الفصل الثالث:
أنواع الجرائم في الإنترنت

obeikandl.com

سيتطرق هذا الفصل لأنواع الجرائم في الإنترنت، ولقد تم تقسيمها إلى الأنواع الآتية:

- جرائم ضد الحكومات
- جرائم سرقة المواقع التجارية
- جرائم الابتزاز
- جرائم الحقوق الفكرية
- جرائم الخصوصية
- جرائم الملاحقة والمضايقة
- جرائم المخدرات والعصابات وغسيل الأموال
- جرائم التمييز العنصري
- جرائم الإرهاب

obeikandl.com

٣-١ جرائم ضد الحكومات

يحفل التاريخ بالكثير من القصص عن أولئك الذين حاولوا خداع القطاعات الحكومية على مختلف مجالاتها. وعلى الرغم من تعدد الطرق والحيل التي يلجأ إليها المجرمون فإنها في الغالب تكون لتحقيق أحد هدفين؛ الأول: هو التهرب من دفع المستحقات، مثل: الضرائب والرسوم وغيرها. والثاني: هو الحصول على بعض المنافع التي لا يستحق المخالف الحصول عليها عادة.

والمتابع لتطور الإنترنت سيلاحظ أنه في الفترة الأخيرة قد كثر الحضور الإلكتروني للقطاعات الحكومية في الشبكة وظهور ما يسمى بـ (الحكومة الإلكترونية)، حيث يندر أن تجد مصلحة حكومية دون أن يكون لها موقع على الإنترنت تقدم خدماتها من خلاله.

وإن كان من المسلّم به أن ارتباط الجهات الحكومية المختلفة بالإنترنت له فوائد جمة، غير أن هذه الفوائد تجلب معها المخاطر أيضاً، حيث تعد الجهات الحكومية من أكثر الجهات تعرضا للهجمات. ويمكن تقسيم الهجمات على الجهات الحكومية إلى أربعة أقسام رئيسة، وهي كالآتي:

٣-١-١ سرقة المنافع

استغل المجرمون تطور الحكومات ودخول الحاسب الآلي في جميع المنافع والإدارات الحكومية، واستطاعوا مهاجمة الإدارات الحكومية المرتبطة بالإنترنت، ثم تعديل البيانات المتعلقة بهم لكي يحصلوا على منافع لا يستحقونها. ومثال ذلك قيام بعضهم بتعديل البيانات الخاصة بالضرائب، وذلك حتى يدفعوا كمية أقل، أو القيام بالدخول على بيانات التأمين الطبي وتعديل البيانات الخاصة بهم وإعطاء أنفسهم صلاحيات ومنافع أكثر مما هو مسموح لهم بها.

obeikandl.com

٣-١-٢ سرقة الأموال

ويشمل هذا النوع اختراق الأجهزة المتعلقة بالنواحي المالية، ثم العبث بها حتى يتم تحويل مبلغ من المال لحساب المستخدم أو لعنوانه. ومن الأمثلة على ذلك ما قام به أحد المجرمين من إدخال بيانات وهمية في نظام المحاسبة الخاص بأحد الإدارات الحكومية، بحيث يتم إرسال شيكات له، وأصبح يقوم بالحصول عليها وإدخالها في حسابه. واستطاع بذلك الحصول على مبلغ ٢,٧٥ مليون دولار.

٣-١-٣ سرقة المعلومات

لاشك بأن الحكومات تمتلك معلومات أكبر عن مواطنيها، وهذه المعلومات مخزنة في قواعد البيانات الخاصة بالجهات الحكومية المختلفة. وهذا ما يجعل المجرمين يستهدفون الشبكات الخاصة بالجهات الحكومية المختلفة، ويقومون باختراقها للحصول على المعلومات الموجودة في قواعد البيانات الخاصة بها.

ويندرج تحت هذه النقطة أيضا التجسس وسرقة المعلومات الحساسة الموجودة في بعض القطاعات الحكومية ذات الأهمية العالية، مثل القطاعات العسكرية أو قطاعات الاستخبارات، واستخدامها فيما بعد ضد هذه الحكومات. ولعل هذا ما يقوم به المجرمون الذين يقومون بالجرائم بدافع التجسس، وسنتحدث عن ذلك في الفصل الرابع.

٣-١-٤ إيقاف أو تعطيل الخدمات الإلكترونية عن العمل

ويعدّ هذا النوع من أخطر التهديدات التي تواجه الحكومات في الوقت الراهن. ومثال

obeikandi.com

هذا النوع من الجرائم ما حدث لجمهورية أستونيا، فقد تعرضت مواقع حكومية ومواقع خاصة بمصارف وشركات اتصالات ومؤسسات إخبارية، لهجمات إلكترونية عبر الإنترنت؛ تعرف بمصطلح الهجمات الموزعة لتعطيل الخدمة، وقد كانت هجمات هائلة ومنظمة وغير مسبوقة، استهدفت البنية التحتية الإلكترونية للدولة على المستويين العام والخاص عبر شبكة الإنترنت، فتسببت هذه الهجمات في تعطيل شبكات البريد الإلكتروني الحكومية، وأدت إلى وقف المؤسسات المالية لتعاملاتها المصرفية التي تجرى عادة عبر شبكة الإنترنت. فضلاً عن تعطيل موقع الرئيس الأستوني ورئيس الوزراء وموقع البرلمان على شبكة الإنترنت، وإغلاق مواقع خاصة بوزارات، نتيجة تعرضها لسيل عارم من الرسائل أدى في النهاية إلى إغلاقها. ويقول خبراء أستونيون كما جاء في جريدة الشرق الأوسط[1] «إن روسيا هي مصدر هذه المشكلة بسبب تغيير أستونيا موقع نصب تذكاري حربي لتمجيد الجيش الأحمر من وسط العاصمة الأستونية في نهاية أبريل ٢٠٠٧، مما أثار غضب الأقلية الناطقة بالروسية واحتجاجات حادة في روسيا التي ما زالت تجد صعوبة في تقبل استقلال هذه الجمهورية السوفيتية السابقة».

ويلاحظ أن جمهورية أستونيا تمتلك عدداً هائلاً من الأهداف التي يمكن مهاجمتها، ذلك أن النجاح الاقتصادي الذي حققته هذه الجمهورية السوفيتية السابقة الصغيرة الحجم قام أصلا على أساس وضعها كمجتمع إلكتروني، فالكثير من التعاملات الحكومية هي إلكترونية، حتى التصويت في الانتخابات يجري عبر شبكة الإنترنت، بل إن الكثير من التعاملات العامة في أستونيا، بما في ذلك التوقيع على الوثائق القانونية تجرى عبر الإنترنت. وقد بدأت الهجمات في ٢٧ أبريل ٢٠٠٧م، بعد مرور ساعات فقط على تغيير موقع النصب التذكاري الذي يعود إلى الحقبة السوفيتية. وكما جاء أيضا في صحيفة الشرق الأوسط أن مسؤولون في أستونيا قالوا: «إن تعليمات وإرشادات حول كيفية تعطيل المواقع الحكومية ظهرت في منابر إنترنت باللغة الروسية». ويعد هذا الهجوم من أنواع الحروب الإلكترونية بين الدول.

١ عدد رقم ١٠٤٠٠ الأحد ٠٣ جمادى الأولى ١٤٢٨ هـ، ٢٠ مايو ٢٠٠٧

obeikandl.com

وقد أدت هذه (هذه التجربة الملموسة) إلى تغيير مهم في طريقة تفكير حلف الأطلسي الذي رد بشكل مباشر بإنشاء مركز امتياز في الدفاع الإلكتروني في تالين عاصمة أستونيا، وتتلقى أستونيا دعما في المشروع من الولايات المتحدة، وألمانيا، ورومانيا، وإيطاليا، وأسبانيا، كما جاء في نفس الصحيفة.

٣-٢ جرائم سرقة المواقع التجارية

وهي الجرائم التي يقوم بها المجرمون الذين يلهثون خلف المال، وتعد من أكثر أنواع الجرائم انتشاراً، وتشمل هذه الجرائم اختراق المواقع التجارية التي تقدم خدمة المبيعات عن طريق الإنترنت، ثم الحصول على قواعد البيانات الخاصة بالزبائن المتعاملين مع هذه المواقع والحصول على معلومات بطاقاتهم الائتمانية، واستخدامها فيما بعد للقيام بعمليات شراء غير قانونية. ومن الأمثلة على ذلك ما قام به أحد المخترقين من سرقة قاعدة البيانات الخاصة بموقع (Geeks.com)، مما أدى بالشركة إلى إرسال رسالة إلى زبائنها تطلب منهم إلغاء بطاقاتهم الائتمانية، واستخراج بطاقات ائتمانية بأرقام جديدة. وهذا بالطبع أدى إلى خسارة الموقع لسمعته ولزبائنه. وكذلك أيضا ما يحدث في بعض المواقع التي تسمح للمستخدم بتخزين رقم بطاقته الائتمانية في الموقع بحيث يستطيع الشراء دون الحاجة لإدخال رقم البطاقة الائتمانية في كل مرة، ولقد لوحظ أن المجرمين يقومون باختراق جهاز المستخدم الساذج والحصول على كلمة السر للموقع التجاري، ومن ثَمَّ شراء ما يريدون دون الحاجة إلى معرفة رقم البطاقة الائتمانية. وهذا ما حدا بموقع أمازون (www.amazon.com) الشهير لتغيير إستراتيجيته ومطالبة المستخدمين بإدخال أرقام بطاقاتهم الائتمانية في كل مرة يقومون بعملية شراء.

obeikandl.com

٣-٣ جرائم الابتزاز

لا يقل الابتزاز جرماً عن السرقة، والفرق الوحيد بينهما هو أن السرقة غالباً ما تتم باستخدام عامل التغافل أو القوة، بينما الابتزاز يتم في الأعم الأغلب بالتهديد بالعواقب الوخيمة مستقبلا، ما لم ينصاع الضحية لمطالب المبتز.

وتوفر الإنترنت مرتعاً خصباً لمن يريد الابتزاز، وتساعد المبتزين بأوجه عديدة، هي:

أولا: توفر وسيلة اتصال آمنة بين المبتز والضحية (كما ذُكر في خاصية انعدام الهوية في فصل سابق).

ثانيا: يمكن استخدام الإنترنت كوسيلة لتحديد الهدف، وذلك لكون الإنترنت مليئة بالمعلومات التي تساعد على ذلك.

ثالثا: تعد الإنترنت وسيلة تهديد مرعبة للضحية، فيكفي المبتز أن يهدد بنشر ما لديه على شبكة الإنترنت ليدب الهلع في قلب الضحية، وذلك لأن وضع شيء على الإنترنت يعني اطلاع الملايين من البشر عليه.

رابعا: يمكن استخدام خدمات الشبكة لتحويل المبالغ المادية الناتجة عن الابتزاز مباشرة دون أن يعرف الضحية رقم حساب أو هوية المبتز.

ولعل من أشهر الأمثلة على ذلك، أحد المواقع الذي ذاع صيته في الولايات المتحدة الأمريكية منذ عدة سنوات، حيث قامت إحدى النساء بوضع موقع لتهديد شخص يدعى بيل (Bill)، وقامت بوضع صور له مع طمس وجهه حتى لا يتم التعرف عليه ، وقامت بتوجيه

obeikandl.com

رسالة له عن طريق الموقع بأنه إن لم ينصع لما تريده، فإنها ستقوم بنشر صوره على الإنترنت. وقد اشتهر هذا الموقع بشكل كبير، وتم عرضه في وسائل الإعلام بشكل كبير وأصبح من المواقع المشهورة. وكل يريد أن يعلم من باب الفضول من هو بيل؟ وماذا فعل؟ ليستحق ذلك. ولكن إلى الآن لا أحد سوى بيل يعلم ما تريد هذه المرأة. ويبدو أنه قد انصاع لما تريده منه.

شكل ٣-١: الموقع الذي يهدد المدعو بيل.

٣-٤ جرائم الحقوق الفكرية

تعد شبكة الإنترنت في الوقت الحاضر أكبر آلة نسخ في التاريخ، فما يقع في أيدي المستخدمين من مواد يمكن نسخه ونشره في ثوانٍ معدودة إلى ملايين المستخدمين الآخرين، ويندرج تحت هذه النقطة الكثير من النقاط الفرعية، فجرائم الحقوق الفكرية في الإنترنت تتباين درجاتها وأهميتها بشكل كبير، فهناك فرق بين سرقة الطالب لمقال في الإنترنت وتسليمه في المدرسة على أنه هو الكاتب الأصلي، وبين سرقة البرامج الأصلية ونسخها وتوزيعها بشكل غير قانوني في المواقع المختلفة. ولعل الناحية الأخيرة هي التي تتلقى جانباً أكبر من الاهتمام. فهناك العديد من الأسباب التي أدت إلى سهولة واتساع عمليات تبادل البرمجيات المقرصنة عبر الشبكة، ولعل من أهمها الزيادة في عدد مستخدمي الإنترنت بشكل مطرد سنوياً، والزيادة في معدل نقل البيانات لاسيما عند استخدام الإنترنت عن طريق التوصيلات السلكية (الكيبل)، أو خدمة الخطوط الرقمية (DSL) أو عن طريق شرائح الجوال أو الشبكات اللاسلكية، علاوة على انخفاض تكلفة الاتصال بالإنترنت في شتى أنحاء العالم ومجانيته في بعضها. وهو الأمر الذي جعل الشركات الكبرى تتخوف بشدة من نمو معدلات القرصنة عبر الشبكة العنكبوتية، وتحذر من الخسائر الضخمة التي مازالت تلحق بصناعة البرمجيات والشركات العاملة فيها.

وفي مؤتمر المنظمة العالمية للملكية الفكرية (WIPO)، حذر روبرت هوليمان الرئيس والمدير التنفيذي لاتحاد منتجي برامج الكمبيوتر التجاري (BSA)، في الكلمة التي ألقاها في المؤتمر من (أن سرقة المطبوعات والمنشورات مباشرة من شبكة الإنترنت تتصاعد إلى أبعاد خطيرة، الأمر الذي يهدد الصناعات الإبداعية إلى جانب عرقلة مسيرة تطوير التجارة الإلكترونية). وذكر أن الخسائر الناجمة عن قرصنة الإنترنت آخذة في الازدياد بحيث تسهم في النسبة المتعاظمة لإجمالي خسائر القرصنة العالمية التي تقدر بمبلغ ١١ مليار دولار أمريكي في السنة تقريباً، ومشيراً في

الوقت ذاته إلى أن: (وطأة التأثير الاقتصادي لهذا النشاط تتجاوز بكثير حدود صناعة البرمجيات مما يلحق الضرر باقتصاديات الدول في العالم قاطبة، وذلك بانخفاض عوائد الضرائب بشكل بالغ وفقدان أعداد هائلة من الوظائف). وتقدر الإحصائيات عدد الذين يفقدون وظائفهم نتيجة لعمليات القرصنة سنويًا في الولايات المتحدة وحدها بحوالي (١٣٠,٠٠٠) شخص، وأنها تحرم الخزانة الأمريكية من تحصيل ضرائب تصل إلى مليار دولار سنوياً.

فهناك أكثر من مليوني موقع على شبكة الإنترنت تقوم بعرض الحصول على نسخ برمجيات غير مشروعة أو التوصيل إليها أو الإشارة إلى مواقع ذات صلة بها، وهي المواقع التي اصطلح على تسميتها بين من يقومون بجرائم القرصنة في الإنترنت بمواقع(WAREZ). وهي تشتمل على برامج مقرصنة من كل الأنواع التي قد يزيد سعرها بعضها عن عشرات الآلاف من الدولارات في السوق، ويمكن لأي شخص جلب أي برنامج منها دون مقابل، أو بمقابل زهيد، وباستخدام زر الفأرة فقط. وتدرُّ هذه المواقع مبالغ طائلة من الإعلانات التي تتدفق عليها بلا حدود في الغالب من مواقع غير قانونية أو مروجة للرذيلة والإباحية. ويتّبع القراصنة طرق مختلفة للحصول على المزيد من الزوار، مما يؤدي إلى مزيد من الإعلانات مثل استخدام خاصية إعادة التنشيط، أو إعادة التوجيه لإجبار المستخدمين على تحميل صفحات متتالية وإظهار المزيد من الإعلانات. وكذلك طريقة (المصيدة) لإلغاء زر الرجوع إلى الخلف عند زيارة الصفحة، فيقع الزائر أسيراً في قبضة الموقع. وقد أشارت المراقبة غير الرسمية لهذه المواقع إلى أن أكثر من ٦٠٪ من البرمجيات المطروحة على مواقع المزاد في أمريكا وأوروبا هي نسخ مقلدة أو مزورة. ويستطيع مرتادو الإنترنت الاطلاع على تقارير كاملة عن القرصنة في العديد من مواقع الإنترنت.

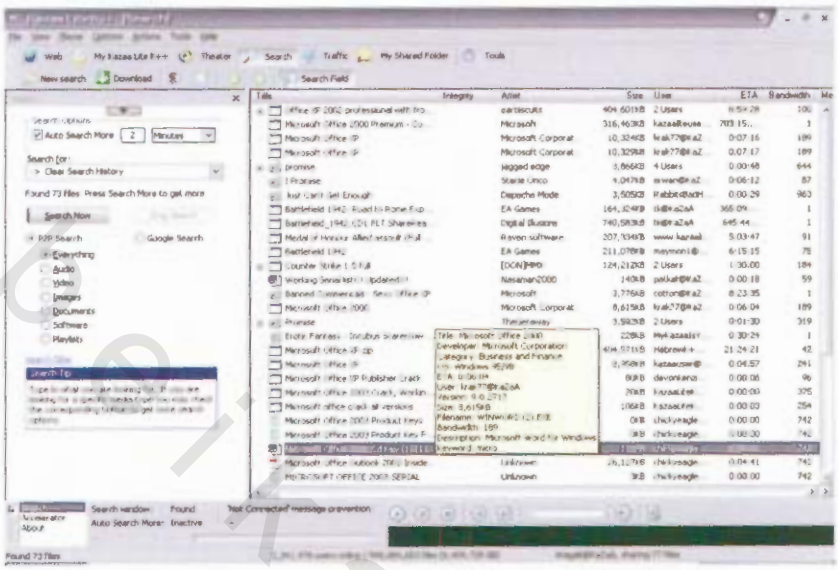
وعلى الرغم من التحذيرات التي تطلق في هذا الصدد التي تركز على أهمية وجود قوانين صارمة لحقوق الطبع والنشر توفر الأسس الكفيلة لوقف قرصنة الإنترنت، وعلى ضرورة أن تكون الإجراءات الاحترازية والعقوبات المفروضة على الانتهاك المباشر لحقوق النشر والطبع كافية لتعويض صاحب الحق ولردع قراصنة الإنترنت، فقد أظهر المقلدون القدرة على التكيف

obeikandl.com

مع تطورات السوق المشروعة وتطورات التقنية وسعوا جاهدين لإيجاد طرق تمكنهم من استخدام أدوات التجارة الإلكترونية لإلحاق الضرر بأصحاب الملكية الفكرية. وقد برهن قراصنة الإنترنت- كمعظم المجرمين- على تميزهم بالدهاء وسرعة التكيف والعمل باستمرار على ابتداع طرق تتفق مع التقنية وتتيح لهم القيام بأعمالهم غير المشروعة.

والشيء العجيب أن لهؤلاء القراصنة مبررات لما يقومون به من أعمال القرصنة وسرقة أموال الآخرين دون وجه حق. فمثلاً يعلن العديد من أصحاب مواقع القرصنة بأنهم يقومون بذلك إسهاماً منهم في نشر المعلوماتية التي تحتكرها شركات البرمجيات الكبرى الشرهة التي تطالب بأسعار مُبَالَغٍ فيها لبرامجها، متناسين بأن بيع البرامج المقرصنة لا يختلف عن بيع أي بضائع مسروقة، إذ يجنون من خلال بيعها بأسعار زهيدة أموالاً طائلة، متجاهلين ما تبذله هذه الشركات من جهد ومال وساعات عمل طويلة في إنتاج هذه البرمجيات. والشيء الأكثر غرابة وإثارة أنهم يقدمون الكثير من هذه البرامج عبر شبكة الإنترنت مجاناً، تباهياً بقدراتهم على اختراق أنظمة حماية النسخ التي توضع على البرامج، أو بحجة غلاء البرامج الأصلية وعدم استطاعة معظم مستخدمي الحواسيب اقتناءها، وهي خدمة-على حد زعمهم- يقدمونها لطلاب المدارس والجامعات الذين يشكلون نسبة كبيرة من مستخدمي البرامج المقرصنة في جميع أنحاء العالم. ولعل بعض ما تم ذكره من أسباب صحيح وواقعي ولكن ذلك لا يجيز -ألبتة- سرقة الحقوق وإهدارها.

ومن الناحية الأخرى فلزائري مواقع القرصنة هم أيضاً مبرراتهم الغريبة، فهم كما يزعمون، يمارسون فلسفة (الاستخدام العادل) طالما أن شروط الاستخدام التي تضعها شركات البرمجيات الكبرى غير عادلة. ويقول بعضهم إنه في حالة إحساسهم بعدم إنصاف قوانين استخدام البرمجيات وإجحافها، فإنهم لن يتقيدوا بها وسيقومون بجلب البرامج من مواقع القرصنة في الإنترنت. ويقول آخرون مثلاً: إن أكثر من ٦٠٪ من برامج الحاسب رديئة، ولا تفي بمتطلباتهم، علاوة على غلاء ثمنها بصورة مبالغ فيها، مما يزين لهم الذهاب إلى مواقع (Warez).



شكل ٣-٢: لقطة لبرنامج كازا الخاص بتبادل الملفات في الإنترنت

وخلاصة القول؛ إن القرصنة مستمرة بخطوات قوية وجريئة وفي جميع مجالات البرمجيات والبيانات المتداولة على الشبكة، إذ لم ينجُ منها مجال من مجالات الإبداع أو الفن أو الأدب، ووصلت إلى مجالات لم تكن تخطر على البال، مثل ترويج محاكيات (Emulators) لأنظمة الحاسب المختلفة، وقرصنة برامجها، وقرصنة الدارات الإلكترونية لمحاكيات أنظمة شركات الألعاب وتحويل الألعاب إلى صيغة رقمية وغير ذلك كثير. ولا أحد يدري على وجه اليقين ما هي المجالات التالية للقراصنة؟ وما مدى استعداد الشركات المنتجة والمبدعين لمحاربة هذه الظاهرة الجُرْمية المستشرية؟

٣-٥ جرائم الخصوصية

بدا واضحاً أن المعلومات الشخصية أضحت تجارة رائجة ومربحة على الشبكة، بالرغم من التحذيرات التي تطلقها كثير من شركات الهاتف، وشركات تقديم الخدمات المختلفة، ومراكز جمع المعلومات وتصريحاتها العلنية، بأنها ستعد جميع المعلومات التي تحصل عليها معلومات غير سرية، وأنّ لها الحق في استخدامها بالطريقة التي تروق لها من نشر، أو نقل إلى جهات أخرى دون قيد أو شرط، أو أي نوع من الالتزام تجاه أصحابها أو المساءلة القانونية.

وبالطبع فإن هذه التحذيرات لم تأتِ من فراغ، لأن النشر والنقل لمعلومات شخصية دون موافقة أصحابها ومعرفتهم المسبقة لما سينشر عنهم، يشكّلُ تحدياً سافراً للخصوصية وحماية الحياة الشخصية على شبكة الإنترنت، وهو يفتح باباً واسعاً للابتزاز والتهديد والتشهير، خاصة في ظل عدم وجود القوانين والتشريعات التي تحمي الأفراد من مثل هذا التعدي للخصوصية، واستخدام المعلومات الشخصية دون تصريح من أصحابها.

ولقد راجت تجارة المعلومات الشخصية منذ زمن طويل، ولكنها وصلت عبر شبكة الإنترنت إلى أبعاد شديدة الخطر، لأنها أصبحت في متناول الجميع دون استثناء، علاوة على أن مهمة جمعها أصبحت سهلة للراغبين في ذلك من مراكز وشركات ومنظمات وأفراد، بغض النظر عن الغرض من جمعها واستخدامها.

ويشمل جمع المعلومات كل شيء بدءاً من التقارير الطبية، وشهادات الميلاد، والوفيات، ورخص قيادة السيارات، والوثائق المختلفة مثل: وثائق الملكية، والأحكام القضائية، وأرقام البطاقات المختلفة التي أصبحت سمة العصر مثل بطاقة الائتمان، وخدمات الهاتف، والتأمين الطبي، والعضوية، وانتهاء ببطاقات الدخول لمواقع العمل أو مراكز البحث.

والشيء المثير للمخاوف في كل هذا هو أن المراكز والشركات والمؤسسات التي تقوم بجمع

المعلومات التي تحمل جميع التفاصيل الخاصة، كما أسلفنا، من اسم الشخص وسنّه وجنسه، وعنوانه، واسم وظيفته ونوعها وعنوانها، والشهادات الدراسية التي حصل عليها، وخبراته العملية، واهتماماته وهواياته ومحلات التسوق المفضلة، بل وحتى نوع المأكولات التي يأكلها، والألبسة التي يلبسها، ونوعية مدارس أبنائه وبناته وعناوينها، ولا تكتفي بجمع المعلومات بمجرد الجمع والترويج للسلع وإنعاش المبيعات، بل تكوّن منها قواعد بيانات خاصة للتسويق والبيع لمن يرغب من أصحاب الشركات الذين يتحرون عن موظفيهم، أو المحامين الذين يريدون معرفة السجلات القضائية لموكليهم، أو لتوريط أشخاص لصالح آخرين أو إلى رجال أعمال الراغبين في معرفة المراكز المالية لشركاء حاليين أو محتملين، أو التحقق من حالة الإفلاس، أو الدخول في صفقات تجارية، أو لرجال عصابات، أو ربما لإرهابيين ينوون ارتكاب جرائم أو القيام بتفجيرات.

ويتمثل خطر المتاجرة بالمعلومات التي تمَّ جمعها وتحويلها إلى قاعدة معلومات أو بيانات توظف لمصالح خاصة لمن جمعها، في الأخطاء التي ترتكب عند إعطاء المعلومات عن الشخص المعني، وبذلك يقع كثيرون ضحايا لهذه الأخطاء. وهناك الكثير من الأمثلة في هذا الخصوص، فهناك مسؤول في مركز صحي مثلاً فُصِل من عمله بسبب خطأ مطبعي في عنوانه، إذ ورد في العنوان أنه يقيم في نادٍ للعراة، وكذلك تعرض موظف آخر إلى مصادرة راتبه، لأن خلطاً حصل بينه وبين أب محكوم عليه بدفع نفقة لابنه وهو يرفض دفعها، وغير ذلك كثير.

٣-٦ جرائم الملاحقة و المضايقة

تنتشر في بعض الدول مشكلة ما يسمى بالملاحقة، وهي ناتجة عن تعلق شخص بآخر (غالباً من الجنس النقيض) دون رغبة أو رضا الطرف الآخر، ومن ثم ملاحقته وتتبع خطواتهم مما يسبب لهم المضايقة وعدم الارتياح. وفي الغالب فإن الملاحقين كثيراً ما يكونون مسالمين ويفعلون ما يفعلونه من تتبع الضحية بدافع الحب والتعلق. ولكن في بعض الأحيان، يصاحبه بعض الأذى مما يحوّل هذا الفعل إلى مضايقة.

تعد شبكة الإنترنت مرتعاً خصباً لمن يريد أن يتتبع أو يلاحق شخصا آخر، فهي تحتوى على الكثير من المواقع التي تساعد على ذلك، منها ما هو غير قانوني كما ذُكر في قسم (جرائم الخصوصية)، ومنها ما هو قانوني، مثل توفير دليل الهاتف على الإنترنت الذي يمكّن من الحصول على رقم الهاتف والعنوان (أحياناً) للشخص الذي يُبحث عنه.

وتتراوح قدرات المواقع والمعلومات التي تزود بها، بين الحصول على معلومات اساسية، مثل: رقم الهاتف والعنوان، إلى معلومات مفصلة، مثل: مكان العمل والمعلومات المتعلقة بالتعاملات المادية. بالطبع فإن هذه المواقع تختلف من بلد لآخر، ففي بلد متطور مثل الولايات المتحدة الأمريكية، فإن معظم قواعد البيانات الكبيرة متوفرة على الإنترنت، ومثال ذلك موقع (www.555-1212.com) الذي يعطي معلومات متكاملة عن الشخص بمجرد إدخال رقم هاتفه. وكذلك موقع (www.usatrace.com) الذي يسمح بإدخال رقم الضمان الاجتماعي (Social Security) الخاص بالشخص (وهو رقم مشابه لرقم بطاقة الأحوال الشخصية) لكي يقوم الموقع بتحديد موقع الشخص المطلوب. ويضاف إلى ذلك الشبكات الاجتماعية مثل: فيسبوك، وتويتر، وجوجل+، وغيرها من مواقع التواصل الاجتماعية التي وصل مشتركو هذه المواقع إلى قرابة المليار شخص، وهذا ما أنشأ سوقاً رديفاً لمن يريد أن يتتبع أو

يستعلم عن أي شخص وماذا لديه من حسابات إنترنتية، وما هي توجهاته وطريقة تفكيره، وهي جزء من الهندسة الاجتماعية. و لا يغالي الإنسان إذا ما قال إن شبكات التواصل الاجتماعي جعلت المرء مكشوفا مثل من يدخل حماما من دون أبواب أو نوافذ!

أما بالنسبة للمضايقة، فيتم ذلك غالبا باستخدام مواقع المحادثة أو باستخدام البريد الإلكتروني. وتبين الإحصائيات أن أغلب من يقوم بالمضايقات هم من الرجال، وأن من يتعرضون للمضايقات هم من النساء والأطفال. وكما ذكر في قسم (الأخطار النفسية) فإن بعض مدمني استخدام الإنترنت لديهم مشاكل نفسية، مما يجعلهم يتعلقون بأشخاص آخرين في الإنترنت بشكل غير صحي، وهذا بدوره يؤدي لقيامهم بمضايقة الطرف الآخر. بل لاحظت الدراسات أن معظم من يقومون بالمضايقات تكون بداية علاقتهم بالطرف الآخر علاقة ود، ما تلبث أن تتحول إلى عداء مع تجاهل الطرف الآخر. ولو كان الخطر الوحيد من المضايقة هو الرسائل الإلكترونية لكان من الممكن تجاهلها، ولكن في أحيان أخرى فإن هذه المضايقة تصل أحياناً إلى مستوى غير محمود، عندما يمتلك من يقوم بالمضايقة معلومات عن الضحية، مثل رقم بطاقته الائتمانية حيث يقوم باستخدامها للانتقام من الضحية. أو الحصول على عنوانها بحيث يتمكن من الوصول إليها شخصياً!

ولقد انتشرت الكثير من المواقع التي تساعد المستخدمين، وخصوصا النساء، لكي لا يتعرضوا للمضايقات على الإنترنت ومن هذه المواقع (www.lovemenot.org) و(www.cyberguards.com/cyberstalking.html). وغيرها من المواقع الأخرى الكثيرة. انظر الشكل ٣-٣.

obeikandl.com

شكل ٣-٣: إحدى صفحات موقع www.lovemenot.org

وكمثال قريب على هذه المضايقات ما حدث في المملكة العربية السعودية مؤخرا في منطقة الإحساء شمال شرق السعودية، من قضاء محكمة سعودية بسجن شاب سعودي وجلده وتغريمه، بعد اتهامه بارتكاب جريمة إلكترونية عبر الإنترنت مثال حي لوجود مثل هذه الجرائم في مجتمعنا، فقد أمرت المحكمة بسجن مواطن وجلده وتغريمه، بعدما ثبت أنه قام باختراق البريد الإلكتروني الخاص بفتاة سعودية، وسحب صورها الشخصية منها، وابتزازها. وكما جاء في صحيفة الوطن السعودية على لسان رئيس المحكمة الجزئية في الإحساء، أن المحكمة عدت الشاب قد ارتكب (جريمة إلكترونية)، وتم معاقبته وفق نظام مكافحة الجرائم الإلكترونية السعودي. وأشار إلى أن الحكم الذي يعد أول حكم قضائي يعاقب فيه متهماً في جريمة إلكترونية كان تطبيقاً لنظام مكافحة الجرائم الإلكترونية.

٣-٧ جرائم المخدرات والعصابات وغسيل الأموال

تقول الإحصائيات إن أرباح تجارة المخدرات في الولايات المتحدة وحدها تتجاوز ثمانين مليار دولار أمريكي سنوياً، وهو رقم يفوق الدخل الكلي لأكبر خمس مئة شركة أمريكية. وقد سهلت الحاسبات المرتبطة بشبكات ثم بشبكة الإنترنت، كافة عمليات هذه التجارة وإجراءاتها، وبذلك قللت من الأخطار التي كان يتعرض لها المهربون والمروجون وخفضت تكاليفها. ويوجد على الشبكة الآن آلاف المواقع التي توفر حتى أدق المعلومات عن تحضير وصناعة أنواع مختلفة من المخدرات، والعقاقير المخدرة، والأقراص، والحقن، وفنون وطرق تعاطيها، وطرق إخفائها ونقلها وترويجها.

ونتيجة للعدد الهائل من الصفقات التجارية على المستوى الدولي التي تعقد يومياً، فقد أصبحت عملية مراقبة صفقات الإجرام ومتابعتها تُعَدُّ شبه مستحيلة، لصعوبة التمييز بين الصفقات المشبوهة وغير المشبوهة. وقد ساعد في هذا المجال أيضاً إمكانية ربط الحاسبات الآلية الصغيرة المحمولة أو الموجودة في المنازل بنظام الحاسب الآلي المركزي التابع لبنك معين، والذي يمكّن المستفيد من التصرف في حسابه المصرفي، وهو في منزله، أو متجره، أو سيارته، أو في الطائرة، أو الباخرة. وهو تطور سيمكن المجرمين من عقد الصفقات المالية المشبوهة، وتمويلها وتنفيذها بكل سهولة ويسر، بمجرد النقر على أزرار هذا الحاسب الصغير بعيداً عن أعين العدالة وقبضتها الصارمة.

وقد ورد في تقرير لبنك دبي الوطني أن عمليات غسيل الأموال في روسيا تشكل من

٢٥-٥٠٪ من الناتج المحلي، و١٠٪ من إجمالي الناتج المحلي لجمهورية التشيك، و٧-١٣٪ من إجمالي الناتج المحلي البريطاني. ومن إجمالي المبالغ المغسولة عالمياً البالغة ٣١ ألف مليار دولار كان نصيب سويسرا (٥٠٠) مليار دولار، والولايات المتحدة الأمريكية (٤٨) مليار دولار، والمكسيك (٣٠) مليار دولار، وكندا (١٧) مليار دولار.

وتمثل تجارة المخدرات المصدر الأول للأموال المغسولة يليها أموال الاحتيال المالي، عبر شركات التأمين وإعلان الإفلاس، علاوة على الرشاوى لموظفي الدول والحكومات وأموال العصابات المنظمة.

وقد عرَّف بعض المختصين مصطلح (غسيل الأموال) الذي هو ترجمة حرفية لعبارة (Money Laundring) بأنها: «العملية التي يلجأ إليها الذين يمارسون الاتجار غير المشروع في العقاقير المخدرة، أو الممنوعات بشكل عام، بهدف إخفاء مصادر دخلهم غير المشروعة، أو لاستخدام هذه الدخل في وجه غير مشروع، ومن ثمّ التمويه على الأجهزة النظامية، ليبدو وكأنه دخل مشروع ولا يثير الشبهات». ولذلك فهم يحتفظون بهذه الأموال بشكل نقدي حتى يسهل عليهم إيداعها في بنوك بلدان أخرى في حسابات سرية. ويطلق على عملية غسيل الأموال أيضاً عبارات، مثل: (تطهير الأموال)، و(تبييض الأموال)، و(تنظيف الأموال)، وهي مصطلحات غير معروفة على المستوى العام مما يسبب مشكلة كبيرة للحكومات في محاربتها، فضحاياها غير معروفين وتأتي متأخرة في قائمة تسلسل الجرائم بعد السطو والسرقة وغيرها من الجرائم.

وتشكل عملية غسيل الأموال هاجساً كبيراً للجهات الأمنية في شتى بقاع الدنيا، لأن بقاء السيولة الضخمة في أيدي المجرمين سيؤدي إلى تفاقم ظاهرة الإجرام وزيادة سطوته الاقتصادية، وتمكين المجرمين من الهيمنة على المشروعات الكبرى واحتكار الأسعار.

obeikandi.com

٣-٨ جرائم التمييز العنصري

إن شبكة الإنترنت كما سبق أن ذكرنا لا تختلف عن عالمنا الذي نعيش فيه، ويتعرض

مرتادوها لما نتعرض له. فالشبكة زاخرة بالمواقع المخصصة لمنظمات عرقية للبيض ولغيرهم، لها شعارات مختلفة ودعوات عنصرية بعضها يتخذ طابعا سياسيا أو دينيا كالصهيونية والنازية، أو منظمات التطرف الديني، أو التمييز العرقي، أو اللوني كما هو الحال في العديد من بلدان العالم التي تبرز فيها مظاهر العنصرية بين الملونين كأمريكا، والتمييز بين الهنود الحمر (السكان الأصليين)، والزنوج وغيرهم من ذوي الأصول الآسيوية. فالشبكة تعكس الواقع المعيشي في كثير من البلدان التي تمارس فيها مثل هذه التفرقة. ويلاحظ المتتبع لمثل هذه المواقع وجود نوعين من العنصرية؛ أولاهما ناجمة إلى حد كبير عن عقليات مضطربة ومشوشة، ونفسيات غير سوية، والنوع الآخر من قبل أشخاص نهجوا نهجاً عدائياً، ووضعوا خططاً تآمرية، فيلجؤون إلى إهانة الآخرين في المنتديات وغرف الحوار، ويعمدون إلى طمس الحقائق، ويدعون آخرين من الذين لديهم صلات بهم إلى ممارسة النهج ذاته مع الآخرين من مرتادي الشبكة الذين يقودهم حظهم إلى مواقعهم.

ومن أكثر مشاكل العنصرية بروزاً على الإنترنت، مشكلة الزنوج والهنود الحمر. فالزنوج لهم تاريخ طويل حافل بالصراع بينهم وبين الرق والاستعباد. وهناك العديد من المواقع على الإنترنت التي تدعو للتفرقة وتطرح مفاهيم في غاية الغرابة والسخف، تقول باستحالة العيش بانسجام بين البيض والسود في أمريكا. وهناك مواقع مثل (www.kkk.com) الخاص بمنظمة تسمي نفسها (The Ku Klux Klan) تنادي بمثل هذا التوجه بقوة وصلف.

وتكمن خطورة هذه المواقع في أنها تمثّل عدداً من الجماعات العنصرية التي لها جمعيات تحمل تسميات عرقية صريحة، مثل: جمعية (The White Race) ومجموعة (American First) و(The Constitution)، إذ إن المنتمين إليها يؤمنون إيماناً قاطعاً بما يقولونه وينشرونه في مواقعهم، ويدعون إليه، لدرجة أن كل مؤلف أو كاتب يوقع على صفحاتهم التي كتبوها، حتى أنهم يشيرون للتظاهرات التي شاركت وستشارك فيها جمعياتهم. وما الجريمة المروعة التي ارتكبها الطالبان (Eric Harris) و(Dylan Klebold) وهما عضوان في عصابة تضم طلابا عنصريين، يكنون كراهية شديدة للزنوج ولأسبان أمريكا اللاتينية والأقليات العرقية الأخرى، أطلقت على نفسها اسم مافيا ترنشكوت (Trenchcoat)، إلا مثالاً واضحاً على هذه العنصرية والحقد والكراهية. وهذان الطالبان مولعان بتقليد الأشرار في كل شيء، حتى في المظهر والحركات، ويطلقان شعارات هستيرية تحض على القتل وكراهية الملونين وخاصة الزنوج. والغريب أن هذين الطالبين ضليعان جداً في استخدام الحاسب، ومولعان بألعاب الحرب، ويملكان مسدسين يفاخران بهما، وبهذين المسدسين نفذا مجزرة مدرسة كولمباين (Columbine) الثانوية في مدينة ليتلتاون بولاية كولورادو الأمريكية، وقتلا خمسة عشر طالباً، وزرعا شحنات ناسفة في سيارة مجاورة للمدرسة. وقد انتهت حياتهما بانتحارهما في مكتبة المدرسة بعد ساعات من ارتكابهما لجريمتهما البشعة في شهر أبريل من عام ١٩٩٩. وبعد ذلك قامت شركة أميركا أونلاين بحجب موقع العصابة -التي أثارت الرعب في أمريكا- على الشبكة.

وأما الهنود الحمر، وهم المواطنون الأصليون في أمريكا، فإنهم يتعرضون للتفرقة من معظم الثقافات والأقليات العرقية الأخرى، وليس من البيض فحسب، وبعبارات واضحة وصريحة على شبكة الإنترنت التي تتيح للكثيرين عرض وجهة نظرهم عنصرية كانت أو غير عنصرية. وتؤثر وجهات النظر هذه بالطبع على كثير من الذين يفتقرون إلى الوعي من الأميين أو محدودي الثقافة والتعليم.

وأما الحملة العنصرية الأكثر شراسة ونجاحا، فهي التي تشنها المواقع الصهيونية ضد العرب على شبكة الإنترنت، وهي تستهدف العرب والنازية ومنتقدي الصهيونية. وتتضح ممارساتها العنصرية في تزييف التاريخ القديم والحديث، بالشكل الذي يخدم مصالح الصهيونية وتشويه صورة العرب وإطلاق تهمة معاداة السامية. والأدهى والأمر أن كمًّا هائلاً من مواقع الإنترنت المعادية للعنصرية تحبُّ جميعها للدفاع عن الصهيونية ومن ينتقدونها وتتهمهم بالعنصرية، خاصة وأن المواقع العربية ليس لها وجود واضح، ولا تملك منهجية واضحة للدفاع عن العرب وفضح ممارسات الصهيونية وجرائمها، بالإضافة إلى عدم عمق الرؤية وأخذ الأمر بالجدية المطلوبة من أشخاص مؤهلين للقيام بمثل هذا العمل.

وتقترن العنصرية في كثير من المواقع بإثارة البغض والكراهية، فقبل عدة سنوات كان عدد المواقع التي تحض على الكره قليلة العدد، ولكن الآن توجد على شبكة الإنترنت مواقع عدة بعضها مثير للاشمئزاز لدرجة الغثيان. فأحد هذه المواقع تديره ما تُعرف بكنيسة الخالق (Church of the Creator) وهي المجموعة التي كان (بنجامين سميث) البالغ من العمر ٢١ عاماً أحد أفرادها حتى تاريخ انتحاره. ومع أن الموقع في غاية السوء،إلا أن هناك مئات المواقع الأخرى تفوقه سوءاً. وقد تعّرف مركز سيمون ويسنثال (http://www.wiesenthal.org) الموجود في لوس أنجلوس، والذي يهتم بمتابعة المواقع المثيرة لنزعات الحقد والكراهية والعنصرية، على أكثر من (١٤٠٠) موقعاً نسيجياً من هذا النوع، وهي تتضاعف عاماً بعد عام، وهذا الرقم ذاته قد يكون أقل كثيراً من الرقم الحقيقي لهذه المواقع السيئة السمعة.

٣-٩ جرائم الإرهاب

إن من أخطر آثار الإنترنت في انتشار الجريمة، هو اشتمالها على مصادر للمعلومات عن صناعة القنابل والمتفجرات، وتعليم مختلف فنون القتال، بل والتدريب على القتل بأعصاب

obeikandl.com

باردة، مع شرح أساليب تعذيب الضحية قبل قتلها، ثم القتل باستخدام وسائل مختلفة بعد التوثيق بالقيود. وقد تم رصد ما يزيد عن (١٥٠٠) موقعاً تشتمل على معلومات لتعليم صناعة القنابل والمتفجرات على الشبكة.

وما دام عالم الشبكة الافتراضي يمثل انعكاساً لحقيقة ما يجري في العالم الواقعي، فإن عالم الشبكة تتوفر فيه دوافع الجريمة والقتل والعنف، كالتمييز العنصري، والتطرف السياسي والديني، والانحراف الفكري، والتطهير العرقي، والكراهية ومحاولات الإفساد وإثارة النعرات في المجتمعات، وكل الأمراض والانحرافات التي تصيب المجتمعات.

والأخطر من وجود العوامل والدوافع هو استثمارها من قبل مجموعة يمكن أن يطلق عليها (القيادة الخفية)، فهي شكل مختلف من أشكال التوجيه والتحكم، وتقوم به مجموعات مختلفة تنشط عبر الإنترنت، وتسعى إلى إخضاع قطاع عريض من الناس للرقابة والمتابعة بهدف دراسة اهتماماتهم وتطويعها، أو توجيه أفكارهم وتغذيتها بالعناصر العدائية تجاه الآخرين، ليكونوا أداة لينة لتحقيق الأهداف والغايات الخاصة بكل مجموعة.

وبلا شك فإن وجود الجريمة يبرر اللجوء إلى اقتناء السلاح، للدفاع عن النفس لعدم الإحساس بالأمان في مجتمع يقتني فيه آخرون السلاح، بهدف ارتكاب جرائم وتهديد أمن المجتمع، وهو أمر متاح تماماً من خلال المعلومات المتوفرة عن صناعة الأسلحة والمتفجرات، أو تسهيل عملية الحصول عليها. فمثلاً يقدم موقع جنة القنّاص على العنوان (www.snipersparadise.com) كما في الشكل ٣-٣، معلومات عن فن القنص وأدوات الترصد الليلي، والتنكر وغيرها من الأدوات اللازمة لقنص الحيوانات والبشر معاً. والقنص هو أحد أهم وسائل ارتكاب جرائم القتل في كثير من البلدان التي تنتشر فيها الجريمة المنظمة، مثل أمريكا وإيطاليا وروسيا. ويعد هذا الموقع واحداً من المواقع التي تروج لبيع الأسلحة عبر الشبكة وتتعاون مع متاجر حقيقية في عمليات البيع. وهناك مواقع تعرض أسلحة

لشركات محددة، وأخرى تقوم بعمليات بيع مباشر كاملة أسوة بالمتاجر الإلكترونية، وأخرى تدعو مرتاديها لتعبئة استمارات أو المراسلة بالبريد الإلكتروني لعقد صفقات الشراء.

أما التأثير الأخطر للإنترنت فهو ما توفره بعض المواقع من معلومات، حول صناعة الأسلحة والقنابل كصناعة قنبلة من الموز مثلاً. وهناك قصة تناقلتها وكالات الأنباء عام ١٩٩٦م، عن طالب جامعي ابتكر طريقة شديدة السهولة لصناعة قنبلة نووية، من خلال مجموعة من المعلومات التي جمعها من الصحف والمجلات ومجموعات النقاش وغرف الحوار. وتتوفر على الإنترنت كذلك معلومات تقود إلى صناعة المتفجرات والمواد السامة.

والمشكلة الحقيقية فيما يتعلق بتجارة الأسلحة عبر الشبكة، هي أن قوانين بعض البلدان تبيحها، وبعضها تحظرها وتعدّها غير شرعية. ولكن تخطي الشبكة للحدود الجغرافية لهذه البلدان وتلك، يجعل هذه التجارة تنطلق إلى بلدان أخرى تحظرها قوانينها. وتوجد على الشبكة آلاف المواقع التي تعمل في تجارة الأسلحة والترويج لها وتقديم الاستشارات لبيع الأسلحة وشرائها. وتقوم كثير من الدول بمتابعة المشاركين في المواقع التي تدعو إلى الإرهاب والإفساد، لتعرية خيوطها من جهة وللحد من انتشارها من جهة أخرى. ومثل هذه المتابعة تحتاج إلى قدرات فنية عالية للتعرف على من يقف خلف هذه الدعوات الإفسادية من جهات داخلية وخارجية.

شكل ٣-٣ صورة أحد المواقع المخصص لبيع الأسلحة