الجريمة في عصر الاتصال الإلكتروني...
حينما تصبح التقنية وسيلة للإجرام

د. منير طبـي
جامعة العربي التبسي - تبسة

الملخص:

تتميز التقنيـة والتكنولوجيـا بتطـورات عديـدة وظهـور لأشـياء جديـدة، هـذا المعطى يؤشر بتطور طرق ووسائل الجريمة الإلكترونية مقارنة بالماضي، الشيء الذي يحتم على الحكومات والدول تحسين سبل محاربة هذه الجرائم وايجاد حلول متناسبة وأشكال هذه الجرائم ودرجة تعقيدها، والملاحظ كذلك تعدد التعريفات التي تناولت الجريمة الإليكترونيـة، ويرجـع ذلـك إلى حداثـة هـذا النـوع مـن الجـرائم، ذلـك أنـه مـع تطـور المعلومـات والاتصـالات وجـد شـكل جديـد مـن المجـرمين، عبروا بالجريمـة مـن ضـفة الجريمة التقليدية إلى الضفة الحديثة التي كثيرا ما صعب التعامل معها، في ظل تعقد الجانب الفني في حين وغياب الجانب القانوني أو ضعفه في أحايين أخرى.

الكلمات المفتاحية:

الجريمة الإليكترونية، الاتصال الإليكتروني، القوانين، التشريعات، الأنظمة.

Abstract

Technology and technology are characterized by many developments and the emergence of new things. This indicates the evolution of the methods and means of electronic crime compared to the past, which necessitates governments and countries to improve ways to fight these crimes and find solutions proportionate to the forms and complexity of these crimes. This is because of the modernity of this type of crime. As the information and communications developed, a new form of criminals emerged. They crossed the crime from the bank of conventional crime to the modern bank, which is often difficult to deal with. The legal aspect or its weakness at other times. **Key words**

Electronic crime, electronic communication, laws, legislation, regulations.

مفهوم الجريمة الإلكترونية وموضوعها:

تعددت الآراء بشأن تعريف الجريمة الإلكترونية، كل رأي تبنى مفهوما بالنظر إلى الزاوية التي رآها، فهناك جانب من الفقه عرفها من زاوية فنية وأخرى قانونية، وهناك جانب آخر يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استنادا لمعايير أخرى حسب القائلين بها.

وهذا ما حدا بالأمم المتحدة – مدونتها بشأن الجريمة المعلوماتية – إلى عدم التوصل لتعريف متفق عليه دوليا، ولكن ورغم صعوبة وضع تعريف لظاهرة هذه الجريمة وحصرها في مجال ضيق، إلا أن مكتب تقييم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاسب الآلي بأنها " الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي "[1]، كما عرفت أيضا بأنها " نشاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني "، وعرفت أيضا بأنها " كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على أي مصلحة مشروعة ، سواء أكانت مادية أو معنوية.[2]

لكن بشكل عام الجريمة الالكترونية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة، وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية، مباشر أو غير مباشر، باستخدام شبكة الاتصالات مثل الأنترنت (غرف الدردشة، البريد الإليكتروني، الموبايل...)[3]

يختلف موضوع الجريمة الإلكترونية من حيث الزاوية التي ينظر إليها منه، فمن ناحية قد يكون الحاسب الآلي أو المعلومات المخزنة فيه موضوعا للجريمة، ومن ناحية أخرى قد يكون فيها الحاسب الآلي أداة للجريمة الإلكترونية ووسيلة تنفيذه:[4]

- **الحالة التي يكون فيها الحاسب الآلي أو المعلومات المخزنة فيه موضوعا** أو محلا للجريمة في هذه الحالة وهي ما يطلق عليها البعض (أداء سلبية) يكون هناك صورتان للاعتداء، اعتداء واقع على المكونات المادية للحاسب الآلي ذاته كالأجهزة والمعدات، والتي تتمثل في جرائم سرقة أو إتلاف شاشة الحاسب أو شبكة اتصالاته الخاصة أو آلة الطباعة؛ ومن ناحية أخرى قد يكون الاعتداء موجها إلى مكونات الحاسب الآلي غير

المادية كالبيانات والبرامج، مثل جرائم الاعتداء على البيانات المخزنة في ذاكرة الحاسب الآلي أو البيانات المنقولة عبر شبكات الاتصال المختلفة، والتي تتمثل في جرائم السرقة أو الإتلاف أو التقليد أو محو أو تعطيل هذه البيانات، والصورة الثانية تمثل الاعتداء ذاته موجها إلى برامج الحاسب الآلي من خلال تزوير المستخرجات الإلكترونية وإفشاء محتوياتها.

ومن نافلة القول أن النوع الأخير من الاعتداءات تعجز حياله نصوص قانون العقوبات الحالية عن احتوائه واستيعابه نظرا لأن محل هذه الاعتداءات مال غير مادي (معنوي) ذو طابع خاص، أي أنه في صورة أخرى غير صورة المال بمفهومه الجنائي التقليدي.

- حالة يكون فيها الحاسب الآلي أداة لارتكاب الجريمة ووسيلة تنفيذها:

ففي هذه الحالة والتي يطلق عليها البعض (أداة إيجابية) يستخدم الجاني الحاسب الآلي في ارتكاب جرائم السرقة أو النصب أو خيانة الأمانة أو تزوير المحررات، وذلك عن طريق التلاعب في الحاسب، وكذلك النظام المعلوماتي بصفة عامة، وفي هذه الحالة نكون بصدد جرائم تقليدية بحتة.

خصائص الجريمة الإلكترونية وأنواعها:

تتميز الجرائم المرتكبة بواسطة الكمبيوتر كأداة أو كهدف للجريمة بالخصائص التالية:[5]

- ✓ **سرعة التنفيذ**: لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكبير، وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر، وهذا لا يعني إنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.
- ✓ **التنفيذ عن بعد**: لا تتطلب جرائم الكمبيوتر في أغلبها (إلا جرائم سرقة معدات الكمبيوتر) وجود الفاعل في مكان الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب...الخ.
- ✓ **إخفاء الجريمة**: أن الجرائم التي تقع على الكمبيوتر أو بواسطته كجرائم (الإنترنت) جرائم مخفية، إلا أنه يمكن أن تلاحظ آثارها والتخمين بوقوعها.

- ✓ **الجاذبية**: نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها، أو سرقة البنوك أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام البطاقات...الخ.
- ✓ **عابرة للدول**: إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان ولا بالزمان وأصبحت ساحتها العالم أجمع.
- ✓ **جرائم ناعمة**: تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح، إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، فنقل بيانات من كمبيوتر إلى أخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.
- ✓ **صعوبة إثباتها**: تتميز جرائم الإنترنت عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة.
- ✓ **التلوث الثقافي**: لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها، وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة.
- ✓ **عالمية الجريمة والنظام العدلي**: نظرا لارتباط المجتمع الدولي إلكترونيا، فقد أصبح مجتمعنا تخيليا مما أدى إلى أن تكون ساحة المجتمع الدولي بكافة دوله ومجتمعاته مكانا لارتكاب الجريمة من كل مكان، مما تطلب أن تمارس الدول المتطورة وخاصة

الصناعية على الدول النامية من أجل سن تشريعات جديدة لمكافحة الجرائم المتصلة بالكمبيوتر مما استدعى أن تكون القوانين ذات صبغة عالمية.

- ✓ **لا يتم – في الغالب الأعم - الإبلاغ عن جرائم الانترنت** إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير، لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة؛ بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة والعدد الذي تم اكتشافه هو رقم خطير، فالفجوة بين عدد هذه الجرائم الحقيقي وما تم اكتشافه فجوة كبيرة.
- ✓ **تعتمد هذه الجرائم على قمة الذكاء في ارتكابها**، ويصعب على المحقق التقليدي التعامل مع هذه الجرائم، إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية.

فيم تتنوع الجريمة الإليكترونية حسب موضوعها وأهدافها إلى:[6]

- ✓ **القرصنة الالكترونية:** يشير مفهوم القرصنة الإلكترونية إلى أي ممارسات غير مشروعة تستهدف التحايل على نظام المعالجة الآلية للبيانات، بغية إتلاف المستندات المعالجة إلكترونيا وذلك من خلال قراصنة الكتابة أو استخدام برامج الكمبيوتر الجاهزة، ويختلف سبب القرصنة من قضية إلى أخرى فيعضها يكون بهدف مهاجمة جهاز الحاسوب لتدميره، أو لتحقيق مكاسب مالية شخصية (مثل سرقة معلومات بطاقات الائتمان، تحويل الأموال من حسابات مصرفية مختلفة إلى حساب المقرصن الخاص أو أي حسابات أخرى بالإضافة إلى ذلك يعتمد بعض المقرصنين على ابتزاز الشركات العالمية وتهديدها بنشر المعلومات الخاصة بها والسرية في حال عدم قيامهم بدفع أو تحويل المبلغ المالي المطلوب) إضافة إلى ما سبق ذكره هناك من يقوم باستهداف المواقع الحكومية الساخنة للحصول على الشهرة من خلال التغطية الصحفية الاعلامية.
- ✓ **استغلال الأطفال في المواد الإباحية**: ويشير هذا المصطلح إلى ظهور الأطفال والقصر (بأنهم الذين تقل أعمارهم عن 18 عاما) في صور أو أفلام أو مشاهد ذات طبيعة

إباحية أو مضمون جنسي، بما فيها مشاهد أو صور للاعتداء الجنسي على الأطفال وهي جريمة يعاقب عليها قانونيا في أغلب دول العالم، كما وتتعامل أغلب دول العالم بحسم وجدية مع هذا النوع من الجرائم على كل من تثبت عليه تهمة الاتجار أو تداول صور أو أفلام إباحية للأطفال، وكذلك المنظمات الدولية بشدة مثل اليونيسف والشرطة الدولية "الإنتربول."

- ✓ **المطاردة الالكترونية**: هو استخدام الإنترنت وغيره من الوسائل الإلكترونية لتعقب أو مطاردة أي فرد لأغراض الإحراج العام، أو المضايقات الشخصية، أو السرقة المالية وغيرها من الأمور بسلوك تهديدي. ويقوم المضايقون بجمع المعلومات الشخصية عن الضحية مثل اسمه، معلومات عن عائلته، أرقام هواتفه، مكان الاقامة ومكان العمل وما الى ذلك عن طريق مواقع الشبكات الاجتماعية والمدونات وغرف المحادثة وغيرها من المواقع.
- ✓ **الفيروسات وطريقة نشرها**: هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بمواقع او أجهزه أخرى، أو السيطرة عليها أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة. يتصف فيروس الحاسب بأنه برنامج قادر على التناسخ والانتشار، الفيروس يربط نفسه ببرنامج أخر يسمى الحاضن، لا يمكن أن تنشأ الفيروسات من ذاتها ويمكن أن تنتقل من حاسوب مصاب لآخر سليم، وأهم طرق الانتقال الآن هي الشبكة العنكبوتية (الإنترنت) تكون وسيلة سهلة لانتقال الفيروسات من جهاز لآخر ما لم تستخدم أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات، وكذلك عن طريق وسائط التخزين مثل ذاكرات الفلاش والأقراص الضوئية والمرنة سابقا ويأتي أيضا ضمن رسائل البريد الإلكتروني.
- ✓ **برامج القرصنة**: يقصد بالقرصنة هنا الاستخدام أو/والنسخ غير المشروع لنظم التشغيل أو/والبرامج الحاسب الآلي المختلفة، وقد تطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت صور القرصنة واتسعت وأصبح من الشائع جدا العثور على مواقع بالإنترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي. ومن هنا وجدت الكثير من الشركات مثل مايكروسوفت ضرورة حماية أنظمتها ووجدت أن أفضل أسلوب هو تعيين هؤلاء الهاكرز بمرتبات عالية مهمتهم محاولة

اختراق أنظمتها المختلفة والعثور على أماكن الضعف فيها، واقتراح سبل للوقاية اللازمة من الأضرار التي يتسبب فيها قراصنة الحاسوب، في هذه الحالة بدأت صورة الهاكر في كسب الكثير من الايجابيات إلا أن المسمى الأساسي واحد.

- ✓ **الاحتيال باستخدام بطاقات الائتمان عبر الإنترنت**: يهدف احتيال الإنترنت في العادة إلى الاحتيال على المستخدمين عن طريق سلب أموالهم (إما بسرقة أرقام بطاقات ائتمانهم أو بجعلهم يرسلون حوالات مالية أو شيكات) لغرض شخصي كالشراء عبر الإنترنت أو دفعهم إلى الكشف عن معلومات شخصية، بغرض التجسس أو انتحال الشخصية أو الحصول على معلومات حسابهم في مركز حساس، ويمكن تعريف احتيال بطاقات الائتمان بشكل عام على أنه خداع الشخص وسرقة معلوماته عن طريق الاستخدام الغير مصرح والغير مشروع به لبيانات البطاقة الائتمانية.

الجريمة الإلكترونية...المنظور النفسي، الاجتماعي والأمني:

يصف أستاذ علم الاجتماع الشهير بول تايلور وأساتذة آخرون في علم النفس، دوافع المجرمين الإلكترونيين بالفضول الشديد والانتقام، وأنهم يعانون من فراغ يسمح لهم بتمضية أوقات طويلة على شبكة الإنترنت، كما أنهم يتّصفون وفقاً لما جاء في كتاب The psychology of cybercrimeأو سيكولوجية الجرائم الإلكترونية، بأنهم يعانون من الوساوس القهرية، فلا يمكنهم السيطرة على رغبتهم في ملاحقة الآخرين وإيذائهم. كما أنهم مصابون باضطراب الشخصية النرجسية، ويعانون من تقدير ذات متدنٍّ، ولا يملكون القدرة على المواجهة أو التعامل مع المشكلات وإدارة العلاقات جيداً، ويفشلون في بناء علاقات صحّية، ويقلل اضطراب الشخصية النرجسية من قدرتهم على تقدير نتائج أفعالهم، ويرتكبون أفعالاً تخدم شهوتهم إلى الانتقام، أو فضول التجسّس لديهم، بغض النظر عن عواقب هذه الأفعال.(7)

كما أنّ استخدام الوسائل الإلكترونية في إيذاء الآخرين وملاحقتهم، متستّرين خلف هوية غير حقيقية، يشعرهم بمزيد من القوة والسيطرة اللتين تتطلّبهما نرجسيّتهم، وهوسهم المرضي بملاحقة ضحاياهم، وهو ما يوفره بسهولة الاتصال الدائم لهم ولضحاياهم على الشبكة العنكبوتية، من خلال أجهزة الهواتف والأجهزة المحمولة

الأخرى، المرتبطة دائماً بالإنترنت، حيث ترتكز استراتيجيتهم في إيذاء الآخرين على الإصرار والمطاردة، وتتبع أصدقائهم ومن يتفاعلون معهم على شبكات التواصل الاجتماعي، ليروّجوا إشاعاتهم عن ضحاياهم وتشويههم أمامهم، وتفيد دراسات أخرى بأن مجرمي الإنترنت هم أشخاص لديهم ميل مرتفع إلى القلق الخارج عن السيطرة، الذي يؤدّي إلى التهور في استخدام الوسائل الإلكترونية في شكل غير مدروس، في تصفية الحسابات والإساءة إلى الخصوم. كما أنّ لديهم اعتقاداً بأن الوسائل الإلكترونية أسرع في نشر الفضائح أو التشهير بالآخرين. وهم كذلك عرضة للاكتئاب أكثر وأسرع من غيرهم، ويشعرون بأن الإساءة الإلكترونية أكثر أماناً لهم، واهمين أن من الصعب الوصول إليهم أو تحديد هويتهم الحقيقية.[8]

ورغم أنه حتى الآن لم تظهر ملامح الصورة واضحة في تحديد صفات مجرمي الأنترنت والمعلومات وشرح سماتهم النفسية وتحديد دوافعهم، خاصة مع قلة الدراسات الخاصة بهذه الظاهرة من جهة، ولصعوبة الفهم الجيد لمداها الحقيقي من جهة ثانية، والتطورات السريعة الحاصلة في ميدان الكمبيوتر والإنترنت من جهة ثالثة، فالمزيد من الوسائل والتكنولوجيات يعني المزيد من التغير في أنماط الجريمة وطرق الاعتداء، مما يساهم في إحداث تغير في سمات مجرمي الإنترنت، ومع ذلك يمكن تصنيف مجرمي الإنترنت حسب المنظور النفسي إلى الفئات التالية:

- ✓ **فئة المتطفلين**:أفراد هذه الفئة يرتكبون هذا النوع من الجريمة بغرض التحدي والإبداع، لدرجة أنهم ينصبون أنفسهم أوصياء على أمن الحاسوب في المؤسسات المختلفة وحمايتها.
- ✓ **فئة المحترفين**:يتميز أفراد هذه الفئة بالخبرة والفهم الواسع للمهارات التقنية، وبالتنظيم والتخطيط للأنشطة المرتكبة، وبالتالي فهي الأخطر مقارنة بباقي الفئات، وأساس اعتداءات هو تحقيق الكسب المادي لهم أو للجهات التي كلفتهم أو مولتهم أو سخرتهم، وقد تهدف إلى تحقيق أغراض سياسية أو التعبير عن موقف معين فكري أو نظري أو فلسفي.

- ✓ **فئة الحاقدين**:أفراد هذه الطائفة يرتكبون اعتداءاتهم الإجرامية بدافع الرغبة في الانتقام والثأر، وقد يكون الهدف هو شن حرب معلوماتية تقوم بها حكومة أو جهة سيادية معينة في مواجهة أخرى معادية لها، تهدف من خلال ذلك إلى شل وتدمير المواقع الخدماتية في إطار ما يسمى بالحكومة الإلكترونية أو المجتمع المعلوماتي، ومن أهم ما يميز أفراد هذه الفئة هو عدم تفاخرهم بأنشطتهم الإجرامية بل يعمدون إلى إخفائها دون وجود أي تفاعل أو تبادل للمعلومات بين أعضائها.أما من المنظور الاجتماعي وفي ظل التطورات الهائلة لتكنولوجيا المعلومات، ونظراً للعدد الهائل من الأفراد والمؤسسات الذين يرتادون هذه الشبكة، فقد أصبح من السهل ارتكاب أبشع الجرائم بحق مرتاديها سواء كانوا أفراداً أم مؤسسات أم مجتمعات محافظة بأكملها، وهو ما دفع العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التي تهدد كل مستخدمي الإنترنت حيث أصبحت أسهل الوسائل أمام مرتكبي الجريمة، فراح المجرمون ينتهكون الأعراض ويغررون بالأطفال، إضافةً إلى اقترافهم لجرائم التشهير وتشويه السمعة عبر مواقع إلكترونية مخصصة لهذا الهدف.إن انتشار وتوسع إطار الجريمة الالكترونية في العالم أمر ليس مستبعدا في ظل التطورات والقفزات الالكترونية الهائلة التي تشهدها الكثير من البلدان، ورغما عن وجود قوانين لجرائم المعلوماتية وما تشتمل عليه من عقوبات رادعة لكل من تسول له نفسه ارتكاب جريمة الكترونية إلا أن الأمر يتطلب كثيرا من الجهد من قبل القائمين على أمر هذه التكنولوجيا، حيث أن انتشار الجريمة الالكترونية قد يؤدي إلى خلل عام قد يهدد المجتمع كله في اقتصاده وسيادته وأمنه القومي بما يتطلب حماية المواقع المهمة والاستراتيجية من خلال استخدام التقنيات المتطورة ووسائل الكشف المبكر عن عمليات الاختراق.[9]

ويؤكد بدرالدين ميرغني أستاذ علم الاجتماع بجامعة الرباط خلال المنتدى الدوري لمركز التنوير المعرفي حول الجريمة الالكترونية، إلى آخر إحصائيات تكلفة الجرائم الالكترونية على مستوى العالم، والتي بلغت 3 مليار دولار سنويا لاستغلال الأطفال جنسيا عبر الانترنت من خلال 100 ألف موقع إباحي للأطفال، وصل متوسط أعمارهم

الـ11 عام ذلك من خلال 26 شخصية كرتونية لاستدراجهم، وقال أن 25% من الاطفال تعرضوا للتحرش عبر الشات بجانب إفصاح 40% منهم عن بياناتهم الشخصية والعائلية بعفوية، وحذر بدرالدين ميرغني الأسر من استخدام أبنائهم للأنترنت وخطورة الموبايل بعد إضافة خدمات الانترنت، مشيرا إلى أن عدد المشتركين في الفيس بوك وصل إلى 500 مليون مشترك، مشددا على أحكام الرقابة على الأطفال وعدم السماح لهم بالاتصال الشبكي بشكل مستمر، ونادى الأسر بضرورة المراقبة اللصيقة لأبنائها ومنعهم من استخدامه بشكل مستدام خاصة عبر الموبايل، مشيرا إلى جهود شرطة المعلومات في مكافحة وصد هذا النوع من الجرائم، لما يترتب عليه من آثار اجتماعية وأخلاقية سيئة، مؤمنا على جهود القوات الأمنية في إجازة قوانين الجرائم الالكترونية حتى تواكب التطور التكنولوجي المتلاحق.[10]

أما المنظور الأمني للجريمة الإلكترونية فيعني بشكل كبير أمن المعلومات من خلال الحماية من الاختراق، والاستخدام أو الوصول غير المصرح به، إضافة إلى عمليات أخرى لا تقل خطورة عما ذكرنا سابقا كالنسخ، الاتلاف، التعديل، التوزيع، النشر، والتدمير...، كل هذه العمليات الخطيرة تبرز أهمية أمن المعلومات في تأمين المعلومات وحمايتها من الأخطار التي تحيط بها، ويقوم هذا الجانب بتوفير الحماية والأمان من مختلف أنواع الجريمة الإلكترونية. إن مناقشة الأمن في ظل هذه التطورات التقنية ليس بالأمر السهل ومصطلح أمن المعلومات مفهوم شامل يحوي عدة أمور منها، أمن الشبكات وأمن الأجهزة المستخدمة وأمن المنظمات والأمن القانوني، ولوضع تصور شامل لحماية وأمن المعلومات، فلا بد أن نأخذ في الحسبان السياسة الأمنية أمن الأجهزة والأدوات أمن الشبكات الأمن المنظم والأمن القانوني، والسياسة الأمنية تعتبر الغطاء الأمني لجميع الجوانب الأمنية، وهي التي تعطي كيفية إنجاز الأمن ويجب بنائها على المتطلبات وليس على الاعتبارات التقنية، والأهداف السياسية لأي سياسة أمنية يجب أن تكون لإبقاء السرية والسلامة والكمال والتوفر لكل أصول الثروة المعلوماتية للمؤسسات واتصالاتها، وتشير السرية إلى المعلومات السرية التي لا يراها إلا البعض مثل: المدراء والمشرفون وبعض المستخدمين، وهذه معلومات يجب أن تبقى خاصة بالمؤسسات وببعض المستخدمين ضمن المؤسسات، وهي أيضاً تحفظ المعلومات من

الاطلاع والكشف الغير مخول أو المفاجئ، وتشير السلامة والكمال إلى معلومات وبيانات المؤسسات، ومن المهم أن تكون دقيقة وحديثة جداً، والتكامل أو السلامة تحمي المعلومات من التعديل الغير مخول أو المفاجئ، أخيراً التوفر ويشير إلى الوصول إلى معلومات ومصادر المؤسسات، ومن المهم جداً أن تكون معلومات ومصادر المؤسسات متوفرة بسهولة، والتوفر يضمن الوصول الموثوق فيه للبيانات متى وأينما دعت الحاجة لذلك، ويجب على السياسة الأمنية أن تضع في الحسبان هذه الأهداف الثلاثة عند دراسة اي تهديدات محتملة على المؤسسة.[11]

وفي مجال قريب من أمن المؤسسات والهيئات، أصدر مكتب التحقيقات الفيدرالي الأمريكي " FBI " تقريراً حديثاً حذر فيه من ارتفاع متوقع لعدد ضحايا رسائل الاحتيال الإلكتروني في قطاع الأعمال، حيث تستهدف هذه الرسائل الشركات التجارية وتتسبب بخسائر مالية ضخمة، وأكد التقرير أن المخططين لهذه الرسائل يبذلون جهداً كبيراً في محاولة مطابقة عناوين البريد الإلكتروني، أو استخدام الهندسة الاجتماعية لانتحال شخصية الرئيس التنفيذي أو محامي الشركة المستهدفة، حيث يقومون بإجراء دراسة عن موظفي الشركة المسؤولين عن العمليات المالية، ويستخدمون صياغة محددة في رسائلهم لخداع الموظفين، ثم يطلبون في هذه الرسالة إجراء تحويل مصرفي مشبوه إلى حساباتهم، ورصد التقرير تنوّع شريحة الضحايا ما بين مؤسسات ضخمة وشركات تقنية وشركات ناشئة ومنظمات غير ربحية، وكانت الهجمات تستهدف الشركات التي لديها أعمال مع مورّدين أجانب، أو الشركات التي تقوم بعمليات تحويل مصرفي بشكل متكرر.[12]

وفي عام 2002 اكتشفت شركة Daewoo Securities أن ما قيمته 21.7 مليون دولاراً من الأسهم التي تديرها قد بيعت بشكل غير قانوني، وذلك نتيجة مباشرة لاختراق شبكة الحاسوب الخاصة بها،[13]وفي عام 2003 قام موظف بإحدى الشركات الروسية باختراق شبكة المعلومات الخاصة بالشركة، وقام بتعديل راتبه الشهري ومجموعة من زملائه بزيادة الرواتب بنسبة معينة مما أدى بخسائر مالية للشركة لعدة شهور لعدم اكتشاف هذا الاختراق.[14]

وأشار التقرير إلى ورود بلاغات عن عمليات الاحتيال هذه من جميع الولايات الأمريكية بالإضافة إلى79 دولة أخرى، كما تم رصد أكثر من 17 ألف ضحية لهذه العمليات ما بين شهرأكتوبر2013 وشهر فبراير 2016، وبالنسبة للخسائر المتوقعة لهذه العمليات فقدرها التقرير بـ 2.3 مليار دولار، مع ازدياد عمليات الاحتيال عبر البريد الإلكتروني بنسبة 270% منذ شهر يناير 2015، كما تراوحت الخسائر في ولاية أريزونا في كل عملية احتيالمابين 25 و75 ألفدولار. يذكر أن عدداً من الشركات الكبيرة تضررت من هذه الرسائل، حيث قام عدد من الموظفين في سناب شات " Snapchat "، وسيجيت "Seagate "، وفاست " Fast " بالوقوع ضحايا لرسائل البريد الاحتيالي، وقاموا بتحويلات مالية إلى هذه الحسابات.[15]

ولذلك فإن الوقاية هي أمثل الأساليب نفعا لصد هذه الجرائم ومن بينها :[16]

- استخدام جدار الحمايةfire well : وهو حاجز يوضع بين الشبكة الداخلية للأنترنت وخادم شبكة الأنترنت، ومن أهم مهامه فحص المعلومات الداخلة والخارجة والسماح لها بالمرور في حالة مطابقتها للمواصفات، وتقديم تقارير عن التحركات المشبوهة، ولكنه يمكن أن يعطل بعض المعلومات ويحدث عطب.
- التشفير: وهو تحويل المعلومة من نص واضح إلى آخر غير مفهوم، وقد أستحسن هذا النوع من النظام لنجاعته في عدم كشف المعلومات على شبكة الأنترنت.
- التوقيع الرقمي: وهو تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية.
- استخدام أنظمة كشف الاختراقات ووضع حلول للثغرات الأمنية
- وضع سياسة أمنية للشبكة وحشد كل الإمكانيات البشرية والمادية لتطبيقها.
- الاحتفاظ بنسخ احتياطية لكل المعلومات الحساسة في أقراص إضافية ليست مرتبطة. بالشبكة.
- تنصيب برامج لمنع ظهور الصور الخلاعية والاتصال بالمواقع الإرهابية.
- ضرورة استخدام بعض البرامج التي صممت خصيصا للكشف والوقاية من الفيروس والبعد عن استعمال كلمة السر البسيطة.
- عند فتح البريد الإلكتروني يجب معرفة من المرسل خشية أن يكون فيروس.

الجريمة الإلكترونية ..التشريعات والأنظمة (نماذج من تشريعات وأنظمة بعض الدول العربية)

تنبهت مؤخرا الدول العربية لمخاطر الجرائم المعلوماتية، مما جعل بعض المشرعين العرب يحاولون التصدي لهذا النوع من الجرائم، والذي فرضته التطورات التكنولوجية الحديثة والمتسارعة التي دخلت مختلف جوانب الحياة السياسية والاقتصادية والاجتماعية، سواء على مستوى الدول والحكومات التي بدأت تطبق التكنولوجيا الحديثة في العمل الإداري اليومي أو ما يسمى بالحكومة الإلكترونية، أو على مستوى القطاع الخاص والأفراد، من خلال الإقبال الكبير والاستخدام المتزايد على الكومبيوتر وتطبيقاته المختلفة الذي تشهده مختلف الدول العربية وإن تفاوت من قطر عربي إلى آخر.

الإمارات العربية المتحدة:

عدد المشرع الإماراتي في القانون رقم 2 للعام 2006م الجرائم التي يمكن أن تقع من خلال استخدام تقنية المعلومات مع عدم الإخلال بأي عقوبة أشد، وهذه الجرائم هي:[17]

1-جريمة اختراق المواقع والأنظمة الإلكترونية : والتي جعل عقوبتها الحبس أو الغرامة، وشدد العقاب إذا ترتب عليها نتيجة تتمثل في إلغاء أو حذف أو تدمير معلومات أو ترتب عليها نتيجة متعلقة بانتهاك معلومات شخصية أو في حال القيام بالفعل أثناء أو بسبب العمل أو التسهيل للغير بالقيام بالفعل.

2-جريمة التزوير لمستندات معترف بها معلوماتياً، والمستندات المعترف بها معلوماتياً هي مستندات الحكومة الاتحادية والمحلية معترفاً بها قانوناً في نظام معلوماتي وتكون عقوبته السجن المؤقت، وتكون العقوبة الحبس أو الغرامة إذا وقع التزوير في أي مستند أخر غير ما ذكر، ويعاقب الشخص الذي استعمل المستند المزور بالعقوبة المقررة لجريمة التزوير إذا ثبت علمه بالتزوير.

3- جريمة السرقة والاحتيال والاستيلاء على السندات وتوقيعها باستخدام الانترنت أو إحدى وسائل تقنية المعلومات، فبحسب المادة 10 من القانون المذكور يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن ثلاثين ألف درهم أو بإحدى هاتين العقوبتين, كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال أو على منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.

4- جريمة تعطيل الوصول إلى الوسائل أو البرامج أو المعلومات أو الشبكات.

5- جريمة العبث بالشبكة المعلوماتية أو إحدى وسائل التقنية، والتي يترتب عليها ضرر موصوف، والضرر الموصوف هو الضرر الذي يؤدي إلى إيقاف الشبكة أو إحدى وسائل التقنية عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات منها.

6- جريمة العبث بالمواقع الإلكترونية : وتشمل هذه الجريمة الدخول غير المصرح به لأي موقع الكتروني كان بقصد تغيير تصاميم هذا الموقع أو إلغائها و إتلافه أو تعديله.

7- جريمة إنشاء موقع أو نشر معلومات عبر الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للإتجار بالبشر.

8- جريمة إنشاء موقع الكتروني أو نشر معلومات للإتجار بالمخدرات أو المؤثرات العقلية وما في حكمها عبر الأنترنت.

9- جريمة انتهاك الحياة الخاصة الكترونياً: حيث عاقب المشرع الإماراتي على الاعتداء على أي من المبادئ أو القيم الأسرية أو نشر أخباراً أو صوراً تتصل بالحياة الخاصة أو العائلية للأفراد حتى ولو كانت صحيحة.

10- جريمة غسيل الأموال عبر الانترنت: حيث يعاقب المشرع الإماراتي بالقانون 2 للعام 2006 على هذه الجريمة بالحبس مدة لا تزيد على سبع سنوات والغرامة التي تتراوح بين ثلاثين ألف إلى مائة ألف درهم.

11- جريمة إنشاء مواقع الكترونية مخالفة للنظام العام والآداب أو استخدام الانترنت لهذه الغاية.

12-جريمة الحصول على معلومات سرية تتعلق بالحكومة عبر الانترنت، وعقوبتها السجن المؤقت، وتعامل البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت التجارية والاقتصادية نفس معاملة البيانات والمعلومات السرية المتعلقة بالحكومة.

13- جريمة العبث بالفحوص الطبية باستخدام الانترنت أو بإحدى وسائل التقنية.

14- جريمة التنصت باستخدام الانترنت أو إحدى وسائل التقنية، ويشمل التنصت التقاط واعتراض ما هو مرسل عبر الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

15-جريمة الاستيلاء على البطاقات الإلكترونية باستخدام الانترنت أو إحدى وسائل تقنية المعلومات.

16- جريمة المساس بالآداب العامة والتحريض على الدعارة باستخدام الانترنت أو إحدى وسائل تقنية المعلومات، وتكون العقوبة الحبس أو الغرامة وتشدد العقوبة إذا كان الفعل موجهاً إلى حدث.

17-جريمة المساس بالأديان عبر الانترنت: ولا يميز المشرع الإماراتي بين الشريعة الإسلامية وبين غيرها من الأديان، متى كانت مضمونة وفقاً للشريعة الإسلامية.

18-الجرائم الإرهابية عبر أو باستخدام الانترنت: وتكون العقوبة الحبس خمس سنوات.

19- جريمة التهديد باستخدام الإنترنت أو إحدى وسائل التقنية.
وتجدر الإشارة أيضاً إلى القانون الاتحادي رقم 7 للعام 2002م والذي نص على حماية مصنفات الحاسب الآلي وتطبيقاتها وقواعد البيانات وما يماثلها بشكل صريح.

دولة قطر:

1- جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية:[18]

المادة 2:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها.

وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة .

المادة 3:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك.

وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنه في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام

المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية ماله أو القائم على إدارته .

المادة 4:

يعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من التقط أو اعترض أو تنصت عمداً، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور .

2ـ جرائم المحتوى:[19]

المادة 5:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من أنشأ أو أدار موقعاً لجماعة أو تنظيم إرهابي على الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو سهل الاتصال بقيادات تلك الجماعات أو أي من أعضائها، أو الترويج لأفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية .

المادة 6:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من أنشأ أو أدار موقعاً إلكترونياً عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، لنشر أخبار غير صحيحة، بقصد تعريض سلامة الدولة أو نظامها العام أو أمنها الداخلي أو الخارجي للخطر.

ويعاقب بالحبس مدة لا تجاوز سنة، وبالغرامة التي لا تزيد على (250,000) مائتين وخمسين ألف ريال، أو بإحدى هاتين العقوبتين، كل من روج أو بث أو نشر، بأي وسيلة، تلك الأخبار غير الصحيحة بذات القصد .

المادة 7:

يعاقب بالحبس مدة لا تجاوز خمس سنوات، وبالغرامة التي لا تزيد على (500,000)

خمسمائة ألف ريال، كل من أنتج مادة إباحية عن طفل بواسطة وسائل تقنية المعلومات، أو استورد أو باع أو عرض للبيع أو الاستخدام أو تداول أو نقل أو وزع أو أرسل أو نشر أو أتاح أو بث مادة إباحية عن طفل بواسطة وسائل تقنية المعلومات.

ويعاقب بالحبس مدة لا تجاوز سنة، وبالغرامة التي لا تزيد على (250,000) مائتين وخمسين ألف ريال، أو بإحدى هاتين العقوبتين، كل من حاز مادة إباحية عن طفل، ولا يُعتد في الجرائم المعاقب عليها في هذه المادة برضا الطفل، ويعتبر طفلاً في حكم هذه المادة كل من لم يتم من العمر ثماني عشرة سنة ميلادية كاملة .

المادة 8:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من تعدى على أي من المبادئ أو القيم الاجتماعية، أو نشر أخباراً أو صوراً أو تسجيلات صوتية أو مرئية تتصل بحرمة الحياة الخاصة أو العائلية للأشخاص، ولو كانت صحيحة، أو تعدى على الغير بالسب أو القذف، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات .

المادة 9:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في تهديد أو ابتزاز شخص، لحمله على القيام بعمل أو الامتناع عنه.

3ـ التزوير والاحتيال الإلكتروني:[20]

المادة 10:

يعاقب بالحبس مدة لا تجاوز عشر سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، كل من زور محرراً إلكترونياً رسمياً أو استعمله مع علمه بذلك.

ويعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، إذا وقع التزوير على محرر إلكتروني غير رسمي واستعمله مع علمه بتزويره .

المادة 11:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلاً من الأفعال التالية:

1-استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في انتحال هوية لشخص طبيعي أو معنوي.

2-تمكن عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، من الاستيلاء لنفسه أو لغيره على مال منقول، أو على سند أو التوقيع عليه، بطريق الاحتيال، أو باتخاذ اسم كاذب، أو بانتحال صفة غير صحيحة .

4-جرائم بطاقة التعامل الإلكتروني:[21]

المادة 12:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلاً من الأفعال التالية:

1-استخدام أو حصل أو سهل الحصول دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

2-زور بطاقة تعامل إلكتروني بأي وسيلة كانت.

3- صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقات التعامل الإلكتروني.

4-استخدم أو سهل استخدام بطاقة تعامل إلكتروني مزورة مع علمه بذلك.

5-قَبل بطاقات تعامل إلكتروني غير سارية أو مزورة أو مسروقة مع علمه بذلك .

المملكة العربية السعودية:

نظام مكافحة جرائم المعلوماتية:[22]

المادة الأولى:

يقصد بالألفاظ والعبارات الآتية -أينما وردت في هذا النظام- المعاني المبينة أمامها ما لم يقتض السياق خلاف ذلك:

1-الشخص: أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة.

2-النظام المعلوماتي: مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.

3-الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الأنترنت)

4-البيانات: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.

5-برامج الحاسب الآلي: مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.

6-الحاسب الآلي: أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له.

7-الدخول غير المشروع: دخول شخص بطريقة معتمدة إلى حاسب آلي، أو موقع، إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.

8-الجريمة المعلوماتية: أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

9-الموقع الإلكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

10-الالتقاط: مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح.

المادة الثانية :

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

1-المساعدة على تحقيق الأمن المعلوماتي.
2-حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
3-حماية المصلحة العامة، والأخلاق، والآداب العامة.
4 - حماية الاقتصاد الوطني.

المادة الثالثة:

يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1-التنصت على ما هو مرسل عن طريق شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح -أو التقاطه أو اعتراضه.

2-الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا.

3-الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

4-المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.

5 - التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.
بشكل عام ليس كلّ الدول العربية تعير اهتماما لهذه الجرائم المستحدثة لكن واضح أن دول الخليج العربي المتمثلة في الإمارات العربية المتحدة تولي اهتماما لهذه الجرائم.

ففي مصر تم لأول مرة إنشاء إدارة عامة لمكافحة جرائم الحاسب الآلي وشبكة المعلومات، فرجال الشرطة المصرية يتلقون تكوينا في مجال مكافحة الجريمة المعلوماتية والتي أفشلت عدّة محاولات لسرقة بطاقة الائتمان عن طريق الانترنيت، التي قام بها شباب جامعي وكذا تم القبض على مهندس قام بإنشاء موقع لتشويه سمعة بنت رجل مصري مهم عن طريق الانترنت.

وقد صادقت تونس والأردن على اتفاقية تسمح بإمكانية استخدام التوقيع الالكتروني مما يفتح آفاق واسعة أمام معاملات الكترونية جديدة، وقد أصدرت تونس قانون 2001 فحواه أن العقد الالكتروني تسري عليه نفس أحكام العقد العادي فيما لا يخالف القواعد الآمرة في القانون.

قائمة المراجع:

(1) مفتاح بوبكر المطردي، الجريمة الإليكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان 23-2012/09/25.

(2) المرجع السابق.

(3) ذياب موسى البداينة، الجرائم الإليكترونية: المفهوم والأسباب، ورقة مقدمة إلى الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن، 2-2014/9/4.

(4) مفتاح بوبكر المطردي، مرجع سابق.

(5) عبد العال الديربي، الجريمة المعلوماتية: تعريفها، أسبابها، خصائصها، المركز العربي لأبحاث الفضاء الإليكتروني، القاهرة، جمهورية مصر العربية.

(6) إدارة مكافحة الجرائم الإليكترونية، الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإليكتروني، وزارة الداخلية، مملكة البحرين.

(7) نورا جبران، سيكولوجيا الجرائم الالكترونية: الأنترنت تعري استعدادنا للجريمة، جريدة الحياة، الرياض، الخميس 02 يوليو/تموز 2015.

(8) المرجع سابق.

(9) رجاء كامل، الجريمة الالكترونية ...الخطر داخل البيوت، تحقيقات وحوارات وزارة الدفاع السودانية، الخرطوم، 7 نوفمبر 2012.

(10) المرجع السابق.

(11)سلمان بن علي بن وهف القحطاني، أمن المعلومات في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة، ورقة مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد رقم 04، دبي – الأمارات العربية المتحدة، 26-2003/4/28.

(12) وزارة الاتصالات وتقنية المعلومات، المملكة العربية السعودية.

(13) خالد بن محمد الغثير، الاصطياد الإلكتروني: الأساليب والإجراءات المضادة، مكتبة الملك فهد الوطنية، الرياض: 2008، ص23.

(14) سليمان بن صالح العقلا، إنشاء الشبكات: المبادئ الأساسية لاختصاصي المكتبات والمعلومات، مكتبة الملك فهد الوطنية، الرياض: 2000، ص98.

(15)وزارة الاتصالات وتقنية المعلومات، المملكة العربية السعودية.

(16) سامر محمد سعيد، الأنترنت: المنافع والمخاطر، دار سعاد الصباح المطابع التعاونية الصحافية، بيروت: 1998، ص74.

(17) سليمان عباس العبد الله، إشكالية الجريمة الإلكترونية في القانون الجنائي المقارن، رسالة ماجستير، جامعة حلب، سوريا، 2009، ص 177.

(18) موقع الميزان، البوابة القانونية القطرية، www.almeezan.qa

(19) المرجع السابق.

(20) المرجع السابق.

(21) المرجع السابق.

(22) نظام مكافحة جرائم المعلوماتية، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية.