# ضرورة تجريم الاعتداء على البريد الإلكتروني

الدكتور عبد الحليم بن مشري
كلـــــية الحقـــــوق والعلـــــوم السيـــــاسية
جامعة محمد خيضر بسكرة

**مقدمة:**

إن التطور الهائل في الحياة السيبيرية قابله أيضا تطور تقنيات عدد كبير من الجرائم التقليدية، حيث أصبحت ترتكب بشكل أسهل وبأقل جهد، ناهيك عن ظهور جرائم جديدة مرتبطة أساسا بهذا الفضاء الافتراضي، حيث أن الإحصائيات تشير إلى أرقام مخيفة(**1**)، وتكمن خطورة هذه الجرائم بداية في مرتكبيها الذين يتسمون بالذكاء، حيث أنهم يستعملون وسائل التدمير الناعمة كالفيروسات والقنابل المنطقية، ولا يلجؤون إلى العنف كما هو الحال في الإجرام التقليدي(**2**)، فهذا المجرم يكون في العادة خبيرا في أنظمة المعالجة المعلوماتية الأمر الذي يصعب من إمكانية تعقبه. كما أن الجرائم المعلوماتية التي تنصب بالأساس على البيانات ذات الطبيعة غير المادية تطرح العديد من المشاكل على المستوى العملي من حيث إثباتها وتعقب مرتكبيها، خاصة وأن الأدلة في هذا المجال سهلة المحو والإخفاء في زمن قصير جدا، كما أن المجرم يرتكب أفعاله عن بعد عبر الشبكة ولا يحتاج إلى التنقل إلى مسرح الجريمة(**3**). وما يزيد في صعوبة مكافحة هذه الجرائم هو عدم التبليغ عن وقوعها، والسبب في ذلك يرجع إلى عدم اكتشافها أو عدم العلم بوقوعها أصلا، فقد قدرت إحدى الدراسات أن حوالي 80 % من ضحايا جرائم الكمبيوتر لا يعلمون بأن أنظمتهم قد اخترقت(**4**). بالإضافة إلى عدم وجود أجهزة كافية ومتخصصة في البحث والحري والتحقيق في هذا النوع من الجرائم، ذلك أن جرائم الكمبيوتر والانترنت تحتاج للكشف عنها وإثباتها ومعاقبة مرتكبيها إلى أشخاص متخصصين في الإعلام الآلي والانترنت، وعلى دراية كافية بكل برامج القرصنة والفيروسات، كما يجب عليهم أن يحسنوا استعمال أجهزة ذات تقنيات عالية من أجل تعقب وضبط المجرمين(**5**).

ولأن البريد الإلكتروني يعتبر أحد أهم مفرزات الشبكة العنكبوتية، فإن أهميته تزداد يوما بعد يوم بازدياد عدد المتصلين بهاته الشبكة، حيث أصبحت هذه الوسيلة على ما توفره من تسهيل الاتصال بين الأشخاص والمؤسسات، لا غنى عنها في الكثير من المجالات، فهي على صعيد

الحياة الخاصة توفر للأفراد طريقة للاتصال المكتوب كبديل للرسالة والفاكس والتلغراف، والاتصال السمعي كبديل للهاتف، وحتى الاتصال المصور بشكل مباشر وغير مباشر. أما على صعيد العمل فالبريد الإلكتروني يوفر للشركات الاتصال فيما بينها، وكذا الاتصال بالعملاء، ويوفر تبادل خطط وبرامج العمل، ويمكن من إبرام العقود والصفقات والاطلاع على التصاميم المختلفة، وهو الأمر ذاته على الصعيد العلمي، فالبريد الإلكتروني يسهل الاتصال بين الباحثين في عمليات الإشراف والمتابعة وتبادل المعلومات والآراء، وكل هذا وأكثر في ظرف ثوان أو دقائق معدودة، وهي المدة التي تستغرقها الرسالة الإلكترونية في الانتقال من أي مكان على الأرض إلى أي مكان آخر يكون متصلا بشبكة الانترنت.

بالنظر إلى أهمية البريد الإلكتروني وخصوصية المعلومات التي قد يتضمنها من جهة، وبالنظر إلى خطورة الجرائم المرتكبة على شبكة الانترنت وصعوبة كشفها والتصدي لها من جهة أخرى، نجد أنفسنا أمام تساؤل جدي مفاده: هل وضع المشرع الجزائري نصوص قانونية كفيلة بحماية البريد الإلكتروني من كل اعتداء قد يقع عليه؟

ويتفرع عن هذا التساؤل الرئيسي مجموعة من التساؤلات الفرعية التي نوجزها فيما يلي: ما المقصود بالبريد الإلكتروني؟ وما مزاياه وعيوبه؟ وما هي الجرائم التي يمكن أن ترتكب على البريد الإلكتروني؟ وهل من مواجهة تشريعية لها في القانون الجزائري؟

للإجابة على هاته الأسئلة قسمنا موضوعنا إلى جزأين أساسيين تناولنا في الجزء الأول ماهية البريد الإلكتروني، أما الجزء الثاني فقد خصص لجرائم الاختراق والإغراق الواقعة على البريد الإلكتروني.

**أولا / ماهية البريد الإلكتروني:**

ظهر البريد الإلكتروني لأول مرة على يد العالم الأمريكي راي توملينسون Ray Tomlinson، حيث صمم على شبكة الانترنت برنامج لكتابة الرسائل يسمى Send message، وذلك لتمكين العاملين على الشبكة من تبادل الرسائل فيما بينهم، ولم ينتظر طويلا ليخترع برنامج جديد أطلق عليه تسمية Cypnet الذي يسمح بنقل الملفات من جهاز كمبيوتر إلى آخر، ثم دمج فيما بعد البرنامجين في برنامج واحد هو البريد الإلكتروني. ولأن الرسائل لم تكن تحمل اسم مرسلها فقد وضع توملنسون الرمز @ بين اسم المرسل والموقع الذي ترسل منه الرسالة ليخرج في خريف 1971 أول عنوان بريد إلكتروني في التاريخ وهو: Tomlinson@bbn-tenexa. وقد عرف البريد الإلكتروني في بلده الأصلي الولايات المتحدة

الأمريكية بتسمية E . Mail وهي اختصار للعبارة Electronic Mail، وترجم في اللغة الفرنسية إلى Courrier électronique، وقد عرف البريد الإلكتروني تعديلات وإضافات كثيرة، حيث ظهر البريد الإلكتروني الصوتي، وتقنية إرفاق الملفات السمعية والمرئية والمكتوبة، كما ظهرت تقنية حفظ الرسائل وترتيبها، وربط البريد الإلكتروني بقوائم العملاء والجهات المرسل إليها البريد بانتظام، كما طورت تقنية استقبال البريد الإلكتروني بواسطة المفكرات الإلكترونية المحمولة باليد وكذا عن طريق الهاتف النقال**(6)**، وهناك العديد من المواقع التي اشتهرت بتقديم خدمة البريد الإلكتروني كوقع Yahoo، Hotmail، Google. وطريقة الاستفادة من خدمات البريد الإلكتروني سهلة وميسورة لكل من يحسن استخدام شبكة الانترنت، خاصة عند إنشاء هذا البريد على المواقع العامة التي تقدم هذه الخدمة مجانا، وهذا عن طريق إبرام عقد يسمى بعقد تقديم خدمة البريد الإلكتروني، وهي عبارة عن استمارة يملؤها المستفيد بمجموعة من البيانات الشخصية (قد تكون هذه البيانات سليمة أو غير ذلك)، ويصادق على مجموعة من الشروط التي يفرضها مقدم الخدمة على الشبكة، ويدخل هذا العقد ضمن عقود الخدمات الإلكترونية، ويمكن أن ينشأ مستقلا أو ضمن عقود الخدمات الإلكترونية الأخرى**(7)**.

بعد هذه التوطئة التاريخية البسيطة نحاول فيما يلي التطرق إلى تعريف البريد الإلكتروني وأهم مزاياه وعيوبه، وذلك من خلال ما يلي:

**1 – تعريف البريد الإلكتروني:**

عرّف القانون الأمريكي لسنة 1986، المتعلق بخصوصية الاتصالات الإلكترونية، البريد الإلكتروني على أنه: "وسيلة يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تيلفونية عامة أو خاصة، وغالبا ما يتم كتابة الرسالة على جهاز كمبيوتر ثم يتم إرسالها إلكترونيا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه حيث يتم إرسالها عبر نظام خطوط التيلفون إلى كمبيوتر المرسل إليه"، كما عرف القانون الفرنسي الصادر في 22 جوان 2004، المتعلق بالثقة في الاقتصاد الرقمي الرسالة الإلكترونية على أنها: "كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صور أو أصوات، ويتم إرسالها عبر شبكة اتصالات عامة، وتخزن عند أخد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها"**(8)**.

أما التعاريف الفقهية فهي عديدة، نذكر منها بأن البريد الإلكتروني هو: "تلك المستندات التي يتم إرسالها واستلامها بواسطة نظام اتصالات بريدي إلكتروني، وتتضمن ملحوظات مختصرة ذات طابع شكلي حقيقي، ويمكنه استصحاب مرفقات به، مثل نظام معالجة أو أية مستندات أخرى يتم إرسالها رفقة الرسالة ذاتها"، كما عرف بأنه: "طريقة تسمح بتبادل الرسائل المكتوبة المتصلة بشبكة المعلومات"، وهو كذلك: "مكنة التبادل الإلكتروني غير المتزامن للرسائل بين أجهزة الحاسب الآلي"(9).

وفي تقديرنا لهذه التعريفات، نشير إلى أنها تعريفات تقنية، تصب في مصب واحد مفاده أن البريد الإلكتروني هو عبارة عن فضاء افتراضي داخل شبكة المعلومات، يحوزه شخص عن طريق اسمه (قد يكون حقيقيا أو مستعارا)، ولا يلج إليه إلا عن طريق رقم سري، ويستطيع الشخص من خلال هذا الفضاء الافتراضي الذي يحوزه أن يرسل أو يستقبل رسائل مكتوبة أو صوتية أو مصورة إلى / من شخص أو مجموعة من الأشخاص لديهم أيضا بريد إلكتروني على شبكة الانترنت، وذلك من خلال عبور هاته الرسائل إلى مقدم الخدمة (الخادم، المقلم، Serveur) على الشبكة لتصل إلى العنوان الإلكتروني المحدد على هاته الرسالة مباشرة إلى المرسل إليه إذا كان متصلا بالشبكة On line، أو تسجل عند الخادم في حالة عدم اتصال المرسل إليه بالشبكة Off line، وتبقى هناك حتى يتصل هذا الأخير بصندوق بريده الإلكتروني ويطلب جلب هذه الرسالة.

**2 – مزايا وعيوب البريد الإلكتروني:**

إن وسائل الاتصال بصورة عامة تعتبر من أكبر النعم على البشرية، بما تقدمه من خدمات جليلة في شتى المجالات، غير أننا نطرق باب معرفة مزايا وعيوب البريد الإلكتروني في سبيل المفاضلة بين هاته الوسيلة وغيرها من وسائل الاتصال من جهة، ومن جهة ثانية فإن عيوب وسائل الاتصال قد لا تكمن في الوسيلة ذاتها وإنما في سوء استخدامها على غرار ما هو موجود من فض للرسائل والاطلاع عليها والتنصت على المكالمات الخاصة في الوسائل التقليدية للاتصال، وعلى هذا سنتطرق في البداية إلى مزايا البريد الالكتروني، ثم نتطرق إلى عيوبه من خلال ما يلي:

**أ – مزايا البريد الإلكتروني:**

للبريد الإلكتروني العديد من المزايا التي حاولنا إجمالها فيما يلي:

– يستخدم البريد الإلكتروني كبديل كامل عن المعاملات الورقية، سواء على مستوى الإدارات أو الشركات التجارية، في إطار ما يطلق عليه الآن تسمية التجارة الإلكترونية.

– يؤمن البريد الإلكتروني للأشخاص الطبيعية والمعنوية حاجياتهم دون عناء التنقل، وذلك من خلال طلب البضائع والاشتراك في الدوريات، بمجرد ذكر بيانات البطاقة الائتمانية، وهو ما يطلق عليه اليوم تسمية السوق الإلكترونية**(10)**.

– يعتبر البريد الإلكتروني وسيلة سريعة للاتصال، حيث لا تستغرق الرسالة أكثر من ثوان أو دقائق لتصل إلى المرسل إليه، بغض النظر عن مكان تواجده سواء كان في البلدة المرسل منها البريد الإلكتروني أو في دولة بعيدة.

– إن تكلفة البريد الإلكتروني لا تزيد عن تكلفة الاتصال بشبكة الانترنت، فهي لا تحتاج إلى رسوم أو طوابع ولا إلى مؤسسة توصيل، كما أن تكلفتها غير مرتبطة بطول أو قصر الرسالة، ولا بطول زمن الاتصال.

– إذا كان العنوان الإلكتروني المرسل إليه صحيحا فإن الرسالة لا تضل طريقها مثلما يحدث في البريد العادي.

– إن الشبكة العنكبوتية مصممة على أن لا تتعرض للأعطال، وعلى ذلك فإن خدمة البريد الإلكتروني متوفرة طوال الوقت، فلا إجازة ولا عطل رسمية وغير رسمية، الأمر الذي يمكن مستعملي البريد الإلكتروني من إرسال بريدهم في أي وقت، ويقابل ذلك استقبال رسائلهم في أي وقت وكذا في أي مكان، طالما كانوا على اتصال بالشبكة وبريدهم متاح.

– كل الرسائل المرسلة أو المستقبلة تكون معنونة، وعليها تاريخ ووقت الإرسال والحفظ والاستقبال، وإن كان هذا التوقيت لا يتسم بالدقة المطلقة.

– يمكن لمستعمل البريد الإلكتروني إرسال أكثر من رسالة لأكثر من شخص في وقت واحد.

– إذا كان البريد الإلكتروني مأمنا بالشكل اللازم، فإن نسبة التطفل والاطلاع على ما فيه تتقلص بشكل كبير**(11)**.

**ب – عيوب البريد الإلكتروني:**

ويمكننا أن نقسم هذه العيوب إلى عيوب متعلقة بالبريد الإلكتروني كوسيلة للاتصال، وعيوب متعلقة بإساءة استخدام هذه الوسيلة.

بالنسبة للعيوب المتعلقة بالبريد الإلكتروني كوسيلة اتصال، فإنه يمكننا حصرها فيما يلي:

– عدم إمكانية استعمال البريد الإلكتروني إلا من خلال جهاز معد لذلك (كمبيوتر، هاتف نقال، مفكرة إلكترونية)، ويجب أن يكون هذا الجهاز متصل بشبكة اتصال، وهو ما ينجر عنه أن تعطل هذه الشبكة أو عدم توفرها يعني عدم إمكانية إجراء الاتصالات المرغوبة.

– إن تخزين الرسائل الإلكترونية يتم في أكثر من مكان في صندوق البريد الإلكتروني مما قد يؤدي إلى مشاكل عملية التخزين.

– عدم وجود هيئة مسؤولة عن إدارة البريد الإلكتروني يتيح فرصة طبع الرسائل من خلال الانترنت بدون موافقة من جهة معينة، كما أن هناك إمكانية لحذف أو تعديل محتوى الرسائل الإلكترونية**(12)**.

أما عن العيوب المتعلقة بإساءة استعمال البريد الإلكتروني فهي كثيرة نذكر منها ما يلي:

– لا توجد وسيلة للسيطرة على المسار الذي يسلكه البريد الإلكتروني خلال رحلته عبر الشبكة، وهذا ما يشكل ثغرة في جدار أمن المعلومات، حيث يستطيع قراصنة الانترنت اصطياد الرسائل والاطلاع عليها وتزييف محتواها أو محوه.

– سهولة تزييف البريد الإلكتروني، انطلاقا من المرسل الذي يمكنه تزييف شخصيته وانتحال صفات الغير، ووصولا إلى إمكانية تزييف محتويات البريد نفسه، وهذا دون ترك أثر يثير الشبهات حول صحة الرسالة**(13)**، أو أنه تم الإطلاع عليها.

– إن حذف الرسالة من البريد الإلكتروني لا يعني عدم إمكانية استرجاعها والاطلاع عليها من طرف الغير.

– إن عدم رسمية إدارة البريد الإلكتروني قد يؤدي إلى الانحراف في استخدام هذه الوسيلة، ذلك أن عدم وجود إدارة منهجية للبريد الإلكتروني المنظمة سوف يحدث ارتباكا في المساحة المخصصة لتخزين الرسائل خاصة عند حذف رسائل معينة، مما يؤدي إلى خلل شديد في العمل الإداري**(14)**، ناهيك عن استغلال الغير سيء النية لهذه الثغرة من خلال إغراق البريد

الإلكتروني برسائل لا قيمة لها من أجل تعطيل خدمة البريد الإلكتروني أو حذف الرسائل ذات الأهمية.

- إمكانية تعرض البريد الإلكتروني لهجمات إلكترونية عن طريق الفيروسات والقنابل المنطقية، مما قد يؤثر على الأداء الإيجابي لهذه الخدمة.

**ثانيا / جرائم الاعتداء على البريد الإلكتروني (الاختراق والإغراق):**

من خلال عرضنا السابق، تبين لنا أن البريد الإلكتروني تزداد أهميته في كل يوم وذلك بزيادة عدد المشتركين من جهة، وبزيادة أهمية وحساسية المعلومات المتبادلة من خلال جهة ثانية، فمع زيادة أهمية البريد الإلكتروني تزداد أيضا خطورة الاعتداء عليه أو إساءة استعماله، فقد ظهرت في الوقت الحالي العديد من الجرائم المتعلقة بالبريد الإلكتروني، ويمكننا أن نصنفها ضمن فئتين أساسيتين؛ حيث تتضمن الفئة الأولى الجرائم المرتكبة بواسطة البريد الإلكتروني، وهي كثيرة لا يمكننا حصرها، نذكر منها جريمة التهديد بالقتل، الابتزاز، النصب والاحتيال، التحريض على القيام بأفعال جرمية، كالتحريض على الفسوق والدعارة والتحريض على القتل، التشهير والدعاية للإجرام، وكذا تبادل الرسائل بين المجرمين الدوليين، وإرسال الصور والرسائل الماجنة، والترويج للمخدرات والإرهاب**(15)**، وغير ذلك الكثير مما يمكننا أن نتصوره من أفعال يعتبر البريد الإلكتروني وسيلة لارتكابها، والملاحظ أن هذه الفئة من الجرائم يمكن إخضاعها لقواعد قانون العقوبات التقليدية، على الأقل من ناحية التجريم والعقاب.

أما الفئة الثانية من الجرائم المتعلقة بالبريد الإلكتروني، فهي الجرائم الواقعة على البريد الإلكتروني، ويمكننا حصرها في جريمتين أساسيتين هما: جريمة اختراق البريد الإلكتروني وتسمى أيضا بجريمة انتهاك سرية رسائل البريد الإلكتروني، وجريمة تضخيم البريد الإلكتروني وتسمى أيضا بجريمة الإغراق بالرسائل الإلكترونية، وسوف نتعرض لهاتين الجريمتين بالتفصيل من خلال ما يلي:

**1 – جريمة اختراق البريد الإلكتروني:**

الهجوم على المواقع واختراقها على شبكة الانترنت من الجرائم الشائعة في عصر المعلومات، وتشمل جرائم الاختراق تدمير المواقع، واختراق المواقع الرسمية والشخصية، واختراق البريد الإلكتروني أو الاستيلاء عليه، وكذا الاستيلاء على اشتراكات الغير وأرقامهم السرية**(16)**،

ويمكننا أن نصنف الاختراق إلى ثلاثة أنواع وهي(**17**): اختراق الأجهزة، اختراق المواقع، اختراق البريد الإلكتروني وهو ما يهمنا في هذه الدراسة، واختراق البريد الإلكتروني مفاده الدخول إلى البريد الإلكتروني والاطلاع على الرسائل الموجودة بداخله بدون إذن من صاحب البريد(**18**). من خلال هذا التعريف نجد أن جريمة البريد الإلكتروني ليست جريمة واحدة فهناك الاختراق وهناك أيضا انتهاك سرية رسائل البريد الإلكتروني، وفعل الاختراق قد يحتاج هو الأخر إلى ارتكاب جريمة أخرى كجريمة اصطياد كلمات المرور(**19**)، أو استعمال إحدى برامج الاختراق(**20**) التي تصنف على أنها برامج محظورة وغير شرعية.

والمهم في هذا المقام أن جميع جرائم الاختراق مع اختلافها إلا أنه يجمعها أمر واحد، وهو كونها جميعها تصب في مصب واحد هو انتهاك خصوصية الأشخاص، وهذا يعتبر سببا كافيا لتجريمها، بغض النظر عن الأضرار المادية والمعنوية التي تلحق بالمجني عليه(**21**).

فالخصوصية وإن لم تكن قضية تكنولوجية، فإنها تعتبر اليوم من أبرز القضايا الاجتماعية والأخلاقية في عصر تكنولوجيا الإعلام الآلي والانترنت، والاختراق يعد بمثابة انتهاك صريح للخصوصية(**22**) أو ما يسمى بالخصوصية الإلكترونية E.privacy. وإن لم يكن هناك اتفاق حول مفهوم الخصوصية سواء على المستوى التشريعي أو الفقهي(**23**)، فإن الأمر الأكيد أن المراسلات بمختلف أنواعها تعتبر من بين الأمور الخصوصية للشخص، والتي لا يحق للغير الإطلاع عليها أو اعتراضها بأي وجه من الأوجه، ولا أدل على قولي هذا من أن مؤتمر رجال القانون الذي انعقد بستوكهولم في ماي 1967 قد عرف الحق في الخصوصية بأنه: "حق المرء في أن يترك ليعيش حياته الخاصة بأقل درجات التدخل وحمايته من:

1 – ...

8 – مراقبة مراسلاته،

9 – الاستخدام السيئ لاتصالاته الشخصية الكتابية والشفوية،

10 – استخدام المعلومات المأخوذة أو المعطاة بواسطته في حالات الثقة المهنية"(**24**).

وهذا الأمر مؤكد دستوريا في الجزائر حيث تنص المادة 39 من الدستور على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون.

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

وإطلاق حكم النص بتوظيف المؤسس الدستوري لعبارة "بكل أشكالها" يجعل من سرية مراسلات البريد الإلكتروني محمية دستوريا من أي اعتداء.

والمطلع على النصوص العقابية المتعلقة بحماية الحياة الخاصة للأشخاص وسرية مراسلاتهم، وخصوصا المادة 303 و303 مكرر من قانون العقوبات الجزائري يجد بأن هذه النصوص في حاجة للتعديل لمواكبة التطورات التكنولوجية الراهنة، حيث جاء في المادة 303 أنه: "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس..."، فالمصطلحات المستعملة في هذه المادة "يفض"، "يتلف" لا يمكن أن تنطبق بأي حال من الأحوال على اختراق وإغراق البريد الإلكتروني. فالمراسلات المحمية بنص هذه المادة هي تلك المسلمة إلى مصلحة البريد، وإن كان هذا الشرط غير منصوص عليه صراحة في متن هذه المادة إلا أنه يستخلص بصفة منطقية من نص المادة 137، والمقصود بالمراسلات في المادة 303 هو الرسالة المغلقة، والبطاقة البريدية، والبرقية (التلغراف)، والمطبوعات والنشريات(**25**).

أما المادة 303 مكرر التي جاء فيها أنه: "يعاقب... كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأي تقنية كانت وذلك:

1 – بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، أو سرية بغير إذن صاحبها أو رضاه،

2 – بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه"،

والملاحظ أنه إذا كانت الفقرة الأولى منسجمة مع نص المادة 39 من الدستور وهذا في عبارة "كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت"، غير أن المشرع لما بدأ في تعداد التقنيات المستعملة للمساس بالحياة الخاصة، أهمل التطرق للتقنيات المستعملة في الاعتداء على البريد الإلكتروني، حيث يفهم من هذا النص أن الأفعال المجرمة تنحصر في الاعتداء على المحادثات التليفونية، المحادثات الخاصة والسرية المباشرة، وأخذ صورة لشخص في مكان خاص(**26**). وحتى إن سلمنا بأن عبارة "الأحاديث الخاصة" تتسع لتشمل مراسلات البريد الإلكتروني، فإنها تنطبق على جزء من هذه المراسلات فقط (غرف الدردشة الخاصة) وليست كل المراسلات هذا من جهة، ومن جهة ثانية فإن القاضي الجزائي مقيد بمبدأ الشرعية ولا يجوز له القياس خاصة في مجال التجريم.

وبالرجوع إلى القسم السابع مكرر من قانون العقوبات الجزائري المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، المستحدث بموجب القانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004، وعند إطلاعنا على المادة 394 مكرر التي جاء فيها أنه: "يعاقب... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 000 150 دج".

وكذا المادة 394 مكرر 1 التي جاء فيها أنه: "يعاقب... كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

نجد بأن هاتين المادتين تنصبان على تجريم الأفعال المنصبة على المساس بأنظمة المعالجة الآلية للمعطيات، وهو ما يطلق على تسميته جرائم الحاسب الآلي أو جرائم الكمبيوتر**(27)**، حيث تقسم هذه الجرائم بحسب دور الكمبيوتر فيها إلى ثلاثة أنواع هي: الكمبيوتر هدف للجريمة وهذا في حالة الدخول غير المصرح به إلى النظام، أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، أو الاستيلاء على البيانات المخزنة أو المنقولة عبر النظام. أما النوع الثاني فهو الحالة التي يكون فيها الكمبيوتر أداة لارتكاب الجريمة، ومثال ذلك استعمال الكمبيوتر في الاستيلاء على الأموال (تحويل الأرصدة) أو ارتكاب جرائم التزوير أو التأثير على برمجيات التحكم في الطائرات والسفن بشكل يؤدي إلى تدميرها وقتل ركابها. أما النوع الثالث فهو الحالة التي يكون فيها الكمبيوتر بيئة للجريمة، وهذا في حال تخزين البرامج التي تمت قرصنتها فيه، أو استخدامه لتخزين مواد غير قانونية أو إباحية كالترويج للمخدرات أو تحميل الصور الإباحية**(28)**. من خلال هذا التقسيم نلاحظ أن المادتين 394 مكرر و394 مكرر 1 وما بعدهما من قانون العقوبات لا تخرج عن النوعين الأول والثالث، أما النوع الثاني فإن العقاب على جرائمه يكون وفقا للنصوص التقليدية لقانون العقوبات.

والسؤال الذي يطرح في هذا المقام هو: ما هو المقصود بنظام المعالجة الآلية للبيانات؟ وعند بحثنا عن إجابة لهذا السؤال وجدنا بأن المعالجة الآلية للمعطيات أو البيانات هي كافة العمليات والمهام التي تخضع لها البيانات معطيات الكمبيوتر بما في ذلك إنشاؤها وإرسالها واستقبالها أو تخزينها أو تجهيزها على أي وجه آخر**(29)**.

ويرى خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية أن المقصود بالجريمة المعلوماتية هي كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها(**30**). من خلال هذين التعريفين يمكننا القول بأن البريد الإلكتروني يندمج ضمن برامج أو أنظمة المعالجة الآلية للمعطيات، ومن ثمة فإن اختراق البريد الإلكتروني مجرم وفقا للمادة 394 مكرر التي تنص على معاقبة "كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"، فمجرد الدخول غير المشروع معاقب عليه، وكذا البقاء، بل وحتى المحاولة على ذلك معاقب عليها وإن كان من الصعب تصور إثبات المحاولة في مثل هذا النوع من الجرائم.

وإن كان هذا التحليل قد جرنا إلى أن اختراق البريد الإلكتروني مجرم في نصوص قانون العقوبات الجزائري، فإننا نعتقد أن مثل هذه التحليلات هي عبارة عن توسيع لمضمون النصوص الجنائية بما لا يوجد فيها صراحة، خاصة إذا علمنا أن القاضي الجزائي ملزم بمبدأ الشرعية الجنائية، ومن ثمة يجب أن لا نحمل النصوص الجنائية ما لا تطيق من معنى، بل يجب على المشرع تدارك هذا النقص والعمومية في النصوص، والعمل على تطويرها وفقا لمتطلبات هذا العصر.

غير أنه وفي تحليل آخر وفقا لما قرره مجلس الشيوخ الفرنسي في إطار تحديده لمدلول النظام الآلي لمعالجة المعطيات في مشروع قانون غش المعلومات الفرنسي رقم 88 لسنة 1988 الصادر في 05 جانفي 1988 الذي عرفه بأنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها يمكن تحقيق نتيجة معينة هي معالجة المعطيات أو التي تتضافر فيما بينها نحو تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية التقنية"، فقد حدد مجلس الشيوخ الشروط التي ينبغي أن تتحقق في وحدات النظام التي تحدد جانبًا منها عبارة المجلس بأنه عبارة عن: مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط. والتي تكشف من جانب آخر عن أن النظام الآلي يتكون من عنصرين :الأول عنصر مادي يتكون من وحدة أو مجموعة من وحدات المعالجة أو الإدخال أو الإخراج أو الربط، والثاني عنصر من طبيعة غير مادية يتكون من البرامج والمعطيات تتضافر أو تتآلف فيما بينها من أجل تحقيق غاية محددة هي معالجة المعطيات(**31**). وبالتالي فإن الحديث هنا لا يخرج عن كون نظام المعالجة الآلية للبيانات لا

يخرج عن جرائم الكمبيوتر وهي لا تتعدى وفقا لهذا التعريف إلى الجرائم الواقعة في حقل الانترنت، وهذا الاتجاه الثاني هو المرجح في تفسرنا لنصوص قانون العقوبات الجزائري، وذلك بالنظر إلى الأهداف المسطرة في مشروع قانون العقوبات رقم 04 – 15 المؤرخ في 10 نوفمبر 2004، وما يؤكد توجهنا هذا هو استعمال المشرع لعبارة "المعالجة الآلية للبيانات" التي تمثل أول صور المعالجة الآلية، وهي أولى تطبيقات الكمبيوتر مع بداية ظهوره، لذا نفضل لو وظف المشرع عبارة نظام المعالجة الآلية للمعلومات**(32)**.

**2 – جريمة تضخيم البريد الإلكتروني:**

يطلق على هذه الجريمة أيضا تسمية الإغراق بالبريد الإلكتروني SPAM**(33)**، وقد عرف الإغراق أو تضخيم البريد الإلكتروني بأنه: "تراسل نسخ مكررة بعدد كبير من نفس الرسالة عبر النظام التراسلي لبريد إلكتروني بما يترتب عليه عدم انتظام سير النظام التقني المعلوماتي"، كما عرف أيضا بأنه: "استقبال عدد كبير من الرسائل الإلكترونية المزعجة"**(34)**، ففي هذه الجريمة يقوم شخص أو مجموعة من الأشخاص بإرسال عدد كبير من الرسائل إلى البريد الإلكتروني لشخص ما بقصد الإضرار به، وهذا من خلال استخدام برامج متخصصة تعمل على استنساخ الرسالة الواحدة بشكل متكرر، وقد يصاحب هذه الرسالة فيروسات، أو صور وملفات كبيرة الحجم، حيث يؤدي هذا العمل إلى ملء المساحة المخصصة للبريد الإلكتروني للشخص المستهدف، وبالتالي تتعطل عنه الخدمة المقدمة من الشبكة ولا يستطيع استقبال أي رسالة، ورسائل الإغراق تستخدم للإضرار بمستخدم البريد الإلكتروني، والتي تصل إلى جهازه مرة واحدة فتؤدي إلى توقفه عن العمل على الفور، نظرا لما تسببه هذه الرسائل من ملء منافذ الاتصال أو ملء المساحة المتاحة لهذا الجهاز وكذا ملء قوائم الانتظار، الأمر الذي يترتب عنه انقطاع الخدمة وبالتالي تكبد خسائر مادية ومعنوية غير محدودة**(35)**.

وبالنظر إلى الضرر الهائل الذي يمكن أن تسببه رسائل الإغراق سواء بالنسبة للأشخاص الطبيعية أو المعنوية، فقد عملت العديد من التشريعات على تجريم هذا العمل غير المشروع، ففي الولايات المتحدة الأمريكية نذكر على سبيل المثال لا الحصر قانون مكافحة تضخيم البريد الإلكتروني لسنة 1989 المعدل في ماي 1990 لولاية واشنطن، وقانون ولاية أوهايو الصادر سنة 2002 الذي نص على تجريم رسائل البريد الإلكتروني مجهولة المصدر. أما في فرنسا فقد قام المشرع بتضمين قانون العقوبات الجديد نصا جرم فيه التعدي على قواعد البيانات

باستخدام أسلوب تضخيم البريد الإلكتروني، حيث جاء في نص المادة 323 – 02 أن: الفعل الذي بمقتضاه يتم إعاقة عمل نظام المعالجة الآلية للبيانات يعاقب عليه بالحبس والغرامة**(36)**.

وبالرجوع إلى نص المادة 394 مكرر وما بعدها في قانون العقوبات الجزائري لا نجد أي نص يجرم إغراق البريد الإلكتروني، ولا وجود حتى لنص عام مماثل لما هو معمول به في التشريع الفرنسي يفيد أن أي عمل من شأنه تعطيل أنظمة المعالجة الآلية للمعطيات يترتب عليه العقاب، ذلك أن الفقرة الأخيرة من المادة 394 مكرر تجرم تخريب نظام اشتغال المنظومة، والأمر الأكيد أن التخريب غير تعطيل نظام المعالجة، هذا إذا سلمنا بأن نظم المعالجة الآلية للمعطيات تتضمن معالجة البيانات والمعلومات على مستوى البريد الإلكتروني.

**الخاتمة:**

ما نخلص إليه في نهاية هذا المقال، أن التطور التكنولوجي الهائل في مجال المعلومات الذي أسهم بشكل كبير في رخاء البشرية في جوانب عديدة من الحياة، هو نفسه الذي وفر ملاذا أكثر أمانا لنوع جديد من المجرمين، وهيأ مجالا خصبا لنمو جرائم جديدة تتسم بالنعومة في ظاهرها وبالخطورة الشديدة في نتائجها المدمرة.

وإن كنا قد ركزنا في هذه الدراسة على جرائم البريد الإلكتروني، فهذا لا يعني أن الجريمة الإلكترونية منحصرة فيها، فهناك كم هائل من الأفعال الجرمية التي وجدت في فضاء الانترنت مرتعا لها، وهي في تطور وتزايد مستمر، إلا أن الاعتداء على البريد الإلكتروني يمثل اعتداء على جانب مهم في حياتنا اليومية ألا وهو الحق في الخصوصية، وتحديدا الحق في سرية المراسلات والاتصالات.

بالإضافة إلى النتائج التي توصلنا إليها خلال هاته الدراسة، هناك مجموعة من التوصيات التي نأمل أن تسهم في تفعيل مكافحة الجرائم الإلكترونية بشكل عام وجرائم البريد الإلكتروني بشكل خاص، وقد أوجزناها فيما يلي:

إن أمن الجريمة الإلكترونية يقوم على جانبين أولهما وقائي والثاني علاجي، فعلى المستوى الوقائي يجب تطوير برامج الحماية من القرصنة والولوج غير المشروع وحماية الكلمات السرية وكذا التصدي للبريد المزعج وهذا بشكل دوري، ذلك أن أساليب الاعتداء في إطار الإجرام المعلوماتي في تطور مستمر، كما يجب على مستخدمي البريد الإلكتروني المواظبة على تعلم استخدام هاته البرامج الوقائية.

دائما وفي الإطار الوقائي يجب على الخوادم على مستوى الشبكة أن يطورا برامجا لحماية البريد الإلكتروني من كل خرق أو إغراق، كما يجب أن يعملوا على حماية بيانات عملائهم وخصوصيتهم، بوضع برامج لمنع التجسس الإلكتروني وبرامج مضادة للفيروسات وأخرى مضادة لفك التشفير.

أما على المستوى الثاني العلاجي، والذي يأتي بعد وقوع الجريمة من أجل جبر أضرارها، فإن المعول عليه في هذا المقام هو تكاثف الجهود والتعاون بين الأفراد ضحية الاعتداء على البريد الإلكتروني ومختلف أجهزة مكافحة الإجرام المعلوماتي المحلية والدولية.

فيجب على الأفراد الذين تعرض بريدهم الإلكتروني للاختراق أو الإغراق التبليغ عن هاته الجرائم للجهات المعنية.

أما الدولة فيجب عليها أن تتدخل لوضع حد لهذه الظواهر الإجرامية، وذلك عن طريق إنشاء هيئات متخصصة في مكافحة الجريمة الإلكترونية، أو باستحداث مصالح على مستوى أجهزة مكافحة الجريمة، تعطى الأولوية في التوظيف فيها للمتخصصين في الإعلام الآلي، كما يجب أن تسهر الدولة على إعادة رسكلة مهارات هؤلاء المتخصصين بشكل دوري، وذلك من خلال دورات تربص بالخارج، وتكثيف الدورات التكوينية على أيدي خبراء محليين ودوليين.

كما يجب على الدولة أن تكثف جهودها في إطار التعاون الدولي لمكافحة الجريمة الإلكترونية، وذلك من خلال المصادقة أو الانضمام إلى الاتفاقيات الدولية المنصبة على تنظيم هذا المجال، وكذا العمل على تسهيل الاتصال والتعاون بين مختلف أجهزة مكافحة الجريمة الالكترونية المحلية والدولية.

كما يقع إلزام على الدولة بتحديث الوسائل التقنية لمكافحة الجريمة الإلكترونية، وذلك باقتناء أحدث الوسائل وأعلاها تقنية أو بفتح المجال أمام الخبراء لاختراع هذه الأجهزة من خلال تدعيمهم ماديا ومعنويا.

ضرورة وضع قانون خاص بمكافحة الجريمة الإلكترونية، يأتي على تفصيل كل الجرائم الراهنة المتعلقة بهذا المجال كمطلب أساسي، واحتياطيا إعادة صياغة نصوص قانون العقوبات الحالية لكي تتمكن من مواجهة هذه الجرائم المستحدثة، فيجب أن تتغير صياغة المادة 303 من قانون العقوبات لتصبح على الشكل التالي: "كل من يعتدي على مراسلات الغير مهما كان شكلها يعاقب..."، كما أن المادة 394 مكرر وما بعدها تحتاج أن يضاف إليها

فقرات جديدة متعلقة بشرح المفردات المستحدثة في مجال الجريمة الإلكترونية، وكذا تخصيص نصوص لكل جريمة على حده، والابتعاد عن النصوص العامة التي رأينا بأنها تتعارض في الكثير من الأحيان مع مبدأ الشرعية. فالسلطة التشريعية ملزمة في هذا المجال بالاستعانة بالقوانين التي توصلت إليها الدول المتقدمة في مجال الحماية من الجرائم الإلكترونية، مع مراعاة متطلبات البيئة الداخلية.

ضرورة تكثيف عقد اللقاءات العلمية في مجال الجريمة الإلكترونية والمعلوماتية، والسهر على حضور متخصصين من مختلف المجالات الذين تنصب اهتماماتهم على مكافحة الإجرام الإلكتروني والمعلوماتي، مع تخصيص دورات تكوينية لرجال القانون(أساتذة، قضاة، محامين، رجال الضبطية القضائية...) وكل المهتمين بهذا المجال من أجل رفع خبراتهم في مكافحة هذا النوع من الإجرام.

**الهوامش:**

(1) تشير الدراسات التي قدمها معهد أمن الحاسب بسان فرانسيسكو التابع لمكتب التحقيقات الفيدرالي أن جملة الخسائر الناجمة عن الجرائم المعلوماتية قد بلغت سنة 2001 حوالي 378 مليون دولار ثم ارتفعت لتصل إلى 526 مليون دولار سنة 2004 في الولايات المتحدة الأمريكية وحدها، كما أكدت إحدى التقارير العالمية أن قطاع تكنولوجيا المعلومات حول العالم يتكبد خسائر تجاوزت 32 مليار دولار خلال سنة واحدة، وجاء في التقرير الذي أصدرته الجمعية الدولية لمنتجي برامج الكمبيوتر التجارية أن خسائر قطاع تكنولوجيا المعلومات قد بلغت سنة 2006 حوالي 32,7 مليار دولار. أنظر: هلالي عبد اللاه أحمد، **جرائم المعلوماتية عابرة الحدود**، القاهرة: دار النهضة العربية، 2007، هامش 5، ص 05 وما بعدها.

(2) عبد الفتاح بيومي حجازي، **النظام القانوني لحماية التجارة الإلكترونية**، الكتاب الأول، الإسكندرية: دار الفكر الجامعي، 2002، هامش 1، ص 80.

(3) جميل عبد الباقي الصغير، **أدلة الإثبات الجنائي والتكنولوجيا الحديثة**، القاهرة: دار النهضة العربية، 2002، ص 113 وما بعدها.

(4) Glenn Wahlert, **Crime in cyberspace : trends in computer crime in Australia**, paper presented at the conference : internet crime, Melbourne, 16 – 17 February 1998, by the Australian institute of criminology, P 04.

(5) Barbara Etter, **computer crime**, paper presented at the 4th national outlook symposium on crime in Australia: new crimes or new responses, Canberra, 21 – 22 June 2001, Australian institute Of criminology, P 02.

(6) خالد ممدوح إبراهيم، **أمن مراسلات البريد الإلكتروني**، الإسكندرية: الدار الجامعية، 2008، ص ص: 53، 54. هلالي عبد اللاه أحمد، مرجع سابق، هامش 5، ص ص: 36، 37.

(7) محمد حسين منصور، **المسؤولية الإلكترونية**، الإسكندرية: دار الجامعة الجديدة للنشر، 2003، ص 30.

(8) خالد ممدوح إبراهيم، مرجع سابق، ص 56. وأنظر كذلك:

Florence Celen, Laurence Lomme, « **Application de la Loi sur la Confiance dans l'Économie Numérique au CNRS** »,Sécurité Informatique, N°: 54, Septembre 2005 , P 03.

(9) خالد ممدوح إبراهيم، مرجع سابق، ص 55.

(10) حسن طاهر داود، **جرائم نظم المعلومات**، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2000، ص 100.

(11) خالد ممدوح إبراهيم، مرجع سابق، ص 52.

(12) المرجع نفسه، ص 53.

(13) حسن طاهر داود، مرجع سابق، ص ص: 98، 99.

(14) خالد ممدوح إبراهيم، مرجع سابق، ص 53.

(15) أنظر أكثر تفصيلا في هذا النوع من الجرائم: هاني خميس أحمد، "**الإرهاب الإلكتروني**"، سلسلة مفاهيم، القاهرة: المركز الدولي للدراسات المستقبلية والإستراتيجية، العدد 27، السنة الثالثة، مارس 2007، ص ص: 12 – 14. محمد محمد الألفي، **المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت**، القاهرة: المكتب المصري الحديث، 2005، ص 46 وما بعدها. عبد الرحمن فرزات، "**المعلوماتية وقانون العقوبات الواقع والآفاق**"، مجلة المحامون، نقابة المحامين، سوريا، السنة 66، العددان: 07، 08، تموز/ آب 2001، ص 643 وما بعدها. عثمان سعيد المحيشي، "**جريمة السطو على الإيميل من جذور الماضي إلى آفاق المستقبل التشريعية**"، ورقة عمل مقدمة إلى المنظمة العربية للتنمية الإدارية، المؤتمر الدولي الأول لقانون الانترنت، 21 – 25 أغسطس 2005، مقال منشور على الموقع: www.mishawi.com.

(16) محمد محمد الألفي، مرجع سابق، ص 38.

(17) منير محمد الجهيني وممدوح محمد الجهيني، **جرائم الانترنت والحاسب الآلي ووسائل مكافحتها**، الإسكندرية: دار الفكر الجامعي، 2006، ص 46.

(18) خالد ممدوح إبراهيم، **أمن الجريمة الإلكترونية**، الإسكندرية: الدار الجامعية، 2008، ص 91.

(19) جريمة اصطياد كلمات المرور تعني: سرقة كلمات السر الإلكترونية، عن طريق تظاهر المجرم بأنه شخص جدير بالثقة أو مؤسسة أعمال، وذلك عبر اتصال إلكتروني يبدوا وكأنه رسمي، ويطلب من صاحب البريد كلمات المرور السرية من أجل خدمات وهمية في حقيقتها. أنظر أكثر تفصيلا لهذا الموضوع في: دانيال لاركين، "**محاربة جرائم الانترنت**"، 17 ماي 2008، مقال انترنت أطلع عليه على الموقع: www.america.gov.

(20) يتطلب الاختراق برنامجا يتم تصميمه خصيصا ليتيح للمخترق الولوج إلى المواقع المحظورة أو أجهزة الكمبيوتر الخاصة أو البريد الإلكتروني، وأشهر هذه البرامج هو برنامج حصان طروادة، الذي يعمل بصورة خفية داخل أنظمة الكمبيوتر أو داخل شبكة الانترنت، وهدفه هو تمكين المخترق من الحصول على كلمة السر. أنظر: مرشد الأمم المتحدة لعام 1999، **التحكم في جرائم الحاسوب وردعها** "**المراقبة الدولية للسياسة الجنائية**"، ترجمة: عمر محمد بن يونس، القاهرة: دار النهضة العربية، 2005، ص ص: 46، 47. محمد محمد الألفي، مرجع سابق، ص 39. منير محمد الجهيني وممدوح محمد الجهيني، مرجع سابق، ص 55 وما بعدها.

(21) محمد محمد الألفي، مرجع سابق، ص 38. لؤي ديب، "**أهمية وجود تشريعات لحماية الخصوصية من أجل الالتحاق بالثورة الرقمية**"، مقال منشور على الموقع: http. Elibs.info/lib-law.

(22) هاني خميس أحمد، "**الخصوصية: انتهاكها وحمايتها في ظل مجتمع المعلومات**"، **سلسلة قضايا**، القاهرة: المركز الدولي للدراسات المستقبلية والإستراتيجية، العدد 34، السنة الثالثة، أكتوبر 2007، ص 06.

(23) أنظر أكثر تفصيلا لمفهوم الخصوصية: أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات** "**دراسة مقارنة**"، القاهرة: دار النهضة العربية، 2008، ص 17 وما بعدها. فريدة بن يونس، **الحماية الجنائية لحرمة الحياة الخاصة في مواجهة الصحافة**، رسالة ماجستير في القانون الجنائي، جامعة بسكرة، غير منشورة، 2006، ص 09 وما بعدها. هاني خميس أحمد، "**الخصوصية: انتهاكها وحمايتها في ظل مجتمع المعلومات**"، مرجع سابق، ص 07 وما بعدها.

(24) زهير حرح، **الحق في الحياة الخاصة**، ط 02، منشورات جامعة دمشق، 2005 / 2006، ص ص: 46، 47.

(25) أنظر أكثر تفصيلا: مكي دردوس، **القانون الجنائي الخاص في التشريع الجزائري**، ج 02، قسنطينة: المطبعة الجهوية ديوان المطبوعات الجامعية، 2005، ص 29 وما بعدها.

(26) أنظر التعليق على المادة 309 مكرر من قانون العقوبات المصري المقابلة للمادة 303 مكرر من قانون العقوبات الجزائري في: محمود أحمد طه، **التعدي على حق الإنسان في سرية اتصالاته الشخصية بين التجريم والمشروعية**، ط 02، القاهرة: دار النهضة العربية، 1999، ص 16 وما بعدها.

(27) مرشد الأمم المتحدة لعام 1999، مرجع سابق، ص 46.

(28) خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، مرجع سابق، ص ص: 62، 63. يونس عرب، "قانون الكمبيوتر: النظرية والمشتملات"، ص 02، بحث منشور على الموقع: www.arablaw.org. وأنظر كذلك:

Hollis Stambaugh and authers, **Electronic crime needs assessment for state and local law enforcment** , U S department of justice, National institute of justice, March 2001, P 09.

(29) يونس عرب، "**مشروع قانون نموذجي عربي لجرائم الكمبيوتر والانترنت وللجرائم الإلكترونية**"، ورقة عمل مقدمة في ملتقى: "تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية"، مسقط – عمان، 02 – 04 أفريل 2006، ص 09، منشور على موقع: www.arablaw.org.

(30) عارف خليل أبو عيد، "**جرائم الانترنت دراسة مقارنة**"، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 05، العدد 03، أكتوبر 2008، ص 82.

(31) محمد حماد مرهج الهيتي، "**المواجهة التشريعية لإتلاف المكونات المادية للنظام الآلي لمعالجة المعطيات**"، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 05، العدد 02، جوان 2008، ص 252.

(32) إن نظام معالجة المعلومات لا يعد هو الآخر آخر تطور لنظم المعالجة الآلية، إذ مرت هذه الأخيرة بأربعة مراحل هي: نظام المعالجة الآلية للبيانات، نظام المعالجة الآلية للمعطيات، نظام معالجة المعارف، النظم الذكية للتعلم الذاتي، غير أن البيانات، والمعلومات، والمعارف، والذكاء، تدمج اختصارا في مصطلح جامع شامل هو "المعلومات"، أنظر أكثر تفصيلا لهذا الموضوع في: نبيل علي، **العرب وعصر المعلومات**، سلسلة عالم المعرفة، الكويت: المجلس الوطني للثقافة والفنون والآداب، العدد 184، أفريل 1994، ص 42 وما بعدها.

) SPAM : Solicited Pornography and Marketing. Guillaume Teissonnière , **La lutte** 33( **contre le spamming : de la confiance en l'économie numérique à la méfiance envers ses acteurs**, Juriscom.net, 2 avril 2004, http://www.juriscom.net. P 03.

(34) خالد ممدوح إبراهيم، **أمن الجريمة الإلكترونية**، مرجع سابق، ص 94. وأنظر نفس المعنى في:

Guillaume Teissonnière , 0P Cit. P 01.

(35) محمد محمد الألفي، مرجع سابق، ص ص: 40، 41. منير محمد الجهيني وممدوح محمد الجهيني، مرجع سابق، ص 67. خالد ممدوح إبراهيم، **أمن الجريمة الإلكترونية**، مرجع سابق، ص ص: 93 – 95. صالح أحمد البربري، "**دور الشرطة في مكافحة جرائم الانترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في 23/ 11/ 2001**"، ص 05، مقال منشور على الموقع: www.arablawinfo.com.

(36) خالد ممدوح إبراهيم، **أمن الجريمة الإلكترونية**، مرجع سابق، ص ص: 95 – 97.