لا زالوا يرتكبون جرائمهم بالطرق التقليدية القديمة المحفوظة لدى كافة العاملين بوزارة الداخلية المصرية وإنما لملاحقة مجرمين على درجة تقنية عالية في مجال الحاسبات وشبكة الإنترنت ويرتكبون جرائمهم بطرق متطورة على المجتمع مستخدمين فيها تكنولوجيا الحاسبات وشبكة الإنترنت ويكون من الصعب إن لم يكن من المستحيل أن تتم ملاحقتهم إلا باستخدام وسائل أكثر تطوراً بواسطة ضباط على أعلى درجة من التدريب والتخصص على تلك التكنولوجيا.

وقد تم إنشاء تلك الإدارة الجديدة بعد أن زاد عدد مستخدمي شبكة الإنترنت خاصة بعد أن أصبح الدخول على الشبكة يتم بسهولة كبيرة جداً ولا يحتاج إلى أي تعقيدات كما كان في أول الأمر عندما كانت في بدأ دخولها إلى مصر إذ أن الدخول على شبكة الإنترنت الآن لا يحتاج إلا إلى خط تليفون وجهاز كومبيوتر بالطبع [1]. وبالطبع ومع زيادة عدد مستخدمي الإنترنت زاد بالتالي من يقومون باستخدام تلك التكنولوجيا استخداماً سيئاً ويستغلونها في ارتكاب جرائمهم معتقدين أنهم يعيدون جداً عن أيدي القانون وبعيدين عن أن ينالوا عقابهم على ما ارتكبت أيديهم فعدد الجرائم التي ترتكب باستخدام تلك الشبكة وعليه كان من الضروري إنشاء تلك الإدارة ليكون في الإمكان الحد من تلك الجرائم ومحاولة منعها نهائياً إن أمكن.

وقد تلاحظ أن معظم تلك الجرائم التي ترتكب على الشبكة أو باستخدام الحاسبات يكون تكييفها القانوني متوافق في معظم الأحيان مع التكييف القانوني التقليدي المنطبق على نفس الجرائم التي ترتكب بالطرق التقليدية مع وجود فراق واحد فقط هو أداة الجريمة أي استخدام الحاسبات أو شبكة الإنترنت INTERNET في ارتكاب الجريمة أي استخدام التقدم التقني MODERN TECHNIQUES في ارتكاب الجرائم بدلاً من الطرق التقليدية التي كانت تلك الجرائم ترتكب بها دائماً في الماضي وهو بالتالي

(1) محمد الجنيبي، مصدر سابق ص ١٤٢- ١٥٢ (٩٨).

ما يضعها تحت طائلة القانون LAW دون الحاجة إلى وجود نصوص قانونية جديدة تجرم تلك الجرائم CRIMES.

ووجد أن معظم ما تم ضبطه من جرائم هي في الغالب جرائم ابتزاز وتشهير ونصب واحتيال وسرقة ودعارة وإنما هي تتم بطرق تكنولوجية حديثة لم يكن في الإمكان كشفها ملاحقة مرتكبيها أو ضبطهم إلا بوجود تلك الإدارة التي تم إنشائها حديثاً.

ونحن نرى أن من أهم ما قامت به تلك الإدارة هو ملاحقة القائمين على المواقع الإباحية التي يتم بثها من داخل البلاد فتلك المواقع بما نبثه من سموم تعمل على إثارة الغرائز فتؤدي إلى ازدياد الجرائم الجنسية وإغلاق تلك المواقع وملاحقة القائمين عليها يعمل على الحد من الجرائم الجنسية التي تقع بسبب زيارة تلك المواقع وما تقوم به من إثارة الغرائز لدى الشباب بصفة خاصة والرجال بصفة عامة.

ونحن نرى أيضاً أن وجود نصوص قانونية يتم تطبيقها على تلك الجرائم الحديثة MODERN CRIMES لا يغني عن الحاجة إلى وضع نصوص قانونية جديدة ومتطورة تغطي تلك الجرائم الجديدة وما قد يستجد عليها من جرائم فالتطور التقني MODERN TECHNIQUES الذي نعيشه حالياً والذكاء ودرجة التقنية العالية التي يكون عليها هؤلاء المجرمين تنبأ بأنه وفي المستقبل القريب سنواجه العديد من الجرائم شديدة التعقيد والتطور والتي لا تجد لها نصاً قانونياً تقع تحت طائلته من تلك النصوص القانونية التقليدية القديمة التي نضع الجرائم التي ترتكب حالياً في

نطاقها فنحن في حاجة إلى نصوص قانونية جديدة بحيث تجرم تلك الجرائم التكنولوجية الجديدة وما قد يستجد عليها من جرائم ومن تطور في أدوات ارتكاب مثل تلك الجرائم حتى لا يأتي الوقت الذي تقف فيه يد القانون عاجزة عن أن تقتص حق المجتمع من تلك الفئة المنحرفة التس تستغل التكنولوجيا الحديثة والتطور التقني MODERN TECHNIQUES في ارتكاب الجرائم بدلاً من استغلالها في ما يفيد المجتمع والاقتصاد الوطني.

على أنه يمكن أن تتم الاستعانة عند وضع مثل هذا القانون الجديد بالقوانين التي وضعتها الدول المتقدمة في هذا المجال للعمل على توحيد القوانين التي تعالج تلك الجرائم في جميع الدول وذلك في محاولة للحد من مثل تلك الجرائم ليس على المستوى المحلي فقط وإنما على المستوى العالمي أيضاً.

وفي هذا المجال يمكن أن يكون للأمم المتحدة الدور الريادي في ذلك فعليها أن تتصدى لمثل هذا الموضوع بأن تعمل على وضع قانون نموذجي موحد UNIFIED MODEL LAW بحيث يكون على الدول عند وضع قانونها المحلي أن تقتبس منه ما هو مناسب لمجتمعها وتقاليدها وبالتالي يكون هناك الحد الأدنى على الأقل في التماثل والتناسق بين القوانين التي تعالج هذا الموضوع على المستوى العالمي وهو ما يعمل على الحد من ارتكاب مثل تلك الجرائم وأيضاً لابد من وجود تناسق في القوانين لمواجهة الجرائم التكنولوجية الحديثة التي تكون في الأغلب الأعم من الحالات هي جرائم عابرة للحدود CRIMES TRANS BOEDER ولمواجهتها لابد

من وجود مواجهة لها من كافة القوانين الموضوعة على المستوى المحلي والدولي.

٦ـ تحقيق الأمن المعلوماتي للكيانات الاقتصادية

تعد الكيانات الاقتصادية متمثلة في الشركات والبنوك وما شابه ذلك من الركائز التي يرتكز عليها أي اقتصاد وطني وعليه فحماية الأمن الإلكتروني لتلك الكيانات هو من الأولويات التي يجب تحقيقها في الاعتبار على وجه السرعة ودون أي إبطاء قد يتسبب في اختراق تلك المنشآت وما قد يتسبب فيه ذلك من خسائر مادية ومعنوية هائلة لتلك المنشآت ومستوى سمعتها العالمية من الثقة والأمان.

وعليه فقد تمت دراسة المحاولات التي يمكن بذلها لاختراق تلك الكيانات الاقتصادية والحلول التي تم وضعها لمنع حدوثها.

١ـ محاولات الاختراق

١- أن ضغط المعلومات على وسيط معلوماتي في حيز دقيق هو بالقطع أمر مفيد للمنشأة ولكنه قد يصبح عنصر خطر فالأسرار التجارية المالية والصناعية يتم تخزينها في وسائط معلوماتية مضغوطة دقيقة الحكم يسهل سرقتها وإخراجها من المنشأة في حيز لا يزيد على علبة السجائر كما يمكن نقل المعلومات المالية والتجارية والصناعية المخزنة إلكترونياً في لحظات معدودة غير شبكات الحواسب والاتصالات.

٢- إن اللامركزية في حفظ واسترجاع المعلومات الحساسة إلكترونياً لها مخاطرها ففي بعض المنشآت يكون للعاملين حرية وقدرة الدخول إلى نظم المعلومات والاتصالات الخاصة بشبكة حواسب المنشأة ويمكن لهم في حالة عدم وجود نظام أمن معلومات وأمن اتصالات أن يغترقوا مثل هذه المعلومات وأن يستخدموها بشكل غير أمين أو غير مشروع يضر بالمنشأة.

٣- إن استخدام وسائل الاتصالات غير المشفرة لنقل رسائل البيانات الإلكترونية وغيرها من المعلومات يعرض المنشأة التجارية لمخاطر أنشطة إجرامية من منشآت منافسة.

٤- إن سهولة نقل المعلومات باستخدام البرمجيات ووسائل الاتصالات الحديثة دون تأمين أدوات المعلومات والاتصالات يعرض أسرار المنشأة التجارية لمخاطر جسيمة.

أن تحرك وتنقل وسفر المسئولين عن المنشأة التجارية بأجهزة حاسبات نقالة غير مؤمنة تحتوي على معلومات دقيقة وحساسة خاصة بالمنشآت وأنشطتها التجارية والمالية يعرض تلك البيانات والمعلومات لمخاطر في حالة سرقة تلك الأجهزة أو الدخول إليها من شخص غير مرخص له.

٦- أن عدم تأمين نظم الاتصالات والحاسبات والمعلومات يعرض ممتلكات الشركة وبياناتها للتخريب والتدمير خاصة في حالة عدم وجود نظم حفظ بديلة.

٧- إن استخدام المقاولين من خارج المنشأة SURCING OUT في عمليات إنشاء أو حفظ أو إدارة نظم الحاسبات والمعلومات والاتصالات الخاصة بالمنشأة قد يعرض المنشاة لمخاطر جسيمة وقد يعرض أسرارها لمخاطر لا يعرف مداها سواء عن طريق الموظفين التابعين لذلك المقاول أو المقاول ذاته سواء كان موجوداً في الموقع – ركز المنشأة – أو يتعامل ويتصل بالنظام من خارج المنشأة وعليه لابد من التأكد من السمعة الممتازة لهؤلاء المقاولين قبل إسناد تلك العمليات لهم مع مراقبة تنفيذ الأعمال بواسطة استشاري متخصص محايد وحسن السمعة.

٨- إن الإدارة التي ليست على قدر من الكفاءة لتدير نظم وشبكات المعلومات والاتصالات داخل المنشأة قد تعرض بيانات المنشأة وممتلكاتها لمخاطر جسيمة ومن ذلك الاختراق من قبل أشخاص أو جهات على مستوى احتراف عال أو من موظفين من ذات المنشأة.

٩- أن ضعف الوعي بأمن المعلومات وآمن الاتصالات في المنشأة قد يكون مصدر خطر ففي المنشأة الكبرى قد يوجد مسئولين أكفاء عن أمن المعلومات وأمن الاتصالات ولكن في الشركات متوسطة الحجم أو المنشأة الفردية قلما يوجد متخصص في أمن المعلومات وأمن الاتصالات.

إضافة إلى الاختراق المادي الملموس لنظم ومنشآت الحاسبات والاتصالات المتمثل مثلاً في سرقة وسائط إلكترونية مشحونة بالبيانات أو تكسير المعدات أو إتلافها الخ فإن من الوسائل الفنية للاعتداء على نظم المعلومات والاتصالات ما يلي:-

١- اختراق شبكات الاتصالات بوسائل مادية بالدخول إلى الخط التليفوني الواصل للمنشأة عبر وصلة سلكية مادية وذلك للحصول على معلومات صوتية أو بيانات منقولة.

٢- التصنت على المكالمات التليفونية باستخدام وسائل فنية مثل (DILER NUMBER RECORDER (DNR.

٣- استخدام وسائل مثل جهاز ماسح الموجات SCANNER للتنصت على الاتصالات الخاصة بالمحمول وخلافه.

٤- وضع أجهزة تنصت في أجهزة الحاسبات أو الاتصالات الخاصة بالمنشأة أو في غرف اجتماعاتها.

٥- عدم الكشف على البرمجيات التي يتم إعدادها للمنشأة من قبل مهندسي برمجيات للتأكد من وجود أو عدم وجود أوامر نائمة أو مدفونة لإساءة استخدام البرمجيات في الحال والاستقبال عند تشغيل تلك البرمجيات.

٦- وجود ثقب HOLE أو ثقوب في نظم الحاسبات أو البرمجيات قد يؤدي إلى إمكانية اختراق نظم المعلومات والاتصالات لاغتراف المعلومات أو تغير البيانات والعبث بها أو تدمير نظم المعلومات والشبكات.

٢- وسائل الأمان التي يجب أن تتبع

يشمل أمن المعلومات والاتصالات استخدام وسائل تقليدية لتحقيق الأمن وكذلك وسائل حديثة غير تقليدية.

أ- الأساليب التقليدية للأمن بالأجهزة والمنشآت:

يشمل ذلك نظم الحراسة والأسوار والبوابات المؤمنة ووسائل الإنذار ضد الاختراق أو الحريق وتكون درجة الأمن التقليدي متناسبة مع أهمية وحساسية وموقع منشآت وأجهزة الاتصالات أو المعلومات أو الحاسبات المطلوب حمايتها ويقوم الأمن التقليدي على عناصر فنية وإدارية وهندسية بوجود إدارات الأمن في المنشآت واستخدام الوسائل والأدوات الفنية التقليدية في الحماية والتأمين إضافة إلى التصميم الهندسي الآمن لتلك المنشآت وصفوة القول في هذا المقام هو ما قرره عالم حديث من أن الأمن التقليدي يتمثل في الحراسة والتحصين والتشريع والتدريع والقفل والفتح.

ب- الأساليب والوسائل غير التقليدية

إن تحقيق أمن المعلومات وأمن الاتصالات في المنشأة يتمثل في ضرورة وجود نظام كفء لإدارة المعلومات MANAGEMENT SYSTEM OF INFORMATION وأمن المعلومات والاتصالات ويشمل ذلك:-

١- تحدي المسئوليات والسلطات درءاً لشيوع المسئولية والالتزام بالنظام من الكبير والصغير.

٢- حصول كل مستخدم لنظام المعلومات والاتصالات على مفتاح الدخول خاص به المختلف عن مفاتيح الغير للدخول إلى النظام.

٣- أن يكون مفتاح الدخول مكون من ستة رموز على الأقل.

٤- وجوب تغير مفتاح الدخول بشكل متكرر وعشوائي.

٥- وجوب تغير مفتاح الدخول في حالة الاشتباه في معرفة غير المرخص له بمضمون المفتاح.

٦- عدم احتواء مفتاح الدخول على أي من الحروف الأولى لاسم المستخدم أو اختصار اسمه أو اسم شهر أو تاريخ ميلاد.

٧- تكوين مفتاح الدخول بشكل عشوائي لتحقق من عدم احتوائه على تسلسل رقمي أو منطقي.

٨- إيجاد الوسائل الفنية الآلية لتسجيل محاولات الاختراق الفاشلة للنظام وتسجيل ميعاد وتاريخ حدوثها وكذلك تحديد الوحدة الطرفية التي تمت من خلالها محاولة الاختراق.

٩- مناقشة وتحليل كل محاولات الاختراق غير الناجحة واتخاذ ما يلزم لتحصين النظام.

١٠- تشفير وترميز المعلومات والبيانات الشخصية.

١١- تغير مفاتيح التشفير بشكل متكرر غير دوري.

١٢. إسناد مهمة إدارة مفاتيح التشفير لشخصين وليس لشخص واحد باستخدام نظام ثنائي منعاً من انفراد شخص بذلك.

١٣- فصل خطوط الاتصالات غير اللازمة للدخول إلى نظم الحاسبات والمعلومات.

١٤- قصر توزيع المعلومات والبيانات المشفرة والحساسة على عدد محدود ومعلوم ومرخص له في تداول تلك البيانات بقدر ما يلزم.

١٥- حصر توزيع المعلومات على الأفراد أو الأقسام التي تكون تلك المعلومات لازمة وضرورية لها للقيام بوظائف تلك الأقسام أو الأعمال دون غيرها.

١٦- الحفاظ على البيانات في بنك بيانات محدد تتوافر له الحماية.

١٧- تحديد مستويات الدخول إلى النظم بشكل متعدد الطبقات.

١٨- متابعة اتصالات الموظفين خارج المنشأة وكذلك تنقلاتهم وحركاتهم بين الأقسام المختلفة على أن يكون دخول الأقسام التي تحتوي على معلوماغت حساسة بترخيص كتابي خاص.

١٩- في حلة استخدام المعاملات المالية المشفرة تحفظ أرقام بطاقات الاعتماد في بنوك بيانات مستقلة غير متصلة بالشبكات ويجب ألا يتضمن تداول البيانات بين الأقسام الرقم الكامل لكارت الائتمان بل آخر ٤ أرقام فقط.

ج- الوسائل والأدوات الفنية لتوفير أمن المعلومات لاتصالات ومنها على سبيل المثال:-

١- تطبيق نظم إدارة وأمن المعلومات والاتصالات.

٢- استخدام خطوط تليفونات واتصالات مأمونة.

٣- استخدام وحدات تليفونات مؤمنة STU .

٤- استخدام قناة اتصالات آمنة.

٥- استخدام تكنولوجيا الفخ الإيجابي TRAPPING POSTTIVE وهو فلتر يقوم بتصيد التداخل في القنوات ويرفض ولوج غير المشتركين إلى تلك الفتاة.

٦- استخدام تكنولوجيا الفخ السلبي TRAPPING NEGATIVE ويتم عن طريقها حجز جزء من الإشارة وبالتالي منع حصول غير المشتركين على الإشارة.

٧- استخدام تكنولوجيا التشفير والترميز.

٨- استخدام تكنولوجيا SSL وهي تكنولوجيا تتضمن بروتوكولاً أمنياً للإنترنت فيكون الولوج إلى النظام لمن هم مرخص لهم بذلك.

٩- استخدام تكنولوجيا التوقيع الرقمي أو الإلكتروني في مهر الرسائل الإلكترونية للتحقق من نسب المستند الإلكتروني لمنشئه ومرسله.

١٠- استخدام خدمات التحقق والتصديق الإلكتروني وهي خدمات متاحة عن طريق سلطات كهيئات البريد في بعض الدول أو بعض الشركات المرخص لها وهي توفر تحققاً للمتعامل في التجارة الإلكترونية من شخصية مرسل البيانات أو الطرف الآخر في العلاقات التعاقدية الإلكترونية.

١١- استخدام وسائل التأكد من صحة وسلامة المراسلات الإلكترونية.

١٢- استخدام البرامج المضادة للفيروسات وتحديثها بانتظام.

١٣- استخدام تكنولوجيا الحوائط النارية لحماية نظم الحاسبات والمعلومات.

١٤- استخدام تكنولوجيا الـ TUNNCLING لتوفر نقل مؤمن للاتصالات عبر الإنترنت أو غيره من الشبكات.

١٥- استخدام تكنولوجيا الكشف عن وسائل التنصت في النظم والشبكات.

١٦- استخدام الـ COOKIES FILE لإزاحة تلك الوسائل التي تستخدم في الدخول غير المشروع للنظام للتلصص عليه.

١٧- استخدام تكنولوجيا العلامات المائية أو الأختام الإلكترونية الخاصة على الوثائق الإلكترونية.

١٨- استخدام الوسائط التكنولوجية الجديدة للدخول إلى النظم ومن ذلك ماسح بصمة اليد أو قزحية أو شبكة العين.

١٩- استخدام تكنولوجيا الإجابة والتأكيد أو تكرار التأكيد.

٢٠- استخدام تكنولوجيا تسجيل حدوث الاتصالات.

٢١- اللجوء لخدمات شخص ثالث مؤمن لإيداع الوثائق الإلكترونية.

٢٢- استخدام النقود الإلكترونية في المعاملات الإلكترونية درءاً للنصب والاحتيال والسرقة.

وأخيراً لابد من تتبلور أي محاولة من المحاولات التي تبذل سواء من مصر أو من أي دولة أو منظمة أخرى لابد من تتبلور تلك المحاولة في إطار عام يتركز حول أمن المعلومات على شبكة الإنترنت:-

أمن المعلومات عبر شبكة الإنترنت

INFORMATION SECURITY TRANS THE INTERNET

للعمل على تحقيق أمن للكم الهائل من المعلومات الموجود على شبكة الإنترنت لابد من اتخاذ العديد من الخطوات إلا أنه يمكن تقسيم تلك الخطوات إلى ثلاثة اتجاهات هي:-

١- سرية المعلومات

SECRECY OF INFORMATION أي ضمان حفظ المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت والخطوات التي يجب اتخاذها هنا تصب جميعاً في عدم إمكانية الاطلاع على تلك المعلومات إلا لمن هم مخول إليهم قانوناً الاطلاع عليها فقط دون أن يتمكن أي من الغير من الاطلاع على تلك المعلومات.

٢- سلامة المعلومات

SAFETY OF INFORMATION أي ضمان عدم تغيير تلك المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة

الإنترنت والخطوات التي يجب اتخاذها هنا تصب جميعاً في عدم إمكانية تغيير تلك المعلومات إلا لمن هم مخول قانوناً إليهم تغييرها فقط دون أن يتمكن أي من الغير من تغيير تلك المعلومات.

٣- وجود المعلومات

REFINDING OF INFORMATION أي ضمان عدم حذف تلك المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت والخطوات التي يجب اتخاذها هنا تصب جميعاً في عدم إمكانية حذف تلك المعلومات إلا لمن هم مخول قانوناً إليهم حذفها فقط دون أن يتمكن أي من الغير من حذف تلك المعلومات.

نفعه أو منعه للجناح أو الانحراف أياً كان شكل ذلك الانحراف، بما فيه الانحراف الإنترنتي، فإنه يجب على القائمين على أمر المجتمع وأصحاب القرار فيه استيعاب حقيقة هامة بخصوص إنترنت، وهي أن الحقيقة التي نحياها هي حقبة الإنترنت الذي هو في تطور يوماً بعد يوم، ولذلك لا غرابة في أن يطلق المختصون تحذيراتهم من أن "أطفال الإنترنت قادمون"، ويقصد الخبراء بالطبع أن مستخدمي الشبكة من الأطفال يتزايد عددهم يوماً بعد يوم بسرعة هائلة، ففي بريطانيا تضاعف عدد الأطفال مستخدمي الإنترنت من عام ١٩٩٧ وحتى ٢٠٠٠، ثلاث مرات، وأنه يجب النظر إلي – تعامل الأطفال والأحداث مع الإنترنت – بواقعية ونظرة علمية وليس نظرة ثانوية قد تؤدي لنتائج ضارة فيما بعد .

ونخلص مما سبق إلى أن دور المجتمع في مواجهة الانحراف الإنترنتي لدى الحدث يقتضي العمل في اتجاهات ثلاثة هي:

١- تكريس دور الأسرة معلوماتياً، بمعنى أن يسارع الأب والأم إلى الإلمام بتقنية الإنترنت والتعامل معها على نحو يمكن كلاهما من مراقبة الطفل أو الحدث حال تجواله على الشبكة ولا تترك له الحرية كاملة في هذا المجال، ويفضل لو وضع جهاز الكومبيوتر في مكان مطروق داخل المنزل، وليس في الحجرة الخاصة بالحدث حتى يكون تجواله على الشبكة تحت بصر ومراقبة الوالدين، ويحبذ لو استعان الوالدين بالبرامج التي تمكنها من استرجاع المواقع التي تصفحها الطفل في غيابهما، أو التي تقوم بعمل نوع من الرقابة التلقائية -PROXY- بحيث تمنع الحدث أو الطفل من التسلل إلى موقع محظور عليه الدخول لها، لأنها سوف تمده بخبرات ضارة كالمواقع الإباحية أو تلك التي تحض على العنف أو الكراهية أو التطرف.

٢- اهتمام المدرسة – في كافة المراحل التعليمية – بتسخير تقنية الإنترنت لأغراض تعليمية، وتدريس ثقافتها للطفل على نحو يعي معه أخطارها قبل المزايا المستمدة منها.

٣- السيطرة على جماعات الأصدقاء والشللية التي قد تدفع الحدث إلى الانحراف الانترنتي سواء من خلال اللقاء على مقاهي الإنترنت أو من خلال اللقاء في غرف الدردشة وتسريب الخبرات الضارة فيما بينهم عن السلوك غير المشروع المستمد من الإنترنت أياً كانت صورته.

إن العصر الذي نعيشه، والعصر القادم، هو عصر – الإنترنت – سيطرت فيه المعلوماتية على كل شيء في حياتنا، وبقدرة التفوق والإلمام بفنونها، تكون القدرة والقوة والسيطرة، وبقدر الخضوع لمثالبها ومساوئها، يكون الهدم في أجيال الشباب التي هي أمل المستقبل، والإنترنت واقع لا مفر منه، ولا يمكن التغاضي عنه أو إصدار قرار بعدم معه. فذلك معناه التخلف عن الآخرين مئات السنين.

كذلك يتعين ألا نصل إلى مرحلة – اليهود المتشددين – الذين حرموا الإنترنت لما تمثله هذه التقنية – مثل التليفزيون- من مخاطر بالغة.

قائمة بأهم المصادر

١- د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية مصر، ٢٠٠٧.

٢- د/ علي محمد شمو، التكنولوجيا الحديثة والاتصال الدولي والإنترنت، الشركة السعودية للأبحاث والنشر.

٣- د/ إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت، بحث مقدم لمؤتمر القانون والكومبيوتر والإنترنت، جامعة الإمارات.

٤- د. جميل عبد الباقي، الإنترنت والقانون الجنائي.

٥- نبيلة هبة هدوال مصدر، الجواني الإجرائية في مرحلة جمع الاستدلالات، دار الفكر، الإسكندرية ٢٠٠٦.

٦- محمد أمين احمد الشوابكة، جرائم الحاسوب والانترنت دار الثقافة، عمان ٢٠٠٤.

٧- د. علي محمد جيار الحسيناوي، جرائم الحاسوب والانترنت، اليازوري، عمان.

٨- أسامة أحمد المناعة، وآخرون، جرائم الحاسب الآلي والانترنت.

٩- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت منشورات الحلبي، ط١، ٢٠٠٧.

فهرس المحتويات

الفصل الأول: التعريف بالإنترنت واستخداماته ٥

الفصل الثاني: جرائم الإنترنت ٢١

الفصل الثالث: الطبيعة القانونية لجرائم الحاسوب والإنترنت ٧٩

الفصل الرابع: الجوانب القانونية للإنترنت ٩١

الفصل الخامس: التحديات والممارسات العملية في مجال ١٢٥

الفصل السادس: الإطار الإقليمي لمكافحة جرائم الإنترنت ١٤٣

الفصل السابع: تجربة جمهورية مصر العربية في مكافحة ١٨٣
جرائم الحاسبات وشبكات المعلومات