الفصل الثاني عشر :

ماذا يخبئ المستقبل على الإنترنت؟

إن أول الحقائق وأهمها والتي يجب أخذها بالحسبان في هذا الخصوص هي أن شبكة الإنترنت تشهد تغيراً وتطوراً مستمرين على الدوام. ولذلك فإن أسئلة عديدة تحول بخاطر الكثيرين، مثل: كيف سيكون حال الإنترنت بعد عشر سنوات، أو عشرين سنة، أو حتى في المستقبل القريب جداً ؟ هل ستشهد الساحة مثلاً تقنيات جديدة، وقوانين جديدة موحدة على نطاق دولي لمواجهة جرائم الإنترنت والاستخدامات الخاطئة لها؟ أم هل ستنشأ جهة مخولة باتخاذ إجراءات قانونية وإيقاع العقوبات بالمجرمين أو المتطفلين والمتسكعين على أبواب المواقع؟ وهل سيؤدي الازدياد الهائل في عدد المستخدمين الجدد للشبكة إلى تغيير واقعها بصورة جوهرية؟

لاشك أن الأسئلة كثيرة ومتباينة والسائلون في ازدياد، ولكن الأجوبة ما تزال قليلة وغير شافية. فواقع الحال يشير بوضوح إلى أن عدد الأخطار ونوعها سيشهدان نوعاً من التغير في المستقبل. وأن المستخدمين سيشهدون المزيد من الخصوصية على الشبكة. ولإلقاء مزيد من الضوء في هذا المجال، يستعرض هذا الفصل فيما يأتي آراء بعض المتخصصين في مجال الإنترنت.

١٢-١ حقائق وتوقعات

فيما يتعلق بالخصوصية ذكر دانيال باريت في كتابه (قطاع طرق على طريق المعلومات السريع)، أن الخصوصية في الإنترنت هي صديق كل مستخدم للشبكة، ولكنها في الوقت ذاته هي مصدر خطر لكل مدير نظام.

ويقول أيضاً: «إننا إن لم تتوفر لنا الخصوصية الكافية في أجهزة الحاسب، فإن هذه الأجهزة ستصبح غير ذات جدوى، وأما إن توفرت لنا خصوصية غير محددة، فإن مديري الحاسب والأنظمة الحكومية لن يستطيعوا القيام بمهمة مراقبة الأعمال غير القانونية التي يمكن أن تلحق الأذى بالمجتمع». ولذلك فهو يرى أن الحل يكمن في توفر برامج أفضل تضمن التحقق من هوية المرسل لأي رسالة، وكذلك في استخدام نظام التشفير الذي يؤمن خصوصية الاتصالات على الشبكة.

وأما فيما يتعلق بالأمن والحماية من خطر الجريمة على شبكة الإنترنت، فهو يقول: «إن الاختراقات الأمنية ستكون في ازدياد حتى يتوفر برنامج أفضل للحماية».

وعليه فإن جرائم التزوير والتزييف والرسائل المنتحلة والخادعة سيزداد عددها، حتى يتم وضع برنامج للشبكات أكثر أمناً وتطوراً، مع ازدياد عدد المستخدمين الذين لديهم القدرة على ارتكاب مثل هذه الجرائم، لأن توفر الأمن عن طريق الغموض والإبهام لن يستمر إلى ما لانهاية. وهو يتوقع أيضاً ظهور المزيد مما يشبه (حروب العصابات) كلما تعلم عدد أكبر من المستخدمين كيفية إلغاء الرسائل الإلكترونية المرسلة من بعضهم إلى بعض.

ولذلك يتضح مما ذكر أن الحلول الموضوعة لحماية الخصوصية ستؤثر أيضاً على الأمن والحماية في الشبكة، لأنه لو توفرت للمستخدمين هويات لا يمكن تزويرها، ونظام تشفير خفي للاتصالات، فإن أعمالهم على الشبكة ستكون أكثر أمناً.

أما براد تيمبلتون الرئيس التنفيذي لصحيفة (كلارينيت كوميونيكيشنز كور)، وهي صحيفة إلكترونية حسنة السمعة تنشر على الإنترنت، فهو يرى فيما يتعلق بمستقبل حماية الخصوصية في الإنترنت، أنه يصعب التنبؤ بما سيكون عليه حال حماية الخصوصية، وأن المتوقع أنه سيكون لها قابلية السير في اتجاهين، وذلك لأن أجهزة الحاسب لها قدرة عظيمة على حماية الخصوصية واختراقها معاً، أكثر من أي تقنية أخرى! وأن ذلك يعتمد بالطبع على طريقة استخدامنا لها، والكيفية التي يسمح لنا القانون أن نستخدم بها التشفير وإغفال ذكر الهوية. ويعتقد تيمبلتون أن التوقيع الرقمي بين الطرفين في الشبكة والتشفير كفيل بأن يجعل الشبكة آمنة بالكامل، فهو لا يعدو كونه تنظيماً للقوانين، والرخص والبروتوكولات. ولذلك فإنه على الرغم من توقع ازدياد معدل الخطر باستمرار، فإن معدل الحماية الأمنية سيجعل المستخدمين أكثر راحة.

ولذلك فهو يرى أن الجريمة على الإنترنت، على الرغم مما ينشر في وسائل الإعلام

المختلفة بخصوصها وتضخيمها، هي قليلة لحد بعيد، وضئيلة جداً إذا ما قورنت بالجرائم التي تقع وسط السكان، وهي لا يمكن أن تزداد بشكل يهدد مستخدمي الشبكة ويجبرهم على الابتعاد عنها.

ويتوقع جول فور، وهو صحفي الإنترنت المشهور، أن تقوم الحكومة الأمريكية بتقديم المساعدة فيما يتعلق بضمان توفر الخصوصية في الشبكة، من خلال إيجاد طرق للتشفير يصعب حل رموزها. ويتمنى (فير) أن يتوفر له برنامجان أحدهما يتيح له تجاهل الحمقى بالكامل، والآخر يمنع تماماً أي شخص من التنصت على اتصالاته. وهو يعتقد بأن وجود الجريمة على الإنترنت سيستمر، ولكن القدرة على فهم الجريمة وما يحيط بها واتخاذ الإجراءات الملائمة، لمحاربتها سيقللان من الوجود الفعلي لها على الشبكة وبدرجة كبيرة.

وأما مايك مير، مستشار الحاسب المستقل، فيرى أن الأشخاص الذين يدفعون أموالهم لصناعة البرامج، هم الذين سيحددون مقدار الخصوصية التي ستتاح للمستخدمين. وهو يعتقد بأن الجريمة على الإنترنت ستزداد لأن الشبكة ستشهد انطلاقة مماثلة لانطلاقة الفاكس، وأن الجميع سيشرعون في القيام بأشياء كثيرة ومتباينة على الشبكة، ولذلك فإن المزيد من المستخدمين يعني المزيد من انتشار الجريمة على الإنترنت.

وفيما يتعلق بمستقبل الأمن والحماية على الإنترنت، والذي سيؤثر بدوره على مستقبل الجريمة على شبكة الإنترنت وسبل مكافحتها، يقول تيم أوريل مؤسس شركة أوريلي ورئيسها، إن العالم يتجه نحو المزيد من المعاملات التجارية الافتراضية التي تحتاج إلى نوع من إثبات الشخصية والتحقق من الهوية، وهو نظام يجب أن يكون متضمناً داخل البرنامج الذي يستخدم على الشبكة. إلا أن المشكلة الكبرى مع نظام التشفير الجيد أنه ليس مدمجاً في البرامج العادية التي نستخدمها كل يوم، ولذلك فإن الحماية تتطلب أن يكون نظام التشفير متضمناً في البرامج، وهو أمر يمكن القيام به بسهولة كبيرة ما لم تعِقْهُ العوامل السياسية التي تحول دون توفر تقنية التشفير.

ويرى أوريلي أن إثارة المخاوف والتنبيه لخطر الجريمة على الإنترنت اليوم، أمر في غاية الأهمية

للمستقبل، عندما تحصل تفاعلات حقيقية أكثر عفوية بين أشخاص لا رابط فعلي بينهم في العالم المادي. فالشخص يتبادل البريد الإلكتروني مع جميع أصناف البشر الغرباء عنه الذين يتحركون في الدوائر الافتراضية ذاتها التي يتحرك هو فيها، فضلاً عن الذين قد يقابل واحداً منهم في مؤتمر مثلاً في أحد الأيام، ويكون معروفا بالنسبة لأشخاص في نطاق دائرة تحركه، فيكون ذلك بداية لتضليل أشخاص بجعلهم يقابلون آخرين في بيئة ليس لها أي وجود مادي.

أما دان كينغز فله رأي آخر، وهو أنه إذا لم تصبح أجهزة الحاسب أكثر ذكاء من البشر، فلن يتوفر برنامج يجعل منها آمنة ١٠٠٪ مهما كانت قوة ما نستخدمه من طرق تشفير، وكلمات سر، وأنظمة ملفات. ولذلك فهو يعتقد أن مستخدمي الإنترنت الجدد سيكونون دائماً عرضة لأن يصبحوا ضحايا لعمليات الخداع والاحتيال، وأن واجب الجميع هو تبصيرهم بكل ما يمكن أن يجنبهم الوقوع ضحايا لخطر الجريمة على الإنترنت. لأنه عندما يذاع على نطاق العالم أن

أحد الأشخاص قد قام بسرقة مجموعة من البنوك بضربة على لوحة مفاتيح أحد الحاسبات الآلية المرتبطة بالشبكة، فإن كل شخص سيتنبه إلى ذلك ومن ثم يحدث انخفاض في معدل الجريمة على الشبكة.

ولكن آبي فرانكومونت جويليوري مدير مجموعة الأخبار يوزنت لشركة تزكاتليبوكا لا

يعتقد أن البرامج هي مشكلة بحجم الأمور الاجتماعية التي يصعب كثيراً حلها، والتي تعد على درجة كبيرة من الخطورة. ويعتقد جويليوري أن الجرائم المرتبطة بشكل كامل بأشياء خاصة

بالإنترنت مثل سرقة كلمات السر أو الاستيلاء على معلومات خاصة، ستظل كما هي. وأما إذا كان المقصود هو استخدام مصادر الإنترنت لارتكاب جرائم حقيقية ليس لها تأثير فعلي على فن استخدام الحاسب، كالخداع والاحتيال الذي يتم عن طريق البريد الإلكتروني مثلاً، فإن هذا النوع من الجرائم سيكون احتمال زيادته كبيراً جداً.

وخلاصة القول هنا حول مستقبل الجريمة على الإنترنت، أن الكثير من عمليات الغش والخداع التقليدية البسيطة التي تعج بها الشبكة ستتضاءل، وتختفي بالتدريج كلما زاد عدد المشتركين في الشبكة وأصبحت هذه الأعمال معروفة لديهم. فعندما يصبح السكان أكثر دراية بشبكة الإنترنت، فإن الغموض فيها والرهبة منها، اللذين يميزانها سيزولان، ولن يكون الناس سريعي التصديق بما يلفق عن الشبكة، وذلك بفضل الخبرات التي اكتسبوها من خلال تعاملهم مع الحواسيب والشبكات.

إلا أنه مع تفاوت درجات المعرفة وتباين القدرات على التعامل مع هذه التقنية المتجددة باستمرار، فإنه سيكون هنالك دائماً أشخاص غير آمنين بسبب ما ينشأ من أنواع جديدة من طرق الخداع الماكرة، لأن من يقومون بأعمال الخداع، ويرتكبون مختلف الجرائم على الشبكة هم دائما أكثر براعة وخبثاً من معظم مستخدمي الإنترنت، ولذلك فإنهم سيسخِّرون جميع مهاراتهم وقدراتهم الفائقة، لابتكار الأسلحة والأدوات اللازمة لمواصلة أعمالهم غير المشروعة على الشبكة وجرائمهم المروعة.

والحل الحقيقي يكمن في وجود القوانين والتشريعات الرادعة والمتفق عليها دولياً، والحرص على تطبيقها على كل من يحاول ارتكاب أي مخالفة على الإنترنت مهما كان حجمها. وذلك هو السبيل الوحيد الذي سيشجع الجميع على نقل الإنترنت إلى واقع حياتهم وأساليب عملهم، والاستفادة من القدرات الهائلة التي تتيحها لهم.

وكمرحلة أولى في اتجاه ذلك يجب على الدول العربية تهيئة نظمها القضائية، لمثل هذا النوع من الجرائم وإعداد القوانين والأنظمة الملائمة لظروف مجتمعاتنا وبيئاتنا. كما تبرز أهمية تقديم البرامج التدريبية المتخصصة للتعامل مع جرائم الإنترنت، وآليات تطبيق القوانين والأنظمة. ولعل ما صدر في المملكة العربية السعودية فيما يخص إصدار نظام مكافحة جرائم المعلوماتية والوارد في الفصل التالي هو من سبيل الاستعداد والاتجاه الصحيح فيما يتجه إليه العالم الآن.

ويهدف هذا النظام الذي بُدئ العمل به إلى حماية المجتمع من جرائم المعلوماتية، واحدّ منها والمساعدة على تحقيق الأمن المعلوماتي، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية، والشبكات المعلوماتية، وحماية المصلحة العامة، والأخلاق والآداب العامة، وحماية الاقتصاد الوطني.