رقم الايداع : 2006 -1257 الترقيم الدولي : 8623- 1112

الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)

La cybercriminalité (étude analytique : définition, caractéristique)

الاستاذة : **معاشـــي سميـــرة**

استاذة مساعدة " أ " - كلية الحقوق و العلوم السياسية

جامعة محمد خيضر - بسكرة / الجزائر

tinhinaneatakor@yahoo.com

تاريخ الإرسال :	تاريخ المراجعة :	تاريخ القبول :
2018/05/27	2018/05/28	2018/06/10

الملخص:

إن الجريمة ظاهرة اجتماعية ارتبطت في طبيعتها وحجمها بالتحولات المختلفة سواء كانت اقتصادية، اجتماعية وثقافية، الوطنية منها أو الدولية.

ومن التحولات الجذرية التي شهدها عصرنا الحالي والتي ساهمت و بطريقة قياسية في ارتقاء البشرية إلى مستويات عليا، ما يسمي بالثورة المعلوماتية و هي الثورة التي تزاوجت فيها شبكات الاتصال بما وصلت إليه من تطور مع الحاسوب ذاك الجهاز الذي يمتلك قدرات هائلة للقيام بالعديد من الوظائف وفي ظرف قياسي .

هذا التمازج الذي مكن الملايين من البشر الاتصال ببعضهم البعض و أتاح لهم الفرص للاطلاع على المعلومات و تبادلها ،القدرة على التفاوض وإبرام العقود و الصفقات في ظل بيئة تحاكي واقع البشرية و هي البيئة الافتراضية أو الرقمية .

غير انه و في المقابل أنتجت هذه الثورة نمط جديد من الإجرام صنف في سياق الجرائم المستحدثة و هي الجرائم المعلوماتية أو الالكترونية و هي جرائم تمس في صميمها قيما جوهرية تخص الأفراد والمؤسسات، و حتى الدول و في جميع مناحي الحياة ، الأمر الذي خلف شعورا بعد الثقة بخصوص التعامل و الاستفادة من ثمار الثورة المعلوماتية.

الكلمات المفتاحية : معلوماتية ،جريمة الكترونية ، جرائم الكمبيوتر .

Résumé :

La criminalité est un phénomène social qui a été lié dans sa nature et son volume à diverses transformations, qu'elles soient économiques, sociales ou culturelles, nationales ou internationales.

Parmi Les transformations radicales a notre époque actuelle, qui ont contribué à améliorer le niveau de vie de l'humanité ; la soi-disant révolution de l'information :une révolution résultat d'une mixité entre les réseaux de communication et l'ordinateur .

Cette interaction, qui a permis à des millions de personnes de communiquer entre eux et leur a donné accès à l'information et à l'échange, la capacité de négocier et conclure des contrats et des transactions dans un environnement qui simule la réalité de l'humanité.

Cependant, cette révolution a produit un nouveau modèle de criminalité classé parmi les crimes nouveaux de notre époque : la cybercriminalité ou les crimes informatiques ou électroniques ; des crimes qui affectent les principales valeurs fondamentales des individus , des institutions, et même les pays et dans tous les domaines de vie

مقدمة:

تعد ثورة المعلومات والتكنولوجيا الحديثة أهم الأحداث التي تعيشها البشرية في عالمنا اليوم، هي الثورة التي تمازجت و تزاوجت فيها تكنولوجيا المعلومة وقطاع الاتصالات بما وصلا إليه من تطور هائل.

الكل يعتبر هذه الثورة و نتيجة للتقنيات العالية التي تقوم عليها و التي تتمثل في استخدام الكمبيوتر والشبكات المعلوماتية قد شكلت قفزة نوعية حضرية في حياة الأفراد و الدول و تركت بذلك أثرا ايجابيا تجلت ملامحه في كونها ساعدت على عولمة المعلومات وسهلت الكثير من الخدمات والأعمال.

فبفضل تقنية تمكنت البشرية من السيطرة على المعلومة من خلال استخدام الحاسب الآلي لتخزين ومعالجة واسترجاع المعلومات ، إلى جانب استخدامه في عمليات التصميم والتصنيع والإدارة ، وكذا تطوير تطبيقاته لتستوعب بذلك الكثير من القطاعات كالتعليم والخدمات الصحية وتسهيل المعاملات والخدمات المصرفية والحجز الآلي لنقل المسافرين ، فضلاء عن انه جعل جميع المعلومات في متناول الجميع من خلال شبكة الاتصال الدولي (الانترنت) وأصبح العالم بذلك مزدحماء بكم هائل من المعلومات التي لا تعرف الحدود الجغرافية ، وشكل بذلك وحدة واحدة تترابط فيه الحاسبات وشبكة المعلومات .

إلا أن الوجه الايجابي لهذه التقنية لا ينفي انعكاساتها السلبية التي ظهرت ملامحها في صورة سلوكات استغل فيها النظام ألمعلوماتي بصورة غير مشروعة و بهدف الإضرار بمصالح الأفراد و الجماعات و كذا الدول وهو ما اصطلح على تعريفه بـ: الجرائم المعلوماتية Cyber Crimes.، هي ظواهر إجرامية تقرع أجراس الخطر لتنبه المجتمع الدولي عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل علي المستويات الاقتصادية والاجتماعية والثقافية والأمنية.

وهو ما يدعو إلى ضرورة تكاتف جهود الدول لمجابهتها و مكافحتها باعتبارها أهم جرائم العصر المستحدثة و حتمية الاتفاق الدولي على ضرورة وضع إطار خاص موحد ونظام قانوني متميز لهذه الجريمة إنطاقا من تحديد تعريف موحد شامل لهذه الجريمة و ما يميزها عن غيرها من الجرائم خاصة وان المتفق عليه أن مشروعية الفعل من عدمه تنطلق أساسا من فكرة تحديد مفهوم له و تجريم الفعل أيضا تنطلق من فكرة عدم إيقاع العقوبة إلا بنص قانوني فإذا لم يحدد الفعل المجرم فلا عقوبة عليه وهو ما سنحاول أن نتناوله بعرض أهم المحاولات الفقهية و التشريعية لتحديد معالم الجريمة المعلوماتية من خلال تعريفها و تبيان أهم خصائصها انطلاقا من طرح إشكالنا الرئيسي : **" إلى أي مدى استطاع التشريع و الفقه تجسيد فكرة الشمولية و التميز لتحديد مفهوم الجريمة المعلوماتية ؟"**

وهو ما سنحاول الإجابة عليه ضمن الخطة التالية:

المبحث الأول:تعريف الجريمة المعلوماتية.

المطلب الأول: الاتجاهات و التصنيفات المختلفة لتعريف للجريمة المعلوماتية.

المطلب الثاني : نقد التعاريف الخاصة بالجريمة المعلوماتية .

المبحث الثاني: خصائص الجريمة المعلوماتية.

المطلب الأول: الخصائص المشتركة مع الجرائم الأخرى.

المطلب الثاني: الخصائص التي تنفرد بها الجريمة المعلوماتية عن الجرائم الأخرى.

الخاتمة.

المبحث الأول : تعريف الجريمة المعلوماتية.

لقد تباينت التعريفات المتعلق بالجريمة المعلوماتية تباين المصطلحات التي أطلقت عليها و التي يرى البعض أنه نتيجة مسيرة نشأة و تطور ظاهرة الإجرام المرتبط بتقنية المعلومات، و هناك من يرى أن إخلاف التسميات يرتبط بالموضوع الذي تنال منه هل هو لارتباطها بالكيان المادي للحاسب الآلي ؟أم لارتباطها بالكيان المعنوي له ؟ .

فبداية بالاحتيال ألمعلوماتي " computer fraud" ثم الجرائم التي يساعد على ارتكابها الحاسب الآلي "computer assisted crimes " ثم التعسف في استعمال الحاسب الآلي أو إساءة استعمال الحاسب الآلي " computer abuse " للدلالة على هذه الظاهرة باعتبارها أشمل و أوسع وهناك من فضل تسمية جرائم الحاسب الآلي "computer crimes " ،كما أطلقوا عليها مصطلح الجريمة المعلوماتية لينتقلوا إلى مصطلحات أكثر حداثة و دقة و هي جرائم التقنية العالية ، جرائم الهاكرزأوجرائم ذوي الياقات البيضاء ثم جرائم الكمبيوتر و الإنترنت [1].

و تقييما للمصطلحات السابقة ،ترى الدكتورة نائلة عادل محمد فريد قورة أن تعبير الاحتيال ألمعلوماتي لا يمثل الجريمة المعلوماتية وإنما هو صورة من صورها، كما أنها لا تتفق و تعبير الجرائم التي يساعد على ارتكابها الحاسب الآلي ذلك أن الحاسب الآلي و نظمه قد يكونا محلا للنشاط الإجرامي .

و هو ما يؤيده البعض على اعتبار أن مصطلح التعسف في استعمال الحاسب الآلي ينصرف إلى الحالات التي تنطوي إلى إساءة استخدام الحاسب الآلي دون أن تصل إلى درجة السلوك الإجرامي [2]

و هو الاتجاه الذي يسايره كثير من الفقهاء في هذا المجال ويفضل مصطلح الجرائم المعلوماتية أو جرائم الكمبيوتر أو الجرائم المرتبطة بالكمبيوتر و إن كان بعض الآخر و بعض الدارسين أيضا حسب

الأستاذ يونس عرب يتمسكون بوجوب التفرقة بين اصطلاح جرائم الكمبيوتر و اصطلاح الجرائم المرتبطة بالكمبيوتر، فالأول يستخدم للدلالة على الأفعال التي يكون فيها الكمبيوتر هدفا للجريمة ، كالدخول غير المصرح به ، و إتلاف البيانات المخزنة في النظم و نحو ذلك ، أما مصطلح الجرائم المرتبطة بالكمبيوتر فيشمل الجرائم التي يكون فيها الكمبيوتر وسيلة لارتكاب الجريمة لا لاحتيال بواسطة الكمبيوتر و التزوير.

إلا أن هذه التفرقة ذابت لاستخدام الاصطلاحين مترادفين منذ ظهورهما فأصبح اللفظان يدلان على كل جرائم الكمبيوتر سواء أكان الكمبيوتر هدفا أو وسيلة أو بيئة للجريمة حتى وبظهور الإنترنت التي يرى البعض أنها تشكل فئتها التجريمية الخاصة بعيدا عن جرائم الكمبيوتر ،إلا أن البعض الآخر و حسب وجهة ، نظر نفس الأستاذ يعتبر أنها أي الإنترنت بالنسبة للمفهوم الشامل لنظام المعلومات مكون من مكونات هذا النظام إذ أنها شبكة متآلفة من العديد من الحاسبات الآلية المرتبطة ببعضها تلفونيا أو بواسطة الأقمار الصناعية أو الكابل لتكون جزءا من شبكة المعلومات و لأن هذا النظام يطلق عليه مصطلح نظام الكمبيوتر.

المطلب الأول: الاتجاهات و التصنيفات المختلفة لتعريف للجريمة المعلوماتية.

لقد ذكرنا أنفا أنه ظهر هناك جدل و اختلاف كبير حول تعريف الجريمة المعلوماتية، باعتبارها ظاهرة إجرامية حديثة، إلى حد الفشل في محاولات وضع تعريف متفق عليه جامع يتناسب وطبيعة الجريمة.

وهو ما حذا بالبعض أمام هذا العجز إلى اعتبار الجريمة المعلوماتية ما هي إلا جريمة تقليدية ارتكبت بأسلوب غير تقليدي ، غير أن الأخذ بذلك يتناقض مع المنطق القانوني الذي يعتبر هذا الصنف من الجرائم له ميزاته الخاصة و خصائصه المنفردة التي تجعل من الصعب تطبيق التعريفات التقليدية عليها[3].

لذلك كان نتاج المجهودات الفقهية المختلفة عدة تعريفات تتفاوت فيما بينها ضيقا و اتساعا، فإذا كانت التعاريف الأولى تحصر نطاق النشاط الإجرامي لجرائم الكمبيوتر في حالات فقط ،فإن التي استندت على منطق التوسيع تجاوزت إلى إدخال سلوكات و تصرفات إجرامية لا تمت بالصلة بالجريمة المعلوماتية .

وعلى العموم يمكن تصنيف هاته التعاريف ضمن الأصناف الأربع التالية [4].

الفرع الأول: تعريفات ترتكز حول وسيلة ارتكاب الجريمة.

من أنصار هذا الاتجاه الفقيه ألماني LAUS TIEDEMAUN و CARLE BENSON و الأستاذ LESLIE DE BALL إذ يعرف الأول الجريمة المعلوماتية على أنها "**كل أشكال السلوك غير المشروع – أو الضار بالمجتمع – الذي يرتكب باستخدام الحاسوب** "[5] أما الأستاذ **LESLIE** فقد عرفها على أنها " **فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية** " و إنها " **الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية** ".

كما عرفها توم فوريستر في مؤلفه عن قصة ثورة تقنية المعلومات تعريفا يكاد أن يطابق التعريف السابق بقوله " **أنها فعل إجرامي تم باستخدام الحاسوب كأداة رئيسية** ".

وعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها " **الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج و المعلوماتية دورا رئيسيا** "

كم عرفها الأستاذان R. TATTY و A. HAND CASTEL بأنها " **تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب و بعبارة أخرى تلك الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر من سبل** "[6]

الفرع الثاني: التعريفات المرتكزة حول موضوع الجريمة.

ويستند أصحاب هذا الاتجاه في تعريفهم للجريمة المعلوماتية إلى وجوب أن يكون الكمبيوتر هو محل الجريمة ، فيجب أن يتم الاعتداء على الحاسب الآلي أو على داخل نظامه ، ويمثل أنصار هذا الاتجاه الفقيه ROSANBLATT الذي عرف الجريمة بأنه "**نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه** " كما عرفتها الدكتورة هدى قشقوش التي تناولت الجرائم المعلوماتية بأنها " **جرائم الاعتداء على الأموال المعلوماتية و هي عبارة عن الأدوات المكونة للحاسب الإلكتروني وبرامجه ومعداته**"[7].

الفرع الثالث: التعريف المستند إلى وجوب إلمام الفاعل بتقنية المعلومات.

يرى دعاة هذا التصنيف و من بينهم الأستاذ DAVID THOMPSON أن تعريف الجريمة المعلوماتية و جب أن يستند إلى معيار شخصي إذ على الفاعل أن يكون ملما بتقنية المعلومات ،واستخدام الحاسب الآلي ، وهو نفس المفهوم الذي سار إليه الأستاذ A.SOLARZ الذي عرفها على أنها " **أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات**". أيضا الفقيه STEIN SCKJOBERG الذي عرفها بأنها " **أي فعل غير مشروع تكون المعرفة بتقنية معلومات أساسية لمرتكبه** " **و التحقيق فيه وملاحقته قضائيا** "[8]

الفرع الرابع: التعريف المستند إلى معايير مختلفة و متنوعة.

لقد أختلف هذا الاتجاه في المعايير المتبناة لتعريف الجريمة المعلوماتية بعيدا عن المعايير السابقة منها التعريف الذي أوره الخبراء البلجيكيون في معرض الإجابة على الاستبيان الذي أجرته منظمة التعاون الاقتصادي والتنمية OCDE حول الغش ألمعلوماتي في اجتماع عقد بباريس في عام1982 وورد فيه أنه"**كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريق مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية**"

في حين يذهب الفقيه الفرنسي الأستاذ (Massa) إلى أن المقصود بالجريمة المعلوماتية

"**الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح**"[9].

أيضا تعريف الخبير الأمريكي PARKER.D الذي قال "**أنها فعل إجرامي ،أيا كانت صلته بتقنية المعلومات ،فيه يتكبد المجني عليه ونتيجة له خسارة ويحقق الفاعل ربحا عمديا**"[10].

ويستند البعض على تعريفا للجريمة المعلوماتية اقترحته مجموعة من الخبراء منظمة التعاون الاقتصادي و التنمية كأساس للنقاش في اجتماع عقد بباريس سنة 1983لبحث الإجرام المرتبط بالمعلوماتية، مقتضاه أنها "**كل سلوك غير شرعي أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و /أو بنقلها**"[11].

المطلب الثاني : نقد التعاريف الخاصة بالجريمة المعلوماتية .

أن ما يمكن قوله حول هاته التعاريف أنها جاءت من خبراء في مجال الجريمة المعلوماتية حددوا مدلولها لإعداد بحوثهم، كما طبقوه بطرق تناسب أغراض بحثهم و يستخدمون الأساليب و المناهج الملائمة للمجال الذي تنتمي إليه الدراسة الأمر الذي يتعذر معه عقد مقارنة بينها وتقييمها غير أن ذلك لم يمنع من تعرض معظمها للنقد و التقييم على الأساس التالي :

الفرع الأول : نقد التصنيف الأول و الآخذ بمعيار وسيلة الجريمة .

لقد تعرض هذا التصنيف إلى انتقاد لاذع خاصة التعريف الذي جاء به الفقيه KLAUS TIEDEMAUN الذي يعاب عليه أنه بالغ العمومية و الأتساع [12]، لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع،كما أن مجرد استخدام الحاسب الآلي لا يضيف إلى السلوك غير المشروع جديدا ،مادام استخدام البيانات و المعلومات و البرامج هو الذي يميز الجريمة المعلوماتية.

إذن فأساس الانتقاد المتجه إلى هذا التصنيف، أن تعريفاته ليست جامعة ولا مانعة كما أنها تتسم بقصور كبير في إعطاء تصور علمي للجرائم المعلوماتية و جاءت مبنية على معيار واحد فقط، كما أن الوسيلة لم تكن موضوع اعتبار لدى المشرع الجزائي فالوسائل أغلبها متساوية ، والتكوين القانوني للجريمة وتوافر أركانها مجتمعة هو موضوع الاعتبار عند انطباق نص التجريم [13].

أيضا فإن الأساتذة ROBERT RINES و MICHAEL و JOHN TABER يرون أن تعريف الجريمة يستدعي "الرجوع إلى العمل الأساسي المكون لها و ليس فحسب إلى الوسائل المستخدمة لتحقيقه "، كما أن الأخذ بهذا المعيار وحيدا يؤدي إلى توسيع كبير لمفهوم الجريمة المعلوماتية ، فتدخل في إطارها العديد من الجرائم التي لا علاقة لها بالمعلوماتية .

الفرع الثاني: نقد التصنيف الثاني القائم على معيار موضوع الجريمة

لقد قيل عن تعريف ROSANBLATT أنه اتسم بنوع من الكمال بالمقارنة مع التعريفات السابقة و يمكن الاعتماد عليه على الصعيد العلمي و العملي، غير أنه هو الآخر لم يسلم من النقد على أساس:

أن التعريف بدأ صحيحا و انتهى معيبا ،ففي حين انه رسخ بداية مبدأ المشروعية على أساس أن الجريمة المعلوماتية من الجرائم المحصورة لكنه أنهاها بتوسع غير مبرر، إذ لم يبين طبيعة هذا التحويل وبذلك فتح الباب واسعا أمام التفسيرات التي يمكن أن تعصف بمبدأ المشروعية [14] ، كما أن تعريفه لم يبين محل الاعتداء، إذن فاعتماد هذا المعيار في تعريف الجريمة المعلوماتية يؤدي إلى إيراد تعريفات عامة ومطلقة ، لا تحدد الأفعال المتصلة بجرائم الكمبيوتر بصورة دقيقة ، و الأخذ به يؤدي إلى اعتبار بعض الأفعال من جرائم الكمبيوتر، مع أنها ليست كذلك في حقيقة الأمر، كإتلاف البيانات قبل معالجتها ، بالإضافة إلى عدم وجود اتفاق حتى الساعة ، على الأفعال المنطوية تحت وصف جرائم الكمبيوتر ، كما أن هذه التعريفات لا تستند في الحقيقة إلى موضوع الجريمة بالمعنى القانوني الذي هو محل الاعتداء ، فركزت على أنماط السلوك الإجرامي و أبرزتها متصلة بالموضوع لا الموضوع ذاته ، أما وبالنسبة للنقد الموجه إلى SOLARZ الذي يتطلب أن يكون الفعل مما يقع ضمن نطاق قانون العقوبات ، فهو تعريف مبني على افتراض مسبق على شمول قانون العقوبات لأنماط السلوك الإجرامي في جرائم الكمبيوتر و هي مسألة لا تراعي الجدل الذي لم ينته بعد حول مدى انطباق قواعد التجريم التقليدية على هذه الأفعال ، و الذي حسم تقريبا لجهة عدم انطباق نصوص القانون القائمة أي النصوص التقليدية و الحاجة إلى نصوص خاصة تراعي العناصر المميزة لهذه الجرائم من غيرها من الجرائم التي عرفها قانون العقوبات.

الفرع الثالث: نقد التصنيف الثالث القائم على القدرات التقنية والفنية لمرتكب الجريمة

أي شرط المعرفة التقنية الشخصية للفاعل، فيلاحظ أن هذه الجرائم وفي كثير من الأحيان ترتكب من قبل مجموعات تتوزع أدوارهم بين التخطيط و التنفيذ و التحضير و المساهمة ، و قد لا تتوفر في بعضهم المعرفة بتقنية المعلومات والتي يطرح بشأنها التساؤل التالي : ما هي معايير تحديد المعرفة التقنية للقول بارتكاب الجريمة ؟ [15] خاصة وأن الحياة المعاصرة ومساعي المتعاملين النشطين

في الميدان تسعى من أجل نشر منتجاتها وتحقيق الأرباح إلى تبسيط وسائل المعالجة وتبادل المعطيات ، وتحويل الجهاز المعقد إلى جهاز بسيط يمكن كل من يجهل علوم الكمبيوتر استخدامه ،فلا تشترط المعرفة بتقنية المعلومات ليتمكن شخص بسيط من إرسال آلاف الرسائل الإلكترونية دفعة واحدة إلى أحد المواقع لتعطيل عملها .

زيادة على ذلك أن جانب كبير من الجرائم المعلوماتية ترتكب عن طريق الشخص المعنوي وهو ما يثير إشكالية مدى مسؤولية الشخص المعنوي عن الجرائم التي ترتكب في البيئة الرقمية .

الفرع الرابع : نقد التصنيف الرابع الذي تبني معايير مختلفة

بالنسب لتعريف الأستاذ DON B PARKE ، الذي اشترط أن يحقق الفاعل ربحا عمديا ، فإن الربح غير متحصل دائما من هذه الجرائم ، كذلك قد يكون بطريق غير عمدي ، إذ قد يحصل بطريق غير مباشر ، وقد لا يحصل أبدا .

أما وفي خصوص تعريف الخبراء البلجيك فقد اعتبره البعض من أفضل التعريفات لشموليته لجملة من العناصر و الخصوصيات التي ضمتها الجريمة المعلوماتية و لم تتناولها التعريفات السابقة ، إلا أن شمولية التعريف انتقدت على أساس إدراجها للأموال المادية ، في حين أن هذا النوع من الأموال محمي بموجب نصوص قانون العقوبات التقليدية و بالتالي فهي ليست بحاجة إلى قانون جديد .

لذا اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية OCDE للجريمة المعلوماتية في اجتماع بباريس عام 1983 من أنها "**كل سلوك غير مشروع أو غير أحلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها** " وهو تعريف تبنى أكثر من معيار يتعلق الأول بوصف السلوك أما الثاني فاتصال السلوك بالمعالجة الآلية للبيانات أو نقلها،و إن اتسم هذا الأخير بالكثير من المرونة و السلوك الذي لا يرتب سوى استهجانه أخلاقيا لعدم التلازم الدائم بين الفعل المستهجن أخلاقيا و ذلك المؤثم قانونا1 .

و يرى الأستاذ يونس عرب في هذا المجال أنه وجب التفرقة بين الظاهرة الجرمية و الجريمة ، فظاهرة جرائم الكمبيوتر تعرف بأنها " **الأفعال غير المشروعة المرتبطة بنظم الحواسيب** " أما تعريف جريمة الكمبيوتر فإنها "**سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرميه محله معطيات الكمبيوتر**" فالسلوك يشمل الفعل الإيجابي و الامتناع عن الفعل ،و هذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ، ومعاقب عليها قانونا لأن إصباغ الصفة الجرمية لا يتحقق في ميدا القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفا للأخلاق .

ومحل جريمة الكمبيوتر هو دائما معطياته بدلالتها الواسعة (بيانات مدخلة ، بيانات ومعلومات معالجة ومحزنة ، البرامج بأنواعها ، المعلومات المستخرجة ، و المتبادلة بين النظم) و أما الكمبيوتر فهو النظام التقني بمفهومه الشامل المزا وج بين تقنيات الحوسبة والاتصال ، بما في ذلك شبكات المعلومات.

أما الأستاذ عبد الفتاح بيومي الحجازي فيرى أن الفقه من جانبه يعرف الجريمة المعلوماتية من زاوية فنية و أخرى قانونية ، فالفنية بالنسبة لهؤلاء تكمن في كون الجريمة المعلوماتية " **نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو كهدف لتنفيذ الفعل الإجرامي المقصود**" .أما التعريف القانوني و تصنيف صورها يتطلب تعريف المفردات الضرورية المتعلقة بأركان الحاسب الآلي و هي :

1-الحاسب ألآلي،2- برنامج الحاسب الآلي ،3-البيانات ،4- الممتلكات ، 5- الدخول ، 6- الخدمات ،7- الخدمات الحيوية [17].

و الجدير بالذكر أن الولايات المتحدة الأمريكية أصدرت قانونا عام يحمل رقم (474-99-100) و رقمه التشريعي 1986/1213المعدل(S,Sm 103 USA) لواجهة جرائم الكمبيوتر ، وقد ورد في هذا التشريع جميع المصطلحات الضرورية لاستيفاء اشتراطات الدستور لتطبيق القانون على الجرائم المعلوماتية ، وبناءا على ذلك صدر قانون ولاية تكساس الخاص بمكافحة الجريمة المعلوماتية ، وفي نفس السياق أقرت وزارة العدل الأمريكية سنة 2000 تصنيفا لجرائم الكمبيوتر ، وذلك بالنسبة لإنقاذ الكمبيوتر الفدرالي لدى المكاتب التحقيقات الفدرالية، الخدمة السرية الأمريكية، خدمة الجرائم و مكتب مكافحة الكحول و التبغ و المخدرات و الأسلحة الناري، و التصنيفات كالتالي :

1. السطو على بيانات الكمبيوتر
2. الاتجار بكلمة السر.
3. حقوق الطبع (البرامج – الأفلام –التسجيل الصوتي) و عمليات الهاكرز (القرصنة).
4. سرقة الأسرار التجارية باستخدام الكمبيوتر .
5. تزوير الماركات التجارية باستخدام الكمبيوتر .
6. تزوير العملة باستخدام الكمبيوتر.
7. الصور الجنية الفاضحة و استغلال الأطفال .
8. الاحتيال بواسطة شبكة الانترنت .
9. الإزعاج عن طريق شبكة الانترنت .
10. تهديدات القنابل بواسطة شبكة الإنترنت .
11. الاتجار بالمتفجرات أو الأسلحة النارية و المخدرات و غسيل الأموال عبر شبكة الإنترنت.

وفي المقابل اعتمد مكتب التحقيقات الفدرالي الأمريكي في أفريل عام 2000 قائمة من سبع جرائم هي[18] :

1. اقتحام شبكة الهواتف العامة أو الخاصة بواسطة الكمبيوتر.
2. اقتحام شبكات الكمبيوتر الرئيسية لأي جهة .
3. انتهاكات السرية المؤرخة على بعض المواقع بالإنترنت أو الجهات.

انتهاكات سلامة الشبكة المعلوماتية.

4. التجسس الصناعي.
5. برامج الكمبيوتر المسروقة.
6. البرامج الأخرى عندمايكون الكمبيوتر هو العامل الأساسي في اقتراف هذه المخالفات.

كما عرفها على أنها:

1. العبث بالحاسب الآلي .
2. الإخلال بأمن الحاسب الآلي .
3. غش الحاسب الآلي .

أما المشرع الفرنسي فعرف أنماط الجريمة المعلوماتية ضمن القانون رقم 19 لسنة 1988 و ميز بين الاعتداء على برامج ومعلومات الحاسب الآلي و بين الاعتداء على أدواته و آلاته و لم ينص هذا القانون على تجريم سرقة البرامج و المعلومات و اعتبارها مالا معلوماتيا، فحدد جرائم الاعتداء على برامج و معلومات الحاسب الرقمي الآلي بجريمتين[19]:

1- جريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات .
2- جريمة إتلاف برامج و معلومات الحاسب الآلي الرقمي .

أما جرائم الاعتداء على أدوات و آلات الحاسوب الآلي الرقمي فهي :

1- جريمة إتلاف آلات و أدوات الحاسوب الآلي الرقمي .
2- جريمة الاستخدام غير المستحق لأدوات وآلات الحاسوب الآلي الرقمي .

أما عن موقف التشريع العربي إزاء الجريمة المعلوماتية، فالمشرع العربي لم يكن بعيدا عن حماية نظم ووسائل الاتصال الحديثة ، فقد صدر القانون العربي – النموذجي – لمكافحة سوء استخدام تكنولوجيا المعلومات و الاتصالات ، في مواد عديدة منه ، موضحا سبل مكافحة الجرائم الواقعة على تكنولوجيا الاتصالات أو بواسطتها خاصة في المواد 1،2،3،4[20].

و قد ورد في المادة الأولى تعريف الجريمة المعلوماتية – ومنها الجرائم التي تقع على نظم الاتصالات الحديثة ، و على الوسيط الإلكتروني بان المقصود به هو شبكة الحاسب الآلي أو الانترنت أو أي شبكة إلكترونية أخرى، أما المادة الثانية من ذات القانون النموذجي فقد نصت على تجريم الاختراق غير المشروع أو البقاء غير المشروع – في النظم المعلوماتية – سواء كان في صورة بسيطة أو صورته

المشددة، وحددت عقوبات جنائية في كل الأحوال.

أما المادة الثالثة فقد جرمت حالات الإتلاف ألمعلوماتي – التي تقع على شبكات المعلومات و تؤدي على إتلاف البيانات أو برامج الحاسب الآلي التي تشغل هذه الشبكات .

و في مادته الرابعة تناول المشرع النصب ألمعلوماتي و التي يترتب عليها الحصول على المعلومات المخزنة أو البيانات عن طريق التحايل أو الالتقاط غير المشروع.

و أخيرا و في المادة الخامسة عالج المشرع جريمة إساءة استخدام الوسائط الإلكترونية في الحصول على خدمات نظم المعلومات أو شبكات الاتصالات بدون وجه حق و مثال ذلك من يقوم باختراق شبكة الحاسب الآلي – لإحدى شبكات الاتصالات – و يجري مكالمة هاتفية دولية – مجانا – دون دفع الرسوم المقررة .

هذا عن الموقف الجماعي للمنظومة التشريعية العربية ، أما على مستوى الجهود التشريعية الفردية العربية فقد حاول المشرع القطري من خلال قانون رقم 11 الصادر بتاريخ 10 مايو 2004 معالجة الجرائم المعلوماتية ضمن المواد من 370 إلى 387 في الفصل الخامس من قانون العقوبات بعنوان جرائم الحاسب الآلي ميز فيها بين الاعتداء على برامج و معلومات الحاسب الآلي و بين الاعتداء على أدواته و آلاته ، و بذلك يكون قد ساير القانون الفرنسي رقم 19 لسنة 1988 [21].

أما النظام السعودي فقد أصدرت حكومة المملكة العربية السعودية "نظام مكافحة الجرائم المعلوماتية " بهدف الحد من وقوع الجرائم المعلوماتية ، و ذلك بتحديد هذه الجرائم و العقوبات المقررة لكل منها ، وبما يؤدي إلى المساعدة على تحقيق الأمن ألمعلوماتي ، و حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية و الشبكات المعلوماتية و كذلك حماية للمصلحة العامة و الأخلاق والآداب العامة ،و حماية الاقتصاد الوطني و يقع النظام في 15 مادة منها المواد 3،4،5،6،7،8،9 التي نصت على الجرائم المعلوماتية المعاقب عليها .

وقد ميز النظام التشريعي السعودي أيضا بين الاعتداء على برامج و معلومات الحاسب الآلي و بين الاعتداء على أدواته و آلاته و بذلك يكون قد ساير المشرع القطري و المشرع الفرنسي .

و أهم الجرائم التي أوردها قانون مكافحة الجريمة المعلوماتية السعودي [22]:

1- جرائم الاعتداء على برامج و معلومات الحاسب الآلي.
2- جرائم الاعتداء على أدوات و آلات الحاسب الآلي الرقمي .
3- جرائم استخدام خدمات شبكة الانترنت للإضرار بالنفس .
4- جرائم استخدام خدمات شبكات الإنترنت للإضرار بالمصلحة العامة .
5- جرائم التحريض و المساعدة و الاتفاق و الشروع في الجرائم المعلوماتية .

أما بالنسبة للتشريع الجزائري و في تعديل قانون العقوبات الجزائري بموجب القانون رقم 15/04 المؤرخ

في 2004/11/10 يلاحظ أن المشرع لم يعرف الجرائم المعلوماتية، بل اكتفى بالعقاب على بعض الأفعال، تحت عنوان« الجرائم الماسة بنظام المعالجة الآلية للمعطيات »،و نظرا للانتقادات الموجهة للقصور الذي شاب معالجة الموضوع في النظام التشريعي الجزائري ،تدخل المشرع مجددا لتدارك ذلك من خلال قانون رقم 04/09 المؤرخ في 26 أوت 2009 المتضمن القواعد الخاصة للوقاية من هذه الجرائم وقد ورد في المادة الثانية منه ". الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[23] و هي المادة التي توضحت من خلالها رغبة المشرع الجزائري تبني مبدأ المرونة في الصياغة التشريعية مثلما فعل التشريع القطري و السعودي حتى تستوعب الأنشطة الإجرامية الإلكترونية التي يتعذر حصرها و تحديدها لسرعة تطور أساليبها نتيجة للتطور التقني مما يتيح للقاضي حرية واسعة في التقدير ،كما حاول المشرع من خلال هذا القانون مسايرة تطور الحركة الجرمية المعلوماتية في الجزائر.

المبحث الثاني: خصائص الجريمة المعلوماتية.

تتميز الجريمة المعلوماتية بطبيعة خاصة ، وهذا من منطلق ارتباطها بالكمبيوتر مع ما يتمتع به من تقنية عالية ، وهو الأمر الذي يجعل السياسة الجنائية تركز على هاته الخصائص من أجل محاولة وضع النصوص القانونية الملائمة لمكافحة هذا النوع من الجرائم المستحدثة .

يمكن القول في هذا الإطار أن هناك بعض الخصائص التي تشترك بها مع غيرها من الجرائم، في المقابل هناك خصائص أخرى تنفرد بها عن الجرائم التقليدية و هو ما سنتناوله فيما يلي :

المطلب الأول: الخصائص المشتركة مع الجرائم الأخرى.

تشترك الجرائم المعلوماتية مع بعض الجرائم التقليدية إن أمكننا قول ذلك مقارنة مع هذه الجريمة في جملة من الخصائص أهمها:

الفرع الأول: خطورة الجريمة المعلوماتية .

إن ما يتميز به عمل الكمبيوتر و الوظائف التي يقوم بها من سرعة في العمل ، وطاقة كبيرة لإسيعاب المعلومات ، جعلت منه يشكل خطورة على حياة الأفراد و أسرار حياتهم الشخصية ، وكذلك اقتصاديات المؤسسات ، وأمن البلاد وسياستها و اقتصادها .

و الخطر يتحقق إذا طال المعلومات وهذا من خلال أسلوب تسجيلها ،ففي فرنسا مثلا وفي عام 1986 ووفقا لإحصاء الجمعية العمومية لشركات التأمين ضد الحرائق و المخاطر المختلفة فقد خسرت هاته الشركات حوالي 7،3 مليار فرنك فرنسي ،و أكدت الإحصاءات ارتفاع حجم الخسائر الناشئة عن التحايل ، حيث قدرت في هذا المجال بما يقارب من المليار و سبعة من عشره [24] ،كما تضاعفت الخسائر الناتجة عن سرقة المال ألمعلوماتي المعنوي ذو النمط الواحد في الفترة بين عامي 1984و1985 لتصل إلى المليار و اثني عشرة من مئة و شكلت جريمة السرقة للمال ألمعلوماتي المعنوي، الذي يتعلق بالكيانات المنطقية ذو النمط الواحد كبرامج التصميم و إدارة البيانات و الأمن و صيانتها نسبة قدرت بثلاث و أربعون بالمائة من الخسائر.

أما في بريطانيا و التي يرى الدارسون أنها من المجتمعات التي تعتمد بشكل ملحوظ على أنظمة المعالجة الآلية للبيانات، فتختلف التقديرات من 500 مليون جنيه إلى 2 بليون جنيه في السنة، ووجدت دراسة تبنتها الحكومة في 1986 أن 40 % من شركات المملكة قد عانت على الأقل مرة من نصب رئيسي في الحاسوب خلال السنوات العشرة الأخيرة [25] .

وفي الولايات المتحدة الأمريكية أعلن معهد المعلومات تقرير نتائج عام 2001 و هو التقرير السادس حول جرائم الكمبيوتر و دراسة أمن المعلومات المسحية ،و هذه الدراسة يتم إجراؤها سنويا من قبل المعهد بالتعاون مع مكتب التحقيقات الفيدرالي الأمريكي ، حيث أظهرت الدراسة تزايد خطر هذه الجرائم و ارتفاع حجم الخسائر الناجمة عنها ، فقد تبين أن 85 بالمائة من المشاركين في الدراسة و تحديدا المؤسسات الحكومية الكبرى كانت ضحية اختراقات للكمبيوتر خلال السنة السابقة و أن 64 بالمائة منهم لحقتهم خسائر مادية بلغت 378 مليون دولار بالمقارنة مع خسائر سنة 2000 التي قدرت بـ حدود 120 مليون دولار [26] .

وتشير الإحصاءات إلى أن جميع الأنشطة التي تستخدم الحاسب الآلي تكون عرضة لخطر الجريمة المعلوماتية ،و يلاحظ أن الاتجاه ألأساسي للجريمة المعلوماتية يستهدف البنوك في حدود 19 % و يستهدف خاصة المنشآت المالية التي تهيمن على الأقل على القيم الرأسمالية ،ثم تأتي بعد ذلك

النقود وهناك السوق السوداء للمعلومات بجانب السوق الشرعي للمعلومات و التي يتم بمقتضاه مقايضة وبيع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين .

كما أن هذا النوع من الجريمة يرتبط بالجزء الأعظم للأنشطة الاقتصادية و الاجتماعية للمجتمع و يخص المعلومات التالية [27] :

- المعلومات المالية .
- المعلومات التجارية و الصناعية.
- المعلومات الشخصية .
- المعلومات العسكرية.

الفرع الثاني: تعتبر الجريمة المعلوماتية من الجرائم العابرة للحدود.

ان البيئة الافتراضية لا تعترف بالقيود و لا الحدود، فغالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر،كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه.

هي نوع من الجرائم التي يتم ارتكابها عبر المسافات حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد و هو ما يعدم التواجد المادي للمجرم ألمعلوماتي في مكان الجريمة ،ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الحاسوب الفاعل و بين النتيجة أي المعطيات محل الجريمة [28] .

يذكر الأستاذ محمد محي الدين عوض :" أن جريمة الحاسوب تعتبر شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية"[29] هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي و كذلك حول تحديد القانون الواجب التطبيق بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام .

ونتيجة لهذه الطبيعة الخاصة للجريمة و نظرا للخطورة التي تشكلها على المستوى الدولي تعالت الأصوات لأجل التعاون الدولي لمكافحتها عن طريق الاتفاقيات و المعاهدات الدولية و إن كانت هناك دول قليلة لديها قوانين ملائمة لمواجهة هذه المشكلة ، إلا أنها لم تحسم كل المسائل القانونية و التنفيذية و الوقائية فيما يتعلق بأنواع السلوك المنحرف الخاص بهذه التقنية . فالجريمة المعلوماتية لا تعترف بالحدود بين الدول و القارات .

إن السمة الغالبة للكثير من جرائم الكمبيوتر، هي أنها من النوع العابر للحدود و بالتالي تثير من المشاكل ما تثيره أمثال تلك الجرائم كجرائم الاتجار بالمخدرات والاتجار غير المشروع في الأسلحة والاتجار في الرقيق الأبيض و الجرائم الاقتصادية و المالية[30].

إذن هي شكل جديد من أشكال الجرائم العابرة للحدود الوطنية و الإقليمية بل و القارية التي تستوجب على جميع التشريعات الدولية التوحد لمجابهتها و التنسيق بينها للإيقاع بالمجرمين وتقديمهم للقضاء من اجل محاكمتهم ،غير أن أهم المشاكل التي تعيق التعاون الدولي في هذا المجال هو عدم وجود مفهوم مشترك للجريمة المعلوماتية ، بالإضافة إلى نقص الخبرة لدى الشرطة و جهات الإدعاء و القضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت و جمع الأدلة .

و بالتالي ومن أجل مكافحة الجريمة المعلوماتية لا بد أن تعمل كل الدول على مستوى داخلي بان كل تقوم بسن قوانين ملائمة لمكافحة هذه الجريمة و على الصعيد الدولي عن طريق عقد اتفاقيات دولية ، حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية ، و غياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج و آثار هذه الجرائم من ناحية ثانية .

المطلب الثاني: الخصائص التي تنفرد بها الجريمة المعلوماتية عن الجرائم الأخرى.

تفرد الجريمة المعلوماتية عن سواها من الجرائم الأخرى بسمات تضفي عليها طابعا مميزا، الأمر الذي يثير جملة من الإشكالات القانونية و التحديات العملية أمام القائمين بمكافحتها و من أهمها :

الفرع الأول: صعوبة اكتشاف الجريمة و إثباتها.

تتسم الجرائم المعلوماتية بالخفاء ، إذ هناك صعوبة في اكتشافها و الاستدلال على مرتكبها ،و مرد ذلك أنها تستهدف المعنويات لا الماديات ،فلا يترك الجناة أثرا ماديا يمكن من خلاله التعرف عليهم بخلاف الجرائم التقليدية ،فضلا عن أن مباشرة التحقيق و الاستدلال يحتاج إلى دراية كبيرة بتقنية المعلومات مما يتعذر على الأجهزة الضبطية و الحقيقية التعامل معها [31] .

إذن يمكن رد أسباب صعوبة اكتشاف الجريمة المعلوماتية التي عادة ما تكتشف بمحض الصدفة إلى عدم تركها أثرا خارجيا مرئيا لأنها من الجرائم التي تتسم باللاعنف [32]، فتنصب على البيانات و المعلومات المخزنة في نظم الحواسيب ووسائط التخزين عبر تغييرها، التلاعب بها، محوها، إتلافها أو نسخها ،فيؤدي ذلك إلى محو أي اثر كتابي للإثبات ،فالجرائم المعلوماتية لا عنف فيها ،ولا سفك دماء ،ولا آثار اقتحام لسرقة أموال، إنما هي أرقام ودلالات وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، و لأنها لا تترك أثرا خارجيا مرئيا، تكون صعبة الاكتشاف ومما يزيد من هذه الصعوبة ,ارتكابها عادة في الخفاء، وعدم وجود اثر كتابي لما يجري خلال تنفيذها من عمليات حيث تتم بالنبضات الالكترونية لنقل المعلومات ، كما أن الجاني في هذه الجريمة يمكنه ارتكاب

جريمته في دول و قارة أخرى نظرا لكونها جريمة عابرة للحدود، و هو ما يضاعف صعوبة كشفها وملاحقتها سيما في ظل اختلاف إجراءات المتابعة الجنائية هذا إن وجدت .

كذلك قدرة الجاني على تدمير دليل الإدانة في اقل من ثانية واحدة يعد سببا إضافيا [33] .

وما يصعب أيضا عملية اكتشاف الجريمة , إحجام مجتمع الأعمال عادة عن الإبلاغ عنها تجنبا للإساءة إلى السمعة و هز الثقة في كفاءة المنظمات المجني عليها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو التي تمنى بخسائر فادحة من جراء ذلك ،عدم الكشف حتى بين موظفيها عما تعرضت له و تكتفي باتخاذ إجراءات إدارية داخلية دون إبلاغ السلطات المختصة عنها تجنبا للأسباب المذكورة أنفا، قد يمتد الأمر إلى ابعد أين يسعى المجني عليه في بعض الأحيان إلى محاولة تجاوز اثأر الجريمة بمكافأة الجاني واستمالته للعمل لصالحه لاتقاء خطر اختراقات هذا الأخير للنظامه الامني .

هناك من يشير إلى أن هذه الجرائم لم يكتشف منها إلا ما نسبته1% فقط و ما تم الإبلاغ عنه إلى السلطات المختصة لم يتعدى 15 % من النسبة السابقة ،و حتى ما طرح أمام القضاء من هذه الجرائم فإن أدلة الإدانة فيه لم تكن كافية إلا في حدود 5/1 [34] .

و من الصعوبات أيضا التي تعترض اكتشاف الجريمة المعلوماتية ضعف رقابة نظم الحواسيب في اكتشاف الجرائم و هو ما يسميه البعض بالدور غير المباشر للمجني عليه في ارتكاب الجريمة ، وذلك بسبب وجوده في ظروف تجعل من قابليته للتعرض للجريمة المعلوماتية مرتفع بشكل كبير,

وللحيلولة دون وقوع ذلك يجب تطوير نظم الأمن الخاصة بأنظمة الحاسبات الآلية دون الدخول في المشكلات المتعلقة بظروف الجاني والأسباب التي أدت إلى ارتكاب الجريمة لإصلاحها و الحيلولة دون ارتكابها ،وهو ما لا يتحقق في مواجهة الجرائم الأخرى [35] .

الفرع الثاني: الخبرة الفنية في التعامل مع لجريمة المعلوماتية.

تتطلب الجريمة المعلوماتية الإلمام بتقنيات الكمبيوتر ونظم المعلومات سواء لارتكابها أو التحقيق فيها أو ملاحقتها قضائيا.

لذلك يجد مأموري الضبط القضائي أحيانا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية و الإجراءات التقليدية مع هذه النوعية من الجرائم ،فضلا عن صعوبة إجراء التحريات السرية وتتبع مسار العمليات الإلكترونية العابرة للحدود .

كما أن رجال الشرطة ومأموري الضبط القضائي قد لا يتعاملون مع ساحة الجريمة خلال المعاينة و الدليل لإلكتروني بمهارة واحتراف ،فقد يتسبب المحقق بدون قصد أو بطريق الخطأ في إتلاف

الدليل الإلكتروني أو تدميره كما في حالة محو البيانات الموجودة في الأسطوانة الصلبة ، وقد يتجاهل المحقق الدليل الإلكتروني ظنا منه انه غير مهم، أو لا يقوم بمصادرة جهاز الكمبيوتر المستعمل في الجريمة أو ملحقاته من طابعة أو ماسح ضوئي[36].

الفرع الثالث: أسلوب ارتكاب الجريمة المعلوماتية

إن الطبيعة الخاصة للجرائم المعلوماتية تبرز بصورة واضحة في أسلوب ارتكابها، فالجريمة المعلوماتية جريمة هادئة ،تقع بمجرد الدوس على أزرار لوحة المفاتيح و اجتياز الحاجز الأمني ليقوم الجاني بهتك سرية المعلومة ،محوها أو تشويهها أو تعطيلها ،إذن كل ما تحتاجه هذه الجريمة قوة علمية و قدرة من الذكاء و مهارة في توظيف ذلك، و الجاني في سبيل تنفيذها لا يحتاج من الوقت إلا ثوان أو دقائق معدودات [37] ، كما تحتاج هذه الجريمة عادة الى شبكة المعلومات الدولية (الإنترنت).

إن الإجرام ألمعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف ،كما ان المجرم ألمعلوماتي عادة ما يكون ذو مهارات تقنية عالية وإلمام بتكنولوجيا المعلوماتية [38] .

الفرع الرابع: عدم وجود مفهوم مشترك للجريمة المعلوماتية.

إن أهم ما تتميز به الجريمة المعلوماتية عدم وجود مفهوم مشترك لماهية الجريمة المعلوماتية ولا تعريف قانوني دولي موحد لها و السبب في ذلك يرجع إلى صعوبة التعامل مع الجريمة باعتبارها من الجرائم المستحدثة ومكافحتها خاصة على الصعيد الدولي شكل معاهدات و اتفاقيات دولية ثنائية أو جماعية ،أو لاختلاف الأنظمة القانونية المنظمة للجريمة ، وهو ما دفع إلى المناداة بوجود توحيد جهود المجتمع الدولي لإيجاد الآليات المناسبة لمواجهة هذه الجريمة و تكييف الأنظمة القانونية الداخلية وفقا للأنظمة الدولية المنظمة لهذه الجريمة ،خاصة في مجال تبادل المعلومات و المحاكمات و تسليم و تبادل المجرمين [39].

فمشروعية الفعل من عدمه تنطلق أساسا من فكرة تحديد مفهوم له و تجريم الفعل أيضا تنطلق من فكرة عدم إيقاع العقوبة إلا بنص قانوني فإذا لم يحدد الفعل المجرم فلا عقوبة عليه ، يضاف إليها أن مشروعية الجريمة أمر نسبي من دولة إلى أخرى.

و في هذا السياق و من جملة الصعوبات التي تواجهها الجريمة المعلوماتية عدم كفاية النصوص الجنائية و الإجرائية القائمة لمعالجتها ،ففي ظل سيادة مبدأ الشرعية الموجب لعدم إيقاع عقوبة إلا بنص قانوني، وفي ظل فعالية مبدأ حظر القياس على النصوص الجنائية، وحيث أن المواجهة التشريعية للجرائم المعلوماتية ضمن النصوص التشريعية الجنائية مازالت في بدايتها بسبب طبيعتها الخاصة التي جعلت هناك تباين كبير في شأن إدراجها ضمن النظام ألتجريمي التقليدي من عدمه و

هي الجرائم المستحدثة التي لها خصوصيتها، فلكل ذلك يفلت العديد من الجناة من دائرة التجريم في هذه الجرائم بالرغم من تحريك الدعوى ضدهم [40].

الفرع الخامس: المتطلبات الرئيسية لارتكاب الجريمة المعلوماتية.

إن الجريمة المعلوماتية تتطلب لارتكابها الاستعانة بالحاسب الآلي كوسيلة لارتكابها و كذا معرفة تقنية باستخدامه و لا يثور الإشكال إذا كان محل الاعتداء هو الحاسوب نفسه، كتعرضه للسرقة ..الخ، لان نصوص قانون العقوبات التقليدية كفيلة بمعالجة الجريمة ، باعتبار أن الحاسوب ما هو إلا مالا ماديا منقولا، لكن المشكلة تثور إذا تعلق الأمر بالاعتداء على ما يسمى بالكيان المعنوي الحاسوب ،كتدمير برامجه ،سرقتها و تقليدها ،أو العبث ببيانات الحاسب أو المعلومات المخزنة وهوالمقصود بالجرائم المعلوماتية و بالتالي يطرح التساؤل هنا عن مدى انطباق نصوص القانون التقليدية عليها نظرا لصعوبة تحديد ما إذا كانت هذه الأموال مادية منقولة اوان لها طابعا خاصا [41].

لقد أصبحت المعلومة بإشكالها المختلفة في البيئة الرقمية هدف الأساسي لمرتكبي الجرائم المعلوماتية وذلك للقيمة الاقتصادية العالية التي تمثلها و التي قد تفوق عادة المال المادي المنقول .

خاتمة:

لقد تبين و نظرا لأهمية وخطورة الجريمة المعلوماتية ، باعتبارها جريمة العصر لما تحملها من خصوصيات ضرورة تدخل كل الباحثين و من مختلف التخصصات العلمية : القانونية ،الاجتماعية، النفسية وحتى المهتمين بمجال تكنولوجيا المعلومات بصفة خاصة ، و هو ما يفسر تباين التعاريف الموضوعة في هذا الشأن (تعريف قانوني ، تعريف فلسفي أو تعريفي تقني بحث) و كلها محاولات جادة لتحديد المعالم الأساسية لهذه الجريمة و التي أصبحت الشغل الشاغل للمختصين في المجال .

وقد اتضح من مختلف التعاريف التي تنوعت ، أن أساس التعريف بني على معيار قد يكون طبيعة وسيلة ارتكاب الجريمة أو محل الجريمة أو بواعث و دوافع ارتكاب الجريمة ووكلها معايير تم انتقادها نظرا لكونها تدخلات حديثة لجريمة مستحدثة، تتداخل الكثير من الملابسات و الظروف لارتكابها و معظمها لا تزال مجهولة في النظام القانوني الجنائي ، سواء منها الموضوعية أو الإجرائية.

إن قاعدة الشرعية الجزائية الدولية و الداخلية تقتضي ضرورة أن يكون هناك نص عقابي لجريمة تم تكييفها أنفا و تحديد كل معالمها لكي لا يفلت الجاني من العقاب و هو ما يفسر المساعي الحثيثة و المتنوعة لرجال القانون و الفقه و علم الاجتماع لوضع تعريف للجريمة المعلوماتية و حصرها في إطارها الخاص بمحاولة وضع نظام قانوني وأحكام متميزة تخرج عن دائرة التجريم التقليدي وهو الأمر الطبيعي و المستساغ نظرا لخصوصية هذه الجريمة التي لا يمكن ان يختلف بشأنها الفقهاء وان تنوعت و اختلفت تعاريفهم .

و هو السبب ذاته الذي تقتضي وجوب توحيد مجهودات المجتمع الدولي وكل المختصين في هذا المجال لوضع تعريف موحد للجريمة المعلوماتية و باعتباره العقبة الأساسية لتحقيق التعاون الدولي لمكافحة هذا الجريمة و مواجهاتها وهو ما جعل الكثيرون يصرحون أن الجريمة المعلوماتية هي التهديد الثالث الأكبر للقوى الكبرى بعد الأسلحة الكيميائية البكتيرية و الأسلحة النووية .

الهوامش :

1- جعفر حسن جاسم الطائي : جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة ، دار البداية ، عمان ،2010 ، ص108.
2- نائلة عادل محمد فريد قورة : جرائم الحاسب الآلي الاقتصادية – دراسة تطبيقية و نظرية – ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، لبنان ،2005 ، ص27.
3- خالد ممدوح إبراهيم : أمن الجريمة الإلكترونية ، الدار الجامعية ، 2008 ، ص 41 .
4- .أحمد خليفة الملط : الجرائم المعلوماتية ، دار الفكر الجامعي الإسكندرية ، 2006 ، ص84 .
5- هشام محمد فريد رسم : قانون العقوبات و مخاطر تقنية المعلومات ،مكتبة الالات الكاتبة ،1995، مصر، ص35 و ما بعدها.
6- سامي علي حامد عياد : الجريمة المعلوماتية و اجرام الانترنت، دار الفكر الجامعي الاسكندرية، 2006، ص39 .
7- هدى حامد قشقوش : جرائم التشريع الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص6 .
8- احمد خليفة ملط ، المرجع السابق، ص86 .
9- محمد علي العريان : الجرائم المعلوماتية، دار الجامعة الجديدة للنشر،الازاريطة ، 2004 ، ص44.
10- محمد سامي الشوا : ثورة المعلومات و انعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، 2003 ، ص19 .
11- نفسه، ص19 .
12- محمد علي العريان،المرجع السابق، ص44 .
13- محمود احمد العبابنة : جرائم الحاسوب و إبعادها الدولية، دار الثقافة و التوزيع، 2005 الاردن ،ص18 .
14- طارق إبراهيم الدسوقي عطية : الأمن ألمعلوماتي- النظام القانوني لحماية المعلوماتية-،دار الجامعة الجديدة ، 2009،مصر، ص 156 .
15- نسرين عبد الحميد نبيه : الجريمة المعلوماتية و المجرم ألمعلوماتي،منشاة المعارف بالإسكندرية،2008،ص59 .
16- عبد الفتاح بيومي حجازي : نحو صياغة نظرية عامة في علم الجريمة و المجرم ألمعلوماتي،الطبعة الأولى، بهجات للطباعة و التجليد ،مصر، 2009 ، ص39 .
17- عبد الفتاح بيومي حجازي : الإثبات الجنائي في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية ، مصر،2007 ، ص13 .
18- ايمن عبد الله فكري : جرائم نظم المعلومات –دراسة مقارنة-،دار الجامعة الجديدة للنشر، 2007 ، ص137 .
19- هدى قشقوش ، المرجع السابق، ص49 الى 73 .
20- عبد الفاتاح بيومي حجازي : الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة،دار النهضة العربية، مصر، 2009 ، ص52 .
21- مصطفى محمود موسى : الحقيق الجنائي في الجرائم الالكترونية،مطابع الشرطة للطباعة و النشر و التوزيع،مصر 2009 ، ص121 و ما بعدها.
22- نفسه، ص 127الى 134 .

23- انطر المادة الثانية من قانون رقم 09-04 مؤرخ في 5غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائ المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها ،جريد رسمية الصادرة بتاريخ 1 غشت 2009 ،عدد47، ص 5 .
24- سامي علي حامد عباد، المرجع السابق، ص61-62 .
25- محمد سامي الشوا،المرجع السابق، ص19 .
26- محمود احمد العبابنة ، المرجع السابق، ص32 .
27- جعفر حسن جاسم الطائي، المرجع السابق، ص117 .
28- عبد الله حسن علي محمود : سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية ، مصر،2002، ص351 .
29- يونس خالد عرب مصطفى: جرائم الحاسوب – دراسة مقارنة- ،رسالة ماجستير،نوقشت بتاريخ 1994/07/02 ،الأردن ، ص81 .
30- يونس عرب، المرجع السابق، ص 91 .
31- محمد رشيد الزعبي و من معه : الجرائم المعلوماتية، ورقة عمل مقدمة إلى الندوة العلمية حول مشروع قانون مكافحة الجرائم المعلوماتية السوداني ، 2006 ، ص86 .
32- الصغير جميل عبد الباقي : القانون الجنائي و تكنولوجيا الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة،1992، ص17 .
33- محمد علي العريان : المرجع السابق،ص54 .
34- محمد حماد مرهج الهيتي : جرائم الحاسوب –دراسة تحليلية- ،الطبعة الأولى، دار المناهج للنشر و التوزيع، الأردن،2006، ص35 .
35- نائلة عادل محمد فريد قورة، المرجع السابق، ص51 .
36- خالد ممدوح إبراهيم : امن الجريمة الالكترونية، الدار الجامعية، مصر، 2008 ،ص46 .
37- محمد حماد مرهج الهيتي ، المرجع السابق،ص36 .
38- احمد خليفة الملط ، المرجع السابق، ص 114 .
39- خالد ممدوح إبراهيم، المرجع السابق، ص49 .
40- يونس عرب، المرجع السابق، ص98 .
41- محمود احمد العبابنة، مرجع سابق، ص36 .