التقنية والجريمة المعلوماتية

تأصيلٌ نقديٌّ لرؤية هانز يوناس التشاؤميّة

عادل عبد السميع عوض [*]

أخذت التقنية في عصر الحداثة وما بعدها سياقاً مهيمناً على حياة الفرد والجماعات الحضارية في المجتمع الغربي، ولعلّ الظاهر الأبرز في هذا السياق من الهيمنة هو التدفق الهائل للمعلومات ونشوء حربٍ افتراضيةٍ كان لها أثرٌ كبيرٌ على بنية المؤسسات والدول.

في هذه الدراسة يسعى الباحث إلى معالجة ظاهرة جرائم المعلوماتية من وجهة نظر عددٍ من الفلاسفة وعلماء الاجتماع وأبرزهم الألماني هانز يوناس الذي يعتبر أحد مؤسسي التيار التشاؤمي في عالم التقنية.

المحرر

يعتقد أنصار النظرة التشاؤمية أن الإنسان قد دخل بسبب التكنولوجيا الحديثة في ثلاثة أنواع من الصراعات: صراعه مع الطبيعة المادية، إذ حقق عليها انتصاراتٍ كبيرةً لإرضاء احتياجاته الضرورية وغير الضرورية. لم تنته المعركة بعد، فقد بدأت الطبيعة في رد العدوان على الإنسان، ما جعل علماء الأيكولوجيا يتوقعون حسم الصراع لصالح الطبيعة. سوف تسحق الطبيعة، من وجهة نظرهم، هذا الكائن المُتطفل الذي كان سبباً في خلل نظامها.

أما الصراع الثاني فيتمثل في: صراعه مع رفاقه (أبناء الجنس البشري)، وعلى الرغم من دعوات أنصار السلام بنزع السلاح، فإن سباق التسلح مازال مستمراً، ومازال يهدد لا

*- باحث وأستاذ في الفلسفة - جامعة المنصورة - جمهورية مصر العربية.

بفناء الإنسان فقط، بل بفناء كلّ الأنواع الحية التي تسكن هذا الكوكب[1].

أما الصراع الثالث فيتمثل في: صراع الإنسان مع نفسه، فقد بات الإنسان -بسبب إساءة استخدام التكنولوجيا- قادراً على التدخل في تعديل صفاته الوراثية وإطالة حياته وتقصيرها، وذلك يشكل خطراً على جوهر وجوده وكرامته بوصفه إنساناً[2].

لقد عارض عديدٌ من الفلاسفة التكنولوجيا، وانصبّ معظم هجومهم عليها في أنها: «مسؤولة عن التلوث وعن تحول المجتمع إلى مجتمعٍ صناعيٍّ زائف، وعن اغتراب العمال، وعن تفتيت الثقافة الحديثة. فقد هاجم معظم الفلاسفة الوجوديين التكنولوجيا هجوماً شديداً، فمثلاً عند كارل ياسبرز نلمس إدانةً شاملةً للتكنولوجيا من خلال ما أدت إليه من تحول الإنسان إلى مجرد وظيفةٍ من الوظائف العاجزة عن وجدان سبيلٍ إلى العلو الجدير بالوجود الإنساني الأصيل. أما «برديائيف» فهو في الكثير من مؤلفاته ولعلّ أبرزها «الإنسان والآلة»، يدين التكنولوجيا التي قصد بها أن تكون طريقاً للتحرر، فإذا بها تتخذ كياناً موضوعياً مغترباً عن الوجود الإنساني. أيضاً إلى المنحى نفسه اتجه معظم المنتمين لمدرسة فرانكفورت، ومنهم «تيودور أدورنو» و «إيريك فروم» استناداً على ما تمخض عن التكنولوجيا من اغترابٍ أضحى الإنسان يعاني منه في كل لحظةٍ من لحظات حياته [3].

الجريمة المعلوماتية نموذجاً لنقد التكنولوجيا

إن ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الإنترنت أضفى عليهما مجموعةً من السمات المميزة عن الجرائم التقليدية الأخرى، وهي:

الجريمة المعلوماتية عابرة للدول: المجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمعٌ منفتحٌ عبر شبكاتٍ تخترق الزمان والمكان.

صعوبة اكتشاف الجريمة المعلوماتية: تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها،

---

[1]- Irving Kristol. "Is Technology a Threat to liberal Society?" in public Interest Vol. 143, No.1, 2001, P. 45. 8p.

نقلاً عن:-

وجدى خيري نسيم، الفلسفة وقضايا البيئة، أخلاق المسئولية هانز يوناس نموذجاً، تقديم أنور مغيت، المجلس الأعلى للثقافة، الطبعة الأولى، القاهرة، 2009، ص133.

[2]- وجدي خيري نسيم، الفلسفة وقضايا البيئة، أخلاق المسؤولية هانز يوناس نموذجاً، مرجع سابق، ص133.

[3]- محمد عبد الحميد يوسف، مرجع سابق، ص45-46.

وإن حدث ذلك، يكون بمحض الصدفة. ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشافها إلى أنها لا تترك أثراً خارجياً بصورةٍ مرئيةٍ.

أسلوب ارتكاب الجريمة المعلوماتية: إذا كانت الجرائم التقليدية تتطلب نوعاً من المجهود العضلي، الذي قد يكون في صورة ممارسة العنف والإيذاء مثل جريمة القتل أو الاختطاف، فإن الجرائم المعلوماتية هي جرائمُ هادئةٌ بطبيعتها لا تحتاج إلى العنف، بل تحتاج القدرة على التعامل مع جهاز الحاسوب بمستوًى تقنيٍّ يوظف في ارتكاب الأفعال غير المشروعة.

تتميز الجريمة المعلوماتية بأنها تتم عادةً بتعاون أكثر من شخص على ارتكابها، لتحقق أضراراً بالجهة المجني عليها.

خصوصية مجرمي المعلوماتية: المجرم الذي يقترف الجريمة المعلوماتية أو الذي يطلق عليه المجرم المعلوماتي، يتسم بخصائص معينةٍ تميزه عن المجرم الذي يقوم بالجرائم التقليدية، فالجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي، أما الجرائم المعلوماتية فهي تتسم بالمعرفة والقدرة على استخدام الحاسوب والتعامل مع الإنترنت[1].

يختلف مجرمو الحاسوب والإنترنت تماماً عن المجرمين العاديين، حيث إنهم يتمتعون بمستوًى عالٍ من التدريب والخبرة والذكاء في مجال تكنولوجيا المعلومات. وفي المستقبل ومع ازدياد هذا النوعٍ من الجرائم سوف يتغير شكل المجرم من مجرد لصٍّ جاهلٍ إلى شخصٍ متعلِّمٍ، فلصوص المعلومات المعروفون بالقراصنة لديهم القدرة على إنشاء برامج للفيروسات ونشرها عبر الإنترنت لتدمير قواعد البيانات[2]. ويمكن تصنيف مجرمي الحاسوب إلى المجموعات التالية:

الأولى: أكثر المجموعات رأفةً ويمثلها طبقةٌ من الشباب لديه قدرٌ لا بأس به من الخبرة المعلوماتية.

الثانية: تزيد على خاصيات المجموعة الأولى بأنّها تلجأ إلى أفعال الاعتداء العمد.

الثالثة: أكثر المجموعات ضرراً، ولها كفاءة المجموعة السابقة، لكنها لا تكتفي بالملاحظة، بل تلجأ إلى أفعال الاعتداء العمد.

---

[1]- نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة، عمان، 2008، ص50-59.

[2]- محمد صلاح سالم، العصر الرقمي وثورة المعلومات، دراسة في نظم المعلومات وتحديث المجتمع، ط1، عين للدراسات والبحوث الإنسانية والاجتماعية، القاهرة، 2002، ص188.

الرابعة: أكثر المجموعات خطورة، ولها هدف المجموعة السابقة نفسه، أي الإرهاب المعلوماتي، ولكن باستخدام وسائل على قدرٍ كبيرٍ من البراعة، كزرع برامج الفيروسات والقنابل المنطقية، والتي ينشأ عنها أضرارٌ جسيمةٌ.

الخامسة: الموظفون الساخطون على مؤسساتهم الذين يعودون لمواقع العمل بعد فترات العمل الرسمية، إما لغرض السرقة أو لغرض التخريب.

السادسة: الموظفون العاملون بمراكز الحاسوب، ويمثلون الغالبية العظمى من مرتكبي تلك الجرائم.

السابعة: فئة العابثين، وهم الذين لديهم سلطة استخدام الحاسوب، ولكنهم مغرمون بالعبث وهم يستخدمونه من أجل التسلية، وليس بغرض التخزين، وغالباً ما يكونون من هواة الحاسوب.

الثامنة: الفئة التي تعمل في مجال الجريمة المنظمة باستخدام الحاسوب، إذ يقوم هؤلاء باستخدام الحاسوب في شكلٍ غير قانونيٍّ في معرفة الأشياء المتعلقة بالأساليب الأمنية المتبعة لتأمين المؤسسات التي يسطون عليها.

التاسعة: فئة صانعي، وناشري الفيروسات[1].

تحمل الجرائم على وجه العموم في طياتها درجةً عاليةً من الخطورة الموجهة ضد أمن واستقرار المجتمعات البشرية، فهي تمثل تهديداً لمختلف نواحي الحياة الاجتماعية، كما تسهم في خلخلة الروابط الإنسانية القائمة في كافة المجتمعات. بالإضافة إلى ما تمثله من تهديدٍ للحقوق الأساسية للإنسان، ولا سيما حقه في الحياة والتملك وسلامة البدن والشرف والاعتبار، أو هي بوجهٍ عام خروج على القيم والتقاليد والأعراف والمثل التي يقوم عليها مجتمع ما من المجتمعات مهدداً للمصالح العامة والخاصة على السواء[2].

تعد جرائم المعلوماتية، أو جرائم الحاسوب والإنترنت، أو جرائم التقنية العالية، أو الجريمة الإلكترونية، أو السيبر كرايم (Cyber crime) ظاهرةً إجراميةً تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر والخسائر الناجمة عنها، بوصفها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات خاصة وتجارية وأمنية وبرامج بكافة

[1]- جعفر حسن جاسم، التطبيقات الاجتماعية لتكنولوجيا المعلومات، دار المناهج للنشر ، عمان ،2006، ص196-197.
[2]- عبد الناصر حريز، الإرهاب السياسي، دراسة تحليلية، القاهرة، مكتبة مدبولي، القاهرة، 1996، ص95.

أنواعها)، فتمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري. فقد بات من الواضح أن جانباً من الفضاء السيبراني أصبح خارجاً عن القانون وتسوده جرائم من نوعٍ جديد، أصبحت تعرف بالجرائم السيبرانية. لقد حددت منظمة التعاون والتنمية الاقتصادية (OECD)، هذه الجرائم كما يلي: «الجريمة الحاسوبية هي كلّ تصرف مخالف للقانون أو مخالف للأخلاق، فالجريمة المعلوماتية إذاً هي سلوكٌ إجراميٌّ يتم بواسطة الحاسوب، أو هي كلّ جريمةٍ تتم في محيط الحاسبات الآلية. ويمكن أيضاً تعريف جريمة الحاسوب بأنها الجريمة التي يتم ارتكابها إذا قام شخصٌ ما بطريقةٍ مباشرةٍ باستغلال الحاسوب أو تطبيقاته بعملٍ غير مشروعٍ وضارٍ للمصلحة العامة ومصلحة الأفراد. ويمكن القول بشكل عام: إن الإجرام المعلوماتي هو ذلك الإجرام الذي يتم عن طريق الحاسوب والإنترنت. كذلك هو إجرام الأذكياء بالمقارنة مع الإجرام التقليدي، والذي يميل فيه المجرم إلى العنف. لذلك فإن الصورة التي نحن بصددها يطلق عليها الإتلاف المعلوماتي الناتج عن تقنيات تدميرٍ ناعم. وتمثل جرائم الإنترنت مجموعة الأفعال غير القانونية التي تتم عن طريق الإنترنت، أو تبث عبر محتوياته، فهو يمثل أحدث تكنولوجيا العصر التي تم استخدامها في مختلف جوانب الحياة [1].

ينقسم الإرهاب الحاسوبي إلى قسمين: الأول يشمل الأعمال والتصرفات التي تستهدف الحاسوب، منها السرقة والسطو عن طريق التطبيقات الحاسوبية، وتحويل البيانات والملفات أو إتلافها أو تغييرها من أجل التخريب أو الابتزاز. أما الثانى فيشمل الأعمال والأفعال التي تستعمل الحاسوب كوسيلةٍ إجراميةٍ، من قبيل تحويل الأموال، أو تحويل معايير أدوية بعض المرضى بقصد الإجرام كما حدث في الولايات المتحدة، أو تبيض أموال الدعارة والمخدرات، أو قرصنة البرمجيات أو المنتجات الثقافية كالأفلام والقطع الموسيقية[2].

السرقة التكنولوجيّة

يمكن تعريف جريمة السرقة بأنّها عبارةٌ عن قيام المجرم بعمل أو أعمال ينتج عنها الاستيلاء أو السيطرة على حقوق الآخرين. أما جرائم السرقة التي تتم عن طريق تكنولوجيا المعلومات، فهي تلك التي يتم خلالها السيطرة على معلوماتٍ فكريةٍ مملوكةٍ للغير، أو الاستيلاء على دسكات أو

[1]- جعفر حسن جاسم، التطبيقات الاجتماعية لتكنولوجيا المعلومات،مرجع سابق، ص192، 193.
[2]- علي مصطفي الأشهر، مصطفي عمر التبر، البهلول على البعقوبى، الأخلاق العلمية والتكنولوجية، المنظمة العربية للتربية والثقافة والعلوم، تونس، 2005، ص159.

أقراص مكتنزة تتضمن معلوماتٍ وبياناتٍ أنتجها الآخرون، وثمة أنواعٌ للسرقات، مثل سرقة الوقت، سرقة الأقراص الصلبة، وسرقة المال[1].

ففي ظل انتشار التجارة الإلكترونية عبر الإنترنت بشكلٍ كبيرٍ، أباح الاعتماد على بطاقات الائتمان وسيلةً مثاليةً لعمليات البيع والشراء، ولكن هذه الطريقة مازالت وسيلةً محفوفةً بمخاطر استيلاء سارقي البطاقات على رقم بطاقة الإئتمان في أثناء إجراء عملية الشراء، وبالتالي احتمال استخدام هذه البطاقة في عمليات شراء يتحمل أصحاب البطاقة قيمتها، وتقدر قيمة المبالغ المسروقة بواسطة بطاقات الإئتمان بحوالي 80 مليار دولار سنوياً، في حين تصل خسائر الشركات المصدرة للبطاقات إلى ثلاثة مليارات سنوياً[2].

يتضح من ذلك، أن الإنترنت أصبح مجالاً لمن له سلعٌ أو خدماتٌ تجاريةٌ يريد أن يقدمها، وبوسائلَ غير مسبوقةٍ كاستخدام البريد الإلكتروني أو عرضها على موقعٍ على الشبكة. ومن الطبيعي أن يساعد استخدام هذه الوسائل في عمليات النصب والاحتيال التي تتميز بقدرة مرتكبيها على الإسراع في الاختفاء والتلاشي. وأنّ كثيراً من صور النصب والاحتيال التي يتعرض لها الأشخاص في حياتهم اليومية منتشرةٌ على شبكة الإنترنت، مثل بيع السلع أو خدمات وهمية أو الإسهام في مشاريعَ استثماريةٍ وهميةٍ أو سرقة معلومات البطاقات الائتمانية واستخدامها، وتعد المزادات العامة على البضائع من أكثر السبل للقيام بعمليات النصب والاحتيال على الإنترنت[3].

فتعد سرقة وقت الحاسوب واحدة من الأنواع الشائعة لجرائم الحاسوب، حيث يقوم المستخدمون المخولون بفتح حسابات الشركات أو المؤسسات لأغراضٍ غير شرعيّة، مثل اللعب بالحسابات الشخصية، ومزاولة بعض أنواع الألعاب في الحاسوب للوصول إلى الأسرار الخاصة بالمؤسسة عن طريق كسر كلمات السر الخاصة بالأنظمة خلال خطوط شبكات الهاتف، بعد ذلك محاولة سرقة وقت الحاسوب[4].

يمكن القول بأن شبكة الإنترنت تعبر عن معلومات، وبالطبع يمكن استخدام المعلومات بطريقةٍ غير شرعيةٍ عن طريق الآخرين. ويتضح هذا الأمر بوجه خاص عند التجارة على الإنترنت، فيقود المروجون على مواقع الوايب معارك ضاريةً لإقناع الأشخاص بأن تبادل المعلومات المتعلقة

[1]- جعفر حسن جاسم، التطبيقات لتكنولوجيا المعلومات،مرجع سابق، ص207.
[2]- حسن عبد الله عباس وصلاح محارب الفضلي، أخلاقيات الكمبيوتر، جامعة الكويت، الكويت، 2005، ص38.
[3]- حسام شوقي، حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية، القاهرة، 2003، ص87.
[4]- علاء عبد الرازق السالمي، تكنولوجيا المعلومات، ط2، دار المناهج للنشر والتوزيع، عمان، 2002، ص432

ببطاقات الائتمان أمرٌ آمن تماماً. وعلى الرغم من هذا الإدعاء فإننا نكاد نؤكد أنه ليس هناك ما هو آمنٌ بنسبة 100% على الإنترنت. على سبيل المثال، لاحظ أحد الأشخاص أنه قد تم تصفية حسابه البنكي، وقاد التحقيق في هذا الأمر إلى أن أحد الأشخاص قد قام باستخدام رقم بطاقة الحساب الخاصة بالأول لشراء مشتريات بحوالي 1400 دولار من موقع (Amazon.com). وقد تمت سرقة رقم البطاقة، من الشخص الأول حال قيامه بشراء أشياءٍ من هذا الموقع[1].

ينقسم جواسيس الحاسوب إلى هواةٍ ومحترفين، وكما هو الأمر في معظم الهوايات. فالهواة هم جواسيسُ عن قصدٍ، مع أنهم قد يملكون أسباباً قويّة للتطفل، إلا أن عيشهم لا يعتمد على هذا، يملك هؤلاء خبرة بالحواسيب أكثر بقليل من المستخدم العادي، لكن هذا لا يعني أنهم تقنيون جداً، إنما يحتاجون وقتاً أكثر بقليل لتعلم التقنيات المتنوعة التي يمكن استخدامها للوصول إلى الأجهزة الحاسوبية. ويميل الجواسيس المحترفون إلى امتلاك خبرةٍ تقنيةٍ أكثر من الجواسيس الهواة، فعملية التجسس على الناس هي جانبٌ من جوانب مهنة المحترفين. وقد يكون التجسس مشروعاً، كما في حالة موظف الاستخبارات ينفذ أمراً قضائيًّا متعلقاً بجريمة قتل، أو قد يكون غير مشروع[2].

إن فرصة التواصل مع الآخر البعيد التي منحتها تكنولوجيا المعلومات أتاحت لكثير من الناس ولا سيما الذين لديهم القدرة على اختراق المجال المعلوماتي والإضرار به خلال ارتكاب جرائم عديدة، ومنها جريمة التجسس والتخريب والقرصنة داخل شبكات المعلومات العالمية. وباتت المؤسسات الأمنية التي كانت مسؤولةً عن حماية الناس والدولة بات أمنها مهدّداً بفعل أولئك الذين بات مكانهم اختراق الحدود الأمنية التي رسمتها تلك الدوائر، بل ودولها أيضاً[3].

برامج «الفيروسات» هي عبارة عن برنامج تصيب جهاز الحاسوب عن طريق ربط نفسه ببعض البرامج الأخرى، وعادة ما يكون جزءًا من نظام التشغيل. لنفترض أنك تُحمّل برنامج «اللعبة العظيمة» من الإنترنت على جهاز الحاسوب الخاص بك. هذا البرنامج قد يكون أكثر من مجرد «لعبة عظيمة»، وكجزءٍ من تنفيذه فإنه قد يهدّد ملف نظام التشغيل على جهاز الحاسوب الخاص بك عن طريق إدراج بعض الرموز الإضافية. وقد يتعلق هذا البرنامج بالتاريخ وعندما يصل إلى تاريخ معين، فإنه يمسح جميع الملفات الموجودة على القرص، فالفيروسات شائعة في بيئة

[1]- بريستون جرالا وشيرى كينكوف، كيف تحمى طفلك من المواقع الضارة على الإنترنت، دار الطارق، القاهرة، 2001، ص29.
[2]- أناستاسيا محمد أكرم، أمن الحاسب وأمان المعلومات، شعاع للنشر والعلوم، حلب ، سوريا، ص11.
[3]- جعفر حسن الطائي، التطبيقات الإجتماعية لتكنولوجيا المعلومات ، مرجع سابق، ص127.

الحاسوب الشخصي، وقد أصبحت شائعةً في الواقع إلى حدّ أن بعض الحواسيب الشخصية تأتي اليوم مصحوبةً بنسخةٍ معدلةٍ من برامج (مضادة للفيروسات). وأكبر خطر قد يتشكل هو عندما تقوم باستخدام برامج من مصدرٍ غير موثوقٍ به، فالتحميل من الإنترنت هو مصدرٌ شائعٌ للفيروسات، ويمكن الكشف عن تلك الفيروسات في وقتٍ مبكرٍ عن طريق مقارنة حجم كافة ملفات النظام ومقارنتها بحجمها الصحيح[1].

المواقع الإباحية والقرصنة

تعد غرف المحادثة (Chat Rooms)، من أكثر خدمات الإنترنت شعبيةً وإقبالاً من قبل مستخدمي الإنترنت، إلا أنها مثل بقية خدمات الإنترنت، يتم إساءة استخدامها من البعض، ولعلّ إساءة الأطفال من أخطر الإساءات التي يتم فيها استخدام غرف المحادثة، فقد أظهرت بعض الإحصائيات أن من بين 24 مليون طفل يستخدمون الإنترنت هناك واحدٌ من كلّ خمسة أطفال يتعرضون للإساءة الجنسية عبر هذه الغرف، وتقدر اليونيسيف أن هناك مليون طفل يجبرون على دخول عالم الدعارة، وهذا الوضع قد دفع العديد من شركات الحاسوب إلى إغلاق غرف المحادثة في العديد من دول العالم[2].

ولقد ساعدت هذه التكنولوجيا الحديثة على إنتاج عددٍ لا حصر له من المواد الإباحية بسرعةٍ أكبرَ وبتكاليفَ أقلَّ مما كان عليه الحال من قبل، كما ساعدت على سرعة انتشارها، فمُتلقّي هذه المواد يستطيع أن يشاهدها، وأن يقوم بتخزينها أو بطباعتها، وأن يقوم بإرسالها من جانب إلى آخر، وذلك خلال مدةٍ زمنيةٍ قصيرةٍ[3]. ويمكن تقسيم المواد الإباحية إلى نوعين «الإباحية البسيطة» و«الإباحية الصريحة»، وتتمثل الإباحية البسيطة في الصور الثابتة التي تظهر جسد الإنسان العاري، وبخاصة المرأة، وتتمثل الخلاعة الصريحة في المقابل في المشاهد المتحركة لجميع أشكال وأنواع الممارسة الجنسية، وبخاصة تلك التي تقع بين الرجل والمرأة، وهي أكثرها تأثيراً في المشاهد الثابتة لما للحركة من تأثيرٍ قويّ في انطباع هذه المشاهد في ذهن الإنسان[4]. تكتظ شبكة الإنترنت بالصور الإباحية، وتمثل سوقاً هائلاً لها، وبالطبع عددٌ كبيرٌ منها يكون على شكل صورٍ متوسطة

[1]- Kevin. W. Bowyer ,ethics & computing, living responsibility in a computerized IEEE. Press, Marketing Second edition, N.Y., 2000, P.82.

[2]- حسن عبد الله عباس وصلاح محارب الفضلي، مرجع سابق، ص ص 37-38.

[3]- نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي ، لبنان، 2005،ص39.

[4]- حسن عبد الله عباس وصلاح محارب الفضلي: مرجع سابق، ص9.

الحجم، والتي تجدها في كثير من المجلات أو في متاجر الكتب، وبخلاف المجلات، يمكن للمستخدمين أن يحصلوا على هذه الصور دون الحاجة إلى البحث عنها في متاجر الكتب، حيث يمكنهم رؤيتها دون خوفٍ أو حرجٍ خلال جهاز الحاسوب الخاص بهم بدلاً من التوجه للمحال التجارية. هذا بالإضافة إلى وجود مواد جنسية أكثر إثارة من التي توجد في المتاجر[1]. ولكي تكون الصورة خادشةً للحياء يجب أن يتوفر فيها الشروط الثلاثة الآتية:

مخالفةُ أعراف المجتمع وتقاليده بشكلٍ يثير الغرائز.

وصفٌ أو عرضٌ لسلوكٍ شاذٍّ، قام بتحديده قانون الدولة، أو يخالف العادات والتقاليد المعروفة.

افتقاد هذه الصور للقيم الفنية والسياسية والعلمية[2].

يتضح من ذلك، أن المرء قد يقرأ كتاباً داعراً أو يشاهد صورةً جنسيةً فاضحةً داخل حدود بيته وفي سريةٍ تامةٍ، ولا يتعرض لأيّ مسؤوليةٍ قانونيةٍ مهما كان مدى الفحش والبذاءة التي ينطوي عليها هذا الكتاب أو هذه الصورة، وذلك استناداً إلى القانون والعرف الأميركي. وأيضاً بالنسبة للقانون المصري الحالي. ولكن بعض أشكال العلاقات الجنسية بين البالغين تعد فاحشةً ومنفرةً للغاية، ويجرم القانون أيّ شخص يقوم بالاتجار فيها أو عرضها على الجمهور العام، والتعبير بالكتابة والصورة والفن وسائر أشكال التعبير الأخرى عن موادّ فاحشةٍ داعرةٍ وعرضها للبيع أمرٌ يحرمه القانون، وتطبق هذه القواعد القانونية في المجتمع الأميركي [3]. وما لا شك فيه هو أن شبكة الإنترنت أتاحت أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الإباحية بشكلٍ علنيٍّ فاضحٍ تقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفانٌ هائلٌ من هذه الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيلٌ في التاريخ. وما يطلق عليه «جنس الأطفال»، هو من أخطر هذه الممارسات في الوقت الحالي[4].

إن الشبكة العنكبوتية ما هي إلا إبداعٌ اجتماعيٌّ أكثر من كونها إبداعاً تكنولوجياً، فما صُممت إلا من أجل مساعدة الأشخاص على العمل، وليست لعبة تكنولوجية، فالهدف الأساسي من الشبكة العنكبوتية هو دعم وتحسين وجودنا أو تواجدنا الشبكي في العالم، إلى أن ظهر متسللون أساؤوا

[1]- بريستون جرالا وشيرى كينكوف: مرجع سابق، ص108.
[2]- المرجع نفسه، ص111.
[3]- بهاء شاهين، الانترنت والعولمة، عالم الكتب،القاهرة، 1999، ص71.
[4]- حسن طاهر داوود، جرائم نظم المعلومات، ط1، أكاديمية نايف لعربية للعلوم الأمنية، الرياض، 2000، ص93.

استخدام هذه الشبكة، وهم ما يطلق عليهم القراصنة، فماذا تعني كلمة قرصنة؟[1] كثر الحديث في الآونة الأخيرة عما يسمى بالقراصنة، والذين يحاولون اقتحام الحواسيب إما لأغراضٍ نبيلة، وإما للسرقة والوصول إلى معلوماتٍ سريةٍ أو للتدمير أحياناً، ويملك هؤلاء المتطلفون خبرةً ودرايةً كبيرة في علوم وبرمجة الحاسوب[2].

لكن تطور معنى كلمة "قرصنة" بطريقةٍ مؤسفة، فقد كانت تعني الشخص الذي لديه دوافعُ إيجابيةٌ ومثمرةٌ في الأساس، وكان القرصان (المتسلل) شخصاً يحب أن يأخذ على عاتقه مشاريع الحاسوب الكبيرة والصعبة لمجرد التحدي. وإذا لم يكن هناك مشروعٌ متاحاً يظل يحلم به حتى يأتي، ونجد أشخاصاً مثل (Brian Kernighan)، (Dennis Ritchie) ، (Ken Thompson)، هم من علماء الحاسوب البارزين الذين لهم الأثر الكبير في تطوير نظام يونكس، هؤلاء الذين اخترعوا مشاريع حاسوب غير رسميةٍ في مختبرات بيل وبونكسس. أما الآن فهذا المصطلح يستخدم لوصف الأشخاص الذين يتسللون على نظام الحاسوب إما للمتعة أو لأسبابٍ أكثر خبثاً. فنرى من حيث الدوافع والقدرة الفنية، أننا نتحدث عن نوعين من الناس فالمتسلل الحق سيكون مبدعاً في الاستخدام غير المصرح به لأنظمة الحاسوب، ومن ناحية أخرى قد يكون المتسلل مدفوعاً بشغفه في القيام بشيءٍ غير مشروعٍ. ومشكلة تباين معاني تلك الكلمة معروفة للجميع. وقد تسبب هذا التباين في إطلاق غالبية الناس على من يخترق أنظمة الحاسوب تسمياتٍ مختلفةً[3].

ومن الممكن إجراء عملية القرصنة عن طريق رشوة عاملين في المؤسسة يتولون الكشف مباشرة على الحاسوب، فمن الناحية القانونية، فإن ملاحظة الذين يمارسون نشاطاتهم بهذا الوجه مشكلة مستعصية. أما بالنسبة لنسخ البرامج فيتم بصورةٍ بسيطةٍ جداً بتشغيل سواقات الأسطوانات الحاسوبية اللينة على الشكل التالي:

تقليد البرامج المعروفة بصورةٍ غير مشروعةٍ، وبغير وجه حق، بعد إجراء التعديلات عليها.

النسخ أو الغش من قبل الموزع الذي يبيع البرامج إلى الزبائن على أنها أصليةٌ.

---

[1]- **Pekka Himanen The Hacker Ethic and the Sprit of the information Age, Random House Inc., USA, New York, 2001, pp. 184--185.**

[2]- نبيل مصطفي صالح، أخلاقيات التطور الثقافي في استخدامات الشبكة الدولية للمعلومات وسرية وأمن المعلومات، مقالة في كتاب، فرج صالح عبد الرحمن وعبد العزيز محمد البونى: أخلاقيات التعامل مع الثقافات الحديثة، ط1، المنظمة العربية للتربية والثقافة والعلوم، جمعية الدعوة الإسلامية العالمية، المنظمة الإسلامية للتربية والعلوم والثقافة، تونس، 2008، ص339.

[3]- **Kevin. W. Bowyer, ethics & computing, living responsibility in a computerized, P.81.**

النسخ غير المرخص به من قبل المستهلكين، فالعديد من الناس ينسخون برامج عن حسن نية، مع جهلهم المسبق بأن الأمر غيرُ شرعيٍّ.

إنتاج برامجَ مماثلةٍ للبرامج الرائجة من قبل الشركات المنافسة وبيعها على أساس أنها أصلية[1].

للحماية من القراصنة والاختراق يجب متابعة كل التغيرات الأمنية الحديثة في أقسام التأمين بالمواقع المختلفة على شبكة الويب. حينما تتصل بالإنترنت يجب منع الإتصال بأجهزة حاسوبٍ أخرى ومنع تشارك الملفات أو الطابعات، فأي شخصٍ آخر يستطيع الحصول على عنوان الإنترنت أثناء الاتصال يمكنه الاختراق بسهولةٍ[2].

اختراق الخصوصية

اهتم الكثير من الفلاسفة بوضع تعريفٍ لمعنى الخصوصية. فالمناقشات تتمحور هنا حول فكرة (الوصول - الولوج)، حيث يعني الولوج التقرب البدني لشخص أو المعرفة عن هذا الشخص. فهناك عمليات شدٍّ وجذبٍ بين الرغبات؛ الحقوق والمسؤوليات الخاصة بالشخص الذي يريد الاستئثار بهذا الولوج لنفسه، وحقوق ورغبات ومسؤوليات الأجانب (الدخلاء) بهذا الوصول. وقد أخذ المفكر السياسي الإيرلندي (أدموند بيرن) بوجهة النظر التي تسعى إلى تقييد هذا الولوج عندما عرف الخصوصية بأنها «منطقة عدم إمكانية الوصول» الذي يحيط بالشخص. فأنت تملك من الخصوصية ما يمكنك من التحكم في الوصول إلى منطقة «صعوبة الوصول». فعلى سبيل المثال، يمكنك ممارسة خصوصيتك عند غلق الباب خلفك عند استخدام المرحاض، يمكنك أيضاً ممارسة خصوصيتك عندما تختار ألا تخبر الكاتب أو الموظف في أحد متاجر الفيديو رقم ضمانك الاجتماعي. ومع ذلك، فالخصوصية ليست الشيء نفسه. فيمكن لإثنين من الناس أن يكون لهما علاقتهما الخاصة، يمكن أن تكون علاقةً جسديةً، والتي فيها يمكن أن يسمح شخص لآخرَ بالتقرب منه جسدياً، ويمكن أن يتسبعد آخرين. وقد تكون علاقةً فكريةً، والتي يتبادلان فيها الرسائل التي تحتوي على أفكارٍ خاصة [3].

عادةً ما تعدّ الخصوصية أحد سمات الاستقلال، إلا أنه بسبب أهميتها في ما يتعلق بتكنولوجيا الحاسوب تستحق أن يتم التعامل معها بشكلٍ منفصلٍ، ذلك أن الخصوصية هي الحرية الممنوحة

[1]- علاء عبد الرازق السالمي، تكنولوجيا المعلومات، مرجع سابق، ص433-434.

[2]- عبد الحميد بسيوني، الحماية من أخطار الإنترنت، دار الكتب العلمية، القاهرة،2003، ص143.

[3]- **Michael J. Quinn, ethics for the information age, grea tobin, pearson Addison Wesley, boston, 2006, p. 213.**

للأفراد للسيطرة على عرضها وإعلانها للآخرين، وهناك تمييزٌ بين الخصوصية المعلوماتية والخصوصية الفكرية. إن الخصوصية الفكرية هي السيطرة على الشخص والبيئة الشخصية للفرد، وتتعلق بالحرية التي يجب تركها دون رقابةٍ أو تدخلٍ من الآخرين. والخصوصية المعلوماتية هي سيطرة الفرد على المعلومات الشخصية في صيغة نصٍّ وصورةٍ وتسجيلاتٍ[1].

عندما ننظر إلى الخصوصية من وجهة نظر الغرباء الذين يسعون إلى الوصول، فالمناقشة تدور حول أين نرسم الخط الفاصل بين ما هو خاصٌّ وما هو عامٌّ، فإن تجاهل هذا الخط وانتهاك خصوصية أي شخصٍ هو إهانةٌ لكرامة ذلك الشخص. فأنت تنتهك خصوصية أي شخصٍ إذا تعاملت معه كوسيلةٍ لتحقيق غايةٍ. لنفترض أن أحد الأصدقاء يدعوك لرؤية فيلم فيديو وهو متاحٌ على شبكة الإنترنت، وتبعته إلى معمل الحاسوب. وقد جلس على أحد الأجهزة المتاحة وبدأ بكتابة اسمه وكلمة المرور الخاصة به، فمن المقبول بوجه عام أنه ينبغي عليك أن تغمض عينيك عندما يقوم شخصٌ ما بكتابة كلمة المرور الخاصة به، فهي شيء يجب ألا يُعرف إلا من قبل المستخدم فقط[2].

إذاً، تعد الحماية الكاملة للفرد سواءً في شخصيته وممتلكاته مبدأ قديماً بقدم القانون العام، ولكن وجد أنه من الضروري من آنٍ لآخر أن يتم تعريف طبيعة ومدى هذه الحماية بشكلٍ محددٍ، وأن التغيرات السياسية، الاجتماعية، والاقتصادية غالباً ما تنطوي على الاعتراف بحقوقٍ جديدةٍ، لذا، فإن القانون العام في بدايته الأولى كان ينمو ليقابل المتطلبات الجديدة للمجتمع. ولذا، كان في العصور الأولى يقدم القانون علاجاً فقط لحالات التدخل الجسدي في الحياة والممتلكات، ثم جاء «الحق في الحياة ليحمي الفرد من الاعتداء بكافة أشكاله[3].

وثمة ثلاثةُ أوجهٍ مختلفةٍ للخصوصية، وهي: خصوصية النشاط، أي ألّا يتم التجسس علينا، وخصوصية المعلومات «بمعنى الحق في الاحتفاظ بها»، والحق في قدرٍ من التحكم في نوعية واستعمال المعلومات التي يحتفظ بها طرفٌ ثالثٌ. ويمثل هذا الأخير مجال حماية البيانات. ويوجد في المملكة المتحدة حقٌّ كافٍ في خصوصية المعلومات الشخصية التي يؤيدها القضاء، ويحاكم القانون على مخالفة هذا الحق. ويمكن انتهاك الخصوصية بواسطة أدوات التنصت، كآلات التصوير المخبأة، واختراق المحادثات الهاتفية والرسائل عن طريق شبكات الحاسوب،

[1]- Philip brey, disclosive computer ethics, in Richard A. spinello, Herman T.Tavani, Readings in cyberthics, P. 63.

[2]- Michael J. Quinn, ethics for the information age, P. 213.

[3]- Samuel D. Warren & Louis D. Brandeis; The Right to Privacy, in Adam, D. Moore; Information Ethics, Privacy , Property and Power, University of Washington Press, U.S.A., 2005, P. 209.

وحتى لو ارادت الشرطة القيام بذلك، يتوجب عليها الحصول على تفويضٍ قانونيٍّ، على الرغم من أن الشرطة تستطيع انتهاك الخصوصية في الحالات الطارئة[1]. ولقد فرق الفلاسفة -بوجه عام- بين القيم الجوهرية، حيث إن قيمة بعض الأشياء في حد ذاتها، والتي تقود إلى تحقيق إنجازاتٍ في نهاية الطريق. وفي تحليل أستاذ فلسفة الأخلاق في جامعة دلفن للتكنولوجيا والسياسة والإدارة «فان دن هوفن» (Jeroen Van Den Hoven) للخصوصية، فرق بين ما هو جوهريٌّ وما هو وظيفيٌّ، فالخصوصية - طبقاً للرأي السابق- تعد قيمةً في حدّ ذاتها، أي قيمة جوهرية[2].

وتمثل الخصوصية ترتيباً اجتماعيًّا يسمح للأفراد بأن يكون لديهم مستوى من السيطرة على من هو قادر على الوصول إلى معلوماتهم الشخصية. وأظهر القانوني «مارتن ليفن» (Martin Levine)، كيف أن إيماننا بحقوق الخصوصية انبثق من حقوق الملكية الخاصة بنا. وكانت تقاليد القانون العام الانجليزى ترى أن (منزل الرجل هو قلعته) ولا يستطيع أحد دخوله[3].

الحق في الخصوصية وجهان متلازمان هما: حرية الحياة الخاصة، وسرية هذه الحياة. فحرية الحياة الخاصة تعني حرية الفرد في اختيار أسلوب حياته دون تدخلٍ من الغير أو السلطة، لكن هذه الحرية ليست مطلقةً لكن مقيدةً بالنظام الاجتماعي داخل المجتمع ويضع القانون حدودها من أجل تنظيم كيفية ممارستها كي لا تضر بالآخرين. وسرية الحياة هي سريّة كلّ ممارسات الفرد في حياته الخاصة، ونطاق سرية الحياة الخاصة نطاقٌ شخصيٌّ يرتبط بالشخص ذاته، فهو يشمل جميع البيانات والوقائع التي يقرر الفرد أن من مصلحته الاحتفاظ بها لنفسه أو لغيره من الأشخاص المتصلين به ويريد إطلاعهم عليها[4].

انتهاك حقوق الملكية

تُعرف الملكية الفكرية بأنها حقُّ امتلاك الفرد لأعماله الفكرية والإبداعية كالاختراعات، والمصنفات الأدبية والفنية، والصور، والرسوم، والنماذج ...إلخ، ولم تكن الملكية الفكرية وليدةَ هذا العصر، بل كانت مبدأ قديماً بقدم القانون العام.

ذهب كثيرٌ من الباحثين إلى القول بأن الملكية بدأت أولاً كملكيّة جماعيةٍ (Propriete collective)، تشترك فيها جميع أفراد القبيلة ولا يستأثر بها أحد منهم، فكانت الأرض والأسلحة

[1]- مايكل هيل: أثر المعلومات في المجتمع ، مركز الإمارات للدراسات الاستراتيجية ، الامارات، 2004، ص207.

[2]- German T. Tavani; Information Privacy; Conccepts, Theories and Controversies, PP. 156--157.

[3]- Michael J. Quinn, ethics for the information age, p. 214.

[4]- نهلاً عبد القادر المومني، الجرائم المعلوماتية،مرجع سابق، ص164، 165.

والعديد من الأمور بوجهٍ خاصٍّ مملوكةً ملكيةً جماعيةً للقبيلة في الحضارة البدوية. ولما استقرت الجماعات على الأرض وتطورت الأرض، تطورت الملكية مع تطور الحضارة، فأصبحت ملكيةً عائليةً، وانتهت الملكية بعد تطور إلى أن تكون ملكيةً فرديةً، ولكن مع بقاء بعض أثار الملكية العائلية كالميراث والنصاب الذي يجب أن يتبقى للورثة دون أن تجوز الوصية فيه. ففي العصور الرومانية القديمة كانت الملكية جماعيةً وعائليةً، وكانت فردية في بعض الأشياء الاستثنائية المحددة، كالمنقولات، وكان معنى الملكية يختلط بالمعنى الديني وبمعنى سيادة الدولة، ولكن ما لبثت العصور الوسطى والعادات الجرمانية أن عقدت الملكية الفردية من جديدٍ وكانت الملكية في العادات الجرمانية ملكيةً فرديةً[1].

تعد ملكية برامج الحاسوب أحد مناطق الجدل في أخلاقيات الحاسوب. وظهرت العديد من وجهات النظر حولها، على سبيل المثال، اعتقد مبرمج الحاسوب «رتشارد ستالمن» (1953م) (Richard Stallman) الذي أنشأ مؤسسة السوفت وير المجانية- أن ملكية البرامج يجب ألا يكون مسموحاً بها للجميع، ويدعي أن كل المعلومات يجب أن تكون مجانيةً، وكل البرامج متاحة للنسخ والدراسة والتعديل من أي شخصٍ يرغب في القيام بهذا. ويعتقد آخرون أن شركات البرامج لا تبذل قصارى جهدها – بالإضافة لما تنفقه من أموالٍ في تطوير البرامج– إذا لم يحصلوا على المقابل في شكل رسوم ترخيص أو مبيعات[2]. ومن ثم، لابد من وضع قوانين خاصة للملكية الفكرية لحماية منتجات الأشخاص الفكرية.

حتى عام 1988م، كانت حقوق الملكية الفكرية على البرمجيات تندرج مع بقية الحقوق الفكرية في إطار قانونٍ واحدٍ، ولكن في ذلك العام صدر أول قانونٍ خاصٍ بحماية الملكية الفكرية للمنتجات الفكرية الرقمية (Digital Copy Right Act)، في الولايات المتحدة الأميركية، وإذا كان هذا القانون يشمل كافة أشكال الملكية الرقمية مثل الصور والتسجيلات الموسيقية والأفلام المخزنة على الأقراص المدمجة، فإن القسم الأكبر منه كان مختصاً لمكافحة سرقة البرمجيات[3]. وانتشرت الانتهاكات الخاصة بالملكية الفكرية على الإنترنت في الأونة الأخيرة بشكلٍ كبيرٍ، وكثيراً ما قام الأفراد بالاستحواذ على الملكيات الفكرية للأفراد الآخرين ونسبوها إلى أنفسهم.

[1]- عبد الرازق أحمد السنهوري، الوسيط في القانون المدني، العقود التي ترد على الملكية، ج4، دار النهضة العربية، القاهرة، 1984، ص423.

[2]- Terrell Ward Bynum; Ethics and the Information Revolution, In Richard A. Spinello & Herman T. Tavani; Reading in Cyberethics, Sudbury Mass, Jones and Bartlett, 2004, P. 22.

[3]- حسن عبد الله عباس & صلاح محارب الفضلي، مرجع سابق، ص136.

لا يسمى الانتهاك انتهاكاً بمجرد الاستحواذ على ملكية الغير فقط، بل إن مجرد الدخول إلى مواقع البريد الإلكتروني والإطلاع على الوسائل الموجودة بداخله دون إذن من صاحبه، يعد جريمة انتهاكاً لسرية المراسلات المكفولة بنصوص الدستور، وقد أصدر الاتحاد الأوروبي توجيهاً عام 1995، والخاص بمعالجة البيانات الشخصية وحرية انتقال مثل هذه البيانات، وحدّد مسؤولية من يتعرض لسرية هذه البيانات والمعلومات، كما اهتمت الهيئات الدولية بإصدار توجيهات بشأن حماية السرية، فقد أصدرت منظمة التعاون والتنمية الاقتصادية، المبادئ التوجيهية لحماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود عام 1980م [1].

وثمة أربعة حقوق، يمكن منم خلالها حماية الملكية الفكرية على الإنترنت وهي:

حقوق الطبع: تحمي غالبية القوانين أعمال التأليف الأصلية من الاستخدام غير القانوني، أو إعادة الطبع غير القانوني، أو التعديل، أو التوزيع، ويحمي كل ذلك حق التعبير عن الأفكار.

العلامات التجارية: تحمي القوانين العلامات التجارية، الأسماء والكلمات.

براءات الاختراع: تحمي القوانين الاختراعات الجيدة والمفيدة والجديدة من العمليات، والآلات، والإنتاج.

الأسرار التجارية: السر التجاري لأيّ معلومةٍ تستخدم في العمل، وتعطي مالكها مميزات عن الآخرين في كيفية معرفتها أو استخدامها[2].

تعد سرقة البرمجيات من أكثر جرائم الحاسوب التي تسحوذ على اهتمام الأوساط القانونية، لما لها من تأثيرٍ على حقوق الملكية، وهي من أكثر جرائم الحاسوب شيوعاً، إذ يقدر أن نسبة البرمجيات المسروقة إلى البرمجيات الأصلية تصل إلى 20% في البلدان المتقدمة في حين تصل إلى 80% في بعض بلدان العالم الثالث. توجد صورٌ عديدةٌ لعملية سرقة البرمجيات، ومن أمثلتها المعروفة نسخ الأقراص المرنة أو المدمجة أو تحميل البرامج عن طريق الإنترنت بطريقةٍ غير مصرحٍ بها، وقدرت خسائر شركات البرمجة من جراء سرقة البرمجيات بحوالي 5.5 مليار دولار في عام 2002 وحده[3].

[1]- خالد ممدوح، أمن المستندات الإلكترونية، الدار الجامعية، الاسكندرية، 2008، ص155.
[2]- رباب البدائية، الأمن وهرب المعلومات، دار الشروق، القاهرة، 2006، ص223.
[3]- حسن عبد الله عباس، صلاح محارب الفضلي: أخلاقيات الكمبيوتر، مرجع سابق، ص29.