مجلة الحكمة للدراسات الفلسفية
Eissn :2602-5264 Issn : 2353-0499
المجلد 5/ العـدد: 3 (2017)، ص: 84-124

إجرام الفضاء السايبيري في الجزائر
بين التنفيذ و العقوبة
Cybercrime between execution and punishmentTitle

مليكة بقاح[1]

[1]جامعة الجزائر 2 كلية العلوم الانسانية – قسم علم الاعلام و الاتصال .

bbeggah@yahoo.fr

تاريخ الاستلام: 2017/07/25 تاريخ القبول: 11 /2017/08 تاريخ النشر: 2017/12/01

ملخص: تتسم الجريمة الالكترونية عن الجريمة التقليدية من حيث مفهومها وخصائصها و اركانها و كذا القانون الواجب التطبيق عليها، حيث اوجد الفقه الجنائي عدة معايير لتحديد ماهيتها منها معيار وسيلة ارتكاب الجريمة و معيار محل الجريمة ومعيار الجمع بين عدة معايير.و وفقا لذلك، اتسمت الجريمة الالكترونية بخصائص عديدة اهمها انها جريمة عابرة للحدود تمارس داخل او بواسطة النظام المعلوماتي ،وترتكب من طرف مجرم معلوماتي يوصف بالسرعة و الذكاء والمهارة ، كما انها صعبة الاثبات مقارنة بالجريمة العادية لأنها سريعة التنفيذ ومتطورة بتطور الوسائل التكنولوجية.و قد تناول البحث الإطار المفاهيمي للجريمة الإلكترونية عامة ومدى اهتمام المشرع الجزائري منها خاصة، وذلك من خلال التعديلات التي أدخلها على القوانين وأهمها فيما يخص الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجرائم التكنولوجية الواقعة على الأشخاص والحريات والكشف عن قانون العقوبات وقانون الإجراءات الجزائية الذي تحويه كل التشريعات العالمية بما سنته من قوانين خاصة بالجرائم الإلكترونية.

كلمات مفتاحية: الجريمة الالكترونية، المفهوم، مجرمي الفضاء الالكتروني، طرق المواجهة

Abstract: Electronic crime is distinguished from traditional crime in terms of its concept, characteristics, and pillars, as well as the law applicable to it. Criminal jurisprudence has created several criteria for determining what it is, including the standard of the means of committing the crime, the criterion of the place of the crime and the standard for combining several criteria.

Accordingly, electronic crime is characterized by many characteristics, the most important of which is that it is a cross-border crime practiced within or by the information system, and committed by an information criminal who is described with speed, intelligence and skill, and it is difficult to prove compared to ordinary crime because it is rapid implementation and advanced with the development of technological means

The research dealt with the conceptual framework of cybercrime in general and the extent of the Algerian legislator's interest in it in particular, through the amendments he made to the laws, the most important of which are with regard to crimes related to information and communication technology, technological crimes against persons and freedoms, and the disclosure of the penal code and the criminal procedure law contained in all legislation. The world, including the laws it enacted for electronic crimes.

Key words: cybercrime –concept-cyber criminals-Methods of confrontation.

***المؤلف المرسل:** مليكة بقاح

1. مقدمة

إن التطور التكنولوجي الذي شملته الوسائل الرقمية بما فيها الكمبيوتر، الهواتف الذكية واللوحات الإلكترونية وغيرها، أدى إلى بروز ثورة تقنية في شبكة الإتصال العالمية، وشيوع استخدامها خلق عالما جديدا لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها.

حيث ترتب عن هذه الثورة بروز أساليب وطرق إجرامية متقدمة، فإذا كانت لشبكة الأنترنت الكثير من المزايا، فإن المجرمون وجدوا في هذه الوسيلة ضالتهم إذ باتت طريقة آمنة للأعمال غير المشروعة. وعمدت عدة دول في سبيل مواجهة الجرائم المعلوماتية، إلى وضع سياسات جنائية تتنوع بين الوقاية والمواجهة، من خلال سن مجموعة من القوانين الموضوعية والإجرائية وذلك من أجل وضع حد لهذه الجرائم التي تكمن خطورتها في كونها جرائم مستحدثة وسهلة الارتكاب نتيجة للاستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات، كما أن آثارها ليست محصورة في النطاق الإقليمي لدولة معينة، فضلا على أن مرتكبيها يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية.

كما تستهدف الجرائم المعلوماتية محلا من طبيعة خاصة أي المعلومات التي يحتوي عليها نظام المعالجة الآلية، والذي هو عبارة عن إشارات ونبضات إلكترونية تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الإتصال العالمية بصورة آلية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة وخاصة فيما يخص إثبات هذه الجرائم وآلية مباشرة إجراءات الإستدلال والتحقيق عبر البيئة الإفتراضية لتعقب كافة المجرمين وتقديمهم للعدالة.

إن الجهات المكلفة بالبحث والتحري عن مجرمي الفضاء السايبيري متعودة على التعامل مع الجريمة بصورتها التقليدية، حيث يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية وملموسة في مسرح الجريمة من بصمات أو آثار أقدام أو بقع دم الا أن المشكلات الإجرائية التي ستواجه هذه الجهات عند تعاملها مع الجريمة الإلكترونية، تبدأ من طبيعة البيئة الإفتراضية التقنية التي ترتكب فيها، فهي لا تترك أي آثار مادية محسوسة، كما أن هذه

الجريمة تتم في الخفاء والظلام الشديد ،إذ كثيرا ما يعمد المجرم الإلكتروني إلى إخفاء نشاطه الجرمي عن طريق تلاعبه عن قصد بكل البيانات والمعطيات بدون دراية من المجنى عليه، إضافة للتمكن الكبير من تدمير الدليل ومحوه من مسرح الجريمة مما يزيد الأمر تعقيدا حيث يصعب كشفه والتحري عليه وكذا تحديد مرتكبيه.

وعلى ضوء ذلك فإن هذه الظاهرة الإجرامية التقنية أثارت العديد من التساؤلات على مستوى قانون الإجراءات الجزائية الذي وضعت نصوصه لتحكم الإجراءات المتعلقة بالجرائم التقليدية التي يجد المشرع صعوبة كبيرة في التحقيق فيها أو إثباتها وهو الأمر الذي دفع بالدول إلى العمل مليا للحد من هذه الجرائم من خلال كشفها باستعمال الوسائل الأمنية الوقائية وكذلك التوعية الازمة، حيث بات من الضروري تطوير السياسات التشريعية عموما والسياسات الجنائية على وجه الخصوص بعدما أضحى سوء استعمال الشبكة العنكبوتية تهديدا مباشرا للمنظومة الحقوقية عامة والشخصية خاصة، وكان لزاما على الدول أن تكثف جهودها لمواجهة كل الآثار السلبية المترتبة على إساءة استخدام تقنية الاتصالات والمعلومات.

وقد كان ذلك بأن قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون04 المتضمن للقواعد الخاصة 22/06 / المؤرخ في 20 ديسمبر 2006، بالإضافة إلى إصداره للقانون09 للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال، ومن خلالهما أوجد المشرع طرقا إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية.

و تهدف هذه الدراسة إلى تسليط الضوء على استغلال وسائل الاتصالات الحديثة ومنها الإنترنت وسائر صور الاتصال الالكتروني عبر الأقمار الصناعية من طرف مرتكبي الجرائم لتسهيل ارتكابهم لجرائمهم.

ولهذا سنسعي في بحثنا هذا الي ابراز التطور التاريخي للجريمة الالكترونية ، مروراً بتعريفها وخصائصها ، والصفات التي يتميز بها مرتكبها ، ومدى مواجهتها من خلال جرائم الأموال المقررة في قانون العقوبات الجزائري .

وبذلك تنقسم الدراسة إلي قسمين رئيسيين :

القسم الأول يتطرق إلى لتطور التاريخي للجريمة الالكترونية ، وتعريفها وخصائصها ، والصفات التي يتميز بها مرتكبها ، وفي القسم الثاني نسلط الضوء على كيفية مواجهتها داخليا بما قام بـه المشرع الجزائري بتعديل في قانون الإجراءات الجزائية للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال، و الطرق الإجرائية التي أوجدها و التي تتفق والطبيعة التقنية للجريمة المعلوماتية و أيضا نبين كيف تم مكافحتها على الصعيدين العربي و الدولي.

2. التطور التاريخي لجرائم الكمبيوتر والانترنت:

عرفت جرائم الأنترنت بتطور تاريخي تبعا لتطور التقنية واستخداماتها، حيث مرت بثلاث مراحل:

1.2 **المرحلة الأولى** : و تمتد من الستينات إلى السبعينات و ذلك منذ بدأ استخدام الحواسيب و التي تضاعف استخدامها مع بداية السبعينات.

2.2 **المرحلة الثانية والثالثة**: بدأت في بداية الثمانينات، حيث برز مفهوم جديد لجرائم الكمبيوتر والانترنت ارتبط بعملية اقتحام نظام الحواسيب عن بعد وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج . كما ظهر مصطلح "الهاكرز" و هو يعني مقتحمي النظم ، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورًا في رغبة المحترفين تجاوز امن المعلومات وإظهار تفوقهم التقني، لكن هؤلاء المغامرون أصبحوا أداة إجرام.

كما برزت طائفة مجرمي المعلوماتية المتفوقون في المجال الالكتروني و القادرين على ارتكاب أفعال تستهدف الحصول على المال أو التجسس أو الاستيلاء

على البيانات السرية والاقتصادية الاجتماعية والسياسية والعسكرية و حتى الشخصية.

أما المرحلة الثالثة فإنها فترة التسعينات التي عرفت ثورة عارمة في مجال التقنية و كذا تصعيدا في مجال الجرائم الالكترونية وتغييراً في مفهومهاً العام مسايرة مع ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات بحيث ظهرت أنماط جديدة:

إنكار الخدمة التي تقوم عل فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة لساعات في خسائر مالية بالملايين، ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت.

وظهرت الرسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على اثارة الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المروجة لمواد غير القانونية أو غير المشروعة.

رغم تزايد الأبحاث و محاولات ابتكار أنظمة تكفل لأي كمبيوتر الحماية اللازمة إلاّ أنه في المقابل يتم تطوير الإجراءات المضادة لهذه الحصون الأمنية، ومعنى ذلك أن خطر انتهاك أمن و سلامة الكمبيوتر مستمرة مدى استمرارية هذه التحصينات.

3. تعريف الجريمة الإلكترونية:

يصعب الاتفاق على تعريف موحد للجريمة المعلوماتية ، حيث اختلفت الاجتهادات في ذلك اختلافاً كبيرا ، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، و تباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى ، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة ، و يكون وسيلة لارتكابها

تارة اخرى، فكلما كان البحث منصباً على الجرائم التي ترتكب ضد النظام المعلوماتي انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي ، أما إذا كان البحث منصباً على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة و كان :" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي (هشام فريد رستم، 1992) . تجدر الاشارة أيضاً إلى أن أهم عوامل صعوبة الاتفاق على تعريف هو أن التقنية المعلوماتية أصبحت تحل محل العديد من التقنيات السابقة كالهاتف و الفاكس و التلفزيون ، فالمسألة لم تقتصر على معالجة البيانات فحسب با تعدتها إلى وظائف عديدة مثل وظيفة النشر و النسخ ، وهو ما يحتم ضرورة التفرقة بين جرائم الإنترنت وشبكات المعلومات بالمعنى الفني عن بقية الجرائم الأخرى التي يستخدم فيها الإنترنت أو الحاسب الآلي كأداة لارتكابها. فيقصد بجرائم الإنترنت وشبكات المعلومات الدخول غير المشروع إلى الشبكات الخاصة كالشركات والبنوك وغيرها وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات مثل تزييف البيانات أو إتلافها ومحوها، و امتلاك أدوات أو كلمات سرية لتسهيل ارتكاب مثل هذه الجرائم التي تلحق ضرراً بالبيانات والمعلومات ذاتها وكذلك بالنسبة للبرامج والأجهزة التي تحتويها وهي الجرائم التي تلعب فيها القنية المعلوماتية دوراً رئيسياً في مادياتها أو السلوك الإجرامي فيها. أما الجرائم التقليدية الأخرى مثل غسيل الأموال، تجارة المخدرات، الإرهاب، الدعارة، الاستخدام غير المشروع للكروت الإلكترونية، ودعارة الأطفال Pornography و جرائم التجارة الإلكترونية ، وكذلك جرائم السب و القذف ، هي جرائم تستخدم التقنية المعلوماتية كأداة في ارتكابها دون أن تكون جرائم معلوماتية بالمعنى الفني وإن كان يطلق عليها الجرائم المعلوماتية.(صالح أحمد البربري، 2001)

نصل إلى أن الجرائم المعلوماتية لها انواع و أصناف عديدة ، وكما أسلفنا القول فإن الجريمة المعلوماتية تتميز بأنها تضم نوعين من الجرائم المستحدثة ، الأول انواعاً مستحدثة من الاعتداء على مصالح محمية جنائياً بالنصوص القانونية التقليدية ، أي أن في هذه الحالات فإن طرق الاعتداء فقط هي المستحدثة لأنها تتم عن طريق التقنية المعلوماتية بعد أن كانت ترتكب بالسلوك المادي الملموس، أما محل الاعتداء فهي المصالح المحمية اصلا حماية جنائية على مر الأزمان و العصور كالأموال و الشرف و الاعتبار، أما النوع الثاني فيضم أنواعاً أخرى من الاعتداءات بالطرق المستحدثة على مصالح مستحدثة لم تعرفها القواعد التقليدية كالشبكات المعلوماتية التي تتعرض للإختراق أو التعطل.

كما 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 استنادًا لمعايير أخرى حسب القائلين بها، وهذا ما حدا بالأمم المتحدة – مدونتها بشأن الجريمة المعلوماتية – إلى عدم التوصل لتعريف متفق عليه دولياً ، 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 " ، كما عرفت أيضا بأنها " نشاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني " ، وعرفت أيضاً بأنها " كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية ، ويهدف إلى الاعتداء على أي مصلحة مشروعة ، سواء أكانت مادية أو معنوية ".

ومن خلال ما سبق نستطيع القول بأن الجريمة الإلكترونية هي عبارة عن أفعال غير مشروعة، يكون الحاسب الآلي محلا لها أو وسيلة لارتكابها .

كما أن بعض الدراسات و النشاطات العلمية قد اتجهت إلي تبني منهج يقوم علي تصنيف النشاطات المتعلقة بالحاسب الآلي إلي فئات و أنواع بمثابة مفترض وضروري لهذا الموضوع .

1.2 خصائص الجريمة الإلكترونية وتصنيفها:

لا شك أن المعلوماتية عادت على الإنسان بالخير الكثير، وطبعت مختلف جوانب حياته بطابع لم يكن ليحلم به قبل وقت قريب، فهذا التقدم العلمي الكبير في مجال المعلوماتية سهل حياة الإنسان ووفر عليه جهداً كبيراً وطبع شتى معاملاته بالسرعة الفائقة.

ولولا هذا التطور لاستغرقت من الوقت الكثير، كما أن هذه المعلوماتية وفرت على الإنسان الكثير من المال الذي كان سينفقه في قضاء حاجات أصبح يمكنه أن يقضيها في بيته بكبسة زر، لكن وفي المقابل فقد ارتبط استعمال هذه الوسائل الفنية الحديثة بظهور جرائم جديدة لم تكن معروفة من قبل، كما ارتبط بزيادة في حدة بعض الجرائم التي كانت موجودة من قبل، فهذه التقنية أوجدت ألوانا جديدة من الجرائم طبعتها بطابعها وأسبغت عليها خصائص ميزتها عن غيرها من الجرائم، سواء تعلقت هذه الخصائص بالشخص الذي يقدم علي هذه الجرائم فميزته عن المجرم التقليدي أو تعلقت بالجريمة ذاتها.

لذلك اختلفت الجريمة الالكترونية عن الجريمة التقليدية في عدة نواح، سواء كان هذا التميز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة.

أولا: خصوصية الجرائم الإلكترونية

للجرائم الإلكترونية مجموعة من الخصائص التي تميزها عن غيرها من الجرائم التقليدية نلخصها فيما يلي:

1: عدم وضوح الجرائم المعلوماتية

تتسم الجرائم الناشئة عن استخدام الانترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقد ا رت فنية تمكنه من جريمته بدقة مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم.(محمد عبيد الكعبي، 2012) كما أن وسيلة تنفيذها التي تميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى الأحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم في فقدان عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل الإثبات في مدة تقل عن الثانية الواحدة. (نهلا عبد القادر المومني، 2011).

حيث أن المجني يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية إذ تحرض أكثر الجهات التي تتعرض أنظمتها المعلوماتية لانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بن موظفيها عما تعرض له وتكتفي عادة بإجراءات داخلية إدارية دون الإبلاغ عنها السلطات المختصة تجنبا للأضرار أو بسمعتها ومكانتها وهو الثقة في كفاءتها (نهلا عبد القادر المومني، 2011).

2- صعوبة إثبات الجرائم الإلكترونية

تتميز الجرائم الإلكترونية بصعوبة إكتشافها، لأنها تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة.(محمد عبيد الكعبي، 2012).

أما إذا اكتشفت وهي حالات قليلة مقارنة بما تم اكتشافه من الجرائم التقليدية فيكون ذلك بمحض الصدفة، وقد ترجع الأسباب التي تقف وراء الصعوبة في اكتشاف هذا النوع من الإجرام إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية.

كما أن الجاني يملك القدرة على تدمير دليل إدانته، في أقل من ثانية مما يشكل عاملا إضافيا في صعوبة إكتشاف هذا النوع من الجرائم، الذي تصل أدلة الإدانة فيها إلى حدود 20% (حسين صالح دويب، 2010). ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلبه لاكتشافها والبحث عنها، وتستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف التقية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي الذي يسعى للقضاء على هذه الظاهرة.

كما أن القوانين التقليدية لم تعد قادرة على مواكبة السرعة الهائلة في التكنولوجيا والتي أدت إلى تطور الجريمة من خلالها، وظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها(طارق الشدى،). ما يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية.

3- الأساليب المستخدمة في ارتكاب الجرائم الإلكترونية

إن الجرائم المعلوماتية تبرز ذاتيتها بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها فإذا كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو حال جريمة السرقة. (ذياب البداينة، 2009).

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية الإنترنت مع وجود مجرم يوظف خبرته وقدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس

أو اخترا ق خصوصيات الغير للتغرير بالقاصرين كل ذلك دون الحاجة لسفك الدماء.

4: ضخامة الخسائر المادية والمعنوية

لجرائم الحاسب الآلي خسائر جسيمة على المستوى الإقتصادي، سواء (ذياب البداينة، 2009) كانت بسرقة البرامج أو محوها، أو تدمير قاعدة البيانات، أو اختلاس مبالغ مالية من بعض الحسابات حيث تصل أحيانا الخسائر إلى ملايير الدولارات.

5: التلوث الثقافي:

إن جرائم الكمبيوتر لا تصيب الأثر المادي فحسب بل يتعدى ذلك ليهدد نظام القيم والأخلاق، خاصة في المجتمعات المحافظة، فنشر المواد الإباحية وغير الأخلاقية في بعض المجتمعات من شأنها أن تؤدي إلى هدم القيم والتلويث في هذه المجتمعات، كما قد يؤدي إلى التفسخ الاجتماعي الذي يؤثر سلبا على المجتمعات الإسلامية (ذياب البداينة، 2009).

6: خاصية اشتراك الأشخاص في الإجرام الإلكتروني

تتميز الجريمة المعلوماتية عادة أنها تتم بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني عليها، وغالب ما يشترك في إخراج الجريمة المعلوماتية إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك أيضا في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون إشراكا سلبيا وهو الذي يترجم بصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيلها وإتمامها، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك ما يتمثل في مساعدة فنية ومادية.

7: الجريمة المعلوماتية جريمة عابرة للحدود

بعد ظهور شبكات المعلومات لم يعد هناك كحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أنّ أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد(.نهلا عبد القادر المومني، 2011).

والسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة أيضا مما جعل بالإمكان اِرتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى .هذه الطبيعة تتميز بها الجريمة المعلوماتية كونها جريمة عابرة الحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة اختصاص القضائي بهذه الجريمة.(Mascala corinne, 2000)

فهل هي الدولة التي وقع بها النشاط الإجرامي، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثارت الطبيعة أيضا الشكوك حول مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة(.نائلة عادل فريد قورة، 2004) الحقيقة أن عملية التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر الوسائل التي تثير الإشكالات في مجال الحاسوب، وبشكل خاص الإجراءات الجنائية والاختصاص والقانون والواجب والتطبيق، وهذا بدوره عامل رئيسي في نماء دعواته تضافر الجهود الدولية لمكافحة هذه الجرائم، ولعل هذه السمة تذكرنا بإرهاصات جرم المخدرات والاتجار بالرقيق وغيرها من الجرائم التي وقف تباين الدول واختلاف مستويات الحماية الجنائية فيها حائلا دون نجاعة أساليب مكافحتها، فلم يكن من يد غير الدخول في سلسلة اتفاقيات ومعاهدات دولية لمكافحتها (جعفر حسن جاسم الطائي، 2007).

وهكذا فإن جرائم الكمبيوتر في نطاق الظاهرة الاجرامية المستحدثة والتي لم تعد كذلك بالنظر إلى أول حالة موثقة للجريمة الإلكترونية والتي تعود لعام 1959 وبالنظر لنحو 36 عاما من التعايش الدولي مع صور مختلفة ومتغايرة من هذ الجرائم كالجرائم التي تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج) وتطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب بوصفه نظاما حقق التزاوج بين تقنيات الحوسبة والاتصالات.

- جرائم الكمبيوتر والانترنت طائفة من الجرائم التي تتسم بسمات مخصوصة عن غيرها من الجرائم، فهي تستهدف معنويات وليست ماديات محسوسة ، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي ان جاز التعبير.
- كما انها تتسم بالخطورة البالغة نظرا لأغراضها المتعددة، ولحجم الخسائر الناجم عنها قياسا بالجرائم التقليدية، ولارتكابها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم امرا صعبا. إضافة لكونها تنطوي بذاتها على سلوكيات غير مألوفة، وبما اتاحته من تسهيل ارتكاب الجرائم الاخرى تمثل ايجاد وسائل تجعل ملاحقة الجرائم التقليدية امرا صعبا متى ما ارتكبت باستخدام الكمبيوتر.
- وتحقيق وتحري جرائم الكمبيوتر والانترنت والمقاضاة في نطاقها تنطوي على مشكلات وتحديات ادارية وقانونية تتصل ابتداء بمعيقات ومتطلبات عمليات ملاحقة الجناة، فان تحققت مكنة الملاحقة اصبحت الادانة صعبة لسهولة اتلاف الادلة من قبل الجناة او لصعوبة الوصول الى الادلة او لغياب الاعتراف القانوني بطبيعة الادلة المتعلقة بهذه الجرائم.
- ونظرا لأنها جرائم لا تحدها حدود وتعد من الجرائم العابرة للحدود، فتثير لذلك تحديات ومعيقات في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

ان جرائم الكمبيوتر قد ترتكب عن طريق حاسب آلي في دولة ما، في حين يتحقق الفعل الاجرامي في دولة أخرى (.الأستاذ Ulrich Seiber، 1994) فجرائم الكمبيوتر والانترنت، لا تحدها حدود ولا تعترف ابتداء – في هذه المرحلة من تطورها بسبب شبكات المعلومات – بعنصر المكان او حدود الجغرافيا.

تتميز أيضا بالتباعد الجغرافي بين الفاعل والمجني عليه، ومن الوجهة التقنية، بين الحاسوب أداة الجريمة، وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدفة بالاعتداء، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكنه، وبفعل سيادة تقنيات شبكات النظم والمعلومات، امتد خارج هذه الحدود - دون تغيير في الاحتياجات التقنية - ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محل الاعتداء.

والحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقق النتيجة من أكثر المسائل التي تثير اشكالات في مجال جرائم الحاسوب وبشكل خاص الاجراءات الجنائية والاختصاص والقانون الواجب التطبيق. وهذا بدوره عامل رئيس في نماء دعوات تظافر الجهود الدولية لمكافحة هذه الجرائم.

ولعل هذه السمة تذكرنا بإرهاصات جرائم المخدرات والاتجار بالرقيق وغيرها من الجرائم التي وقف تباين الدول واختلاف مستويات الحماية الجنائية فيها حائلا دون نجاعة أساليب مكافحتها، فلم يكن من بد غير الدخول في سلسلة اتفاقيات ومعاهدات دولية لمكافحة هذه الجرائم، وذات الامر يقال الان بشان انشطة غسل الاموال، وهي في ذات الوقت الأسباب ذاتها التي تجعل موضوع جرائم الارهاب والجرائم المنظمة والجرائم الاقتصادية المواضيع الرئيسة على اجندة اهتمام المجتمع الدولي.

ولمواجهة مثل هذه الجريمة (جريمة الحاسوب) العابرة للحدود مواجهة فعالة، يجب تجريم صورها في القانون الوطني للمعاقبة عليها، وان يكون هناك

تعاون وتضامن دولي لمواجهة مشاكلها من حيث مكان وقوعها واختصاص المحاكم بها وجمع المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد صورها وقواعد التسليم فيها وايجاد الحلول لمشكلاتها الاساسية وابرزها:

1. غياب مفهوم عام متفق عليه بين الدول -حتى الآن- حول نماذج النشاط المكون للجريمة المتعلقة بالكمبيوتر والانترنت.
2. غياب الاتفاق حول التعريف القانوني للنشاط الاجرامي المتعلق بهذا النوع من الاجرام.
3. نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة ان وجدت وجمع المعلومات والأدلة عنها للإدانة فيها.
4. عدم كفاءة وملاءمة السلطات التي ينص عليها القانون بالنسبة للتحري واختراق نظم الكمبيوتر، لأنها عادة متعلقة بالضبط والتحري بالنسبة لوقائع مادية هي الجرائم التقليدية وغير متوائمة مع غير (الماديات) كاختراق المعلومات المبرمجة وتغييرها في الكمبيوتر.
5. عدم التناسب بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري في الجرائم المتعلقة بالحاسوب.
6. السمة الغالبة للكثير من جرائم الكمبيوتر هي أنها – كما اوضحنا اعلاه - من النوع العابر للحدود Transnational وبالتالي تثير من المشاكل ما تثيره أمثال تلك الجرائم كجرائم الاتجار بالمخدرات والاتجار غير المشروع في الأسلحة والاتجار في الرقيق الأبيض والجرائم الاقتصادية والمالية وجرائم التلوث البيئي.
7. عدم وجود معاهدات للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي أو عدم كفايتها ان كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر وديناميةالتحريات فيها وكفالة السرعة بها". ويمثل مشروع الاتفاقية الاوروبية لجرائم الكمبيوتر في الوقت الحاضر المشروع الاكثر

نضجا لموجهة جرائم الكمبيوتر بل وواحدا من اهم ادوات التعاون الدولي في هذا الحقل.

وعوضا عن هذه المشكلات، فإننا نرى أن من أبرز المشاكل التي تواجه سياسات مكافحة جرائم الحاسوب لا على الصعيد الدولي بل وفي نطاق التشريعات الوطنية، عدم التعامل معها كوحدة واحدة في اطار الحماية الجنائية للمعلومات. وقد عالجنا هذه المسألة في الكتاب الاول من هذه الموسوعة حيث أن التعامل على الصعيد الدولي، وكذلك على صعيد التشريع الوطني بشأن توفير الحماية الجنائية للمعلومات قد تم -كما يذكر الفقيه Utrich seiber- من خلال السعي لتشييد الحماية الجنائية لكل من الحياة الخاصة، الأموال (المعلومات المجسدة للمال على ما نرى) والحقوق الذهنية ازاء اجرام تقنية المعلوماتّ،(الأستاذ Ulrich Seiber ، 1994) كل على حده.

ثانيا: السمات الخاصة بالمجرم المعلوماتي

تتطلب الجريمة المعلوماتية مقدرة عقلية وذهنية خاصة لدى الجاني حيث أن الاعتداءات المرتكبة لا تتطلب إجراءات تميل إلى العنف بقدر ما تتطلب المامًا بقدر معين من المعرفة، فهو مجرم ذو كفاءة عالية في مجال التقنّية يحتاج إلى جهاز حاسوب موصول بشبكة الإنترنت إلى جانب درايته بمختلف الأنظمة المستعملة في هذا المجال ويمكن حصر هذه السمات على النحو التالي:

1: المهارة والخبرة المكتسبة لتنفيذ الفعل الإجرامي:

تعني المهارة والخبرة على التعرف بكافة الظروف التي تحيط بالجريمة المراد تنفيذها، وامكانيات نجاحها، واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائهم بالتعرف على كافة الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم، وتميز المعرفة بمفهومها السابق مجرمي

الانترنت، حيث يستطيع .مجرم الانترنت أن يكون تصورا كاملا لجريمته (طارق إبراهيم الدسوقي عطية، 2009).

يتمتع مجرمي الانترنت بقدر لا يستهان به من المهارة بتقنيات الحاسوب والإنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ جريمة الإنترنت يتطلب قدار من المهارة لدى الفاعل التي قد يكتسبها المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات.(Mascala courinne,2000)

ان إجرام الإنترنت هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فمجرم الإنترنت يسعى بشغف إلى المعرفة طرق جديدة مبتكرة لا يعرفها أحد سواه وذلك من أجل اختراق الحواجز الأمنية في البيئة الالكترونية ثم نيل مبتغاه.

2 :مجرم الانترنت يبرر ارتكاب جرائمه

يوجد شعور لدى مرتكب فعل إجرام الانترنت أن ما يقوم به لا يدخل في عداد الج ا رئم أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند قهر نظام الكمبيوتر وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص، الأمر الذي يعدونه غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.

إذ أن هؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب ويبدو أن الاستخدام المتزايد للأنظمة المعلوماتية، قد أنشأ مناخًا نفسيا ملائما لتصور استبعاد فكرة الخير والشر، مما ساعد على عدم وجود احتكاك مباشر بالأشخاص ومما لا شك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل

والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على لإيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.(نهلا عبد القادر المومني، 2011).

3: الإرتباك والخوف من كشف الجريمة

يتصف المجرمون عبر الانترنت بالخوف من كشف الجرائم المختلفة التي يرتكبونها وكذا افتضاح أمرهم، وبالرغم من هذا الخوف الذي يصاحب المجرمين على اختلاف أنماطهم، إلاّ أنّها تميز مجرمي الانترنت بصفة خاصة، لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان. (نهلا عبد القادر المومني، 2011).

كما تساعد طبيعة الأنظمة المعلوماتية نفسها مجرمي الانترنت على الحفاظ على سرية أفعالهم، ذلك أن الكثير ما يعرض المجرم إلى اكتشاف أمره هو أن تحدث أمور أثناء تنفيذه لجريمته غير متوقعة لا يمكن التنبؤ بها، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المرتكبة عبر الانترنت هي آلات الحواسيب التي تؤدي عملها غالبا بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى.

4: الميل إلى تقليد المهارات في ارتكاب الجرائم:

يبلغ الميل إلى التقليد أقصاه حينما يوجد الفرد وسط الجماعة، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير الغير عليه، ويظهر ذلك في مجال الجريمة المرتكبة عبر الانترنت، لأن أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية مِما يؤدي به الأمر إلى ارتكاب الجرائم.ولا شك أن ذلك نتيجة لعدم الاستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط أخلاقية يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط به، فينتهي به الأمر إلى التقليد وارتكاب الجريمة (أيمن عبد الحفيظ، د س).

5: التخطيط التنظيم:

في عالم الشبكات الالكترونية وخاصة شبكة العالمية للأنترنت، كما هو الحال في العالم الحقيقي يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة، حيث ترتكب أغلب الجرائم من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معين ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمنا فيها متخصص في الحاسبات يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب ولتحويل المكاسب إليه، كما أن من عادة من يما رسون التلصص والقرصنة على الحاسبات وشبكات المعلومات بصفة منتظمة حول أنشطن هم عقد المؤتمرات. (هشام محمد فريد، دس)

6: التكيف الاجتماعي:

تعتبر هذه الخاصية امتدادًا لسمة التخطيط والتنظيم، حيث أن التكيف الاجتماعي ينشأ بين مجموعة لها صفات مشتركة فمثلا جماعة صغار نوابغ المعلوماتية لا شك أنهم يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم صفات وروابط تساعدهم على ارتكاب جرائمهم وتتعدى تلك الروابط والصلات النطاق المحلي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي، ولاشك أن إقامة تلك المؤتمرات ا رت الدولية في هؤلاء المجموعات خير دليل على وجود تلك الصلات والروابط الدولية بينها. (أيمن عبد الحفيظ، د س).

بالإضافة إلى أن مجرمي الإنترنت هم عادة أناس اجتماعيون قادرين على التكيف في بيئتهم الاجتماعية، ولا يضعون أنفسهم في حالة عداء مع المجتمع الذي يحيط بهم، بل قادرين على التوافق والتصالح مع مجتمعهم باعتبارهم أناس

مرتفعو الذكاء، بل أن خطورتهم الإجرامية قد تزداد إذا تمت زيادات تكيفهم الاجتماعي مع توافر الشخصية والدوافع الإجرامية لديهم.

7: سلطة الشفرة التي يتميز بها المجرم المعلوماتي

وهي التي تمكنه من ارتكاب جريمته فقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات وتعديل أو محو المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها وقد تتمثل هذه السلطة في الحق في استعمال الكمبيوتر أو إجراء بعض التعاملات. وقد تكوف هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

8: الهدف من ارتكاب الجريمة

قد لا تختلف في الكثير من الأحيان عن الهدف من ارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي، وبطريق غير مشروع، يظل الهدف الأول من ارتكاب الجرائم الإلكترونية، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الكمبيوتر، وتخطي حواجز الحماية الدائرة حوله وأخيرا الانتقام في كثير من الأحيان من رب المسؤول في العمل أو من أحد الزملاء.

9: التطور في السلوك الإجرامي

يساهم وجود المجرم في الانترنت في جماعة إجرامية إلى التأثير في قدرته العقلية وسرعة اكتسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى أعلى معدلات المهارة التقنية المتمثلة في اثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة (أيمن عبد الحفيظ، د س). وبناءًا على ما تقدم يمكن أن نقسم المجرم المعلوماتي إلى مجموعة من الطوائف المختلفة:

القراصنة المخترقون : يتحد في هذا الإطار نوعين من المخترقين أو المتطفلين:

- الهاكرز: (Les hackers) -

يعرف الهاكرز بأنه الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي،(أسامة سمير حسين، 2011) ويقصد بهم الشباب البالغ المقترن بالمعلوماتية، والحاسبات الآلية، وبعضهم يطلق عليهم صغار نوابغ المعلوماتية، وأغلب هذه الطائفة هم من الطلبة والشباب حاصلين على معرفة في مجال التقنية المعلوماتية.

أما الباعث الأساسي لهذه الطائفة هو الاستمتاع باللعب والمزاح باستخدام هذه التقنية، لإثبات مهاراتهم وقدراتهم باكتشاف وإظهار مواطن الضعف في الأنظمة المعلوماتية، دون أي إلحاق ضرر بها، بحيث يمتلكون الرغبة في المغامرة والتحري وكذا الرغبة في الاكتشاف. (عبد الفتاح بيومي حجازي، 2006).

- الكراكز: les crackers

كلمة مستمدة من الفعل الإنجليزي (Crak)، وتعني الكسر والتحطيم وهو ما يتميز به هؤلاء القراصنة، فهم يستخدمون البرامج والتقنيات في محاولاتهم لاختراق الأنظمة المعلوماتية بهدف الحصول على المعلومات أو القيام بعمليات تخريبية. (محمد قدري حسن عبد الرحمان، 2011)

وتعكس اعتداءات هؤلاء المخترقين ميولات إجرامية جد خطرة وهو ما أكدته بعض التشريعات المحلية في الولايات المتحدة الأمريكية، حيث اعتبرت مصطلح الكراكر مرادفا للهجمات الإجرامية الحاذقة والمؤذية.(محمد دباس الحميد، 2007)

تعرف هذه الطائفة بالمجرمين البالغين أو المخربين المهنيين وأعمارهم تتراوح بين 25-45 عاما. ومن أبرز سمات وخصائص أفراد هذه الطائفة، أنهم ذوي مكانة في المجتمع وأنهم دائما ما يكونوا من المتخصصين في مجال التقنية الالكترونية.

حيث أنهم يتمتعون بالمهارات، ومعارف فنية في مجال الأنظمة الالكترونية أو المعلوماتية تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات.(صلاح بوتاني دلخار، 2016).

- المجرمون المحترفون:

تتميز هذه الطائفة بسعة الخبرة والإد راك الواسع للمها رات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي تتركب من قبل أفرادها، وهكذا فإن هذه الطائفة تعد الأخطر من بين مجرمي التقنية حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم وللجهات التي كلفتهم اعتداءاتهم في مقابل تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم الكمبيوتر، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي، بحيث يعملون بشكل مجموعات إجرامية تتميز بالتنظيم والتخطيط لكافة أعمالهم.(أحمد محمود مصطفى، 2010).

هذه الفئة تعكس اعتداءات وميولات إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب ويتميز هؤلاء بقد راتهم التقنية الواسعة، وخبرتهم في مجال الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون أضرار كبيرة.

- المجرمون المهنيون أو الحاقدون:

هذه الطائفة لا يغلب عليها عدم توافر الأهداف وأغراض الجريمة المتوفرة لدى الطوائف التي سبق ذكرها، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارية، وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لصاحب العمل معهم، أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام، بوصفهم موظفين أو مشتركين أو علاقة بالنظام محل

الجريمة، أو إلى غرباء عن النظام حيث تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم.

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يسعى الواحد منهم إلى كافة عناصر المعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه، وتغلب على أنشطتهم الناحية التقنية واستخدام تقنيات الفيروسات والبرامج وكذا تعطيل النظام أو الموقع المستهدف إن كان من مواقع الانترنت.(أحمد محمود مصطفى، 2010)

كما قد تكون دوافعهم لارتكاب الجرائم هي تحقيق غايات شخصية وليس هناك ضوابط محددة بشأن أعمارهم، كما لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة ولا يفاخرون بأنشطتهم بل يعمدون على إخفاءها، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد على ذلك.(نهلا عبد القادر المومني، 2008)

- فئة صغار السن:

كما يسميهم البعض "صغار نوابغ المعلوماتية" يصفهم بأنهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية ، فإن من بينهم في الحقيقة فئة لم تزل دون سن الأهلية مولعين بالحوسبة والاتصال، وقد تعددت أوصافهم في الدراسات الاستطلاعية والمسحية.

وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح" المتلعثمين"، الدال حسب تعبير الأستاذ "توم فو رلستر "على الصغار المتحمسين للحاسوب، والشعور بالبهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب ويسميهم البعض كذلك بمجانين معدلات ومعدلات عكسية، بالاستناد إلى كثرة استخدامهم لتقنية المعدل والمعدل العكسي "الموديم"، الذي يعتمد على الاتصال الهاتفي لاختراق شبكة النظم.(نسرين عبد الحميد نبيه،)

ويثير مجرمو الحوسبة من هذه الطائفة جدلا واسعا ،ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، على الأقل مواصلتها العبث بالحواسيب ظهرت مؤلفات ودراسات تدافع عن هذه الفئة، لتخرجها من دائرة الإجرام إلى دائرة العبث، وأحيانا البطولة من هذه المؤلفات على سبيل المثال، كتاب "خارج نطاق الدائرة الداخلية كيف تعملها؟ "لمؤلفه الأمريكي بيل لاندري، وكتاب "الدليل الجديد للمتلعثمين" لمؤلفه هوجوكوزن، وكتاب "المتلعثمون، أبطال ثورة الحاسوب" لمؤلفه ستيفن ليفي.(جعفر حسن جاسم الطائي،)

ومن الأمثلة الشهيرة لجرائم الكمبيوتر التي ارتكبت من طرف هذه الفئة، العصابة الشهيرة التي أطلق عليها (عصابة 414) والتي انتسب إليها ارتكاب 60 فعل تعد في الولايات المتحدة الأمريكية على ذاكرات الكمبيوتر، والتي تسببت في أضرار كبيرة لحقت بالمنشآت العامة والخاصة، كما سبب متلعثمو ألمانيا الغربية عام 1984 فوضى عارمة، عندما دخلوا شبكة (الفيديو تكس)، حيث نجح بعض المتلعثمون الفرنسيون لإيجاد مدخل إلى الملفات السرية لبرنامج ذري فرنسي.(عمر أبو الفتوح عبد العظيم الحمامي، 2010)

ويمكن رد الاتجاهات التقديرية لطبيعة هذه الفئة وسمات أفرادها، ومدى خطورتهم في نطاق ظاهرة جرائم الحاسوب إلى ثلاثة اتجاهات:

- **الإتجاه الأول**

اتجاه لا يرى إصباغ أية صفة جرمية على هذه الفئة، أو على الأفعال التي تقوم بها، ولا وجوب لتصنيفهم ضمن الطوائف الإجرامية لمجرمي المعلوماتية، استنادا لا يرى إصباغ أية صفة جرمية على هذه الفئة، أو على الأفعال التي تقوم بها، ولا وجوب لتصنيفهم ضمن الطوائف الإجرامية لمجرمي المعلوماتية، استنادا إلى أن صغار السن لديهم ببساطة ميل للمغامرة والتحدي والرغبة في الاكتشاف، وقلما تكون أهداف أفعالهم المحضورة غير شرعية.

- **الإتجاه الثاني**

هذا الإتجاه يحتفي بهذه الفئة ويناصرها ويعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية، ويصفهم بالأخيار وأحيانا بالأبطال الشعبيين، ويتمادى هذا الإتجاه في تقديره لهذه الطائفة أو الفئة بالمطالبة بمكافئتهم باعتبارهم لا يسببون ضررا للنظام، ولا يقومون بأعمال الإحتيال.

- **الإتجاه الثالث**

يرى أصحاب هذا الإتجاه أن مرتكبي جرائم المعلوماتية من هذه الطائفة، يصنفون ضمن مجرمي الكمبيوتر كغيرهم دون تمييز، استنادا إلى أن تحديد الحد الفاصل بين العبث في الحواسيب وبين الجريمة أمر عسير من جهة، ودونما أثر على وصف الفعل قانونا من جهة أخرى، واستنادا إلى أن خطورة أفعالهم التي تتسم بالنتهاك الأنظمة واختراق الحواسيب.

كما أن تجاوز إجراءات الأمن والتي تعد بحق من أكثر جرائم الحاسوب تعقيدا من الوجهة التقنية، عوضا عن مخاطرها المدمرة، حيث يدعم صحة هذا الإتجاه التخوفات التي يثيرها أصحاب الإتجاه الأول ذاتهم، حيث يخشون من الخطر الذي يواجه هذه الطائفة، والمتمثل باحتمال الإنزلاق من مجرد هو صغير لاقتراف الأفعال غير المشروعة إلى محترف لأعمال السلب والإحتيال.

هذا إلى جانب آخر أكثر خطورة يتمثل في احتضان منظمات الإجرام ومجرمين غارقين في الإجرام لهؤلاء الشباب، واستغلالهم من طرف منظمات الإجرام المنظم.

2.4 الإجراءات الوطنية والدولية لمواجهة جرائم الكمبيوتر:

أولا: على المستوى الوطني

قام المشرع الجزائري بتعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال و كان ذلك

بموجب القانون رقم لأمر15/04 المؤرخ في2004/11/10 المتمم والمعدل لأمر 156/66المتضمن لقانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات ، فقد أثار المشرع الجزائري إستخدامه لمصطلح لدلالة على كلمة المعلومات والنظام الذي يحتوي عليها ويخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة إرتكابها وحصرها فقط في صور الأفعال التي تشكل إعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها. (سعيد نعيم، 2012)

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها ، فقام بحماية هذه المعطيات من أوجه عدة. ثم في مرحلة لاحقة اختيار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن أنواع الجرائم و مكافحتها.(سعيد نعيم، 2012)

ونجد المشرع الجزائري تطرق إلى تعريف الجريمة المساس بأنظمة المعالجة الآلية للمعطيات في المادة 2 من القانون رقم 04/09وجرم الأفعال الماسة بأنظمة المعالجة للمعطيات في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات .

1- آليات مواجهة الجرائم الالكترونيةفي إطار القوانين الخاصة

إن المواجهة الفعالة للجرائم الإلكترونية بمختلف أنواعها تقتضي محاصرتها بنصوص خاصة الى جانب القواعد العامة، فلما كان مجال الملكية الفكرية والأدبية حقلا خصبا لوقوع مثل هذه الجرائم سارع المشرع الجزائري إلى

إحاطته بحماية جنائية وذلك من خلال تجريم الأفعال التي تشكل اعتداءا على حقوق المؤلف.

ولتعزيز جهوده في مكافحة الإجرام الالكتروني لجأ إلى وضع قواعد أكثر ملائمة و تماشيا مع خصوصيات الجرائم المتعلقة بوسائل الإعلام والاتصال وذلك من خلال القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أ:استحداث تدابير وقائية في قانون 04/09

يتميز هذا القانون بكونه الإطار القانوني الأكثر ملائمة مع خصوصيات الجرائم المتعلقة بوسائل الإعلام والاتصال، وخاصة الجرائم المستحدثة والنابعة من الاستخدام غير المشروع لشبكة الانترنيت. لقد عمد االمشرع الجزائري إلى استحداث تدابير جديدة غير مألوفة في القوانين السابقة وذلك للتصدي للجرائم الإلكترونية المتصلة بتكنولوجيا الإعلام والإتصال، وبالرجوع لفحوى هذا القانون يتبين لنا بأن هذه التدابير وقائية تتمثل في المساعدة على الكشف المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها وكشف مرتكبيها وتدابر اخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائية.

- **التدابير الوقائية المستحدثة**

لقد جاء في القانون04/09 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع الجرائم المعلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر، وهي كالتالي:

-مراقبة المراسلات والإتصالات الالكترونية:

نصت المادة 04 منالقانون04/09 على أربعة حالات خاصة يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي:

- الوقاية من الأفعال التي تحمل وصف جرائم الارهاب والتخريب والجرائم التي ترتكب ضد امن الدولة.
- توافر المعلومات عن احتمال وقوع اعتداء على منظومة معلوماتية بنحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.
- عند ضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.
- في حالة تنفيذ طلبات المساعدات القضائية الدولية المتبادلة .

-إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم الإلكترونية:

وذلك من خلال فرض مجموعة من الالتزامات عليهم والمذكورة في المواد10 ،11 و12 كما يلي:

- تعزيز التعاون مع مصالح الأمن المكلفة بالتحقيق القضائي، والإلتزام بجمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرف المصالح المعنية مع مراعاة سرية هذه الإجراءات في عملية التحقيق.
- العمل على حفظ المعطيات المتعلقة بحركة السير وكل المعلومات التي من شانها أن تساهم في الكشف عن الجرائم ومرتكبيها، وهذين الالتزامين موجهين لكل مزودي أو مقدمي خدمات الاتصالات الالكترونية بلا استثناء.
- لالتزام بالتدخل الفوري لسحب المحتويات التي تسمح لهما لاطلاع عليها بطريقة مباشرة او غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الوصول اليها غير ممكن.
- الالتزام بوضع ترتيبات تقنية للحد من امكانية الدخول الى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم بوجودها.

ونشيرإلى ان هذين الالتزامين يخصان فقط مقدمي الدخول إلى الأنترنت.

ب:استحداث تدابير إجرائية.

إضافة الى التدابير الوقائية السالفة الذكر تبنى المشرع الجزائري في القانون رقم 09/ 04 إجراءات جديدة يدعم بها تلك المنصوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجيا الإعلام والاتصال تتلخص فيما يلي:

- السماح للجهات القضائية المختصة وضباط الشرطة بالدخول لغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها واستنساخها، مع إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى التي يمكن الولوج إليها بواسطة المنظومة الأصلية، بشرط إخطار السلطات المختصة مسبقا.
- الاستعانة بالسلطات الأجنبية المختصة في بعض الأحيان للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل .
- إمكانية توسيع دائرة اختصاص الهيئات القضائية الجزائرية لتشمل النظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال،المرتكبة من طرفا لأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية والدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة.
- اللجوء إلى التعاون المتبادل بين السلطات الجزائرية المختصة والسلطات الأجنبية في مجال التحقيق والتحري وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال عبر الوطنية ومرتكبيها، وذلك عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطارا لاتفاقيات الدولية ومبدأ المعاملة بالمثل.

ج:مشروع قانون الوقاية من الجريمة الإلكترونية.

إن مشروع هذا القانون يكتسي أهمية كبيرة بالنسبة للمنظومة التشريعية الوطنية التي تعنى بمحاربة أشكال جديدة من الجرائم كونه سيساهم أكثر في التصدي لتلك المرتبطة بالتكنولوجيات الحديثة والتي لها صلة مباشرة بالعمليات الإرهابية او تبييض الأموال.

كما أن مشروع القانون جمع بين القواعد الإجرائية المكملة لقانون الإجراءات المدنية،وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة مع التدخل السريع لتحديد مصدرها والتعرف على مرتكبيها. وقد منح نص المشروع دورا ايجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم وكشف مرتكبيها حيث تنص المادة الثالثة منه على وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية. نص مشروع القانون على أربع حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها : الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية، عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

يحدد القانون طبيعة الترتيبات التقنية الموضوعة لتجميع وتسجيل معطيات ذات صلة بالوقاية من الاعتداء على أمن الدولة ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

وعلى هذا الأساس، يجوز للجهات القضائية وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي. ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها. أيضا ولأجل إشراك مزودي خدمات الإنترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم التكنولوجية، يلزم مشروع القانون هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات الملزمين بحفظها. تشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات المستعملة في الاتصال، والخصائص التقنية وتاريخ وزمن ومدة كل اتصال، والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وعناوين المواقع المطلع عليها.

أما بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعلومات التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه، على أن يلتزم متعاملو الهاتف بالاحتفاظ بالمعطيات لمدة سنة ابتداء من تاريخ التسجيل. ويتضمن مشروع القانون أيضا إجراءات عقابية حيث أنه ولتفادي أي تهرب من التزامات القانون، يسلّط هذا الأخير على الأشخاص الطبيعيين الذين يعرقلون سير التحريات القضائية عقوبة السجن من خمس إلى ست سنوات وغرامة مالية تتراوح ما بين خمسة ملايين إلى خمسين مليون سنتيم، مع معاقبة المؤسسات المخالفة بالغرامات المالية المنصوص عليها في قانون العقوبات.

من جهة أخرى يجبر مشروع النص التشريعي مقدمي خدمات الأنترنت على الالتزام بالتدخل الفوري لسحب المحتويات التي بإمكانهم الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين، وتخزينها أو جعل الدخول إليها غير ممكن، إضافة إلى وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة وإخطار المشتركين لديهم بوجودها.

ثانيا : على المستوى العربي:

في مصر لم يصدر قانون خاص بالجرائم الالكترونية بينما عقدت الجمعية المصرية للقانون الجنائي مؤتمرها السادس في القاهرة في الفترة من 25 إلى 28 أكتوبر 1993م وناقشت موضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات من خلال الأبحاث والدراسات المقدمة من الباحثين والتي دارت حول تحديد أنواع الجرائم المختلفة المتعلقة بنظم المعلومات من اعتداء مادي على الأجهزة وأدوات الكمبيوتر بالسرقة أو التخريب أو الإتلاف إلى اعتداء على البيانات والمعلومات المختزنة في قواعد المعلومات بالغش أو التزوير أو السرقة، والحصول على تلك البيانات والمعلومات دون إذن أو الاتجار فيها، والتحايل على الأجهزة للحصول على الأموال، وتحويل ونقل الأموال المتحصلة من الجرائم لغسلها.

وأوضحت البحوث والمناقشات أن الاعتداء قد يحدث أثناء إدخال البيانات والمعلومات أو إخراجها أو من خلال المعالجة الآلية لها، وذلك بالحذف أو المحو أو الإضافة أو التعديل دون حق، وأن هذه المعلومات قد تكون ثقافية أو سياسية أو عسكرية أو اقتصادية أو علمية أو اجتماعية.

وقد بينت الأبحاث والدراسات والمناقشات صعوبة اكتشاف جرائم نظم المعلومات واثباتها، وأكدت على ضرورة تدريب رجال الشرطة القضائية ورجال

التحقيق ورجال القضاء، كما حذرت من تزايد احتمالات انتهاك حرمة الحياة الخاصة عن طريق التجسس والتنصت على الكابلات الرابطة بين القواعد الأساسية والوحدات الفرعية.

وفي ختام المؤتمر قد تمكن المؤتمرون من تجريم الأفعال المتعلقة بالكمبيوتر والتوصية باتخاذ التدابير والإجراءات اللازمة والتي تكون على النحو التالي:

- تجريم الأفعال المتعلقة بالكمبيوتر:

1. حصول الشخص لنفسه أو لغيره على أموال عن طريق اختراق نظم المعلومات للاستيلاء عليها دون وجه حق.
2. حصول الشخص لنفسه أو لغيره على بيانات أو معلومات أو مستندات عن طريق اختراق نظم المعلومات دون إذن.
3. حصول الشخص لنفسه أو لغيره على أموال دون وجه حق عن طريق التحايل على الأجهزة.
4. تحويل أموال دون حق عن طريق اختراق الأجهزة.
5. تحويل أموال مستمدة بطريق غير مشروع عن طريق الأجهزة بقصد غسلها وتمويه مصدرها.
6. إتلاف أو تشويه البيانات أو المعلومات أو المستندات المختزنة في قاعدة المعلومات.
7. استخدام المعلومات المختزنة في قاعدة نظم المعلومات بقصد المساس بحرمة الحياة الخاصة للغير أو حقوقهم.
8. تغيير الحقيقة في البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات عن طريق الإضافة أو الحذف أو المحو الكلي أو الجزئي أو التعديل.
9. حصول الشخص على نسخة من البرامج المختزنة في قاعدة نظم المعلومات دون إذن.

10. حصول الشخص على البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات بقصد إفشائها أو قيامه بإفشائها فعلا أو الانتفاع بها بأي طريق.
11. الاطلاع بأي طريق على المعلومات أو البيانات أو المستندات التي تحويها قاعدة نظم المعلومات دون إذن بقصد معرفتها.
12. التسبب خطأ في حصول الغير على أموال أو بيانات أو معدات أو معلومات أو مستندات أو في ارتكاب فعل من الأفعال المذكورة أعلاه.

- الإجراءات والتدابير الواجب اتباعها :

1. مساءلة الأشخاص الطبيعيين والأشخاص المعنويين والمؤسسات الفردية إذا اقترنت الجريمة لصالح الأشخاص والمؤسسات أو بأسمائها بالإضافة إلى مساءلة الأشخاص الطبيعيين من مقترفيها وشركائهم.
2. إدماج نصوص جرائم نظم المعلومات في قانون العقوبات الوطني على أن يفرد لها فصل خاص.
3. تدريب رجال الشرطة القضائية ورجال التحقيق والقضاء على كيفية استخدام أجهزة المعلومات وأدواتها وأشرطتها وآلات الطباعة الخاصة بها والإحاطة بكيفية إساءة استخدامها.
4. تدريب رجال الشرطة القضائية والتحقيق والقضاء على كيفية الكشف عن هذه الجرائم وإثباتها.
5. حث الدول على التعاون فيما بينها خاصة في مجال المساعدات والإنابة القضائية للكشف عن هذه الجرائم، وجمع الأدلة لإثباتها، وتسليم المجرمين المقترفين لها، وتنفيذ الأحكام الأجنبية الصادرة بالإدانة والعقوبة على رعايا الدولة المقترفين لها بالخارج.

ومن جانب آخر تعكف جامعة الدول العربية ممثلة في الأمانة العامة لمجلس وزراء الداخلية العرب على إعداد مشروع اتفاقية عربية لجرائم الكمبيوتر

وكذلك إنشاء لجنة تتألف من ممثلي عدد من الدول الأعضاء لمتابعة كافة المستجدات التقنية والاتفاقيات الدولية المتعلقة بجرائم الكمبيوتر والعمل على توحيد التشريعات العربية بهذا الشأن،

ثالثا: على المستوى الدولي

يعتقد مركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من جرائم الكمبيوتر تعتمد على الأمن في إجراءات معالجة المعلومات، والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر، ومنفذي القانون، والتدريب القانوني، وتطور أخلاقيات استخدام الكمبيوتر. والأمن الدولي لأنظمة المعلومات. ففي المجال الدولي هناك حاجة للتعاون الدولي المتبادل، والبحث الجنائي والقانوني عن بنوك المعلومات، ففي أوروبا قدمت لجنة جرائم الكمبيوتر توصيات تتعلق بجرائم الكمبيوتر تمحورت في النقاط التالية:

- المشكلات القانونية في استخدام بيانات الكمبيوتر والمعلومات المخزنة فيه في التحقيق الجنائي.
- الطبيعة العالمية لبعض جرائم الكمبيوتر.
- تحديد معايير لوسائل الأمن المعلوماتي وللوقاية من جرائم الكمبيوتر.
- مشكلة الخصوصية وخرقها في جرائم الكمبيوتر.
- موقف ضحايا جرائم الكمبيوتر، هذا وقد لخص التقرير الصادر عن اللجنة الأوروبية جرائم الكمبيوتر في التالي:

1. الاحتيال.
2. حذف وتدمير البيانات أو المعلومات أو البرمجيات في الكمبيوتر.
3. الدخول غير القانوني.
4. الاعتراض غير القانوني للاتصال بين الكمبيوتر وخاصة في مجال التحويل المالي.
5. الإنتاج غير القانوني لبيانات، أو معلومات أو برمجيات الكمبيوتر.

6. وقد أقر الوزراء الأوروبيون في اجتماعهم بتاريخ 1989/09/13
7. التوصيات التالية:

1. إدراك أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالكمبيوتر.
2. أن يؤخذ بالحسبان أن الجرائم المتصلة بالكمبيوتر ذات خاصية تحويلية.
3. الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني.

4. خاتمة:

لقد خلف عصر المعلوماتية ورائه آثاراً سلبية نجمت عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية ليم استعمالها في غير الغرض الذي خلقت من أجله ، الأمر الذي أثر على حقوق الأفراد وحرياتهم حيث وفرت الأنظمة المعلوماتية وسيلة جديدة في أيدي مجرمي المعلوماتية لتسهيل ارتكاب العديد من الجرائم ، كما أضحى النظام المعلوماتي ذاته محلاً للاعتداء عليه وإساءة استخدامه.

حيث عمل المشرع الجزائري لسد الفراغ التشريعي لمواجهة هذه الجرائم إلا أن نصوصه لا تزال ناقصة خاصة فيما يتعلق بالاعتداءات على الأموال المعلوماتية .بحيث تبنى سياسة مزدوجة للتصدي لظاهرة الجرائم الإلكترونية ، بحيث اهتدى من جهة الى تعديل الجوانب الموضوعية والإجرائية للتشريعات العقابية العامة من قانون العقوبات وقانون الإجراءات الجزائية، حيث سعى لجعلها تواكب التحديات الجديدة الناتجة عن التطورات الهائلة التي عرفها قطاع التكنولوجيات الحديثة لوسائل الإعلام والاتصال. وقد أخذ المشرع الجزائري بما جاء فـي اتفاقية بودابست لمكافحة الإجرام الالكتروني،خصوصا فيما يتعلق بتعريف المنظومة المعلوماتية ومن جهة ثانية عمل على استحداث قوانين أخرى خاصة تتجاوب والطبيعة الخاصة للجرائم الإلكترونية. وهذا التنوع التشريعي من شانه أن يساهم بشكل فعال على الأقل في الوقت الراهن في الحدّ من تفاقم ظاهرة الجرائم الالكترونية في الدولة الجزائرية.

قائمة المراجع:

- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دراسة مقارنة،ط1، دار النهضة العربية، القاهرة، 2010، ص 8 .
- أسامة سمير حسين، الاحتيال الالكتروني، الوجه القبيح للتكنولوجيا، الحنادرية للنشر والتوزيع، الأردن، الطبعة الأولى،2011 .، ص 134.
- الأستاذ Ulrich Seiber، جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الإتصال، ترجمة الدكتور سامي الشوا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي،25-28 أكتوبر 1994،ص 8 .
- أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون ذكر دار النشر، دون ذكر بلد النشر، ص 34
- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة المعلوماتية، دار البداية، عمان.2007، ص 92
- حسين صالح دويب، القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، 06 أفريل 2010.
- ذياب البداينة،جرائم الحاسب والأنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكادمية نايف العربية للعلوم الأمنية 2009، ص 111 .
- سعيد نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية، جامعة الحاج لخضر باتنة 2013 2012 ، ص41

- صلاح بوتاني دلخار، الحماية الجنائية الموضوعية للمعلومات، دار الفكر الجامعي،2016، ص90 .
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة للنشر،177.، الإسكندرية،2009 ، ص176
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى،2006 ، ص46
- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010، ص 80-81
- محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، دار حامد للنشر والتوزيع، عمان، الطبعة الأولى، 2007 .، ص73 .
- محمد قدري حسن عبد الرحمان، جرائم الاحتيال الإلكتروني، بحث منشور في مجلة الفكر الشرطي، إمارة الشارقة، الإمارات العربية المتحدة، المجلد 20،العدد 79،أكتوبر 2011، ص 118 .
- نائلة عادل فريد قورة ،جرائم الحاسب الاقتصادية، دراسة نظرية تطبيقية، دار النهضة العربية، الإسكندرية، 2004، ص54
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، 2011، ص 59
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، الأردن،2008، ص50 .
- هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة،أسيوط،1992.ص29.

- Mascala corinne ، «criminalité et contrat électronique» ، Travaux de l’association ، CAPITANT ، Henir ، journées national ، paris ، 2000 ، p119.