السمات المميزة للجرائم المعلوماتية عــن الجرائم التقليديـــة

الأستـــاذ/ حكيـــــم سيـــاب
جامعـــة 20 أوت 1955 سكيكـــدة

ملخـــص البحـــث

جرائم المعلوماتية، طائفة تتسم بسمات مخصوصة عن غيرها من الجرائم، **فهي تستهدف معنويات لا ماديات محسوسة (بيئتها معنوية ليست مادية)**، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعنوي (المعلومات).

كما أنها تتسم **بالخطورة البالغة لأغراضها المتعددة**، يتضح ذلك في **حجم الخسائر الناجمة عنها قياسا بالجرائم التقليدية**، وكون **مرتكبيها من بين فئات متعددة** تجعل **التنبؤ بالمشتبه بهم أمرا صعبا**، ولأنها تنطوي على **سلوكات غير مألوفة**، وبما أتاحته من **تسهيل ارتكاب الجرائم الأخرى**.

وأن التحقيق والتحري والمقاضاة في جرائم المعلوماتية **ينطوي على مشكلات وتحديات إدارية وقانونية**.

فتثير بذلك تحديات ومعوقات في **حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش ...**

فما هي السمات والخصائص المميزة لجرائم المعلوماتية عن الجرائم التقليدية؟.

الخطـــــة

المطلب الثاني: أهم أنواع وأشكال الجريمة المعلوماتية.

المبحث الثاني: السمات الخاصة بالمجرم المعلوماتي.

المطلب الأول: تحديد المجرم المعلوماتي وخصائصه.

المطلب الثاني: أهم أنواع مجرمي المعلوماتية.

الفصل الثاني: سمات النصوص التشريعية للحماية من الجرائم المعلوماتية.

المبحث الأول: مدى صلاحية نصوص القانون الجنائي التقليدية للحماية من الجرائم المعلوماتية.

المطلب الأول: مدى صلاحية نصوص قانون العقوبات.

المطلب الثاني: مدى صلاحية نصوص قانون الإجراءات الجزائية.

المبحث الثاني: مدى حماية الأموال المعنوية من الجرائم المعلوماتية بمقتضى القوانين الخاصة.

المطلب الأول: مدى الحماية بموجب أحكام القانون المدني.

المطلب الثاني: مدى الحماية بموجب قانون الملكية الفكرية والحقوق المجاورة.

الخاتمة.

التوصيـــــات.

الملحق.

قائمة المراجع.

مقدمة

لقد مرت البشرية في تطورها التاريخي بمجموعة من الثورات الصناعية، ابتداء من اكتشاف الفحم كمصدر للطاقة والاعتماد عليه في تشغيل الآلة البخارية، إلى اكتشاف البترول والكهرباء، وما صاحباهما من تطور تكنولوجي، وصولا إلى الطاقة النووية، التي تجسدت في الثورة الصناعية الثالثة، لكن رغم ما صاحبها من ظهور أشكال جديدة للطاقة، وطرق حديثة للنقل والاتصال، فإن الثورة المعلوماتية **Informatic revolution**

أخذت قدم السبق بفضل الوسائل التكنولوجية الحديثة، والمتمثلة أساسا في الحاسب الآلي **computer** الذي ترك بصمات واضحة على حياتنا الحديثة، فأثّر على تطور أنشطتنا اليومية؛ من حيث الإنجاز والسرعة والشكل والمضمون والزمان والمكان**1[1]**.

لا شك أن الحاسب الآلي أصبح على مدى العشرين عاما الماضية ركيزة أساسية لأهداف التطور في كل مجالات الحياة**2[2]**، لما فيها من أنشطة مختلفة سواء كانت اقتصادية، علمية، اجتماعية، صناعية أو زراعية... وأدى الاستخدام المضطرد للمعلوماتية، سواء في شكل أموال معنوية أو أساليب مستحدثة، إلى ظهور ما يعرف بالإجرام المعلوماتي **Delinquency Informatic** كنتيجة حتمية لكل تقدم تقني مستحدث، سواء كان الحاسوب كأداة للجريمة أو كهدف لها.

حيث انتشرت شبكات الحاسب الآلي والمعلومات بطول العالم وعرضه، ودخلت تطبيقاتها في أوساط المجتمعات المعاصرة، فأسهمت ولا شك في تعزيز التواصل الحضاري والثقافي، وتعزيز التفاهم الإنساني وكسر حواجز العزلة بين الشعوب، إلا أنها في الجانب الآخر ساعدت على شيوع الجريمة بمختلف أشكالها، لتقود إلى ما يمكن تسميته **بعولمة الجريمة**، والمتأمل في حال شبكة الإنترنت على وجه الخصوص، يدرك ما قدمته هذه الوسيلة من تسهيلات كبرى للأنشطة الإجرامية –المنظمة والفردية على السواء– جاعلة الأمن الاجتماعي والاقتصادي والقومي أيضا لكثير من البلدان، عرضة لمخاطر أنماط جديدة من الجريمة الذكية، والعابرة للحدود التي باتت اليوم تهدد كيان المجتمع الدولي.

وجرائم المعلوماتية، طائفة تتسم بسمات مخصوصة عن غيرها من الجرائم، **فهي تستهدف معنويات لا ماديات محسوسة (بيئتها معنوية ليست مادية)**، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعنوي (المعلومات).

كما أنها تتسم **بالخطورة البالغة** بالنظر لأغراضها المتعددة، يتضح ذلك في **حجم الخسائر الناجمة عنها قياسا بالجرائم التقليدية، وكون مرتكبيها من بين فئات متعددة** تجعل **التنبؤ بهم أمرا صعبا**، ولأنها **تنطوي على سلوكات غير مألوفة في القوانين التقليدية.**

---

[2] – **الدكتور محمد بوشيبة.** "حماية برامج الحاسوب طبقا لقانون 02– 00، المنظم لحقوق المؤلف والحقوق المجاورة"، مجلة القضاء والقانون، المغرب، 2000، ص 84.

[2][2] – للمزيد من المعلومات حول تطبيقات الحاسب الآلي في شتى مجالات الحياة أنظر:

– **الدكتور محمود سرى طه.** "الكمبيوتر في مجالات الحياة"، الهيئة المصرية العامة للكتاب، القاهرة، مصر، 1990.

– **الدكتور هشام محمد فريد رستم.** "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، أسيوط، مصر، 1994، ص 5 و ما بعدها.

وأن **التحقيق والتحري والمقاضاة في هذه الجرائم**، والتي نصطلح عليها (جرائم المعلوماتية)3[3] **ينطوي على مشكلات وتحديات إدارية وقانونية.**

فتثير بذلك تحديات ومعوقات في **حقل الاختصاص القضائي، والقانون الواجب التطبيق، ومتطلبات الملاحقة والضبط والتفتيش والتحقيق...**

ونظراً لطبيعة الموضوع، وغايته المتمثلة في محاولة تأصيل المفاهيم، وإبراز السمات والخصائص المرتبطة بالظاهرة محل البحث، فقد اعتمدنا على المنهج الوصفي، المستند على البحوث المكتوبة في الموضوع كمصدر رئيس للمعلومات، كما تمت زيارة مواقع مهمة تخصصت في رصد وتتبع الظاهرة الإجرامية المتعلقة بالمساس بأنظمة المعلوماتية، والاستفادة من حداثة المعلومات المقدمة من خلال انتهاج المنهج المقارن، بين ما توصل إليه التشريع الدولي لبعض الدول المتطورة في مكافحة هذه الجرائم، ومقرنتها مع التشريع الجزائري الحديث النشأة نسبيا في مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات4[4].

ومن خلال هذه المنهجية يسعى البحث إلى رصد وفهم وتحليل الظاهرة محل البحث بدقة، وإضافة إلى وصف الظاهرة، يعني البحث بالوقوف على الخصائص والسمات المميزة لهذه الظاهرة.

فما هي السمات والخصائص المميزة لجرائم المعلوماتية عن الجرائم التقليدية؟، أي هل الفاعل (المجرم) في الجريمة المعلوماتية هو نفسه في الجريمة التقليدية؟، وهل محل (موضوع) الجريمة هو ذات محل الجرائم الأخرى؟، وهل البيئة التي تُرتَكب فيها هذه الجرائم هي نفسها (البيئة المادية)؟، وهل وسيلة ارتكاب جرائم المعلوماتية هي نفس وسيلة الجرائم التقليدية؟...

وهل تصمد نصوص التشريعات الجنائية والإجرائية المعمول بها، في مواجهة هذا الصنف الجديد من الجرائم؟.

نجيب على ذلك وفق الآتي.

الفصل الأول: سمات الجريمة والمجرم في مجال المعلوماتية.

---

[3]3– إذ تتوجب علينا الإشارة إلى أنه يوجد فرق بين الجريمة المعلوماتية التي هي محل دراستنا والجريمة الإلكترونية، وسنبين ذلك في موضوع تعريف الجريمة المعلوماتية.

[4]4– هكذا سماها المشرع الجزائري، "**إذ لم يوفق في هذه التسمية، إذ تعتبر غير دقيقة فلم تحدد عناصر الجريمة المعلوماتية وكذلك أنواعها**"، ذلك في القسم السابع مكرر من قانون العقوبات المعدل بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 الجريدة الرسمية عدد 71 ص 8 وما بعدها.

جرائم المعلوماتية؛ جرائم تطال المعرفة؛ الاستخدام؛ الثقة؛ الأمن؛ الربح والمال؛ السمعة؛ الاعتبار... ومع هذا كله فهي لا تطال حقيقة غير البيانات (المعلومات)؟.

عرف الدكتور نعيم مغبغب المعلومات بأنها: "جملة البيانات والدلالات والمعارف والمضامين التي توصل إلى نتائج، وتساعد المهتمين بزيادة المعرفة وتطويرها، فالمعلومات توضح مفهوم الشيء وسماته وخصائصه وتبين استخداماته ووظائفه"**5[5]**.

وعرف القانون السعودي البيانات أنها: "المعلومات أو الأوامر أو الرسائل أو الأصوات أو الصور التي تعد أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه ومعالجته ونقله وإنشاؤه بوساطة الحاسب الآلي كالأرقام والحروف والرموز وغيرها"**6[6]**.

لكن المعلومات –بأشكالها المتباينة في البيئة الرقمية– تصبح شيئا فشيئا المعرفة، ووسيلة الاستخدام وهدفه، وهي الثقة، وهي الربح والمال، وهي مادة الاعتبار والسمعة.

فجرائم المعلوماتية بحق هي جرائم العصر الرقمي.

فما هي السمات الخاصة بالجريمة المعلوماتية؟، وما هي السمات المميّزة للمجرم المعلوماتي؟.

نجيب على ذلك من خلال المبحثين التاليين.

المبحث الأول: السمات الخاصة بالجريمة المعلوماتية.

لقد أفرزت ثورة الاتصالات والمعلومات وسائل جديدة للبشرية تجعل الحياة أفضل من ذي قبل، غير أنها فتحت الباب على مصراعيه لظهور صور من السلوك الإجرامي التي لم يكن من الممكن وقوعها في الماضي، والتي تخرج عن دائرة التجريم والعقاب القائمة، لأن المشرع لم يتصور حدوثها أصلاً**7[7]**.

فمن جهة أولى سمحت نظم الحاسوب بظهور صور جديدة من الجرائم لم تكن موجودة في الماضي، وذلك مثل سرقة المعلومات والأسرار المودعة في قواعد المعلومات، ومن جهة ثانية أتاحت هذه النظم الفرصة لارتكاب الجرائم التقليدية بطرق حديثة بأكثر دقة وسرعة، كما هو الشأن بالنسبة لجرائم الغش وإتلاف وإفساد المعلومات المخزنة في الحواسيب.

نتطرق لذلك في محاولة لوضع مفهوم للجريمة المعلوماتية؛ وتبيان أهم خصائصها في مطلب أول، وتحديد المجرم المعلوماتي؛ وإبراز أهم مميزاته في مطلب ثاني.

---

[5]5– **الدكتور نعيم مغبغب**. "حماية برامج الكمبيوتر" الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2006، ص 31.

[6]6– المادة 01 من "قانون نظام مكافحة جرائم المعلوماتية السعودي"، الصادر بالمرسوم الملكي السعودي رقم م/ 17 بتاريخ 27 أفريل 2008.

[7]7– في هذا المعنى راجع: **الأستاذ الدكتور محمد محيي الدين عوض**. "مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)"، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، المنعقد بالقاهرة، في الفترة 25–28 أكتوبر 1993، حول: مشكلات المسئولية الجنائية في مجال الإضرار بالبيئة والجرائم الواقعة في مجال تكنولوجيا المعلومات، منشور ضمن أعمال المؤتمر، دار النهضة العربية، القاهرة، مصر، 1993، ص 360.

المطلب الأول: مفهوم الجريمة المعلوماتية وخصائصها.

إن إيجاد مفهوم دقيق للجريمة المعلوماتية وتبيان أهم خصائصها، مر بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ففي المرحلة الأولى من شيوع استخدام الحاسوب في الستينات ومن ثم السبعينات، ظهرت أول مُعَالَجَات لما يسمى **جرائم الكمبيوتر** آنذاك –وكان ذلك في الستينات– فاقتصرت المعالجة على مقالات صحفية، ناقشت التلاعب بالبيانات المخزنة وتدمير أنظمة الحاسوب والتجسس المعلوماتي، والاستخدام غير المشروع للبيانات المخزنة في نظم الحاسب الآلي، وترافقت هذه النقاشات مع **التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر، أم ظاهرة إجرامية مستجدة؟، بل ثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني، أم مجرد سلوكات غير أخلاقية في بيئة المعلوماتية؟**، وبقي التعامل معها أقرب إلى النطاق الأخلاقي منه إلى النطاق القانوني، ومع تزايد استخدام الحواسيب الشخصية في منتصف السبعينات، ظهر عدد من الدراسات القانونية والمسحية (التعدادية)، التي اهتمت بجرائم المعلوماتية؛ وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكات مستهجنة أخلاقيا. وفي الثمانينات ظهر مفهوم جديد لجرائم المعلوماتية؛ ارتبط بعمليات اقتحام نظم المعلومات عن بعد، وأنشطة نشر وزراعة الفيروسات، التي تقوم بتدمير الملفات أو البرامج، وشاع اصطلاح (الهاكرز) وغيرها من عناصر الجريمة المعلوماتية بالمفهوم الحديث.

ندرس ذلك في فرعين، فنخصص الأول لتعريف الجريمة المعلوماتية، والثاني لتبيان أهم أنواعها وأشكالها.

الفرع الأول: تعريف الجريمة المعلوماتية[8][8].

تُعرَف الجريمة عموما، في نطاق القانون الجنائي، بأنها: **"فعل غير مشروع؛ صادر عن إرادة جنائية؛ يقرر له القانون عقوبة أو تدبيرا احترازيا..."[9][9]**، وعلى الرغم من التباين الكبير في تعريفات الجريمة بين فقهاء القانون، وبينهم وبين علماء الاجتماع والنفس... إلا أننا تخيرنا

---

[8][8]– جدير بالذكر أن حداثة هذه الجرائم جعـلها ليست محل اتفاق بين الباحثين: فالبعض يطلق عليها: **"جرائم الحاسبات"**، في حين أن فريق ثان يطلق عليها: **"الغش المعلوماتي"**، ويذهب فريق ثالث إلى استخدام تعبير: **"الجرائم المعلوماتية"**، وهو ما اعتمدناه في المتن، –لأننا نرى أنه أكثر تعبيراً عن المقصود–، فهي ليست جرائم حاسوب فقط لأن بعضها يتعلق بالإنترنت على وجه الخصوص؛ وليست جرائم غش معلوماتي فقط؛ لأن بعضها الآخر يدخل ضمن زمرة الجرائم ضد الأشخاص كالقتل والتحريض عليه...

[9][9]– **الأستاذ الدكتور محمود نجيب حسني.** "شرح قانون العقوبات، القسم العام"، الطبعة السادسة، دار النهضة العربية، القاهرة، مصر، 1989، ص 40.

هذا التعريف استنادا إلى أن التعريف الكامل –**كما يرى الفقه– هو ما حدد عناصر الجريمة إلى جانب بيانه لآثارها**10[10].

نود التأكيد على أهمية هذه القاعدة في تعريف الجريمة، فبيان عناصر الجريمة –السلوك غير المشروع المخالف للقانون، الإرادة الجنائية وأثرها، العقوبة أو التدبير الذي يفرضه القانون– من شأنه في الحقيقة أن يعطي تعريفا دقيقا لوصف الجريمة عموما، ويُميّز بينها وبين الأفعال المستهجنة في نطاق الأخلاق، أو الجرائم المدنية أو الجرائم التأديبية.

يقصد بالجريمة المعلوماتية –في نظرنا–: **"كل سلوك؛ غير مشروع؛ معاقب عليه قانونا؛ صادر عن إرادة إجرامية؛ محله معطيات الحاسوب"**11[11]، فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الإجرامية، ومعاقب عليه قانونا، لأن إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع، ومن خلال النص على ذلك حتى ولو كان السلوك مخالفا للأخلاق.

تقدير:

إن تعريف الجريمة عموما يتأسس على بيان عناصرها المناط بالقانون تحديدها، إذ من دون نص التشريع على النموذج القانوني للجريمة لا يتحقق إمكان المساءلة عنها –استنادا إلى قاعدة المشروعية الجنائية التي توجب عدم جواز العقاب عند انتفاء النص، وسندا إلى أن القياس

---

[10]10– بهذا قال **الأستاذ الدكتور كامل السعيد**. "شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن"، الطبعة الثانية، دار الفكر للنشر والتوزيع، عمان، الأردن، 1983، ص 28.

[11]11– وجدير بالذكر أن هناك عدة تعريفات للجريمة المعلوماتية، ومن هذه التعريفات:

– ما ذهب إليه خبراء متخصصون من بلجيكا أن (جريمة الكمبيوتر) هي: (كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية). أنظر: **عفيفي كامل عفيفي**. "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة"، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003، ص 32.

– في حين يذهب الفقيه الفرنسي (Massa) إلى أن المقصود بالجريمة المعلوماتية: (الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح). راجع ذلك في موقع الإنترنت: www.arablaw/Download cyber crimes_General,doc

– بينما يذهب رأي ثالث إلى أنها: (كل فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب، أو التي تحول عن طريقه). راجع: **يونس عرب**. "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت"، الجزء الأول، الطبعة الأولى، منشورات إتحاد المصارف العربية، القاهرة، مصر، 2001، ص 213.

– في حين يذهب رأي رابع إلى أنها: (سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها). أنظر: **الدكتور علي عبد القادر القهوجي**. "الحماية الجنائية لبرامج الحاسب"، بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية، التي تصدرها كلية الحقوق، جامعة الإسكندرية، مصر، العدد 24، 1992، ص 172.

– في حين أن **منظمة التعاون الاقتصادي والتنمية OCDE** وضعت التعريف التالي للجريمة المعلوماتية: (كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية). راجع: **الدكتور هشام محمد فريد رستم**. المرجع السابق، ص 34.

محظور في ميدان النصوص التجريمية الموضوعية–، وهو ما يستوجب التمييز بين الظاهرة الإجرامية والجريمة.

ومحل جريمة المعلوماتية هو دائما معطيات الحاسوب بدلالتها الواسعة –بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة، المعلومات المستخرجة والمتبادلة بين النظم ، البرامج بأنواعها، – وأما الحاسوب فهو النظام التقني بمفهومه الشامل المزاوج بين تقنية الحوسبة والاتصال، بما في ذلك شبكات المعلومات**12.[12]**

ولكن السؤال الذي يثور هنا، هل محل الجريمة المعلوماتية تقنية نظم المعلومات، أم المعلومات ذاتها وفق دلالتها الواسعة، والتي يعبر عنها على نحو أشمل وأدق بتعبير (المعلوماتية)؟.

الفرع الثاني: خصائص الجريمة المعلوماتية.

في سياق الجريمة وظروف ارتكابها باستخدام الحاسوب ومن خلال شبكة الإنترنت، حدد بعض الخبراء أن لأفعالها خصائص متفردة، لا تتوافر في أي من أفعال الجرائم التقليدية، لا في أسلوبها، ولا في طريقة ولا وسيلة ارتكابها، والتي نوجزها في الآتي:

الخاصية الأولى: الحاسوب هو أداة ارتكاب الجرائم المعلوماتية.

فحوى هذه الخاصية أن كافة الجرائم المعلوماتية –يكون الحاسب الآلي هو الأداة لارتكابها، فلا يمكن تسمية هذه جريمة أو وصفها بجريمة معلوماتية دون استخدام الحاسوب، لأنه هو وسيلة الإجرام في هذا الصنف، وبالتالي وسيلة تنفيذ الجريمة أيا كان نوعها.

الخاصية الثانية: الجرائم ترتكب عبر شبكة الإنترنت.

تعد شبكة الإنترنت في **معظم** الجرائم المعلوماتية**13[13]**، هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات الصناعية وغيرها من الأهداف، التي ما تكون غالبا الضحية لتلك الجرائم، وهو ما دعا معظم تلك الأهداف إلى اللجوء إلى نظم الأمن المعلوماتية، في محاولة منها لحماية نفسها من تلك الجرائم، أو على الأقل لتحد من خسائرها عند وقوعها ضحية لها.

الخاصية الثالثة: الجريمة المعلوماتية لا حدود جغرافية لها.

---

[12][12]– **عباس الحسيني**. النجف الأشرف، العراق، مقال بعنوان، "جرائم الكمبيوتر والإنترنت" منشور على موقع الإنترنت الفريق العربي للأمن والحماية المعلوماتية www.atsdp.com

[13][13]– نشير هنا إلى أنه يوجد بعض أنواع جرائم المعلوماتية التي لا تستخدم فيها شبكة الإنترنت، مثال ذلك سرقة موظف ما مرخص له باستعمال حاسوب مؤسسة ما لبيانات موجودة على ذلك الجهاز، إذ لا حاجة في هذه الحالة إلى شبة الإنترنت.

شبكة الإنترنت ألغت أي حدود جغرافية فيما بين الدول، فيمكن التحدث بين أشخاص ليس في بلدان مختلفة، وإنما في قارات مختلفة حتى، وفي نفس الوقت على الشبكة، من خلال الدردشة **chat**.

وعليه فإن أي جرائم ترتكب عبر شبكة الإنترنت فإنها تتخطى حدود الدولة التي ارتكبت فيها لتتعدى أثارها كافة البلدان على مستوى العالم.

هذا فضلا عن مجموعة من الخصائص الفرعية نوجزها في:

أولا: أنها جريمة لا تترك أثر لها بعد ارتكابها.

ثانيا: صعوبة الاحتفاظ الفني بآثارها هذا إن وجدت أصلا لسهولة إخفاء معالم الجريمة.

ثالثا: أنها تحتاج إلى خبرة فنية، ويصعب على المحقق التقليدي التعامل معها.

رابعا: أنه يسهل (نظريا) ارتكاب الجريمة ذات الطابع المعلوماتي.

خامسا: يلعب البعد الزمني (اختلاف المواقيت بين الدول)، والمكاني (إمكانية تنفيذ الجريمة عن بعد)، والقانوني (أي قانون يطبق) دورا هاما في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم.

سادسا: هذه الجرائم تتسم بالغموض حيث يصعب إثباتها، والتحقيق فيها، ليس كما هو الحال في الجرائم التقليدية.

سابعا: كثيرا من الجرائم المعلوماتية لا يتم الإبلاغ عنها، إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير.

ثامنا: أنها تعتمد على قمة الذكاء في ارتكابها.

وتحدث الجريمة المعلوماتية عادة في إحدى ثلاث مراحل هي:

المرحلة الأولى: مرحلة إدخال البيانات، ومن ذلك على سبيل المثال قيام المجرم المعلوماتي بتغيير أو تزوير البيانات مثل التسلل إلى البيانات المتعلقة بفاتورة الهاتف قبل طبعها في شكلها النهائي، بحيث يتمكن من حذف بعض المكالمات من الفاتورة قبل طباعتها وإرسالها، ومثل قيام أحد الطلاب بتغيير درجاته المسجلة على الحاسب الآلي في مادة معينة أو تغيير تقديره الفصلي أو العام.

المرحلة الثانية: مرحلة تشغيل البيانات، ومن ذلك على سبيل المثال قيام المجرم بتغيير، أو تعديل البرامج الجاهزة **Software** التي تقوم بتشغيل البيانات للوصول إلى نتائج محددة أو مقصودة بطريق غير شرعي، ومن ذلك مثلاً استخدام برنامج معين لتقريب الأرقام المتعلقة بالعمولات البنكية على حساب أحد الأشخاص، أو تجميع الفروق بين الأرقام المقربة والأرقام الفعلية، وإضافتها لحساب سري آخر لنفس العميل، وقد تبدو هذه الفروق بسيطة ولكنها ستكون كبيرة إذا تمت إضافتها خلال عدة سنوات.

المرحلة الثالثة: مرحلة إخراج البيانات، ومثل ذلك سرقة بعض البيانات الالكترونية أو المعلومات الآلية المتعلقة بمراقبة مخزون إحدى الشركات، أو إفشاء معلومة متعلقة بإحدى الشركات، أو إفشاء معلومة متعلقة بأحد العملاء.

المطلب الثاني: أهم أنواع وأشكال الجريمة المعلوماتية.

من الصعوبة تماماً حصر أنواع الجريمة المعلوماتية، حيث أن أشكالها متعددة، وهي تزداد تنوعاً وتعداداً كلما أوغل العالم في استخدام الحاسب الآلي وشبكة الإنترنت**14[14]**.

فمن المعروف أن أكثر تلك الجرائم يكون من ضمن أهدافها الأساسية، الحصول على المعلومات، التي تكون إما محفوظة على أجهزة الحواسيب، وإما منقولة عبر شبكة الإنترنت، وأخرى يكون هدفها الاستيلاء على الأموال، وثالثة تستهدف الأفراد أو الجهات بعينها، وأخيرا جهاز الحاسب الآلي، فنلخصها فيما يلي:

1- المعلومات: ثمة العديد من الجرائم التي ترتكب بهدف يتعلق بالمعلومات، ويتمثل هذا الهدف بالحصول على المعلومات، أو تغييرها، أو حذفها نهائيا، هذا حسب درجة أهمية الهدف (المعلومات).

فمعظم تلك الجرائم التي يكون الهدف منها المعلومات، هي في الأغلب الأعم الجرائم الاقتصادية، وتكون بغرض الحصول على مزايا، أو مكاسب اقتصادية، فالحرب الاقتصادية لا تقل في ضراوتها وشدتها حاليا عن الحرب العسكرية، إلا أنها تتم باستخدام الحاسب الآلي وعبر شبكة الإنترنت.

2- الاستيلاء على الأموال: تستهدف أكثر تلك الجرائم تحديدا عناصر الذمة المالية، ويكون الطمع وراء ارتكابها، والحصول والاستيلاء على تلك الأموال، وفكرة المكسب السريع التي تحرك مرتكبيها، وقد ترتكب أحيانا لمجرد قهر نظام منشأة (مؤسسة) مثلا، وتخطي حواجز الحماية، أو بدافع الانتقام من صاحب تلك المنشأة أو أحد عناصرها.

3- الأشخاص أو الجهات: معظم الجرائم التي ترتكب في مجال المعلوماتية تستهدف إما أشخاص وإما جهات بعينها، وغالبا ما تكون تلك الجرائم هي جرائم مباشرة، ترتكب في صورة ابتزاز أو تهديد أو تشهير، أو هي جرائم غير مباشرة ترتكب في صورة الحصول

14[14]- أنظر في أنواع وأشكال الجرائم المعلوماتية:

- بالعربيـــــة: **الدكتور جميل عبد الباقي الصغير**. "القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي"، الكتاب الأول، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 1992.

- بالفرنسيـــــة: **-Pieere Catala,** "information Théorie Juridique de" 1983, paris. **Ebauche Duune.**

- بالإنجليزيـــة: **-Andre Lucas**, "Protiction of information Bases", Kuwait First Conference, Ministry of Justice – 15-17 Feb, 1999, Kuwait.

على البيانات، أو المعلومات الخاصة بتلك الجهات أو الأشخاص، لاستخدامها بعد ذلك في ارتكاب جرائم مباشرة.

4- أجهزة الحاسب الآلي: وعندما يكون الهدف من ارتكاب تلك الجرائم هو أجهزة الحاسب الآلي، فالغالب يكون الهدف، تخريب أنظمة تلك الأجهزة نهائيا، أو على الأقل تعطيلها لأطول فترة ممكنة، ومعظم تلك الجرائم تتم بواسطة استخدام الفيروسات.

حالات عملية شهيرة من واقع الجرائم المعلوماتية15[15].

والأحداث الشهيرة في هذا الحقل كثيرة ومتعددة، فسنكتفي في هذا المقام بإيراد أبرز الحوادث التي حصلت خلال السنوات الماضية**16[16]**.

قضية مورس: هذه الحادثة هي أحد أول الهجمات الكبيرة والخطرة في بيئة المعلوماتية ففي نوفمبر عام 1988 تمكن طالب يبلغ من العمل 23 عاما ويدعى **ROBER MORRIS** من إطلاق فيروس عرف باسم (دودة مورس) عبر الإنترنت، أدى إلى إصابة 06 آلاف جهاز يرتبط معها حوالي 60.000 نظام عبر الإنترنت، من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة، بحوالي مائة مليون دولار، إضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم على مورس بالسجن لمدة 3 أعوام وعشرة آلاف دولار غرامة.

قضية الجحيم العالمي: تعامل مكتب التحقيقات الفدرالية **FBI** مع قضية أطلق عليها اسم مجموعة الجحيم العالمي **GLOBAL HELL** فقد تمكنت هذه المجموعة من اختراق مواقع البيت الأبيض والشركة الفدرالية الأمريكية، والجيش الأمريكي، ووزارة الداخلية الأمريكية، وقد أدين اثنين من هذه المجموعة جراء تحقيقات جهات الأمن الداخلية في الولايات المتحدة، وقد ظهر من التحقيقات أن هذه المجموعة تهدف إلى مجرد الاختراق أكثر من التدمير، أو أخذ المعلومات الحساسة، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة.

فيروس ميلسا: وفي حادثة هامة أخرى، انخرطت جهات تطبيق القانون وتنفيذه في العديد من الدول، في تحقيق واسع حول إطلاق فيروس شرير عبر الإنترنت عرف باسم فيروس **MELISSA** حيث تم التمكن من اعتقال مبرمج حاسوب من ولاية نيوجرسي، في شهر أفريل

---

[15]15- **يونس عرب.** "جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات"، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، الإمارات العربية المتحدة، 10-12 /2002/02، ص 38-41.

[16]16- لتفصيل أكثر أنظر الملحق.

عام 1999، واتهم باختراق اتصالات عامة والتآمر لسرقة خدمات الحاسوب، وتصل العقوبات في الاتهامات الموجهة له إلى السجن لمدة 40 عام، والغرامة التي تقدر بحوالي 500 ألف دولار، وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها 19 مذكرة.

المبحث الثاني: السمات الخاصة بالمجرم المعلوماتي.

في بداية ظهور جرائم المعلوماتية، شاع الحديث عن المجرمين الذين يرتكبون مختلف أنواع الاعتداءات على نظم الحاسوب، وتحديدا الاختراقات بدافع التحدي واثبات المقدرة العلمية والتقنية لهم، وكان ثمة حديث عن استغلال منظمات الجريمة لهؤلاء النابغين، وتحديدا استغلال ميولهم، وأحيانا احتياجاتهم المادية لتسخيرهم للقيام بأنشطة إجرامية تتصل بالتقنية تعود بمنافع لمنظمات الجريمة، ومع تنامي الظاهرة وتعدد أنماط هذه الجرائم، ونشوء أنماط جديدة متصلة بشبكات الحاسوب وتحديدا الإنترنت، اتجهت جهات البحث و منها الهيئات العاملة في ميدان السلوك الإجرامي، لمحاولة تصنيف مرتكبي جرائم المعلوماتية والإنترنت وبيان السمات الأساسية لكل فئة، بغرض بحث أنجع الوسائل لردع هذه الفئات والحد من نشاطها**17[17]**.

نتطرق لذلك في مطلبين فنخصص الأول لتحديد المجرم المعلوماتي وخصائصه، والثاني لبيان أنواعه.

المطلب الأول: تحديد المجرم المعلوماتي وخصائصه.

إن دراسات علم الإجرام الحديثة في ميدان الإجرام المعلوماتي تسعى في الوقت الحاضر إلى إيجاد تصنيف منضبط لمجرمي المعلوماتية، لكنها تجد صعوبة في تحقيق ذلك، بسبب التغير السريع الحاصل في نطاق هذه الظاهرة، والمرتبط أساسا بالتطور الرهيب في ميدان المعلوماتية.

الفرع الأول: تحديد المجرم المعلوماتي.

يمكن تصنيف المجرم المعلوماتي في أربع مجموعات رئيسة وهي:

المجموعة الأولى: الموظفون العاملون بمراكز الحاسب الآلي، وهم يمثلون الغالبية العظمى من مرتكبي الجرائم المعلوماتية، وذلك بحكم سهولة اتصالهم بالحاسب ومعرفتهم بتفاصيله الفنية.

المجموعة الثانية: الموظفون الساخطون على مؤسساتهم أو شركاتهم، والذين يستغلون معرفتهم بأنظمة الحاسب الآلي، في شركاتهم وسيلة لإيقاع الضرر بهم عبر نشر البيانات، أو استعمالها، أو مسحها.

---

[17][17]– **يونس عرب.** "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت"، الجزء الأول، الطبعة الأولى، المرجع السابق، ص 27.

المجموعة الثالثة: فئة العابثين مثل الهاكرز **Hackers** أو الكراكرز **Crackers** وهم الذين يستغلون الحاسب الآلي من أجل التسلية في أمور غير قانونية وليس بغرض التخريب.

المجموعة الرابعة: الأفراد الذين يعملون في مجال الجريمة المنظمة باستخدام الحاسوب.

الفرع الثاني: خصائص المجرم المعلوماتي.

الخاصية الأولى: مرتكب الجريمة هو شخص ذو خبرة في مجال الحاسب الآلي.

لاستخدام الحاسب الآلي لارتكاب جريمة، لا بد وأن يكون مستخدم هذا الحاسوب، على دراية فائقة وذو خبرة كبيرة في مجال استخدامه، والتي تمكنه من تنفيذ جريمته والعمل على عدم اكتشافها، ولذلك نجد أن معظم من يرتكبون تلك الجرائم، هم من الخبراء في مجال الحاسب الآلي، وأن الشرطة تبحث أول ما تبحث عن الخبراء في مجال الحاسب الآلي للتحري عن مرتكبي الجرائم المعلوماتية.

الخاصية الثانية: أعماره تتراوح عادة بين 18 إلى 46 سنة والمتوسط العمري له 25 عاما**18[18]**.

الخاصية الثالثة: الحرص الشديد وخشية الضبط وافتضاح الأمر.

الخاصية الرابعة: ارتفاع مستوى الذكاء لديه ومحاولة التخفي.

المطلب الثاني: أهم أنواع مجرمي المعلوماتية19[19].

إنه لمن الصعوبة أيضا؛ حصر أنواع المجرم المعلوماتي، ذلك لتعدد تقسيمات المختصين في هذا المجال لهم، كل حسب الزاوية التي ينظر منها إليهم، إذ نصنفهم كالآتي:

1- المخترقون أو المتطفلون: Crackers & Hackers

علما أن بين الاصطلاحين تباينا جوهريا، فالهاكرز متطفلون يتحدَّون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، وإنما ينطلقون من دوافع التحدي وإثبات المقدرة، أما الكراكرز، فإن اعتداءاتهم تعكس ميولا لجريمة خطرة تنبئ عنها رغباتهم في إحداث التخريب، ومع أن هذا المعيار غير منضبط، إلا أن الدراسات والمعالجات في حقل جرائم المعلوماتية –بل بعض التشريعات المحلية في الولايات المتحدة الأمريكية– تعتمد هذا التمييز، فاصطلاح الكراكرز مرادف للهجمات الحاقدة والمؤذية، في حين أن اصطلاح الهاكرز مرادف في الغالب لهجمات التحدي، طبعا دون أن يؤثر هذا التمييز على

---

[18][18]- **الدكتور محمود صالح العادلي.** ورقة عمل بعنوان، "الجرائم المعلوماتية، ماهيتها وصورها"، مقدمة لورشة العمل الإقليمية حول: تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، اليمن، 2-4 أفريل 2006، ص 8.

[19][19]– لتفصيل أكثر في خصائص المجرم المعلوماتي وأهم أنواعه راجع **يونس عرب.** "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت"، الجزء الأول، الطبعة الأولى، المرجع السابق، ص 30 وما بعدها.

مسؤولية مرتكبي الأنشطة من كلا الطائفتين، ومساءلتهم عما يلحقونه من أضرار بالبيانات المستهدفة.

2- مجرمو الحاسوب المحترفون:

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة الإجرامية التي ترتكبها، ولذلك فإن هذه الطائفة تعد الأخطر من بين مجرمي التقنية حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم، أو للجهات التي كلفتهم وسخرتهم لارتكاب الجرائم، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي.

3- الحاقدون:

هذه الطائفة يغلب عليها عدم توفر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارة الفنية، وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر، كأثر لتصرف صاحب العمل أو المنشأة المعنية معهم، ولهذا فإنهم يكونون إما مستخدمي للنظام بوصفهم موظفين، أو مشتركين، أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة.

الفصل الثاني: سمات النصوص التشريعية للحماية من الجرائم المعلوماتية.

لا ينسب النجاح إلى أي تشريع فيما وضع لأجله إلا إذا تحققت فيه أربعة عناصر، أولها أن يؤدي الغرض الذي وضع من أجله، وثانيها أن يتم له ذلك في أقل زمن، وثالثها أن يكون ذلك الغرض قد تحقق بأقل ما يمكن من التكاليف، وآخرها ألا تكون سلبياته أكثر من إيجابياته، فإذا انعدم عنصر واحد من هذه العناصر لم يكن التشريع ناجحا ولا فعالا في ما وضع من أجله.

وفي موضوع مكافحة الجريمة فإن النجاح مرهون بالتقليل من نسب الجريمة، في زمن قياسي، مع اجتناب التكاليف الباهظة، والإفرازات السلبية التي تخلفها عملية المكافحة**[20]**.

لقد تباينت اتجاهات الدول في التعامل مع ظاهرة الجرائم المعلوماتية، فبينما توجد في بعض الدول نصوص قابلة للتطبيق على الجرائم التي ترتبط بالحاسبات الآلية، تجد دولا أخرى تعجز تشريعاتها عن التعامل مع مثل هذه الحالات، ويرجع ذلك بصفة أساسية إلى اختلاف الأنظمة القانونية لهذه الدول من ناحية، وإلى اختلاف تجربة كل منها مع الجريمة المعلوماتية من ناحية ثانية، ومن ناحية ثالثة فإن النتائج الاقتصادية التي تترتب على جرائم الحاسب الآلي تختلف من دولة لأخرى.

---

[20]- **الدكتور منصور رحماني**. "علم الإجرام والسياسة الجنائية"، دار العلوم للنشر والتوزيع، عنابة، الجزائر، 2006، ص 194-195.

المبحث الأول: مدى صلاحية نصوص القانون الجنائي التقليدية للحماية من الجرائم المعلوماتية.

لقد غيرت المعلوماتية بشكل كبير العديد من المفاهيم القانونية خاصة في القانون الجنائي، نظرا لظهور قيم حديثة ذات طبيعة خاصة، محلها معلومات ومعطيات، فقد أصبحت جريمة إفشاء بيانات الحاسوب والاعتداء عليها بالقرصنة أو الاستغلال غير المشروع، من أخطر أنواع الجرائم التي أوجدتها المعلوماتية، ويعد هذا ضربا حقيقيا ليس فقط للحقوق الخاصة بمرتكبيها، بل وأيضا مسا خطيرا بحقوق المجتمع ككل، مما ينعكس سلبا على الاقتصاد الوطني مع ما يمكن أن يرافقه من زعزعة للأمن الاجتماعي[21][21].

ولا أدل على ذلك، من أن بعض الأعمال في مجال المعلوماتية التي يبدعها بعض المؤلفين المتخصصين، مستغلين كل الإمكانيات الهائلة التي تتيحها النظم، وكذا العديد من مناصب الشغل، الشيء الذي يدفعنا إلى لفت الانتباه للخسائر التي يمكن أن تمني بها هذه الأعمال، حال تعرضها للقرصنة، والاحتيال المعلوماتي، والسرقة الإلكترونية[22][22]...

إن الاعتداء على الكيانات المادية **Hardware** للحاسوب وأجهزة الاتصال يخرج عن نطاق جرائم المعلوماتية، لأن هذه الكيانات محل صالح لتطبيق نصوص التجريم التقليدية المنظمة لجرائم السرقة، الاحتيال، النصب، خيانة الأمانة، التخريب والإتلاف... باعتبار أن هذه السلوكات تقع على مال مادي منقول، والأجهزة تنتسب إلى هذا النطاق من الوصف كمحل للجريمة.

أما ومحل الجريمة المعلوماتية مال معنوي، فهل تفلح نصوص التجريم التقليدية هذه في التصدي لهذه الأوصاف الحديثة من الجرائم؟.

المطلب الأول: مدى صلاحية نصوص قانون العقوبات.

إن المعلومة عنصر من عناصر المعرفة التي تضيف الشيء الجديد سواء يقيناً أو زوالا للشك، ويبقى العلم بالمعلومة أمر نسبي فهناك المعلومات المعروفة لدى بعض الناس دون غيرهم، ولابد من التميز بين المعلومات والبيانات المعالجة، فالعنصر الأساسي للمعلومة هو الدلالة التي تهدف لها؛ لا الدعامة التي تثبت عليها[23][23].

---

[21][21]– **حكيم سياب**. "دروس في الإعلام الآلي والقانون"، ألقيت على طلبة السنة الأولى حقوق LMD، كلية الحقوق، جامعة 20 أوت 1955 سكيكدة، الجزائر، السنة الجامعية 2008-2009.

[22][22]– أنظر الملحق.

[23][23]– **الدكتور محمد حسين منصور**. "المسئولية الالكترونية"، طبعة 2003، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2003، ص 265.

وتعتبر المعلومة أهم سلعة متداولة في العصر المعلوماتي، فلا بد من الحصول على الاحتياجات من المعلومات الصحيحة والدقيقة في الوقت المناسب، لو استغلت تجارة المعلومات ستكون دخلاً قومياً يدعم ميزانية الدول والمؤسسات المتيحة لهذه المعلومات**24[24]**.

تتعدد صور الاعتداء على المعلومات بوصفها مال معنوي، فقد يقع الاعتداء على سير نظام المعالجة الآلية للبيانات بمختلف التصرفات التدليسية، كالدخول الغير مشروع عن طريق ثغرات في نظام الحماية، أو البقاء فيه وما يترتب على ذلك من إتلاف للبيانات والبرامج، ومجرد الدخول قد يترتب عليه تعطيل البرامج أو استغلال الفرصة لزرع الفيروسات**25[25]**.

ونظرا إلى أن استغلال المعلومات يدخل اليوم في ميدان البرامج الإلكترونية، وقواعد البيانات والحاسبات الآلية، فكان لابد من وجود قوانين خاصة وحديثة تعمل على متابعة الاعتداءات الواقعة على هذه البرامج، وهذا ما فعله المشرع الجزائري عندما أضاف القسم السابع مكرر في قانون العقوبات لسنة 2004 لمعالجة المساس بالأنظمة الآلية للمعطيات**26[26]**.

والإرهاب اليوم لم يعد يقتصر على تهدد الناس في أمنهم سلامتهم الشخصية للوصال إلى أغراضه غير المشروعة؛ بل امتد ليشمل استعمال التقنية الإلكترونية لاستكمال مشروعه التدميري الكبير، ولذا فإن أي فعل يستهدف أمن الدولة واستقرار المؤسسات، وبث الرعب في أوساط السكان والاعتداء المعنوي أو الجسدي على الأشخاص وتعريض حياتهم وأمنهم للخطر، أو المساس بممتلكاتهم **بأي وسيلة كانت** يعتبر إرهاباً**27[27]**.

لكن مع قلة النصوص القانونية الخاصة بهذه الجرائم الحديثة، أيمكن الاستعانة دائما بالقواعد العامة في التجريم كمبدأ عام؟، هل هي كافية للتصدي لأخطار التعدي على برامج الحاسوب؟، أم لابد من تدعيمها بقواعد تجريمية جديدة تتناسب والطبيعة الخاصة لبيئة الحاسوب؟.

يقول الأستاذ Solarz في تعريفه للجرائم المعلوماتية: "أنه يتطلب أن يكون الفعل مما يقع ضمن نطاق قانون العقوبات وفي هذا، افتراض مسبق على شمول نصوص قانون العقوبات لأنماط السلوك الإجرامي في جرائم الحاسب الآلي، وهي مسألة لا تراعي الجدل الذي لم ينته بعد حول مدى انطباق قواعد التجريم التقليدية على هذه الأفعال، والذي حسم تقريبا لجهة عدم

---

[24]24– **حمد بن إبراهيم العمران**. مقال بعنوان، "حرية المعلومة" مجلة المعلوماتية، المملكة العربية السعودية، العدد 08، منشورة على الموقع الإنترنت،

ww.informatics.gov.sa/modules.php?

[25]25– **محمد أمين الشوابكة**. "جرائم الحاسوب والانترنت، الجريمة المعلوماتية"، طبعة 2007، دار الثقافة للنشر والتوزيع، عمان، 2007، ص 222.

[26]26– **القانون رقم 04-15** المؤرخ في 10 نوفمبر 2004 "المتضمن تعديل قانون العقوبات"، جريدة رسمية عدد 71.

[27]27– **أحمد إبراهيم مصطفى سليمان**. "الإرهاب والجريمة المنظمة"، مطبعة العشري، القاهرة، مصر، 2006، ص 31.

انطباق نصوص القانون القائمة والحاجة إلى نصوص خاصة تراعي العناصر المميزة لهذه الجرائم عن غيرها من الجرائم التي عرفها قانون العقوبات"**28**[28].

ويقول الدكتور محمود نجيب حسني: "ثمة نظريات للقسم الخاص لا صلة بينها وبين تطبيق القسم العام، ويكفي أن نشير إلى نظريات العلانية في جرائم الاعتبار (الفعل الفاضح والسب)، والضرر في جرائم التزوير، والحيازة في السرقة والتدليس في النصب... لقد أنتجت دراسة القسم الخاص نظريات لا تقل من حيث الخصوبة عن نظريات القسم العام... وعليه، يمكن القول بوجود نظريات عامة للقسم الخاص في مجال جرائم المعلوماتية"**29**[29].

المطلب الثاني: مدى صلاحية نصوص قانون الإجراءات الجزائية.

إن كانت متابعة الجرائم المعلوماتية والكشف عنها وإقامة الدليل عليها من الصعوبة بمكان، حيث أن هذه الجرائم لا تترك أثرا، إذ ليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في ملفات وسجلات.

معظم الجرائم المعلوماتية تم اكتشافها بالصدفة، وبعد وقت طويل من ارتكابها، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها.

إذ الدليل القانوني هو ما يستمد من أعمال التحقيق الذي يختلف بطبيعته عن أعمال الاستدلال التي لا يتولد عنها أدلة بالمعنى القانوني، ولا يجوز أن يكون سند القاضي في الحكم أدلة وردت في محضر الاستدلال.

ولكن يمد النيابة العامة بما يسمح برفع الدعوى الجنائية بناء على هذه الأدلة كأساس للتحقيق الذي يستخلص منه الدليل في معناه القانوني**30**[30].

فعلى الأجهزة الأمنية أن تتعامل مع تطبيقات الحياة المعلوماتية الحديثة، من الأجهزة الرقمية التي يمكن أن تستخدم في الأنشطة الإجرامية، لذلك لابد لهم من إتباع معايير محددة، وليس بناء على خبرات سابقة من قضايا مختلفة، لأن استخلاص الأدلة الدقيقة الشرعية والقانونية،

---

[28][28]– **يونس عرب.** "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت"، الجزء الأول، الطبعة الأولى، المرجع السابق، ص 16 وما بعدها.

[29][29]– **الأستاذ الدكتور محمود نجيب حسني.** "شرح قانون العقوبات، القسم الخاص"، دار النهضة العربية، القاهرة، مصر، 1992. ص 4.

[30][30]– **راجع في ذلك:**

– **الدكتور أحمد فتحي سرور.** "الوسيط في قانون الإجراءات الجنائية"، دار النهضة العربية، القاهرة، مصر، دون الإشارة لتاريخ النشر، ص 340 وما بعدها.

– **الدكتور محمود نجيب حسني.** "شرح قانون الإجراءات الجنائية"، دار النهضة العربية، القاهرة، مصر، دون الإشارة لتاريخ النشر، ص 400 وما بعدها.

يتطلب إتباع أساليب محددة لا تسمح بأي انحراف أو تعديل، تؤدي في النهاية إلى القبض على الجناة وتقديمهم للمحاكمة**31**.**[31]**

في هذا الإطار ظهر علم التحليل والتحري الجنائي للأدلة الرقمية كأحد العلوم الحديثة، فإدارات الأدلة الجنائية والأجهزة الأمنية، أصبحت مضطرة للتعامل مع التكنولوجيا الرقمية الحديثة.

إن عملية التحري الرقمي تختلف عن التحري في الجرائم المعتادة، لأنها تتعامل مع وسائط وأجهزة رقمية وأدلة غير ملموسة، وعلى أجهزة التحري أو مسؤولي أمن المعلومات مثلا تحديد من قام باختراق النظام؟، وكيف تم هذا الاختراق؟، وما هي الأضرار الناتجة عن هذا الاختراق؟، كل ذلك وفقا لمعايير وأطر عملية تمنع فقدان ومسح الأدلة.

هذه الأسئلة من المهم الإجابة عنها لأنها سوف تستخدم لتدعيم الإجراءات الجزائية والمدنية والإدارية ضد مرتكبي الجرائم المعلوماتية، فالحصول على أدلة رقمية ذات فائدة سوف، يوفر الوقت والموارد البشرية والمالية، بل أن الدور الفعال للمعايير والأطر في بناء منهجية تحتوي على خطوات ومحددات، يؤدي بناؤها وتعميمها من قبل مختلف الدول إلى إدارة ناجحة للجرائم والتحريات الرقمية، وحفظ للتكاليف، ونقل للتجارب والخبرات. وهذه بعض النماذج لبعض محاولات إيجاد أنظمة التعامل مع الجرائم المعلوماتية.

نماذج عن بعض المشاريع والدراسات لوضع إطار عملي للتعامل مع الجرائم المعلوماتية:

1- من هذه النماذج **Mandia and prosis** اللذان قاما بوضع إطار عملي للتعامل الفني مع جرائم المعلوماتية، ويشتمل هذا الإطار على الإعدادات الأولية لما قبل الحدث، الاستجابة الأولية، ثم صياغة إستراتيجية الاستجابة، التحقيق والتحري، تطبيق المقاييس الأمنية، فحص الشبكة، الاستدعاء، كتابة التقرير والنتائج، وأخيرا المتابعة.

وقد اشتمل هذا الإطار على تفاصيل دقيقة في تحليل أنظمة التشغيل مثل ويندوز وليونكس وغيرهما.

2- قامت وزارة العدل الأميركية أيضا بوضع إطار عملي حدد خطوات أساسية عدة تشتمل على أنشطة فرعية وعلى جمع الأدلة، ثم فحصها ومن ثم التحليل وأخيرا كتابة النتائج في تقرير.

هذا النموذج يتميز بأنه يوضح أنواع الأدلة والمعلومات المستخلصة منها، وأماكن وجود هذه المعلومات في الأجهزة وأنظمة المعلومات المختلفة، كما أنه يربط كل مجموعة من المعلومات بنوع محدد من جرائم المعلوماتية، فمثلا يحدد هذا النموذج قائمة بالأماكن المعتادة التي يمكن

---

[31][31]- **الدكتور سلطان محيا الديحاني**. جامعة الكويت، مقال بعنوان، "معايير وأطر عملية في إدارة الجرائم والتحريات الرقمية، التحري وجمع الأدلة في مجال الجرائم المعلوماتية"، منشور على موقع الإنترنت، www.atsdp.com

العثور فيها على الملفات المخفية والملغاة، وأيضا يحدد أنواع المعلومات الأخرى، مثل الصور وكلمات السر وأرقام الهويات، مثل رقم الضمان الاجتماعي، وهذه المعلومات بالذات مفيدة في التحري، بأنواع محددة من جرائم المعلوماتية مثل التعدي على الهويات والصور الفاضحة، فالتعرف على أنواع المعلومات المفيدة وأماكن إخفائها في الأجهزة الرقمية المختلفة، يعتبر خطوة إيجابية تساعد على تقديم أدلة قانونية يعتد بها عند تقديم الجناة للمحاكمة أمام القضاء.

3- قام كل من الدكتور محمد بن عبد الله القاسم والدكتور رشيد بن مسفر الزهراني بدراسة تحت عنوان **"نموذج وطني مقترح للتعامل مع جرائم المعلوماتية بالمملكة العربية السعودية"32[32].** إذ حاولا من خلالها طرح نموذج للتعامل مع جرائم تقنية المعلومات في المملكة العربية السعودية، إذ حدد هذا النموذج عدة مسائل مهمة في مجال الجريمة المعلوماتية ومكافحتها نوجزها في الآتي:

1- مسارات الجريمة وأنماطها ومنافذها.

2- دور الجهات المختلفة –حكومية، أهلية- في منظومة التعامل مع تلك الجرائم.

3- أسلوب متكامل للتعامل مع الجرائم قبل وبعد وقوعها.

4- متطلبات تنفيذ النموذج على المستويين الفني والتنظيمي.

والحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود، وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني والدولي**33[33].**

---

[32]32- **الدكتور محمد بن عبد الله القاسم و الدكتور رشيد بن مسفر الزهراني.** دراسة بعنوان، **"**نموذج وطني مقترح للتعامل مع جرائم المعلوماتية بالمملكة العربية السعودية"، الدراسة منشورة على موقع الإنترنت، www.arablawinfo.com

[33]33- حول المسائل الإجرائية لجرائم الكمبيوتر والإنترنت أنظر بالعربية:

- **يونس عرب.** "جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات"، المرجع السابق. ص 43 وما بعدها.

- اتفاقية المجلس الأوروبي "لحماية الأشخاص بشأن المعالجة الآلية للبيانات الشخصية" المؤرخة سنة 1981.

- "الاتفاقية الأوربية المتعلقة بالتعاون الدولي في مجال مكافحة جرائم الإنترنت"، الموقعة في بودابست في 23-11-2001.

- **الدكتور هلالي عبد الإله أحمد.** "تفتيش نظم الحاسب الآلي"، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 1997.

-Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age ,by :Tom Douglas Brian Loader, Thomas Douglas,1st edition, Routledge, 2000.

-Digital Evidence and Computer Crime, by :Eoghan Casey, 1st edition Academic Pr. 2000.

-Criminal Profiling: An Introduction to Behavioral Evidence Analysis, by :Brent E. Turvey, Diana Tamlyn, Jerry Chisum , 1 edition , Academic Press Limited 1999.

-Fighting Computer Crime: A New Framework for Protecting Information, by :Donn B. Parker, 1 edition, John Wiley & Sons 1998.

-Information Warfare Principles and Operations, by :Edward Waltz 1998.

-Cyber Crime: How to Protect Yourself from Computer Criminals by :Laura E. Quarantiello, Tiare Publications, 1996.

وتبدو أكثر المشكلات جسامة لا في مجال صعوبة اكتشاف وإثبات جرائم الحاسب بل وفي دراسة هذه الظاهرة في مجملها هي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة، وهو ما يعرف بالرقم الأسود **Black Number34[34]**. حيث لا يعلم ضحايا هذه الجرائم شيئا عنها إلا عندما تكون أنظمتهم المعلوماتية هدفا لفعل غير مشروع، أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل**35[35]**.

ويلزم للمجتمع المعلوماتي في مجال قانون الإجراءات الجزائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق في مجال جرائم المعلوماتية.

المبحث الثاني: مدى حماية الأموال المعنوية من الجرائم المعلوماتية بمقتضى القوانين الخاصة.

نبين ذلك في مطلبين، الأول نخصصه لمدى حماية القانون المدني للتعاملات باستعمال المعلوماتية، والثاني لمدى حماية نصوص قانون الملكية الفكرية، لمنتجات المعلوماتية (برامج، بيانات...)

المطلب الأول: مدى الحماية بموجب القانون المدني.

لقد جرى العرف واستقر العمل على تدوين المحررات الرسمية والعرفية على الأوراق وبالحروف الخاصة بلغة المتعاقدين أو اللغة التي يعتمدانها لتحرير العقد، فإن اللجوء إلى تدوين المحررات على وسائط إلكترونية من خلال ومضات كهربائية**36[36]**، وتحويلها إلى اللغة التي يفهمها الحاسب الآلي، يثير التساؤل عن مدى اعتبار المحرر الإلكتروني من قبيل الكتابة**37[37]**.

34[34] – **Dr. j. Francillon** .Les crimes informatiques et dautres crimes dans le domaine de la technologie informatique en france Rev. int pen, 1990, vol 64, p 293.

35[35] – في إحدى الوقائع الشهيرة تعرض بنك Marchant bank city في بريطانيا لنقل 8 مليون جنيه من أحد أرصدته إلى رقم حساب في سويسرا، وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور، ولكن البنك بدل الإدعاء على الفاعل، قام بدفع مبلغ مليون جنيه له، بشرط عدم إعلام الآخرين عن جريمته، وشريطة إعلام البنك عن الآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحاسوب البنك الرئيس.

– راجع في ذلك أيضا:

– **يونس عرب**. "جرائم الحاسوب، دراسة مقارنة"، المرجع السابق، ص 72.

36[36] – لتفصيل أكثر أنظر **المستشار هشام محمد عبد الوهاب**. مدير إدارة تراخيص التوقيع الإلكتروني لهيئة تنمية صناعة تكنولوجيا المعلومات، مقال بعنوان، "الضوابط الفنية والتقنية لإضفاء ذات الحجية القانونية للتوقيعات الإلكترونية"، موجود على موقع الإنترنت:

www.electronicsignature.gov.eg

37[37] – **عمر أنجوم**. "الحجية القانونية لوسائل الاتصال الحديثة، دراسة تحليلية في نظام الإثبات المدني"، أطروحة دكتوراه في الحقوق، جامعة الحسن الثاني، عين الشق، المغرب، السنة الجامعة 2004/2003 ص 137.

فمن الجدير بالتأكيد أنه ليس هناك في القانون أو في اللغة ما يلزم بالاعتقاد في أن الكتابة لا تكون إلا على الورق، وتأكد هذا المعنى في مرجع **LAMY** في قانون المعلوماتية، حيث أشار إلى أن المشرع لم يشر إلى دعامة من نوعية معينة، هذا وتأكيدا لما سبق فإن الكثير من الاتفاقيات الدولية تتبنى هذا الرأي ومنها على سبيل المثال، اتفاقية الأمم المتحدة بشأن النقل الدولي للبضائع لسنة 1981 التي تنص المادة 13 منها على أنه، "فيما يخص أغراض هذه الاتفاقية ينصرف مصطلح الكتابة أيضا على المراسلات الموجهة في شكل برقية أو تلكس"**38[38]**، لذلك يتضح أن الكتابة لا ينظر إليها من حيث ارتباطها بالدعامة أو الوسيط المستخدم في التدوين على دعامة مادية محددة، بل بوظيفتها في إعداد الدليل على وجود التصرف القانوني وتحديد مضمونها بما يمكن الأطراف من الرجوع إليه في حالة نشوب خلاف وقد اتفق الفقه أنه وحتى تقوم الكتابة بهذا الدور فلابد أن يكون الوسيط مقروءا وأن تتصف الكتابة المدونة عليه بالاستمرارية والثبات.

لذلك وحتى يمكن الاحتجاج بمضمون المحرر المكتوب في مواجهة الآخرين فإن المحرر يجب أن يكون مقروءا، وبالتالي يجب أن يكون مدونا بحروف أو رموز معروفة ومفهومة للشخص الذي يراد الاحتجاج عليه بهذا المحرر، فإذا ما رجعنا إلى المحررات الإلكترونية نجد أنه يتم تدوينها على الوسائط بلغة الآلة، فلا يمكن أن يراها الإنسان بشكل مباشر، وإنما لابد من إيصال المعلومات في الحاسب الآلي الذي يتم دعمه ببرامج لها القدرة على ترجمة لغة الآلة إلى اللغة المقروءة للإنسان، وبالنظر إلى أنه يضمن قراءة هذه المحررات في جميع الأحوال باستخدام الحاسب الآلي، وهو ما يعني استيفاءها للشرط المتعلق بإمكان القراءة والفهم طالما أن اللغة التي تظهر على الشاشة هي لغة مفهومة ومقروءة**39[39]**.

ورغم ذلك، وتأكيدا لما سبق ذكره فإن منظمة المواصفات العالمية **ISO** وبخصوص المواصفات الخاصة بالمحررات أكدت أن المحرر هو: **"مجموعة المعلومات والبيانات المدونة على دعامة مادية... يسهل قراءتها عن طريق الإنسان أو باستخدام آلة مخصصة لذلك"40[40]**.

وأضاف المشرع الفرنسي في شأن الإثبات عن طريق الوسائل الإلكترونية نص المادة 1316 من القانون المدني، والتي عرفت المحرر المستخدم في الإثبات بأنه: **"كل تتابع للحروف أو**

---

[38]**38**- عمر أنجوم: المرجع نفسه، ص: 140

[39]**39**– **حسن عبد الباسط جميعي**. "إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنيت"، دار النهضة العربية، القاهرة، مصر، 2000، ص 19-20.

[40]**40**- **محمد أخياط**. مقال بعنوان، "بعض التحديات القانونية التي تثيرها التجارة الالكترونية"، منشور بمجلة الإشعاع، العدد 25، 2002، المغرب، ص 14-15.

الرموز أو الأرقام أو أي إشارات أخرى تدل على المقصود منها ويستطيع الغير أن يفهمها..."

بالإضافة على اشتراط كون المحرر الكتابي مقروءا، يشترط أيضا للاعتداد بالكتابة في الإثبات أن يتم التدوين على وسط يسمح بثبات الكتابة عليه واستمرارها، بحيث يمكن الرجوع إلى المحرر كلما كان ذلك لازما، لمراجعة التصرف أو لعرضه على القضاء عند حدوث خلاف بين أطرافه**41[41]**.

المطلب الثاني: مدى الحماية بموجب قانون الملكية الفكرية والحقوق المجاورة.

تعتبر المعلومة حسب الأصل العام من الأمور التي لا يمكن الاستئثار بها، ويمكن للجميع الاستفادة منها والتعامل بها، ومن هنا نشأت فكرة الحق في المعلومات، وبما أن المعلومة هي مجموعة من البيانات والدلالات التي تفيد في تحقيق نتيجة معينة، فيمكن لبعض الناس أن يستعمل المعلومات بشكل مطور يظهر فيه شخصيته، أو يسخر المعلومة من أجل أن يصل إلى اختراع جديد؛ ففي هذه الأحوال وأخرى لابد من حمايتها تتعدد صور حماية المعلومات؛ فيمكن حمايتها بموجب قوانين حقوق الملكية الفكرية، خاصة قانون حقوق المؤلف، حيث نظم المشرع الجزائري قانوناً جديداً لحقوق المؤلف يتماشى مع التطورات السائدة في ميدان المعلوماتية**42[42]**، ويمكن أن تتم الحماية من خلال قانون براءة الاختراع،

---

[41][41]– لمزيد من التفصيل في حجية الإثبات عن طريق الوسائط الإلكترونية راجع كل من:

– **إبراهيم الدسوقي أبو الليل**. "الجوانب القانونية للتعاملات الإلكترونية، دراسة للجوانب القانونية للتعامل عبر أجهزة الاتصال الحديثة التراسل الإلكتروني"، الطبعة الأولى، لجنة التأليف والتعريب والنشر، جامعة الكويت، الكويت، 2003، ص 32 ومابعدها.

– **إدريس العلوى العبدلاوى**. "وسائل الإثبات في التشريع المغربي"، طبعة 1977، مطبعة النجاح الجديدة، المغرب، 1977، ص 120 وما بعدها.

– **عبد الرزاق السنهوري**. "الوسيط في شرح القانون المدني. نظرية الالتزام بوجه عام"، الجزء الثاني، دار النهضة العربية، القاهرة، مصر، 1964. ص420.

– **محمد محمود لطفي**. "استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامها"، دون الإشارة لدار النشر، 1993، القاهرة، مصر، ص23.

– **حسن عبد الباسط جميعي**. "إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت"، طبعة 2000، دار النهضة العربية، القاهرة، مصر، 2000، ص61 وما بعدها.

– **حاجى صليحة**. "الوفاء الرقمي عبر الإنترنت، المظاهر القانونية"، أطروحة لنيل الدكتوراه في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، وجدة، المغرب، السنة الجامعية 2004–2005، ص 151.

– **محمد السعيد رشدي**. "التعاقد بوسائل الاتصال الحديثة ومدى حجتها في الإثبات"، منشأة المعارف، الإسكندرية، مصر، 2005.

– **أحمد شرف الدين**. "عقود التجارة الإلكترونية (تكوين العقد وإثباته)"، دروس مقدمة لطلبة الدكتوراه، دبلومي القانون الخاص وقانون التجارة الدولية، جامعة عين شمس، مصر، 2004.

– **حسن عبد الباسط جميعي**. "إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت"، دار النهضة العربية، القاهرة، مصر، 2000.

[42][42]– بموجب الأمر 03–05 المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف و الحقوق المجاورة.

والذي حرص فيه المشرع الجزائري على حماية صاحب البراءة، واعتبار أن كل من يمس حقوق صاحب البراءة بشكل غير مشروع يعتبر معتدي، وتتشكل جريمة التقليد**43**.**[43]**

الخاتمة.

إن ظاهرة الجرائم المعلوماتية، ظاهرة إجرامية مستجدة نسبياً؛ تقرع في جنباتها أجراس الخطر لتُنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، (بيانات، معلومات، برامج بكافة أنواعها)، فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسوب.

وهذا وحده – عبر دلالته العامة – يظهر مدى خطورة الجرائم المعلوماتية، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية، وتهدد إبداع العقل البشري.

لذا فإن إدراك ماهية جرائم المعلوماتية، والطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعتها؛ وخصائصها؛ ومخاطرها؛ وحجم الخسائر الناجم عنها وسمات مرتكبيها ودوافعهم، يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة، ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية.

وإذا كانت مجتمعاتنا العربية لم تتأثر بعد بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام، فإن خطر الجرائم المعلوماتية المحتمل في البيئة العربية، يمكن أن يكون كبيراً باعتبار أن الجاهزية التقنية والتشريعية والأدائية (استراتيجيات حماية المعلومات) لمواجهتها ليست بالمستوى المطلوب، إن لم تكن غائبة تماماً، وبالمقابل فقد أمست جرائم المعلوماتية من أخطر الجرائم التي تقترف في الدول المتقدمة، تحديداً الأمريكية والأوروبية، ولهذا تزايدت خطط مكافحة هذه الجرائم، وانصبت الجهود على دراستها المعمقة وخلق آليات قانونية للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية خاصة المنظمات والهيئات الإقليمية الأوروبية، وإدراكاً لقصور التشريعات الجنائية بما تتضمنه من نصوص التجريم التقليدية كان لابد للعديد من الدول من وضع قوانين وتشريعات خاصة بهذه الظاهرة.

خلاصة القول أن الجرائم المعلوماتية وإن كانت تبدو أنها منظمة بشكل كافي من طرف المشرع الجزائري، إلا أنها تثير العديد من الصعوبات، وخصوصا ما يتعلق بالإثبات؛ وشخص الجاني؛ وخصوصا حينما يكون مقيما خارج الدولة، لأنه من الصعب تحديد المسؤول جنائيا، ويظهر ذلك جليا في حالة وقوع جريمة على شبكة الإنترنت، لذلك يجب

---

[43][43]– بموجب الأمر 03-07 المؤرخ في 19 جويلية 2003 المتعلق ببراءات الاختراع.

على المشرع ألا يكون قاصرا على تنظيم ما هو موضوعي فقط، وإنما عليه أن يصاحب ما هو موضوعي بما هو إجرائي لكي يتم تحقيق نوع من التوازن بين الحق وطريق الوصول إليه (حمايته).

التوصيـــــات

نخلص من هذا العرض إلى حقيقة أن الجرائم المعلوماتية عمل أو سلوك غير شرعي ينتظر فرصة فنية للوثوب على الضحية، أو ثغرة قانونية للإفلات من طائلة العقاب، أو حتى إجراء إداري غير مدروس للتغلغل في شبكة الإدارة المستهدفة، وتحقيق غايات تخدم مرتكبه. ومن خلال منطلقات وأهداف البحث، ومن خلاصة ما توصلنا يمكن تصنيف جملة من التوصيات العامة التي قد تساهم في التقليل من الآثار السلبية لكثير من التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، وتندرج هذه التوصيات تحت المحاور الثلاث الآتية:

أولاً: في مجال التعليم والتدريب.

إنشاء معاهد دولية وإقليمي ووطنية؛ متخصص في التدريب على التحقيق في الجرائم التقنية المعاصرة، والنظر في تضمين مناهج التحقيق الجنائي في المعاهد والكليات.

تشجيع الباحثين في هذا المجال بالدعم المعنوي والمادي، لإجراء المزيد من البحوث والدراسات حول الجرائم المعلوماتية.

عقد دورات مكثفة للعاملين في حقل التحقيق، والمرافعات، حول المعلوماتية والجرائم المرتبطة بها.

خلق ثقافة اجتماعية جديدة تصور جرائم المعلوماتية على أنها أعمال غير مشروعة مثلها مثل أنماط الجريمة الأخرى، والتأكيد على أن المجرم المعلوماتي يستهدف الإضرار بالآخرين، ويستحق العقوبة بدل نظرات وعبارات الإعجاب.

ثانياً: في مجال التشريعات والأنظمة.

مبدأ الوقاية في جرائم المعلوماتية خير من العلاج، وبشكل خاص فيما يتعلق بالتشريعات.

إدراك أن الجرائم المعلوماتية ذات بعد دولي تتطلب الانخراط في اتفاقيات دولية، والاهتمام بالتعاون الدولي في مجال المكافحة.

إعطاء جرائم المعلوماتية حقها من الأهمية في مؤسسات التشريع الوطنية، وإدراجها ضمن التشريعات الوطنية المختلفة.

تعديل بعض التشريعات الحالية بما يتلاءم مع طبيعة جرائم المعلوماتية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح.

ثالثاً: في مجال الإجراءات الفنية والإدارية.

مساعدة شركات التقنية والمعلوماتية في اتخاذ إجراءات أمنية مناسبة سواء من حيث سلامة المنشآت، أو ما يخص قواعد حماية الأجهزة والبرامج.

مساعدة شركات إنتاج البرامج العربية في مجال تطوير أنظمة التشغيل، وبرامج تطبيقات عربية، وكذلك برامج حماية عربية للتخفيف من الاعتماد على الصادرات في هذا المجال مع ما تحمله من مخاطر أمنية محتملة.

وضع سياسات عمل، وإجراءات إدارية وفنية، واضحة فيما يختص بأمن المعلومات، والحرص على أن يطلع عليها العاملون في الإدارة.

أهمية المرونة المالية في شراء العتاد، والبرمجيات التي تكفل بناء، وصيانة أنظمة، وشبكات معلومات متكاملة تتوفر لها الحماية في جميع الأوقات.

عقد اجتماعات دورية للمسؤولين عن تقنية المعلومات، لتبادل الخبرات، والمعلومات فيما يختص بأمن المعلومات وجرائم المعلوماتية.

إعادة رسم الأولويات الوطنية مع التأكيد على أن المعلومات في عصر المعلومات ثروة وطنية تستحق كل الجهود، والموارد المالية والبشرية للمحافظة عليها وصيانتها.

إن تطبيق هذه التوصيات مرهون بالتشريعات المحلية والالتزامات الدولية، مع الأخذ في الحسبان الحماية المناسبة لحقوق الأفراد، ويجب قدر الإمكان تطبيق هذه التوصيات بطريقة تجنب أو تقليل من تنازع قوانين الدول المختلفة، وهو ما يمثل غالباً العقبة الأساسية في مواجهة التعاون الدولي لأجهزة الأمن.

"إن أكبر خدمة للإنسانية يمكن أن يقدمها الباحث القانوني في هذا العصر، هي إيجاد نظرية عامة لقانون المعلوماتية".

الملحق رقم 01

جدول: خسائر جرائم المعلوماتية وفق الدراسة للأعوام من 97 حتى 2001

2001	2000	1999	1998	1997	مصدر الخسائر / الجريمة ونوع الهجوم
151,230,100	66,708,000	42,496,000	33,545,000	20,48,000	**Theft of proprietary info.** سرقة المعلومات المتعلقة بالملكية
5,183,100	27,148,000	4,421,000	2,142,000	4,285,850	**Sabotage of data networks** إتلاف او تخريب معطيات الشبكات
886,000	991,200	765,000	562,000	1,181,000	**Telecom eavesdropping** تصنت الشبكات
19,066,600	7,885,000	2,885,000	1,637,000	2,911,700	**System Penetration by outsider** اختراق النظام من الخارج
35,001,650	27,984,740	7,576,000	3,720,000	1,006,750	**Insider abuse of Net access** إساءة الدخول للشبكة من داخل المنشأة
92,935,500	55,996,000	39,706,000	11,239,000	24,892,000	**Financial Fraud** الاحتيال المالي
4,283,600	8,247,500	3,255,000	2,787,000	N/a	**Denial of Service** انكار الخدمة
N/a	N/a	N/a	N/a	512,000	**Spoofing** التلاعب والخداع بطريق سبوفنغ
45,288,150	29,171,700	5,274,000	7,874,000	12,498,150	**Virus** الفايروسات
6,064,000	22,554,500	3,567,000	50,565,000	3,991,605	**Unauthorized insider Access** الدخول غير المصرح به من الداخل
9,041,000	4,028,000	773,000	17,256,000	22,660,300	**Telecom Fraud** احتيال الاتصال
0	5,000,000	20,000	245,000	N/a	**Active Wiretapping** استراق السمع – المادي -
8,849,000	10,404,300	13,038,000	5,250,000	6,132,200	**Laptop Theft** سرقة الحاسوب المحمول
377,828,700	**265,586,24**	**123,799,00**	**136,822,00**	**100,119,55**	المجموع

قائـــمة المراجـــع:

1- الأمر رقم 66-156 المؤرخ في 18 صفر1386 الموافق ل 08 جوان 1966 المتضمن قانون العقوبات الجزائري المعدل و المتمم.

2- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات، جريدة رسمية عدد 71.

3- الأمر 03-05 الموافق ل 19 جويلية 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة.

4- الأمر 03-07 الموافق ل 19 جويلية 2003 المتعلق ببراءات الاختراع.

5- القانون المدني الفرنسي.

6- اتفاقية المجلس الأوروبي عام 1981 "لحماية الأشخاص بشأن المعالجة الآلية للبيانات الشخصية".

7- "الاتفاقية الأوربية المتعلقة بالتعاون الدولي في مجال مكافحة جرائم الإنترنت"، **الموقعة في بودابست في** 23-11-2001.

8- **الدكتور محمد بوشيبة.** "حماية برامج الحاسوب طبقا لقانون 00- 02 المنظم لحقوق المؤلف والحقوق المجاورة"، مجلة القضاء والقانون، المغرب، 2000.

9- **الدكتور محمود سرى طه.** "الكمبيوتر فى مجالات الحياة"، الهيئة المصرية العامة للكتاب، القاهرة، مصر، 1990.

10- **الدكتور هشام محمد فريد رستم.** "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، أسيوط، مصر، 1994.

11- **الدكتور نعيم مغبغب.** "حماية برامج الكمبيوتر" الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2006.

12- المرسوم الملكي السعودي رقم م/ 17 الصادر بتاريخ 27 أفريل 2008، المتضمن "قانون نظام مكافحة جرائم المعلوماتية السعودي".

13- **الأستاذ الدكتور محمد محيي الدين عوض.** "مشكلات السياسة الجنائية المعاصرة فى جرائم نظم المعلومات (الكمبيوتر)"، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، المنعقد بالقاهرة في الفترة 25- 28 أكتوبر 1993، حول : مشكلات المسئولية الجنائية في مجال الإضرار بالبيئة والجرائم الواقعة في مجال تكنولوجيا المعلومات، منشور ضمن أعمال المؤتمر، دار النهضة العربية، القاهرة، مصر، 1993.

14- **الأستاذ الدكتور محمود نجيب حسني.** "شرح قانون العقوبات، القسم العام، الطبعة السادسة"، دار النهضة العربية، القاهرة، مصر، 1989.

15- **الأستاذ الدكتور كامل السعيد.** "شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن"، الطبعة الثانية، دار الفكر للنشر والتوزيع، عمان، 1983.

16- **عفيفي كامل عفيفي.** "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة"، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.

17- **يونس عرب.** "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت، الجزء الأول، الطبعة الأولى"، منشورات إتحاد المصارف العربية، القاهرة، 2001.

18- **الدكتور علي عبد القادر القهوجي.** "الحماية الجنائية لبرامج الحاسب"، بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية، التي تصدرها كلية الحقوق، جامعة الإسكندرية، العدد 24، الصادر عام 1992.

19- **الدكتور منصور رحماني.** "علم الإجرام والسياسة الجنائية"، دار العلوم للنشر والتوزيع، عنابة، الجزائر، 2006.

20- **عباس الحسيني.** النجف الأشرف، العراق، مقال بعنوان، "جرائم الكمبيوتر والإنترنت" منشور على موقع الإنترنت الفريق العربي للأمن والحماية المعلوماتية www.atsdp.com

21- **الدكتور جميل عبد الباقي الصغير.** "القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي"، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992.

22- **يونس عرب.** "جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات"، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي 10-12 /2002/02.

23- **الدكتور محمود صالح العادلي.** ورقة عمل بعنوان، "الجرائم المعلوماتية، ماهيتها وصورها"، مقدمة لورشة العمل الإقليمية حول: تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط 2-4 أفريل 2006.

24- **حكيم سياب.** "دروس في الإعلام الآلي والقانون"، ألقيت على طلبة السنة الأولى حقوق نظام LMD، كلية الحقوق، جامعة 20 أوت 1955 سكيكدة، الجزائر، السنة الجامعية 2008-2009.

25- **الدكتور محمد حسين منصور.** "المسئولية الالكترونية"، طبعة 2003، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2003.

26- **حمد بن إبراهيم العمران.** مقال بعنوان، "حرية المعلومة" مجلة المعلوماتية، المملكة العربية السعودية، العدد 08، منشورة على الموقع الإنترنت، ww.informatics.gov.sa/modules.php?

27- **محمد أمين الشوابكة.** "جرائم الحاسوب والانترنت، الجريمة المعلوماتية"، طبعة سنة 2007، دار الثقافة للنشر والتوزيع، عمان، 2007.

28- **أحمد إبراهيم مصطفى سليمان.** "الإرهاب والجريمة المنظمة"، مطبعة العشري القاهرة، مصر، 2006.

29- **الأستاذ الدكتور محمود نجيب حسني.** "شرح قانون العقوبات، القسم الخاص"، دار النهضة العربية، القاهرة، مصر، 1992.

30- **الدكتور أحمد فتحي سرور.** "الوسيط في قانون الإجراءات الجنائية"، دار النهضة العربية، القاهرة، مصر، دون الإشارة لتاريخ النشر.

31- **الدكتور محمود نجيب حسني.** "شرح قانون الإجراءات الجنائية"، دار النهضة العربية، القاهرة، مصر، دون الإشارة لتاريخ النشر.

32- **الدكتور سلطان محيا الديحاني.** جامعة الكويت، مقال بعنوان، "معايير وأطر عملية في إدارة الجرائم والتحريات الرقمية، التحري وجمع الأدلة في مجال الجرائم المعلوماتية"، منشور على موقع الإنترنت، www.atsdp.com

33- **الدكتور محمد بن عبد الله القاسم و الدكتور رشيد بن مسفر الزهراني.** دراسة بعنوان، **"**نموذج وطني مقترح للتعامل مع جرائم المعلوماتية بالمملكة العربية السعودية"، الدراسة منشورة على موقع الإنترنت، www.arablawinfo.com

34- **الدكتور هلالي عبد الإله أحمد.** "تفتيش نظم الحاسب الآلي"، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 1997.

35- **مقال المستشار هشام محمد عبد الوهاب.** مدير إدارة تراخيص التوقيع الإلكتروني لهيئة تنمية صناعة تكنولوجيا المعلومات، بعنوان، "الضوابط الفنية والتقنية لإضفاء ذات الحجية القانونية للتوقيعات الإلكترونية"، موجود على موقع الإنترنت:

www.electronicsignature.gov.eg

36- **عمر أنجوم.** "الحجية القانونية لوسائل الاتصال الحديثة، دراسة تحليلية في نظام الإثبات المدني"، أطروحة دكتوراه في الحقوق، جامعة الحسن الثاني، عين الشق، السنة الجامعة 2004/2003.

37- **حسن عبد الباسط جميعي.** "إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنيت"، دار النهضة العربية، القاهرة، مصر، 2000.

38- **محمد أخياط.** مقال بعنوان، "بعض التحديات القانونية التي تثيرها التجارة الالكترونية"، منشور بمجلة الإشعاع، العدد 25، 2002، المغرب.

39- **إبراهيم الدسوقي أبو الليل.** "الجوانب القانونية للتعاملات الإلكترونية، دراسة للجوانب القانونية للتعامل عبر أجهزة الاتصال الحديثة التراسل الإلكتروني"، الطبعة الأولى، لجنة التأليف والتعريب والنشر، جامعة الكويت، الكويت، 2003.

40- **إدريس العلوى العبدلاوى.** "وسائل الإثبات في التشريع المغربي"، طبعه 1977، مطبعة النجاح الجديدة، 1977، المغرب.

41- **عبد الرزاق السنهوري.** "الوسيط في شرح القانون المدني. نظرية الالتزام بوجه عام"، الجزء الثاني، دار النهضة العربية، القاهرة، مصر، 1964.

42- **محمد محمود لطفي.** "استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامها"، دون الإشارة لدار النشر، القاهرة، مصر، 1993.

43- **حسن عبد الباسط جميعي.** "إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت"، طبعة 2000، دار النهضة العربية، القاهرة، مصر، 2000.

44- **حاجى صليحة.** "الوفاء الرقمي عبر الإنترنت، المظاهر القانونية"، أطروحة لنيل الدكتوراه في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، وجدة السنة الجامعية 2004-2005.

45- **محمد السعيد رشدي.** "التعاقد بوسائل الاتصال الحديثة ومدى حجتها في الإثبات"، منشأة المعارف، الإسكندرية، مصر، 2005.

46- **أحمد شرف الدين.** "عقود التجارة الإلكترونية (تكوين العقد وإثباته)"، دروس الدكتوراه دبلومي القانون الخاص وقانون التجارة الدولية، جامعة عين شمس، مصر، 2004.

47- **حسن عبد الباسط جميعي.** "إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت"، دار النهضة العربية، القاهرة، مصر، 2000.

-Pieere Catala, Ebauche Duune. " Théorie Juridique d'Information", 1983, paries.

-Andre Lucas, "Protiction of information Bases", Kuwait First Conference, Ministry of Justice -15-17 Feb, 1999, Kuwait.

-Tom Douglas Brian Loader, Thomas Douglas, Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age, 1st edition, Routledge, 2000.

-Eoghan Casey Digital Evidence and Computer Crime, 1st edition Academic Pr. 2000.

-Brent E. Turvey, Diana Tamlyn, Jerry Chisum Criminal Profiling: An Introduction to Behavioral Evidence Analysis, 1 edition, Academic Press Limited 1999.

-**Donn B. Parker** Fighting Computer Crime: A New Framework for Protecting Information, 1 edition, John Wiley & Sons 1998.

-**Edward Waltz** Information Warfare Principles and Operations, 1998.

-**Laura E. Quarantiello** Cyber Crime: How to Protect Yourself from Computer Criminals, Tiare Publications, 1996.

-**Dr. j. Francillon** .Les crimes informatiques et dautres crimes dans le domaine de la technologie informatique en france Rev. int pen, 1990, vol 64, p 293.