الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة غرداية
كلية الحقوق و العلوم السياسية
قسم الحقوق

مكافحة جرائم الحاسب الالي

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي
في مسار الحقوق تخصص جنائي

من اعداد الطالب:
– مدني صيفية

تحت اشراف الأستاذ:
د/شول بن شهرة

السنة الجامعية:

1437هـ–1438هـ/2016م–2017م

الإهداء

أهدي هذا العمل الى روح والدي الزكية عبد القادر

والى روح أخي الأصغر قرة عيني رفيق حبيب الله

شكر وعرفان

أشكر أستاذي المشرف الدكتور شول بن شهرة

والشكر موصول الى الاستاذ المشرف المساعد الاستاذ مراد مشوش

والشكر كذلك الى كل أساتذتي والى كل أساتذة الحقوق بجامعة غرداية

واشكر كل من ساعدني في إنجاز هذا البحث

تحية تقدير الى كل زملائي في الجامع وخاصة زملائي في الدفعة

ملخص البحث بالعربية:

تعتبر جرائم الحاسب الآلي من أخطر الجرائم في زماننا هذا، وذلك لما تتسم به هذه الجرائم من نعومة وبعدها عن العنف وكذلك السرعة الفائقة، بالمقابل يمتاز المجرم بالمهارة والمعرفة والسلطة مع الباعث المحرك للفعل الإجرامي، وقد يكون الحاسب الآلي هو المسؤول عن إحداث الجريمة كما قد يكون هو محل الجريمة، وعليه فقد تصدى المجتمع الدولي لهذه الظاهرة عن طريق إبرام إتفاقيات ولعل أبرزها إتفاقية بودابست فكان لزاما على كل الدول أخذ إجراء وموقف جاد اتجاه التعامل مع جرائم الحاسب الآلي، وهذا ما راح إليه المشرع الجزائري الذي لم يبقى منعزلا عن العالم فقد بذل مجهوده في التصدي لهذا النوع من الجرائم عبر قانون 15/04 وقانون 04/09 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ولكن بالرغم من ذلك يبقى هذا المجهود التشريعي لا يلبي الاحتياجات المطلوبة موازاتا مع التطور السريع والرهيب لجرائم الحاسب الآلي.

ملخص البحث بالفرنسية:

Les crimes informatique sont oujourdhuit de plus en plus graves en se caracterisant par la rapidite, la souplesse et loin le lacte violant.
En plus le criminel est une personne douee, connaisseur et maihise parfaitement lacte criminal. Lordinateur peut etre le reponsale du crim comme il peut comme il peut etre lobjet du crime, cest pour cette raison, la communaute international se moilisait a travers la, signature des accords pour faire face a ce phenomene parmis les quels laccord de budapest qui responsabilise tous les pays dagir severement contre ce crime.
Dans ce sens, le legislature algerien a traver les lois 15/04 et 04/09 contenant les regles de prevention et la lutte contre ces crimes lies aux technologies de linformation et de la communication. Toute fois, le develappement accelere des crimes informatioques exiges une legislation plus achealisee

مقدمة

تمهيد:

تضافرت مجموعة متنوعة ومتداخلة من الأسباب والعوامل والإعتبارات على جعل الجرائم المتصِلة بالحاسب الآلي ظاهرة

بالغة الخطورة على أمن المجتمعات الوطنية، وعلى أمن المجتمع الدولى بوجه عام، وقد جرى الإنتباه إلى أهمية التعاون الدولى للتصدى لهذه الظاهرة الخطيرة، وأهمية الوسائل الوقائية لإجهاض هذه النوعية من الجرائم قبل وقوعها، بما يؤدى إلى قمع هذه الجرائم وإنزال العقاب الرادع بالفاعلين لها، بيد أن الأمر الواقع هو أن الحاسب الآلي والأنترنت قد صارا وسائط عالمية للتعامل بين الدول والشركات ويُمثِلان حاليا البنية الأساسية لكل المرافق التي تُدار بالحاسب الآلي، ومن ثم فإن عدم التعامل معهما يخرجنا تماما من الدائرة الدولية.

والحاصل أن كلما ظهرت وسائل جديدة يستخدمها الانسان في حياته، يقترن بها إساءة الاستخدام من قبل الأشخاص الذين يجدون فيها وسيلة ميسرة لارتكاب الجريمة، وكثيراً ما كان يقتصر تأثيرها على أسلوب الجريمة دون أن يؤثر في موضوعها بأي تغيير تخالف به بنيانها التي أسست عليه، فكان التجريم يقتصر على الاعتداء بتلك الوسيلة في مجال الجريمة وتجريم بعض السلوكيات التي ترتبط بها، مثال ذلك ما حدث عند استخدام السيارة كوسيلة لانتقال الأفراد فقد تم تجريم أفعال الإصابة الخطأ أو القتل الخطأ إلى غير ذلك من الأفعال التي ترتبط بتلك الوسيلة.

أما في مجال نظم المعلومات فإن الأمر جد مختلف فنظم المعلومات تدخل في مجالات عديدة في حياة البشر ومرشحة لأن تشمل كافة مجالات الحياة، حيث تعتمد القطاعات المختلفة في الوقت الحاضر في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظراً لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها ومن ثم نقلها وتبادلها بين الأفراد والجهات المختلفة.

غير أن الجانب الايجابي والمشرق لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي افرزتها هذه التقنية العالية والمتمثلة في اساءة استخدام الانظمة المعلوماتية واستغلالها على نحو غير مشروع، حيث أدى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجرائم اصطلح عليها بجرائم الحاسب الآلي كما أن هذه الجرائم الحديثة يختلف مرتكبوها عن المجرمين التقليديين، فهذه الطائفة الجديدة من المجرمين التي تمارس هذه الجرائم متمتعين بقدرات ذهنية غير عادية لا يميل إلى استعمال العنف بل أساليبه تتسم بالهدوء و ذات فعالية كبيرة و مؤثرة.

إشكالية الموضوع:

و مع ظهور هذا النوع المستجد من الجرائم، يهدف هذا البحث إلى محاولة الإجابة على الإشكالية التالية:

كيف تعامل المجتمع الدولي مع جرائم الحاسب الآلي وماهي لمسات المشرع الجزائري في مواجهة هذه الجرائم ؟

و سنحاول الإجابة عن ذلك من خلال الإجابة على التساؤلات التالية:

- **ما هو مفهوم جرائم الحاسب الآلي من خلال تعريفها و خصائصها و أنواعها؟**
- **من هو المجرم المعلوماتي و ماهي سماته ؟**
- **ماهي الجهود الدولية و الإقليمية التي تركت بصمتها في هذا المجال؟**

أسباب أو دوافع اختيار الموضوع:

هناك جملة من الأسباب التي دفعتني إلى اختيار هذا الموضوع، نذكر منها:

- الجرائم المعلوماتية من أخطر الجرائم في العصر، فآثارها لا تقتصر على فرد أو مؤسسة أو على الدولة الواحدة بل تتجاوز الحدود الإقليمية.
- أهمية الوقوف على هذا النمط الجديد من الجرائم الذي بدأ يغزو المجتمعات خاصة مع زيادة استخدام جهاز الكمبيوتر في جميع مناحي الحياة و سهولة الحصول عليه تسبب في كثرة الانتهاكات الواقعة بواسطته وقلة الحماية القانونية
- كون هذه الجريمة تحتاج في مكافحتها تعاون الدول فيما بينها، وأصبحت أساليب هذه الجرائم مستعملة من طرف العصابات المنظمة.
- محاولة الإلمام و معرفة الأساليب الحديثة المتبعة من طرف المجرم المعلوماتي، ومحاولة التصدي لها عن طريق ما نص عليه المشرع الجزائي الجزائري من خلال قانون العقوبات والقوانين الأخرى.

التعرف على الجهود الدولية والإقليمية لمكافحة هذه الجريمة ومدى انعكاسها على الجهود الوطنية

أهمية الموضوع:

إن النشاطات غير المشروعة في مجال المعلوماتية أو جرائم الحاسب الآلي تعد من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني الإقليمي والدولي، والتي ينبغي على المشرع الجنائي مواجهتها بتشريعات حاسمة لمكافحتها وعقاب مرتكبيها، و تتبلور أهمية الموضوع على:

أولا: حيث أن الموضوع يتعلق بالجانب التكنولوجي والجرائم الناجمة عن هذا التطور وهي جرائم مستحدثة مما يجعلها تختلف في ميكانيزماتها عن الجرائم التقليدية.

ثانياً: تثير المعلوماتية باعتبارها علم المعالجة الآلية للبيانات مشكلات قانونية عدة إذ يساء استخدامها لارتكاب الجريمة عن بعد من ناحية، أو أن تكون محلاً للاعتداء عليها من ناحية أخرى، مما يثير مسألة تكييف الاعتداء و ما إذ كان يشكل جريمة أم لا.

ثالثاً: السلوك الإجرامي لمجرم الحاسب الآلي يختلف عن السلوك الإجرامي للمجرم التقليدي، فمجرم الحاسب الآلي استغل هذا التطور في ابتكار اساليب جديدة يجب التصدي لها و معرفة كيفية التعامل معها.

رابعاً: تمثل المعلومة قوة مستحدثة مما يجعلها في مقدمة الأولويات لحمايتها لكي لا تستخدم على نحو غير مشروع.

أهداف الدراسة:

يسعى هذا البحث إلى تحقيق هدفه الرئيسي والمتمثل في محاولة تقديم دراسة تسمح لنا تمييز جرائم الحاسب الآلي من خلال استظهار سماتها وتتبيان أنواعها، بالإضافة إلى التعرف عن مجرم الحاسب الآلي وما يتميز به بالنظر إلى المجرم التقليدي.

كما نحاول تقديم أهم الجهود الدولية والاقليمية في مواجهة الجرائم المعلوماتية ومدى أنعكاسها على القوانين الجزائية في الجزائر.

الدراسات السابقة:

بدأت الدراسات العربية في مجال الجرائم المعلوماتية متأخرة بما هو عليه الحال في الدراسات الأجنبية التي رافقت انتشار الكمبيوتر، وربما يعود ذلك إلى تأخر التقنية الحديثة في معظم الدول العربية ومنها الجزائر، ومن بين الدراسات المتخصصة في هذا المجال:

- رسالة ماجستير أنجزت من طرف الباحث العزام أحمد حسين بعنوان الحكومة الالكترونية في الأردن مع امكانية التطبيق، الأردن، 2001

- رسالة ماجستير أنجزت من طرف الباحثة أمال قارة بعنوان الجريمة المعلوماتية، بن عكنون الجزائر، 2002
- رسالة ماجستير أنجزت من طرف الباحث حمزة بن عقون بعنوان السلوك الإجرامي للمجرم المعلوماتي، باتنة، الجزائر، 2012
- رسالة ماجستير أنجزت من طرف الباحث يوسف صغير بعنوان الجريمة المرتكبة عبر الأنترنت، تيزي وزو، الجزائر، 2013
- رسالة ماجستير أنجزت من طرف الباحث صغير يوسف بعنوان الجريمة المرتكبة عبر الانترنت.تيزي وزو, الجزائر,2013,

الصعوبات المعترضة:

كانت هناك صعوبات ولعل أهمها قلة المراجع المتخصصة في المكتبات الجامعية وخصوصاً ما تعلق بالجهود الدولية والإقليمية، وحتى إن تمكنت الحصول على البعض من المراجع فإنها غالباً لا تتناول الموضوع في التشريع الجزائري.

كما نلمس ندرة التطبيقات القضائية في هذا المجال، نظراً لحداثته وكذلك لاتصاله بالجانب التقني والفني بالنظام المعلوماتي بشقيه المادي و المعنوي.

المناهج المتبعة:

نحاول من خلال هذا البحث بشكل مجمل تقديم صورة عامة لأبرز التحديات المصاحبة لهذه التكنولوجيا، وفق منهجية تطمح إلى تقديم نظرة للظاهرة الإجرامية، لهذا نعتمد على المنهج الوصفي التحليلي، و ذلك بوصف الجريمة وخصائصها وأنواعها والتحليلي بذكر الجهود الدولية والإقليمي لمكافحة هذه النوعية من الجرائم وتحليل الأساليب المتبعة من طرف المشرع الجزائري لذلك.

تقسيم الدراسة :

و في سبيل إعداد هذا البحث ارتأينا تقسيم هذه الدراسة إلى فصلين:

- تعرض الفصل الأول الإطار المفاهيمي لجريمة الحاسب الآلي من خلال تحديد خصائصها من خلال المبحث الأول، أما المبحث الثاني فتطرقنا إلى تصنيف جرائم الحاسب الآلي وسماتها التي تتميز بها بالنظر للمجرم التقليدي.

- و لأن الإشكالية الأساسية تدور حول مكافحة جرائم الحاسب الآلي، فقد تم تخصيص الفصل الثاني في معرفة مواجهة جرائم الحاسب الآلى عبر الجهود الدولية والإقليمية في المبحث الأول وصولاً إلى جهود المشرع الجزائي الجزائري لمواجهة هذه الجريمة في المبحث الثاني.

وأنهي البحث بخاتمة ضمنتها بالنتائج المتوصل إليها.

الفصل الأول

جرائم الحاسب الآلي

تمهيد:

نظراً لأن الجريمة المعلوماتية جريمة حديثة نسبياً، وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، ونتيجة لحداثة هذه الجريمة فقد كانت هناك اتجاهات مختلفة في تعريفها، كما أنها اتسمت بمجموعة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم التقليدية والجرائم الأخرى، كما انها جلبت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية.

ولذلك وفي هذا الفصل سوف نتطرق لأهم الخصائص التي ميزتها عن غيرها من الأنماط الأخرى للجرائم (المبحث الأول)، أما المبحث الثاني فسنعرض فيه على تصنيف جرائم الحاسب الآلي على حسب الشكل الذي اقترحناه.

المبحث الأول : خصائص جرائم الحاسب الآلي

للحديث عن خصائص جرائم الحاسب الآلي يجدر التكلم عن أهم تعريف وعن بعض المصطلحات، فلقد ذهبت مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية (OECD) في عام 1983 الخاص بالاستبيان حول الغش المعلوماتي الذي أوردته بلجيكا في تقريرها إلى تعريف الجريمة المعلوماتية أنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[1].

لقد خصص المشرع الجزائري من خلال القانون 09-04[2] المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الفصل الأول منه للمصطلحات حيث نصت المادة 2:

"الفقرة أ: جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الكترونية.

الفقرة ب: منظومة معلوماتية هي أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين.

الفقرة ج : معطيات معلوماتية هي أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

---

[1] نائلة عادل محمد قورة، جرائم الحاسب الإقتصادية دراسة نظرية و تطبيقية، ط1 ، دار النهضة العربية، القاهرة، 2003 ، ص 23

[2] قانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الجريدة الرسمية، 47، الصادر في 16 أوت 2009 .

إن طبيعة وأبعاد ظاهرة الجرائم المعلوماتية، سيما في ظل تطور انماطها يوما بعد يوم مع تطور استخدام الشبكات وما أتاحته الأنترنت من فرص جديدة لارتكابها مما يضطر المشرع من وضع تعريفات ونصوص جديدة قادرة على الاحاطة بمفردات ومتطلبات وخصوصية هذا النوع من الجرائم وأنه يجب مراعاة عدة اعتبارات مهمة عند وضع تعريف للجريمة المعلوماتية منها :

- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.
- أن يراعى هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.
- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي.
- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.[3]

فتتميز الجريمة المعلوماتية بخصائص وسمات تميزها عن غيرها من الجرائم الأخرى، فأول ما يلفت النظر في هذا النوع من الجرائم هو نعومتها وبعدها عن العنف فلا تتطلب لارتكابها الشدة ولا استعمال الأدوات الخطرة كالأسلحة ولا تحتاج إلى مداهمات وكسراً للأبواب أو تسلق الجدران، فنقل بيانات ممنوعة أو التلاعب بالأرصدة البنكية مثلاً لا تحتاج إلا إلى لمسات أزرار، ثم إن الجريمة المعلوماتية تمتاز أيضاً بإمكانية تنفيذها بسرعة فائقة أي ترتكب في وقت قياسي كما تتميز أيضاً بإمكانية إرتكابها عن بعد فلا تتطلب لوجود الفاعل في مكان الجريمة بل يمكنه تنفيذها في مكان بعيد عن مسرح الجريمة، فالشخص القائم على الحاسوب في أحد المصارف في طوكيو مثلاً يستطيع تحويل مبلغاً من المال إلى أحد فروع المصارف في برلين في ألمانيا، وإن نسبة معتبرة من الجرائم المعلوماتية ترتكب عبر شبكات الأنترنت Internet حيث يكون الجاني في دولة والمجني عليه في دولة أخرى مما جعل التعاون الدولي[4] أمراً حتمياً لمكافحة هذ الظاهرة الإجرامية الجديدة، كما أن الجريمة المعلوماتية صعبة الإثبات لعدم وجود تلك الآثار المادية عند الجرائم التقليدية (بقع الدم ، تكسير، خلع ....).

---

[3] قانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الجريدة الرسمية، 47، الصادر في 16 أوت 2009 .

[4] تجدر الإشارة إلى مؤتمر الامم المتحدة الثامن لمنع الجريمة ومعاقبة المجرمين، هافانا 1990، وفي القرار المتعلق بالجرائم ذات الصلة بالحاسوب ناشد الدول الأعضاء أن تكثف من جهودها كي تكافح بمزيد من الفعالية عمليات إساءة إستخدام الحاسوب من خلال التعاون الدولي عير آليات قانونية، محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2005 ص 361

دون أن نغفل في سرد الخصائص والسمات التي تتميز بها الجريمة المعلوماتية عن غيرها من الجرائم عن الفاعل أو مرتكب هذه الجريمة الذي أصبح يعرف **بالمجرم المعلوماتي** [5] لتميزه أيضاً عن المجرم التقليدي في أسلوبه المنفرد في تنفيذه للجريمة وسرعته ومهارته.

وسنحاول فيما يلي التطرق إلى بعض السمات الخاصة بالجريمة المعلوماتية من خلال الفرع الأول، أما الفرع الثاني سنخصصه بدراسة أهم سمات التي تميز المجرم المعلوماتي.

الفرع الأول: السمات الخاصة بالجريمة

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح، سواء كان هذا التمييز في السمات العامة لها أو 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.

أولاً : خصوصية الجريمة المعلوماتية : تتسم الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها ؛ ويرجع ذلك إلى عدة أسباب من بينها :

- وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم؛ فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة6. فعلى سبيل المثال أحصت وزارة الداخلية في فرنسا عام 1986 حوالي 1200 جريمة معلوماتية في حين كان هناك حوالي **53600** جريمة ضد الأشخاص و**900** 18 جريمة تندرج تحت وصف جرائم الآداب و**3 مليون جريمة ضد الأموال**، وفي أحدث تقارير مركز شكاوى احتيال الانترنت (**IFFC**) الأمريكي أظهر التحليل الشامل للشكاوى التي قدمت للمركز خلال سنة 2004 قد بلغت **6 384** شكوى من ضمنها **273 5** حالة تتعلق باختراق الكمبيوتر عبر الانترنت و814 تتعلق بوسائل الدخول والاقتحام الأخرى كالدخول عبر الهاتف أو الدخول المباشر إلى النظام بشكل مادي؛ مع الإشارة إلى أن هذه الحالات هي فقط التي تم الإبلاغ عنها ولا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي7.

---

[5] نائلة عادل محمد قورة، جرائم الحاسب الإقتصادية دراسة نظرية وتطبيقية، ط1، دار النهضة العربية، القاهرة، 2003، ص 49

[6] د نائلة عادل محمد قورة، المرجع السابق، ص50

[7] د هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن،-الطبعة الأولى، دار النهضة العربية، القاهرة، 1992، ص53

- وفي مقابل انخفاض نسبة جرائم المعلوماتية في مواجهة الجرائم التقليدية؛ ترتفع الخسارة الناجمة عن الجرائم المعلوماتية بصورة كبيرة بالمقارنة بغيرها من الجرائم، فعلى سبيل المثال وفي بحث منشور عبر شبكات الأنترنت للمركز الوطني للبيانات (**NCCCD**)[8] للباحث **Berrnard Standlar** كانت الخسارة الناجمة عن **000 8** حالة سرقة في فرنسا عام 1986 حوالي **561** مليونا من الفرنكات الفرنسية؛ في حين يتضاعف هذا الرقم في حالة الجرائم المعلوماتية على الرغم من انخفاضها نسبة **8 مرات**؛ وفي الولايات المتحدة الأمريكية توصل مكتب التحقيقات الفيدرالية F.B.I. إلى أن متوسط الخسائر التي تحققها الجريمة المعلوماتية يبلغ حوالي 500.000 دولار في حين لا تزيد الخسائر التي تخلفها جرائم السرقة العادية عن 3500 دولار[9].

- عدم اتسام الجريمة المعلوماتية بالعنف الذي تتميز به عن غيره من الجرائم التقليدية الأخرى، حتى أنه لا يوجد شعور حقيقي بعدم الأمان في مواجهة الجريمة المعلوماتية كالذي يوجد بصورة دائمة في مواجهة غيرها من الجرائم، حيث تكاد تختفي الصورة التقليدية للمجرم مصدر الخطر.

- غياب الشعور العام بعدم أخلاقية الفعل أو المساس بمصالح وقيم يحرص المجتمع على حمايتها بل إن الكثير من العاملين في مجال المعلوماتية لا يجدون حرجاً في استعمال الشفرات والدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة أو نسخ البرامج بدلاً من شرائها، وهذا لا ينفي وصف الجريمة على هاته الأفعال من حيث اعتدائها على مصالح لها أهميتها في المجتمع ومن تم تستحق الحماية القانونية ومعاقبة من يمس بها.[10]

ثانيًا: الطبيعة لدولية للجريمة المعلوماتية

يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعددة الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال؛ قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، كما أن السرعة الهائلة التي يتم من خلالها

---

[8] Berrnard Standlar، computer crime law، 2014/04/20، www.google.com

[9] Rose Philipe, La criminalité informatique à l'horizon analyse prospective, 2005,p49

[10] سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير، جامعة أبو بكر بلقايد تلمسان ،الجزائر، 2010 ص 19

تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة.

ومن القضايا التي لفتت النظر إلى البعد الدولي للجريمة المعلوماتية، قضية عرفت باسم مرض نقص المناعة (الأيدز)، وتتلخص وقائعها عام 1989 عند قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج التي يهدف في ظاهره إلى اعطاء بعض النصائح الخاصة بهذا المرض، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)[11] ، وكان يترتب تعطيل الجهاز بمجرد تشغيله، ثم تظهر عبارة على الشاشة يقوم فيها الفاعل بطلب مبلغ مالي يرسل على عنوان حتى يتمكن المجني عليه من الحصول على مضاد لهذا الفيروس، وفي الثالث من فبراير 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة، وتقدمت المملكة المتحدة بطلب تسليمه لمحاكمته لديها باعتبار أن النشاط الإجرامي المتمثل في إرسال البرنامج تم في أراضيها، وأياً ما كان الأمر فإن لهذه القضية الأثر البالغ من ناحيتين، الأولى: أنها المرة الأولى التي تتم فيها تسليم متهم في جريمة معلوماتية والثانية: أن يتقدم شخص للمحاكمة بتهمة إعداد برنامج مخرب.

ولقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي ؛ أم تلك التي توجد بها المعلومات محل الجريمة ؛ أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب[12]، كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة[13] ؛ ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم،فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية".

وتعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية وتجنب خلق ما يسمى "بجنة جرائم المعلوماتية" **Computer Crime Havens**، إلا أن الوصول إلى

---

[11] برنامج له القدرة على التمويه ببرنامج بديل، وعند تشغيل البرنامج يبدأ نشاطه التدميري و يؤدي إلى تعديل ومحو بعض أو كل البيانات

[12] إن المشرع الجزائري قد عقد الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبي وتستهدف الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، المادة 15 من قانون 04/09

[13] د. نائلة عادل محمد فريد قورة –المرجع السابق– ص54.

إبرام هذه الاتفاقيات يقتضي بطبيعة الحال التنسيق بين قوانين الدول المختلفة لضمان تحقق "مبدأ ازدواجية التجريم" فيما يتعلق بجرائم المعلوماتية.

ونجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم. وإن كان مشرعنا قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات، والذي استحدث نصوصًا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات بالإضافة إلى قانون 04/09 المؤرخ في 05 08 2009 المتضمن القواعد الخاصة للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته وسنّ أحكام خاصة بالتعاون والمساعدة القضائية الدولية[14]. ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المختلفة في محورين :

- **الأول** : داخلي بحيث تتلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.
- **الثاني** : دولي عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرمو المعلوماتية عن عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى.

الفرع الثاني : السمات الخاصة بمجرم الحاسب الآلي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين. ولقد اختلف الباحثون في تحديد هذه السمات[15]، ويعد الأستاذ **Parker** واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة ؛ وبالمجرم المعلوماتي بصفة خاصة، إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه، فكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء، وإن كانت – في رأيه- لا تتطابق معها.

فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه على درجة من العلم والمعرفة وإن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو الحال في جرائم

---

[14] و قد علق المشرع الجزائري التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال على شرط احترام الاتفاقيات الدولية والاتفاقيات الثنائية والمعاملة بالمثل، أنظر سفيان سوير، المرجع السابق، ص22

[15] . نائلة عادل محمد فريد قورة، المرجع السابق، ص54

ذوي الياقات البيضاء، كما يتفق مجرمو المعلوماتية مع ذوي الياقات البيضاء في أن الفاعل في الحالتين يبرر جريمته، بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ويرمز إليها الأستاذ Parker بكلمة S.K.R.A.M وهي تعني :

- **المهارة Skills**،
- **المعرفة Knowledge**،
- **الوسيلة Resources**،
- **السلطة Anthority**،
- **و أخيرا الباعث Motives**[16].

وتعد المهارة : المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين، إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما المعرفة : فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها ومكانيات نجاحها واحتمالات فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته، كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو النظام المعلوماتي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

أما الوسيلة: فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها، كما يستطيع نظراً لمهارته ابتكارها، إذ وأنه كلما كان النظام المعلوماتي غير مألوف ويتميز بالخصوصية كانت تشكل تحدياً للمجرم المعلوماتي وكانت الوسائل المتطلبة أكثر صعوبة[17].

---

[16] Parker Donn , Computer Abus , Stanford Research، المرجع السابق، ص114

[17] د. نائلة عادل محمد فريد قورة ، المرجع السابق ، ص55

أما السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته ؛ قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها، وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات.

و أخيرا يأتي الباعث وراء ارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية[18]، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الانتقام من رب العمل أو أحد الزملاء، حيث يفرق مرتكبي هذه الجرائم بين الأضرار بالأشخاص الأمر الذي يعدونه غاية اللاأخلاقية، وبين الاضرار بمؤسسة أو جهة في استطاعتها اقتصاديًا تحمل نتائج تلاعبهم، وهو ما يطلق عليه أعراض روبن هود **The Roben Hood Syndrome**[19]. وبناءا على ما تقدم يمكن أن نقسم مجرمي المعلوماتية **Cyber criminals** إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية ويمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة وتتمثل هذه الطوائف فيما يأتي[20] :

- **تضم الطائفة الأولى Pranksters** : الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث).

- **أما الطائفة الثانية Hackers** : فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

- **وتتضمن الطائفة الثالثة "Malicious Hackers** : هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترقي فيروسات الحاسبات الآلية وموزعيها.

---

[18] ويرى البعض أن أغلب مجرمي المعلوماتية ليس لديهم أطماع مادية بقدر ما يحاولون حل مشكلات مادية تواجههم لا يستطيعون حلها باللجوء إلى الجرائم الأخرى أنظر ،Parker (DonnB)ouvrage ، المرجع السابق ، ص142

[2] د هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1995، ص38

[20] د نائلة عادل محمد فريد قورة ، المرجع السابق ، ص 58

- **أما الطائفة الرابعة Personnel Problem Solvers**: فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.

- **وتتضمن الطائفة الخامسة Career Criminals** مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على أفعالهم وصف الجريمة المنظمة، أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل ؛ ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي[21] .

- **أما الطائفة السادسة Extreme Advocates** : فتدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، ويركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه؛ وان اعتماد المؤسسة المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفًا جذابًا لهذه الجماعات؛ ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوربا باسم " The Red Brigades" بتدمير ما يزيد عن 60 مركزا للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها ومعتقداتها[22].

- **أما الطائفة السابعة The Criminally Negligent** والتي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية وفي أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح؛ ففي نيوزلندا على سبيل المثال قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائرة لهذا التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60 راكبا على متنها، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ.

---

[21] Parker Donn B ، المرجع السابق ، ص147

[22] د نائلة عادل محمد قورة ، المرجع السابق ، ص 63

المبحث الثاني: تصنيف جرائم الحاسب الآلي

تعدد محاولات الفقه لتحديد أنواع الجرائم المعلوماتية وذلك لصعوبة حصر هذه الأنواع بصفة دقيقة بالنظر لحداثة ظهور هذه الجريمة وكذا عدم وجود تعريف عام متفق عليه وكذا تحديد مجالها بالنظر للتطور التكنولوجي في كل صوره، ونظراً لذلك تعددت تقسيمات الجرائم المعلوماتية إلى طوائف مختلفة تتميز كل منها بسمات خاصة بها بالنظر إلى اختلاف المعيار المعتمد في التقسيم، فهناك من قسم الجرائم المعلوماتية إلى ثلاث طوائف تتمثل في جرائم الحاسب الآلي الاقتصادية وجرائم الحاسب الآلي التي تهدد المصالح القومية وكذلك السلامة الشخصية للأفراد[23].

وقسمها آخرون بالاعتماد على معيار أنماط السلوك المختلفة التي تمثل الجريمة المعلوماتية ومدى اتفاقها أو اختلافها مع القواعد التي تحكم القانون الجنائي إلى ثلاث طوائف تتمثل في الدخول والاستعمال غير المصرح بهما لنظام الحاسب الآلي، أما الثانية تتمثل في الاحتيال المعلوماتي وسرقة المعلومات والطائفة الأخيرة تتمثل الجرائم التي يساعد الحاسب الآلي على ارتكابها[24]، لكن ومن الملاحظ أن هذه التقسيمات لم تراع بعض أو كل خصائص هذه الجرائم من خلال موضوعها والحق المعتدى عليه لاعتمادها على معيار واحد للتقسيم متناسية معايير أخر، بحيث يرى بعض من الفقهاء أنه يجب مراعاة في كل محاولة للتقسيم اعتباران وهما

- التطور المستمر للجريمة المعلوماتية
- معيار الجريمة المعلوماتية نفسها أي كل ما يدخل في إطار المعلوماتية وما يخرج منها (E/S)[25]

ومراعاة للاعتبارين السابقين ذهب الفقه الراجح إلى تقسيم الجرائم المعلوماتية إلى طائفتين رئيسيتين على محل الجريمة المعلوماتية التي تنصب على معطيات الحاسوب التي تطال المعلومات نفسها بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة إذ تقتضي في ارتكاب النشاطات الإجرامية استخدام الحاسب الآلي.

وتتمثل الطائفة الأولى في الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي أما الطائفة الثانية تتمثل في الجرائم المعلوماتية الواقعة على النظام المعلوماتي، وهذا ما سنتطرق إليه.

---

[23] André Lucas , le droit de l'informatique , Paris , PUF , 1987.pag 27

[24] نائلة عادل محمد قورة ، المرجع السابق ، ص256

[25] on appelle **Entrées–Sorties** les échanges d'informations entre le processeur et les périphériques qui lui sont associés, Les *sorties* sont les données émises par l'unité centrale à destination d'un périphérique (disque, réseau, écran…). David Fayon, L'informatique, Vuibert, 1999 p 15 ،

المطلب الأول : الجرائم الواقعة بواسطة النظام المعلوماتي

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية ويعد فيها الحاسب الآلي في هذه الطائفة من الجرائم الوسيلة التي تسهل بها النتيجة الإجرامية ومضاعفة جسامتها، حيث يهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة من خلال اعتدائه على أموال الغير، فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته كوسيلة لتنفيذ جريمته.[26]

كما تتعدد صور الجريمة المعلوماتية المرتكبة باستخدام النظام المعلوماتي بعضها ذكرها المشرع الجزائري، في حين أن البعض الآخر رأى الفقه امكانية تطبيق القواعد القانونية القائمة في قانون العقوبات عليها وسنتعرض لهذه الأفكار من خلال النقطتين التاليتين.

الفرع الاول: جرائم الحاسب الآلي الواقعة على الأشخاص

تقع هذه الجرائم على الأشخاص من خلال نوع الحق المعتدى عليه ودور النظام المعلوماتي في اقترافها.

وتتمثل هذه الاعتداءات في الجرائم الواقعة على حقوق الملكية الفكرية والأدبية، أما النوع الثاني تكمن في الجرائم الواقعة على حرمة الحياة الخاصة للفرد وكما نشير أنه هذه الحرمة يدخل في نطاقها أمواله.

أولاً: طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية والأدبية

يمكن أن يكون النظام المعلوماتي وسيلة فعالة للاعتداء على الملكية الفكرية والأدبية، ومثال ذلك استخدام النظام المعلوماتي في السطو على قاعدة معلومات التي تتضمن معلومات أياً كان نوعها ملكاً لشخص آخر دون إذنه أو علمه كمن يعتدي بنسخ مقال أو بحث في صدد الإنجاز من جهاز أو دعامات التخزين **les supports de stockage**[27] أخرى دون إذن صاحبها وينسبها لنفسه حيث تمثل اعتداء على حق من حقوقه والأدبية ومنها المادية كون أن للمعلومات قيمة من خلال نشرها أو تسويقها، ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع[28].

---

[26] نائلة عادل محمد قورة ، المرجع السابق ، ص265

[27] Les supports de stockage de grande capacité, autre que le papier, permettant l'enregistrement de données، David Fayon ، المرجع السابق، ص21

[28] أحمد خليفة الملط ، المرجع السابق، ص 184

وقد نص المشرع الجزائري على حقوق الملكية والفكرية وبراءات الاختراع من خلال عدة نصوص قانونية نذكر منها المادة 38 من الدستور الجزائري التي تنص على " حرية الابتكار الفكري والفني والعلمي مضمون للمواطن".

كما أن حقوق المؤلف يحميها القانون من خلال الامر رقم 05/03 المؤرخ في 19 07 2003 المتعلق بحقوق المؤلف والحقوق المجاورة وكذا الامر 07/03 المؤرخ في 19 07 2003 المتعلق ببراءة الاختراع حيث لا يجوز حجز اي مطبوع أو تسجيل أو اية وسيلة أخرى من وسائل التبليغ والاعلام إلا بمقتضى أمر قضائي.

ثانياً: طائفة الجرائم المعلوماتية الواقعة على الحياة الخاصة

لقد كفلت جل الدول الحياة لمواطنيها بالحماية وقد حذا الدستور الجزائري بموجب المادة 39 من الدستور الجزائري "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة" كما يدخل في هذه الحماية حماية الأموال والممتلكات.

ولا شك أن الحاسبات الآلية بما لها قدرة فائقة على تخزين مقدار كبير من المعلومات، ولأهمية المعلومات التي تحتويها هذه الانظمة، أصبحت هذه الحسابات هدفاً لما لها من دور مهم في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مادية ومعنوية مختلفة.[29]

وعليه يمكن استخدام النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد، كأن يقوم شخص بإعداد ملف معلوماتي يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه، كما يقوم بنشر معلومات على شكل صور أو حقائق من خلال اختراقه لحساب شخص وتشويه السمعة أو الاطلاع على معلومات بعلم الشخص المعني ويقوم بحفظها واطلاع الغير عليها أو أسرار مكتوبة أو سير ذاتية، مذكرات قصد التشهير بشخص أو جماعة معينة أو بيعها لتحقيق مصالح مختلفة كالحصول على عائد مادي أو للضغط على أصحابها مقابل القيام بعمل أو الامتناع عنه[30].

كما تقع هذه الجرائم لإفشاء الأسرار سواء كانت الاسرار عامة تتعلق بالأفراد والمؤسسات المختلفة أو تخص مصالح الدولة ونظام الدفاع عنها والأسرار المهنية.

وهذه الجرائم تسبب أضرار لأصحابها لذا حرص المشرع الجزائري على حماية الاسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات الجزائري بالإضافة

---

[29] نائلة عادل محمد قورة، المرجع السابق ، ص 275

[30] أحمد خليفة الملط ، المرجع السابق ، ص 190

للمادة 394 مكرر 03 من نفس القانون التي نصت " تضاعف العقوبات المنصوص عليها في هذا القسم[31] إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد" حيث حذا المشرع الجزائري مختلف التشريعات لا سيما عندما يكون إفشاء هذه الأسرار المتعلقة بالدفاع الوطني.

كما تعاقب مختلف التشريعات كل من يقوم بالدخول غير المصرح له إلى النظام المعلوماتي وإفشاء معلومات توجد داخلها، حيث حمت تلك التشريعات الأسرار المهنية حيث ألزمت أصحاب المهن على غرار المحامي والطبيب بالمحافظة على الأسرار التي يقرها له الزبون أو العميل[32].

الفرع الثاني : الجرائم الواقعة على الحاسب الآلي

هذا النوع من الجرائم لا يستلزم تدخلاً لإتلاف الوظائف التقنية للنظام المعلوماتي ولا تعديلا على المعلومات المعالجة، بل يقتصر في غالب الأحيان الولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة الكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى.

أولاً: الدخول غير المشروع للمعلومات المعالجة آلياً

تقوم هذه الصورة بوجود المجرم داخل احد المراكز المعلوماتية بهدف الولوج إلى المعلومات التي تمت معالجتها آلياً والاطلاع عليها دون تصريح وقد يكون هذا الولوج إما مباشرًا أو غير مباشر.

أما المباشر فيعد من أكثر الأفعال المرتكبة وأسهلها تنفيذاً ويتخذ عدة صور إذ يستطيع الجاني الاستيلاء على المعلومات المخزنة لدى الأنظمة بعدة طرق باستخدام آلة الطباعة أو بالقراءة المباشرة أو باستخدام مكبر الصوت، ومن أمثلة ذلك الولوج المباشر، قيام شخص بأحد البنوك الأمريكية الذي كان يعمل في النظام المعلوماتي الخاص بالبنك نقل معلومات المالية المخزنة في النظام ونقلها لرئيسه الجديد بعد حصوله على كلمة السر من زميل سابق له[33].

وأما الولوج غير المباشر ظهر بظهور تقنيات مستحدثة، لها الصلة بالنظام المعلوماتي كالمعالجة عن بعد، إذ هذه التقنيات أدت إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للولوج والاستفسار عن بعد من المراكز

---

[31] القسم السابع تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من قانون 04-15 مؤرخ في 10 نوفمبر 2004 ، الجريدة الرسمية، العدد 71، 10 نوفمبر 2004

[32] أحمد خليفة الملط ، المرجع السابق ، ص 200

[33] محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية،1994. ص 67

المعلوماتية، إذ أنه أثناء بثها تكون عرضة للالتقاط والتسجيل غير مشروعين في كل فترة من فترات هذا التحويل ما بين المرسل والملتقط [34]، ولعل من أبسط هذه التقنية هي تقنية البلوتوث [35]Bluetooth.

ثانياً: إساءة استخدام البطاقات الائتمانية

أدى إدخال النظام المعلوماتي في مجالات عمليات البنوك إلى ظهور هذا النوع الجديد من الجرائم المعلوماتية، التي تعد من أخطر الجرائم لاسيما في المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور والحداثة، ويتخذ هذا النوع من الجرائم على صورتين :

أولاهما في الإساء في استخدام الحسابات المصرفية أو للبطاقات الائتمانية وذلك عن طريق عدم احترام العميل المصدر إليه البطاقات الائتمانية شروط العقد المبرم بينه وبين المؤسسة المصرفية كأن يستعمل بطاقة منتهية الصلاحية أو بطاقة تم إلغاؤها أو الشراء بأكثر من قيمتها ...[36]

وأما الصورة الثانية تتمثل في استخدام الغير لتلك الحسابات أو البطاقات كأن يقوم المجرم استعمال البطاقة للحصول على سلع أو خدمات او سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي مثلاً أو السحب باستخدام بطاقات ائتمانية مزورة[37].

المطلب الثاني : الجرائم الواقعة على الحاسب الآلي

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية بالتصنيف الذي يقوم على محل الجريمة ويتمثل في الجرائم الواقعة الحاسب الآلي نفسه التي قد تستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية والمعلومات المدرجة بالنظام .

وهذا ما سنتطرق إليه بشيء من التفصيل من خلال الفرعين التاليين :

الفرع الأول : جرائم الاعتداء على المكونات المادية للحاسب الآلي

يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والكابلات ... إلخ، وكنتيجة للطبيعة المادية لهذه المكونات فالاعتداء عليها يكون عن طريق جرائم

---

[34] أحمد خليفة الملط ، المرجع السابق ، ص 196

[35] Bluetooth est une spécification de l'industrie des télécommunications. Elle utilise une technique radio courte distance destinée à simplifier les connexions entre les appareils électroniques ، David Fayon، المرجع السابق، ص25

[36] أحمد خليفة الملط، المرجع السابق، ص 192

[37] أحمد خليفة الملط، المرجع نفسه، ص 196

عادية وتقليدية، كأن تكون محلاً للسرقة أو خيانة الأمانة أو الإتلاف العمدي كالحرق والتكسير أو خربشة الشريط وإفساد الأسطوانات ويترتب على ذلك ضياع للمعلومات وخسائر كبيرة.

ومن أمثلة ذلك ما حدث في فرنسا حيث أدى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية إلى خسائر مادية معتبرة حصلت ب 5 ملايين يورو[38].

ويرى البعض من الفقهاء أنه يندرج ضمن هذه الطائفة من الجرائم سرقة وقت الآلة، فقد يلجأ العاملين بالنظام المعلوماتي إلى استخدامه في أعمال خاصة بهم، وعليه تكون واقعة السرقة منصبة على وقت الجهاز الذي يمكن تقويمه ماليا وليس على الأشياء المادية بمعنى الكلمة، وتجدر الإشارة أن خطورة واقعة السرقة لا تكمن في الشيء المسروق لضآلة قيمته، بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسائرها بأموال طائلة.

الفرع الثاني : جرائم الاعتداء على المكونات المنطقية للحاسب الآلي

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة، وقد تقع هذه الجرائم إما على البرامج التي منها البرامج التطبيقية أو برامج التشغيل.

أولاً : الجرائم الواقعة على البرامج التطبيقية

يقوم الجاني في هذه الصورة بتحديد البرنامج أولاً ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية.

أ- **تعديل البرنامج** : الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود وتكثر هذه الجرائم في مجال الحسابات[39].

ومن أمثلة ذلك قيام مبرمج في أحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick وحصل على إثر ذلك على مئات الدولارات كل شهر وكان من الممكن أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل ليكتشف بعدها حقيقة هذا المبرمج[40].

ب- **التلاعب في البرامج** : يأخذ التلاعب في البرامج عدة أشكال فقد يتم عن طرق استعمال القنبلة المنطقية[41] أو عن طريق قيام أحد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح

---

[38] Rose Philipe ، المرجع السابق ، ص 58

[39] أحمد خليفة الملط ، المرجع السابق ، ص 173

[40] Duleroy ,Les escrocs a l'informatique ,le nouvel économiste , octobre 2002 , p 202

[41] و هي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو في كل فترة زمنية منتظمة و يتم وضعه في شبكة معلوماتية للتسهيل بالقيام بعمل غير مشروع، د أحمد خليفة الملط ، المرجع السابق ، ص 545

له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي، وبهذا يصعب اكتشاف هذا البرنامج لصغره ودقته.

ثانياً: الجرائم الواقعة على نظام التشغيل

تعد برامج التشغيل هي المسؤولة عن عمل النظام المعلوماتي، من حيث قيامها بتنظيم وضبط وترتيب المعلومات الخاصة بالنظام.

وتقوم الجريمة في هذه الصورة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[42]، ويتحقق هذا النوع من الجرائم في نوعين :

أ- **المصيدة** : تتمثل هذه الصورة من خلال إعداد برنامج به أخطاء وعيوب عمداً، لا يكتشف بعضها عند استخدام البرنامج، إذ يترك المبرمج ممرات خيالية وتفرعات في البرنامج حتى يستطيع بعدها تنفيذ التعديلات الضرورية للولوج داخل النظام المعلوماتي والوصول إلى كل المعلومات التي تحتويها الذاكرة.

ب- **تصميم برنامج وهمي**: وتقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه معد خصيصاً لارتكاب الجريمة، ومن أمثلة ذلك قيام إحدى شركات التأمين الأمريكية بواسطة مبرمجيها من تصميم برنامج وهمي يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 46 000 بهدف تقاضي هذه الشركة من اتحاد شركات التأمين عمولات من نظيراتها[43].

ثالثاً: جرائم الاعتداء على المعلومات المدرجة بالحاسب الآلي

للمعلومة في حد ذاتها باعتبارها الأساس الذي يقوم عليه النظام المعلوماتي، وبهذا اصبحت هدفاً للجريمة المعلوماتية من خلال التلاعب فيها أو عن طريق إتلافها.

أ- **التلاعب في المعلومات** : يتم التلاعب في المعلومات الموجودة داخل النظام بطريق المباشر أو غير المباشر، أما الطريق المباشر يتم عن طريق ادخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، ويتم هذا التلاعب بإضافة معلومات غير مؤسسة كإضافة أسماء غير موجودين في العمل أو الإبقاء على مستخدمين تركو العمل...

---

[42] أحمد خليفة الملط ، المرجع السابق ، ص 175

[43] Duleroy ، المرجع السابق ، ص 210

في حين أن الطريقة غير المباشرة يتم عن طريق التدخل غير المباشر لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام احد وسائط التخزين أو الدعامات، فقد قام في هذا الصدد أحد الموظفين بأحد فروع الشركة **Isoverst Gobain** بإرسال شريط ممغنط يحتوي على 139 إذن دفع، وعند معالجته بالبنك تم رفض نسخه لعيب في الشريط، وقد علق الخبراء أنه لو نجحت العملية لتم النصب على البنك بحوالي 21 مليون فرنك[44].

ب- **إتلاف المعلومات:** قد يهدف الجاني من خلال ارتكابه للجريمة المعلوماتية المخزنة داخل النظام، وقد يأخذ هذا التلاف عدة صور الحذف التغير استبدال المعلومة ...إلخ

ويشكل استبدال المعلومة نوع من أنواع جرائم الغش والتزوير المعلوماتي وهو على درجة كبيرة من الخطورة لأنه في حال نجاحه يستمر لوقت طويل قبل اكتشافه ويتولد عيه اضرار كبيرة كتغير رقم بآخر أو اسم بغيره [45]، فقد قام شخص يدعى Vladimir Loriblitt يعمل بوزارة المالية بتغير فواتير وهمية للنظام وتحويل ما تم سداده لحساب شركات وهمية الذي جنى منها 10 ملايين دولار قبل أن يتم اكتشافه[46].

أما محو المعلومات فهو من أسهل طرق الاتلاف كون أنه من خصائص الجرائم المعلوماتية في قدرة المجرم المعلوماتي من محو آثار الجريمة في فترة وجيزة لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو عن طريق الفأرة، فمثلاً قام شخص باختلاس ما يقدر ب 00 61 دولار مرسلة من شركة تأمين إلى إحدى المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام المعلوماتي بالمركز وجعلها غير قابلة للتحصيل.

خلاصة:

تطرقنا في هذا المبحث إلى السمات الخاصة التي تتميز بها جريمة الحاسب الآلي عن غيرها من الجرائم الأخرى ووجدنا أنها جرائم عابرة للحدود ويصعب اكتشافها واثباتها كما أنها تتم بأسلوب لا يتسم بالعنف.

كما تناولنا أبرز سمات الخاصة بمجرم الحاسب وعرفنا أنه يتميز عن المجرم التقليدي بالمهارة والمعرفة وعدم ممارسة العنف اثناء ارتكابه للجريمة تناولنا كذلك أنواع جرائم الحاسب الآلي التي يكون الحاسب الآلي فيها محلاً للاعتداء والجرائم التي تقع بواسطة هذا الحاسب الآلي.

---

[44] Duleroy ، المرجع نفسه ، ص 212

[45] أحمد خليفة الملط، المرجع السابق، ص 175

[46] Duleroy ، المرجع السابق، ص 215

الفصل الثاني
مواجهة جرائم الحاسب الآلي

تمهيد

لقد شهد العالم في السنوات الأخيرة تطورًا غير مسبوق في مجالات الإعلام والاتصال نظرًا إلى توغل وانتشار وسائل التكنولوجيا والابتكارات المستحدثة في الأنشطة المعلوماتية ودخولها في جميع نواحي، الحياة بل أصبح العالم قرية صغيرة بفضلها، وهو ما قد يترتب عليه الخطر الكبير على البنيات المختلفة جراء الاستخدام غير المشروع لهذه التقنيات والمساس بالحياة الخاصة للأفراد، والخطر الأكبر هو أن الجرائم المعلوماتية قد تستهدف الأمن القومي بارتكاب جرائم تمس جهات حكومية وأمنية، ليس هذا فحسب بل حتى الإضرار بالاقتصاد كونه أصبح يعتمد بصورة متزايدة على تقنية المعلومات الاقتصاد الرقمي مما قد يؤثر هذا الإجرام التقني تأثيرا كبيرا على اقتصاد الدولي والمحلي، الأمر الذي أدى إلى الإسراع من أجل محاولة التصدي لهذه الظاهرة الإجرامية المستحدثة، فتظافرت الجهود من أجل إيجاد سبل مكافحتها بفعالية ونجاعة أكثر.

يتضح جلياً خطورة هذا النوع من الجرائم، حيث أن القوانين التقليدية المطبقة لم تعد مجدية نظراً لاختلاف الكبير بين الجرائم التقليدية وجرائم المعلوماتية التي يعود بالأساس إلى الطبيعة اللامادية لها والتي هي من أهم الصعوبات التي تعتري سبل مكافحتها وبفعل ما أثاره التطبيق القضائي لنصوص القوانين الجنائية على جرائم الحاسوب من مشكلات، ولضمان عدم افلات الجناة من العدالة لعدم كفاية القوانين أو عجزها عن الانطباق على هذه الجرائم المستحدثة، وصونًا لمبدأ الشرعية الذي يقضي بأن لا جريمة ولا عقوبة بغير نص قانوني، لهذه الأسباب، ولمواجهة الخطر المحدق والخسائر الفادحة التي تسببها جرائم الحاسوب، اتخذت المواجهة التشريعية لجرائم المعلوماتية ثلاثة مستويات :

أما المستوى الأول فهو المستوى الوطني، فلقد سارعت دول العالم المتقدم التدابير اللازمة لمواجهة هذه النوعية من الجرائم، فبعض هذه الدول حرصت على أن تُضَمن تشريعاتها بخصوص هذه الجرائم إما عن طريق نصوص مستقلة ومثال ذلك قانون جرائم الحاسب الآلي 1987، وإما عن طريق تحديث قوانينها وإدماجها في قانون العقوبات ومن أبرز هذه النوعية فرنسا من خلال قانون العقوبات الجديد الصادر سنة 1992 والذي أضاف فصلاً ثالثاً للباب الثاني من القسم الثالث تحت عنوان " انتهاكات نظم المعالجة الآلية للبيانات atteintes aux Des systèmes de traitement autorisé de données " و يتكون هذا الفصل من المواد 1/321 إلى 7/323.[47]

[47]. Clément ENDRELIN , Les moyens juridiques de lutte contre la cybercriminalité , Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen , 2011 , p76

ومن بين المحطات التالية من محطات التجريم المعلوماتي في فرنسا فكانت عام 2004[48] عندما أضاف المشرع الفرنسي بموجبه جريمة أخرى هي جريمة التعامل في الوسائل التي تصلح أن ترتكب بها جريمة الدخول أو البقاء غير المصرح بها أو جريمة التلاعب بالمعطيات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات.

وتجدر الاشارة أن المشرع الجزائري قد حذا حذو المشرع الفرنسي من خلال تعديل قانون العقوبات وإدراج جرائم المعلوماتية من خلال تجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات من إحداث قسم جديد في قانون العقوبات هو القسم السابع (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل لقانون العقوبات من المواد 394 مكرر إلى 394 مكرر7).[49]

وثانيها على المستوى الاقليمي، فلقد حرص المجلس الاوروبي على التصدي للاستخدام غير المشروع للكمبيوتر وشبكات المعلوماتية وفي عام 1989 نشر المجلس الأوروبي دراسة تضمنت توصيات تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسب وهي التوصية التي لحقتها دراسة أخرى في عام 1995 حول الإجراءات الجنائية في مجال الجرائم المعلوماتية، وعلى أساس المبادئ التي تضمنتها التوصيات قام المجلس الأوروبي في عام 1997 بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي وذلك بقصد إعداد اتفاقية في هذا الإطار وتجلى ذلك في اتفاقية بودابست[50] Convention on cybercrime والموقعة في 23 نوفمبر 2001 والتي سنعكف على دراستها في المطلب الثاني من هذه الدراسة.

وثالثها على المستوى الدولي وتتمثل في جهود الامم المتحدة التي تبتذلها في هذا المضمار.

وعليه فسنقسم هذا الفصل من الدراسة إلى مبحثين، أما المبحث الأول فسنخصصه للجهود الدولية لمكافحة جرائم الحاسب الآلي ففي المطلب الأول على المستوى الدولي أما المطلب الثاني على المستوى الاقليمي (المجلس الاوروبي واتفاقية بودابست).

المبحث الثاني فسنتطرق إلى جهود المشرع الجزائري في مجال مكافحة جرائم الحاسب الآلي من خلال قانون العقوبات في المطلب الاول، أما المطلب الثاني من خلال قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

المبحث الأول : الجهود الدولية لمكافحة جرائم الحاسب الآلي

---

[48]. القانون رقم 575 لسنة 2004 في 06/21 /2004 المتعلق بالثقة في الاقتصاد الرقمي

[49]. نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير حقوق ، جامعة الحاج لخضر باتنة، الجزائر، 2012 ، ص79

[50]. نعيم سعيداني ، المرجع نفسه ، ص 85

تتسم جرائم المعلوماتية بالنظر لطبيعتها بطابع دولي، لكن اختلاف التشريعات في تأسيس اختصاصها الجنائي نتيجة تعدد الأسس التي يقوم عليها هذا الاختصاص قد يؤدي إلى تنازع الاختصاص بين الدول، فقد يحدث أن ترتكب الجريمة المعلوماتية في دول معينة، ويكون المجرم المعلوماتي مرتكب هذه الجريمة أجنبياً، فتخضع هذه الجريمة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الاقليمية ، وتخضع كذلك لاختصاص الدول الثانية على أساس مبدأ الاختصاص الشخصي في جانبه الايجابي.[51] وقد تكون الجريمة المرتكبة على اقليم الدولة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتخضع للاختصاص الجنائي الاقليمي من جهة، وتخضع لاختصاص الدولة المجني عليها استناداً إلى مبدأ الاختصاص العيني من جهة أخرى، كما تثور فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الاقليمية، كما لو قام الجاني ببث معلومات غير مشروعة على اقليم دولة معينة وتم الاطلاع عليها في دولة أخرى، فوفقاً لمبدأ الاقليمية فإن الاختصاص الجنائي والقضائي يثبت لكل دولة من الدول التي مستها الجريمة، سواء تلك التي وقع فيها الفعل الإجرامي (فعل البث) أو تلك التي حدثت نتيجة الفعل فيها (تلقي المعلومات غير المشروعة)، الأمر الذي يؤدي إلى الاطاحة بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة، ولذلك لا بد أن يكون هناك تعاون دولي يتفق مع طبيعة جرائم المعلوماتية التي تتميز بطابع خاص يقتضي أن تكون هناك ردود فهل سريعة لأن هذا التنسيق الفعال والعاجل يساعد على الحد من الأضرار الناجمة عن هذه الجرائم وكذلك تجنب المجرم المعلوماتي الإفلات من العقاب ومثال ذلك ما قام به "أونيل دو غوزمان" الذي استخدم فيروس "أحبك I love you "[52] سنة 2000 الذي انتشر في كل أنحاء العالم عن طريق البريد الالكتروني حيث قدرت الخسارة ب 7 مليارات دولار[53] .

المطلب الأول : على المستوى الدولي

وإذا كان التعاون الدولي هو الآلية الفعال لمكافحة جرائم المعلوماتية، فإن هذا التعاون يقتضي التخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية لأن التباعد بين هذه الانظمة يجعل المجرم المعلوماتي يبحث عن الأنظمة الأكثر تسامحاً (قضية دو غوزمان التي أشرنا إليها)، ولذلك أبرمت العديد من الاتفاقيات الدولية في مجال التعاون الدولي من أجل مكافحة جرائم المعلوماتية وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ

---

[51]. جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة ،2002 ، ص 73

[52]. هي دودة حاسوب ضربت العديد من أجهزة الكمبيوتر في عام 2000، عندما تم إرسالها كمرفق برسالة بريد إلكتروني مع النص "I LOVE YOU" في عنوان الرسالة الدودة وصلت في صناديق البريد في 4 مايو 2000، مع هذا العنوان البسيط "I LOVE YOU" ومرفق ."LOVE-LETTER-FOR-YOU.txt.vbs" عند فتح المرفق ،ترسل الدودة نسخة من نفسها للجميع في قائمة العناوين، متنكرة في زي للمستخدم. كما أنها تحدث العديد من التغييرات الضارة لنظام المستخدم. ويكيبيديا، فيروس أحبك 2014/05/14، فيروس أحبك http://ar.wikipedia.org/wiki/

[53]. راسل تاينر، أهمية التعاون الدولي في منع جرائم الإنترنت، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19 06 2007 ، المملكة المغربية، ص

اجراءات التحقيق وجمع الأدلة وتسليم والاعتراف بالأحكام الجنائية، بحيث أن هذا القانون الدولي لا ينال من سيادة الدولة، بل بالعكس عدم التعاون يزيد من التباعد بين الأنظمة العقابية مما يساعد على تزايد هذه النوعية من الجرائم.

وفي اطار دراسة حالة تعد من أبرز الأمثلة لأهمية التعاون الدولي في مجال مكافحة جرائم المعلوماتية هي عملية كاتريك Catterick Operation[54] وتتعلق هذه العملية بالابتزاز الذي قامت به شركات القمار عبر الإنترنت في الفترة من مايو إلى أكتوبر 2004 وفي هذه العملية، كان المجرمون يرسلون إلى إحدى الشركات يطلبون منها أموالا، مهددين إياها بأن يشنوا على موقعها "هجمات حجب الخدمة الموزعة" في حالة امتناعها عن الدفع، وتحدث هذه الهجمات بأن تزور آلاف أو مئات الآلاف من أجهزة الكمبيوتر من جميع أنحاء العالم موقعا معينا في الوقت نفسه،

ما يؤدي إلى تدمير الموقع وبعد تنفيذها للهجمات تعرض حوالي 57 شركة في أنحاء العالم، منها 10 شركات بالمملكة المتحدة، تجاوزت خسائرها 30 مليون جنيه إسترليني .وبالإضافة إلى الأثر الذي تتعرض له المواقع نفسها، فإن مقدار البيانات التي يتم توجيهها عبر قسم من الوصلات الرئيسة لشبكة الإنترنت يكاد يتسبب في تدمير هذه المواقع، ومع مباشرة التحقيقات لكل من المملكة المتحدة والولايات المتحدة باعتبارهما الأكثر تضرراً وقد قادتهم التحريات التي تمت بين أجهزة الشرطة في البلدين إلى لاتفيا، حيث قامت قوات الشرطة لديها بعملية مراقبة سرية أسفرت عن إلقاء القبض على 10 أشخاص يُشتَبه في تورطهم حيث تم تحديد موقع جهاز كمبيوتر تم اختراقه في مدينة بالاكوفو في روسيا.

بدأت الشرطة الروسية على إثره بإجراء تحقيق بمفردها تحول بعد ذلك إلى تحقيق فعال مشترك؛ تم توقيف عدد من الأشخاص، وضبط عدد من أجهزة الكمبيوتر ووجهت إلى المتهمين تهم الابتزاز ونشر فيروسات علي أجهزة الكمبيوتر، وحُكم عليهم بالسجن ثماني سنوات.

وعليه يجد التعاون الدولي في مجال مكافحة جرائم المعلوماتية بصفة عامة تبريره في بعض الاعتبارات منها[55] :

- أنه يعتبر خطوة على طريق تدويل القانون الجنائي، ذلك أن ثمة قواعد موضوعية واجرائية تهيمن على أذهان العديد من مشرعي هذه الحقبة ومن شأن تشابه هذه القواعد أن يخلق نوعاً من التقارب بين التشريعات الحالية.
- أنه يعتبر من قبيل التدابير المانعة من ارتكاب هذه النوعية من الجرائم، لان المجرم المعلوماتي سوف يجد نفسه محاطاً بسياج مانع من الإفلات من المسؤولية الجنائية عن الجريمة التي ارتكبها، أو من العقوبة التي حكم عليه بها، فإذا ارتكب جريمته في دولة ما وتمكن من الهروب إلى دولة أخرى فإنه سوف

---

[54]. راسل تاينر، المرجع نفسه، ص 114

[55]. جميل عبد الباقي الصغير، المرجع السابق، ص 74

يكون عرضة للقبض عليه أو ترحيله إلى البلد الأول، ومن شأن كل ذلك أن يجعل المجرم المعلوماتي يعزف عن سلوك سبيل الجريمة.

إن التعاون الدولي في مجال مكافحة الجريمة المعلوماتية قد يأخذ مظهران، الأول يتعلق بضرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة والتي تعبر اختصاصات قضائية متعددة ذات نظم قانونية مختلفة، ويتمثل في التعاون القضائي، والثاني يتعلق بالسعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة في مرحلة التنفيذ[56].

أما التعاون القضائي الدولي في مواجهة الجريمة المعلوماتية يعد الآلية الرئيسية للكفاح ضد ها فإن فعالية التحقيق والملاحقة القضائية غالبا ما تقتضي الحاجة إلى مساعدة من السلطات في البلد الذي كان منشأً للجريمة، أو من السلطات في البلد الذي عبر من خلاله النشاط المجرم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة، فقد يكون مرتكب الجريمة المعلوماتية من جنسية دولة ما مستعملا في جريمته حواسيب موجودة في دولة أخرى وتقع آثار جريمته في دولة ثالثة فمن البديهي أن يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المعلوماتية ومتابعة مرتكبيها قضائيا تؤكد على أهمية المساعدة القضائية[57] المتبادلة بين الدول.[58]

وتتخذ المساعدة القضائية الدولية عدة صور أهمها:

- **تبادل المعلومات**: يولي المجتمع الدولي لتبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموما والجريمة المعلوماتية خصوصا لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القانون، ويشمل مبدأ تبادل المعلومات تقديم البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة معلوماتية ما، بحيث يسمح بالاتصال المباشر بين الأجهزة القضائية والأمنية في الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين[59].

- **نقل الإجراءات** :ويقصد بهذه الصورة قيام دولة ما بمقتضى اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد التحقيق في جريمة معلوماتية ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من

---

[56]. نعيم سعيداني، المرجع السابق، ص 92

[57]. تعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم، سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، مذكرة دكتوراه ،جامعة عين شمس، 1997 ، ص425

[58]. لقد نص المشرع الجزائري في القانون 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها المؤرخ في 5 أوت 2009 على مبدأ المساعدة القضائية الدولية المتبادلة في المادة 16 منه معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، نعيم سعيداني ، المرجع السابق، ص 89

59. وعلى المستوى التشريعي الوطني فقد نصت المادة 17 من قانون 04/09 على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل ، نعيم سعيداني ، المرجع نفسه ، ص 90

الشروط، أهمها التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها، بمعنى أن تكون مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة وأن تكون هذه الإجراءات ذات أهمية من شانها أن تؤدي دورا مهما في الوصول إلى الحقيقة، ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية[60] وكذا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية في باليرمو سنة 2000.

– **الإنابات القضائية الدولية** : يقصد بهذه الصورة طلب اتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك عند الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة لتعذر قيامها بهذا الإجراء بنفسها[61]، وتهدف هذه الصورة إلى تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية، التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى لسماع شهود أو إجراء تفتيش أو غيرها، ويحدث بدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلا من المرور عبر القنوات الدبلوماسية.

– **تسليم المجرمين** : استقر الفقه القانوني على اعتبار أن تسليم المجرمين شكل من أشكال التعاون الدولي في مكافحة الجريمة، وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ومنها مجال الاتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم، كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل امتد إلى أكثر من إقليم، حيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في دولة معينة ويشرف على تنفيذها في بلد آخر، وقد يفر إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة، فالمجرم المعلوماتي أصبح بالتبعية مجرما دوليا، ولكون أنه لا يمكن لأي دولة أن تجاوز حدودها الإقليمية لممارسة أعمالها القضائية على المجرمين الفارين، كان لابد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها، تتمثل في تسليم المجرمين الفارين لها، وهذا الإجراء يقوم أساسا على أن الدولة التي يتواجد على إقليمها المتهم بارتكاب جريمة معلوماتية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة، فهو يحقق بذلك مصلحة الدولتين الأطراف في عملية

---

4. اعتمدت هذه المعاهدة بموجب قرار الجمعية العامة للأمم المتحدة 45/118 بتاريخ 1990/12/14 في الجلسة 68 للجمعية العامة للأمم المتحدة وتقضي باتفاق أطرافها على أن يقدم كل منهم للآخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية للدولة طالبة المساعدة، سالم محمد سليمان الأوجلي، المرجع السابق، ص427

61. جميل عبد الباقي الصغير، المرجع السابق، ص 83

التسليم، إذ يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وفي ذات الوقت يحقق مصلحة الدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون، ولذلك فقد حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين.[62]

أما المظهر الثاني من مظاهر التعاون الدولي في مجال مكافحة الجريمة المعلوماتية فهو التعاون الفني إذ لا يقتصر هذا التعاون الدولي على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول، ذلك أن العنصر البشري سواء على مستوى الأجهزة القضائية أو الأجهزة الأمنية ليس بذات الجاهزية والمستوى لمواجهة الجريمة المعلوماتية، وإنما يختلف من دولة إلى أخرى بحسب تقدم تلك الدولة ورقيها، حيث نجد أن جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة قد دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها[63]، ذلك أن التقدم المتواصل في تكنولوجيات المعلومات يفرض على الجهات القضائية والأمنية أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها ومحو آثارها، وبالتالي فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق الأجهزة القضائية المختصة من قضاة تحقيق وقضاة حكم، وكذا رجال الضبطية القضائية، لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة في التعامل مع الجريمة المعلوماتية والمجرم المعلوماتي.

ومن هذا المنطلق كانت الدعوة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال القضاء والضبطية القضائية للاستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء ومؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة، والتدريب المقصود هنا ليس التدريب التقليدي فحسب، فلا يكف أن تتوافر لدى رجال القضاء الخلفية القانونية، ولدى الضبطية القضائية خصائص عمل الُشرطي وإنما لابد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية، وهذه الأخيرة لا تتأت دون تدريب تخصصي يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب[64].

---

[62]. ومنها المشرع الجزائري الذي أخذ بهذا الإجراء كمظهر من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الإجراءات الجزائية في المواد 694 وما يليها، نعيم سعيداني، المرجع السابق ، ص 92

[63]. انظر المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في الدورة الخامسة والعشرون المؤرخ في 15 نوفمبر 2000، موقع الأمم المتحدة، الدورة الخامسة والعشرون، http://www.un.org/arabic/documents،2014/05/14

[64]. ومن أمثلة أنماط التدريب في كندا دورات متخصصة في أساليب التحقيق في الجريمة المعلوماتية لمدة 4 أسابيع : أساسيات الحاسبات، برمجة الحاسوب، أمن الحاسبات والشبكات، الاثبات في الجريمة المعلوماتية، د حسين بن سعيد بن سيف الغفري، المنشاوي للبحوث والدراسات، الجهود الدولية في مواجهة جرائم الأنترنت ،الرياض، 2007 ، ص 43

أما بالنسبة للمنهج التدريبي فيجب أن يشمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلي وتحديد أنماط ونوعية الجرائم المعلوماتية، وبيانا لأهم الصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكابه للجريمة المعلوماتية، وفيما يتعلق بمنهج التدريب على التحقيق في الجريمة المعلوماتية فإنه لابد أن يشتمل على إجراءات التحقيق، التخطيط للتحقيق، تجميع المعلومات وتحليلها، أساليب المواجهة والاستجواب، طرق مراجعة النظم الفنية للمعلومات وأساليب المعمل الجنائي، بالإضافة إلى ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على الأدلة[65].

بالرغم من ضرورة وحتمية التعاون الدولي في مجال مكافحة الجريمة المعلوماتية والذي بات مطلبا تسعى إلى تحقيقه أغلب الدول، إلا أنه ثمة صعوبات ومعوقات تجعل هذا التعاون ليس بالأمر اليسير وذلك لوجود عدة عقبات نذكر منها:

- **عدم وجود نموذج موحد للنشاط الإجرامي** :إذ لم تتفق الأنظمة القانونية في بلدان العالم على صورة محددة ونماذج معينة يتم الاتفاق المشترك بين الدول حولها تندرج في إطار الجريمة المعلوماتية[66]، فما يكون مجرما في بعض الأنظمة قد لا يكون كذلك في أخرى.
- **اختلاف النظم القانونية الإجرائية:** إذ بسبب هذا الاختلاف قد تكون هناك طرق للتحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كما هو الحال مثلا بالنسبة للمراقبة الإلكترونية، فإذا ما اعتبرت أن طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى .بالإضافة إلى أنه قد لا تسمح دولة ما باستخدام دليل إثبات جرى جمعه بطرق ترى هذه الدول أنها طرق غير مشروعة.
- **التجريم المزدوج** : يعتبر التجريم المزدوج من أهم شروط تسليم المجرمين، وقد يكون هذا الشرط عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجريمة المعلوماتية، سيما وأن معظم الدول ما زالت نصوصها العقابية خالية من هذا النمط الإجرامي.

وفي الحقيقة فإن المصلحة المشتركة للدول تقتضي البحث عن الوسائل التي تساعد في التغلب على هذه الصعوبات وإيجاد تعاون دولي حقيقي يتفق مع طبيعة هذا النوع المستحدث من الجرائم للتخفيف من خلو الفوارق بين الأنظمة القانونية العقابية الداخلية من خلال القضاء على العقبات والصعوبات التي تواجه القضاء الدولي منها :

---

[65]. هشام محمد فريد رستم، المرجع السابق، ص 496

66. عبد الفتاح بيومي حجازي، مبادىء الاجراءات الجنائية في جرائم الكومبيوتر والانترنت، بهجات للطباعة والتجليد،مصر،2009، ص 188

- فيما يتعلق بالعقبة الأولى المتمثلة في عدم وجود نموذج موحد للنشاط الاجرامي فإن الأمر يقتضي توحيد هذه الأنظمة القانونية[67]، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على ايجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم ويخفف من غلو الفوارق بين الأنظمة العقابية، وتتمثل هذه الوسيلة في التحديثات التشريعية المحلية المعنية بالجرائم المعلوماتية وابرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم وحصرها.
- أما العقبة الثانية المتعلقة باختلاف النظم القانونية الإجرائية نجد أن توصيات الصكوك الصادرة عن الأمم المتحدة غالباً ما تشجع الاطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح الباب أمام تعاون الدولي فعّال، فمثلاُ المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة المنعقدة في باليرمو سنة 2000 تشير في هذا الصدد إلى التسليم المراقب والمراقبة الالكترونية وغيرها من أشكال المراقبة والتعقب، كما أن الاتفاقية الاوروبية للإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على هذه العقبة والتي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يومياً طوال الاسبوع لكي تؤمن المساعدة المباشرة للتحقيقات وتشمل تسهيل تطبيق الإجراءات بصفة مباشرة.
- ولأجل القضاء على مشكلة التجريم المزدوج والذي يعد من أهم الشروط الخاصة بتسليم المجرمين ركزت الاتجاهات والتطورات التشريعية على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين إما بسرد الأفعال والتي تتطلب أن تجرم كجرائم أو افعال مخلة بمقتضى قوانين الدولتين معاً أو بمجرد السماح التسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة.

الفرع الأول: جهود الأمم المتحدة في مجال مكافحة جرائم الحاسب الآلي

بذلت الأمم المتحدة جهوداً كبيرة في سبيل العمل على مكافحة جرائم المعلوماتية، وذلك لما تسببه هذه الجرائم من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء، وإيماناً منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به[68] .

توصلت منظمة الأمم المتحدة في مؤتمرها الثامن المنعقد بهافانا 1990 حول منع الجريمة ومعاملة المجرمين United Nations Congress on the Revention of Crime and the Treatement of the

---

[67]. حسين بن سعيد بن سيف الغفري، المرجع السابق، ص 43

[68]. عواطف محمد عثمان عبد الحليم، جرائم المعلوماتية، مجلة العدل، العدد الرابع والعشرون، ص 69

Offender إلى اصدار قانون خاص بالجرائم المتعلقة بالحاسوب، وأشار القرار إلى أن الأجرام الدولي لمواجهة الجرائم المستحدثة يتطلب من الدول الأعضاء اتخاذ عدة إجراءات[69] تتلخص فيما يلي :

- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة من تحقيق وقبول الأدلة على نحو ملائم وإدخال التعديلات إذا دعت الضرورة لذلك.
- اتخاذ تدابير أمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان
- رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة على مكافحة هذا النوع من الجرائم.
- التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع و تدريس الآداب المتخذة في استخدام الحاسوب في المناهج التعليمية.
- حماية مصالح الدولة وحقوق ضحايا جرائم الحاسوب.

لكن تزايد جرائم المعلوماتية وما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية ديسمبر سنة 2000، رقم 55/63 الجلسة العامة، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بالإضافة الذي يمكن أن تقوم به المنظمة والمنظمات الإقليمي الأخرى.

عقدت كذلك الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية بالبرازيل أيام 12 إلى 19 أفريل 2010 ، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخير في استخدام التكنولوجيا من طرف المجرمين والسلطات المختصة في مكافحة الجريمة.

تبقى منظمة الأمم المتحدة الإطار الأمثل لمكافحة جرائم المعلوماتية حيث وضعت مجموعة من القواعد الموضوعية وإجرائية[70] لمواجهة هذه النوعية من الجرائم.

أولاً القواعد الموضوعية : تتضمن هذه القواعد النص على قائمة الحد الادنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم المعلوماتية وتحديثها دورياً والمتضمنة :

- **جريمة الاحتيال أو الغش المرتبط بالكمبيوتر** : ويشمل ذلك الادخال والاتلاف والمحو لمعطيات الكمبيوتر أو برامجه أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى الحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.
- **جريمة التزوير التي تطال برامج الكمبيوتر أو التزوير المعلوماتي** : ويشمل ذلك ادخال أو الاتلاف أو المحو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى العادي لمعالجة البيانات ترتكب

2. نعيم سعيداني ، المرجع السابق ، ص 93

[70]. عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية و الأنترنت دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، 2007 ، ص111

باستخدام الكمبيوتر وتعد فيما لو ارتكبت بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.

- **جريمة تخريب و اتلاف الكمبيوتر**: ويشمل ذلك ادخال أو الاتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات والشبكات.
- **جريمة الدخول غير المصرح به** : وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن.
- **جريمة الاعتراض غير المصرح به** : وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات.

ثانيًا القواعد الإجرائية : تتضمن بعض الأسس الواجب مراعاتها[71] :

- وجوب تحديد السلطات التي تقوم بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، وخاصة ضبط الاشياء المتعلقة بها وتفتيش الحاسب.
- وجوب أن يكون هناك قدر كبير من التعاون الفعال بين الأطراف لكي تكون المعلومات متاحة في صورة يمكن استخدامها للأغراض القضائية في حل هذه الجرائم.
- السماح للسلطات العامة باعتراض الاتصالات داخل البيئة المعلوماتية لاستخدام الأدلة التي يمكن ان يتحصل عليها.
- ادخال بعض التعديلات التشريعية في حالة الضرورة ما يتماشى مع طبيعة جرائم المعلوماتية داخل القانون الوطني وكذلك القواعد القائمة في مجال الإثبات الالكتروني من حيث مصداقية الأدلة وما يمكن أن تثيره من مشاكل عند تطبيقها.
- يجب أن يوضع في الاعتبار كل المسائل المرتبطة ببيئة تكنولوجيا المعلومات، مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسارة الاقتصادية، كلفة إعادة بناء قواعد البيانات كما كانت وإعادتها إلى الواضع السابق قبل اجراء أي تفتيش أو تحقيق.

الفرع الثاني: جهود المنظمات الدولية في مجال مكافحة جرائم الحاسب الآلي

قد اتخذت مبادرات من قبل العديد من المنظمات كالاتحاد الدولي للاتصالات (ITU)، الإنتربول/يوروبول، منظمة التعاون الاقتصادي والتنمية (OECD)، مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN)والمنظمة الدولية لتوحيد المقاييس(ISO) ، واللجنة الكهروتقنية الدولية (IEC) وفرق عمل هندسة

1. عبد الله عبد الكريم عبد الله، المرجع نفسه، ص 114

الإنترنت وFIRST منتدى الاستجابة للأحداث ومجموعات الأمن لآسيا والمحيط الهادئ، ومنظمة التعاون الاقتصادي للمحيط الهادئ وآسيا (APEC) ومنظمة الدول الأميركية (OAS) ورابطة دول جنوب شرق آسيا (ASEAN)وجامعة الدول العربية، والاتحاد الأفريقي.

أولاً : منظمة التعاون الاقتصادي والتنمية (OECD)

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية، بدأت هذه المنظمة الاهتمام بجرائم المعلوماتية منذ عام 1978، حيث وضعت مجموعة من الأدلة وقواعد إرشادية تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها.[72]

فأصدرت سنة 1983 تقريراً بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى من لأفعال سوء استخدام الحاسوب والتي على الدول تجريمها وتشمل هذه الأفعال[73] :

- الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به
- الإفشاء غير مصرح به للمعلومات المعالجة آلياً والنسخ والإتلاف أو التخريب ما يحويه من بيانات وبرامج والإعاقة غير المشروعة للوصول لمصادر الحاسب من منع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة داخله.

وفي عام 1992 وضعت المنظمة توصيات وإرشادات خاصة بأنظمة المعلومات وأوصت بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء مبادئ عامة[74] تتمثل في :

- **حدود التجميع** : يتعين فرض قيود على تجميع البيانات.
- **نوعية البيانات** : حيث تنص على أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله.
- **تعيين الغرض** : بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورة و محددة سلفا.
- **حدود الاستخدام** : يقتضي الالتزام بعدم إفشاء البيانات الشخصية ونشرها لغير المصرح لهم بذلك.
- **الوقاية الأمنية** : ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة وحازمة في إحاطة البيانات.

---

1. يوسف صغير ، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير حقوق، جامعة مولود معمري تيزي وزو، الجزائر، 2013 ، ص 96
2. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الانترنت) ،مذكرة دكتوراه ، الجامعة الإسلامية، لبنان ،2004 ، ص92
74. علي جبار الحسناوي، جرائم الحاسوب والأنترنت، دار اليازوي العلمية للنشر والتوزيع، عمان، 2009 ، ص 154

- **الانفتاح** : أن تكون السياسة العامة للتطوير والخطط والتطبيقات معلنة فيما يتعلق بالبيانات ذات الطبيعة الشخصية.
- **المشاركة الفردية** : حق الأشخاص المعنية في الوصول والتعرف على البيانات التي تخصهم فضلاً عن رقابة مدى صحتها.
- **المسائلة والمحاسبة** : التي تقتضي محاسبة الأشخاص والجهات المرخص لهم الوصول والاطلاع على البيانات والتعامل معها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة.

ثانياً : الأنتربول

وضعت منظمة الإنتربول[75] نظاما خاصا للتعاون، وهو النظام الوطني الخاص بالنقطة المرجعية المركزية[76] NCRPويوجد في كل دولة من الدول الأعضاء في الإنتربول مكتب مركزي وطني يُعد نقطة الاتصال مع الإدارات الأجنبية التي تجري تحقيقات خارج حدودها وتضم شبكة من المحققين العاملين في الوحدات الوطنية المعنية بجرائم لتيسير الاتصالات الميدانية بين البلدان الأعضاء وتسريعها قدر الإمكان ومن مهامها هذا النظام إنماء الاستراتيجيات والتقنيات والمعلومات بشأن أحدث الأساليب الجرمية في مجال جرائم تكنولوجيا المعلومات وهناك فرق عاملة إقليمية لإفريقيا والأمريكيتين وآسيا وجنوب المحيط الهادئ وأوروبا والشرق الأوسط وشمال إفريقيا[77].

كما قامت منظمة الإنتربول بوضع برنامجاً خاصاً لمكافحة الإجرام المعلوماتي يرتكز على التدريب والعمليات ويعمل على مواكبة التهديدات الناشئة مبادرات ويهدف هذا البرنامج[78] :

- توفيردورات تدريبية لوضع معايير مهنية والتقيد بها.
- تعزيز تبادل المعلومات بين البلدان الأعضاء عن طريق الأفرقة العاملة والمؤتمرات الإقليمية.
- تنسيق العمليات الدولية ودعمها

---

2. الأنتربول بالإنجليزية Interpol هي اختصار لكلمة الشرطة الدولية بالإنجليزية International Police والاسم الكامل لها هو منظمة الشرطة الجنائية الدولية بالإنجليزية International Criminal Police Organization وهي أكبر منظمة شرطة دولية أنشئت في عام 1923 مكونة من قوات الشرطة لـ 190 دولة، ومقرها الرئيسي في مدينة ليون بفرنسا، ويكيبيديا، منظمة الشرطة الجنائية الدولية، 2014/05/14 ، http://ar.wikipedia.org/Interpol

3. جان فرنسوا هنروت، أهمية التعاون الدولي بين عناصر الشرطة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 جوان 2007 ، المملكة المغربية، ص 100

[77] الأنتربول ، الإجرام السيبراني، 2014/05/14 ، مجالات-الإجرام/الإجرام-السيبيري/الإجرام-السيبيريhttp://www.interpol.int/ar

[78] الإنتربول ، المرجع نفسه ، ص1

- إعداد قائمة عالمية بأسماء ضباط الاتصال ووضعها بتصرف المحققين في مجال الإجرام السيبيري على مدار الساعة
- مساعدة البلدان الأعضاء على التحقيق في الهجمات أو الجرائم السيبيرية عن طريق توفير خدمات في مجال التحقيق وقواعد البيانات
- إقامة شراكات استراتيجية مع المنظمات الدولية الأخرى وهيئات القطاع الخاص.
- تحديد التهديدات الناشئة وتبادل معلومات الاستخبار في هذا المجال مع البلدان الأعضاء.
- توفير بوابة آمنة على الويب لنشر معلومات ووثائق عملياتية.

المطلب الثاني : على المستوى الإقليمي

تعد الاتفاقية الأوربية بمثابة دعوة موجهه إلى دول العالم للتفاعل مع الجرائم المستحدثة والتي جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها، فبتاريخ 20 أفريل 2000 تقدمت اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية ، بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من اصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001 (اتفاقية الجرائم الالكترونية – سايبر كرايم) وكان قد طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات وأطلق ضمن مواقع عديدة أوروبية وأمريكية على شبكة الأنترنت لجهة التباحث وإبداء الرأي . وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ اكثر من عشرة أعوام[79] .

ومن أهم الأسباب التي أدي إلى إبرام الاتفاقية هو الحاجة على إتخاذ تدابير تشريعية لمكافحة جرائم المعلوماتية ومخاطرها المدمرة على الدول خاصة في ظل شيوع شبكات المعلومات وفي ظل التوسع والنماء الكبير لأنظمة الحوسبة المفتوحة ونقل وتدفق المعلومات، إضافة إلى التشديد على أهمية مكافحة كافة الأنشطة التي تستهدف أمن المعلومات ونظم الكمبيوتر.[80]

هذه التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على اهمية التعاون المحلي والاقليمي والدولي مع وجوب اقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الاساسية والسيادة ، ولأن هذه الاتفاقية جاءت حصيلة

1.. يونس عرب ، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، 2-4 ابريل 2006، مسقط، ص15

2. عبد الله عبد الكريم عبد الله، المرجع السابق، ص126

جهود دولية واقليمية فقد أكدت المقدمة أيضا على أهمية ما أنجز من جهود في حقل جرائم المعلوماتية من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوربي ومجموعة الدول الصناعية وبالنتيجة فأن مشروع الاتفاقية قد ركزت على عناصر أساسية ثلاثة[81]-:

- أهمية التدابير التشريعية الموضوعية) نصوص التجريم.
- أهمية التدابير التشريعية الاجرائية) النصوص الاجرائية.
- أهمية تدابير التعاون الدولي والاقليمي في مجال مكافحة الجرائم.

إن هذه الاتفاقية تقدم ولأول مرة إطارًا لتحديد قائمة جرائم الكمبيوتر وأنماطها وطوائفها، إذ حتى الآن وبالرغم من الجهود التشريعية والتدابير الاقليمية والدولية على مدى السنوات الثلاثين الماضية لم تتوفر رؤية شاملة او اطار واضح يحدد قائمة الجرائم أو بين أساس التقسيم، ولهذا فان أهم ما يسجل لهذه الاتفاقية – بعيد عن الاتفاق والخلاف على الأساس الذي اعتمدته – أنها تطرح اطارًا للتقسيم والتحديد بشأن القواعد الموضوعية لجرائم الكمبيوتر والأنترنت، وبالرجوع الى المعيار التي اعتمدته، نجده بالأساس يقوم على فكرة دور الكمبيوتر بالجريمة[82].

تتكون الاتفاقية من مقدمة وأربعة فصول، فبعد أن استعرضت المقدمة أهداف الاتفاقية ومنطلقاتها ومرجعياتها السابقة وما تقوم عليه من جهود ارشادية وتوجيهية وتدابير اقليمية ودولية، جاء الفصل الأول لتغطية المصطلحات الأساسية (مادة 1) ، تضمن الفصل الثاني الذي جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى الوطني، ثلاثة أقسام : الأول، ويضم المواد من 2–13 ويعالج النصوص الموضوعية لجرائم الكمبيوتر، والقسم الثاني ويضم المواد من 14–21 وتتعلق بالقواعد الإجرائية والقسم الثالث ويضم المادة 22 وتعلق بالاختصاص .

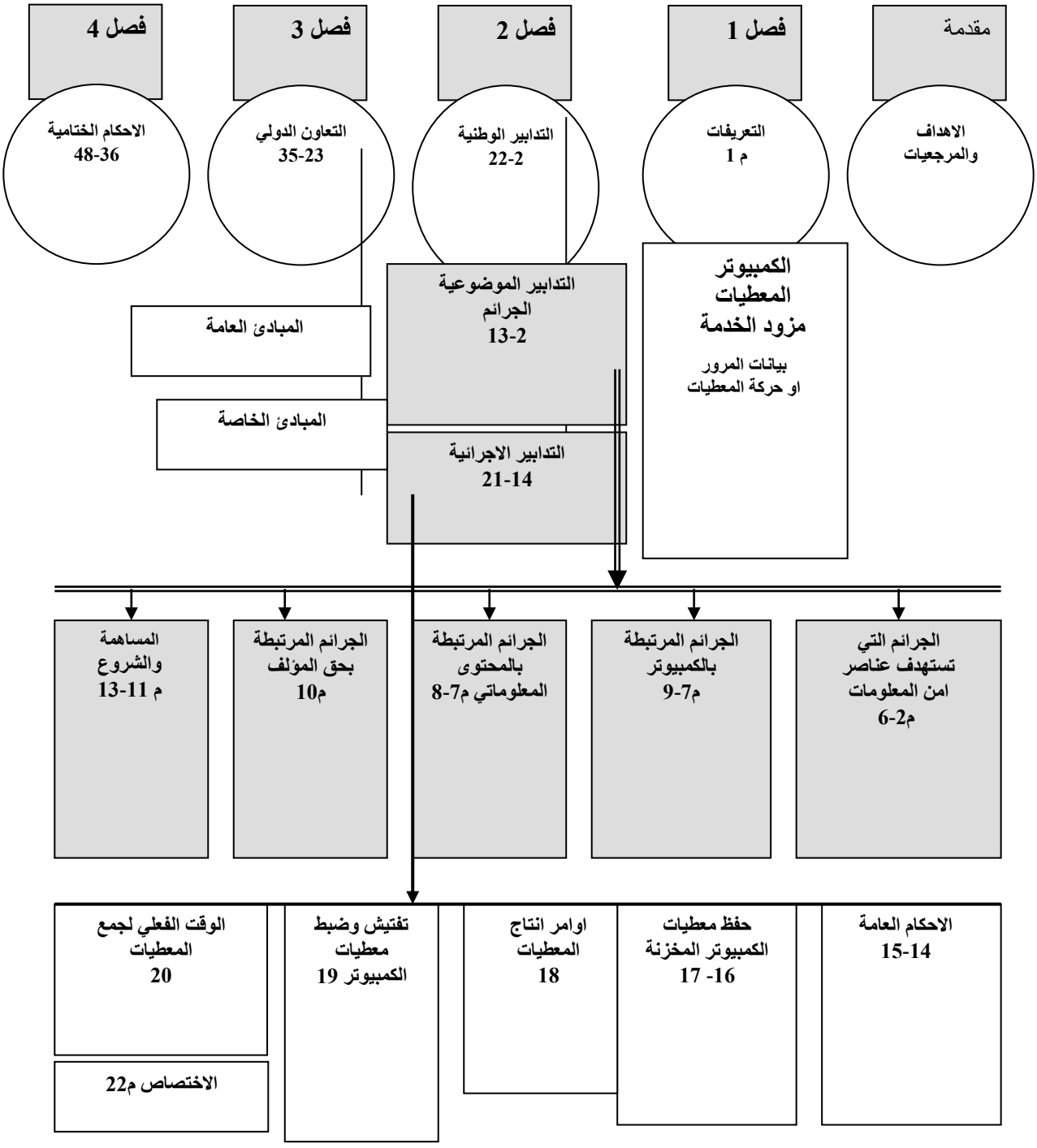
أما الفصل الثالث من الاتفاقية والذي جاء تحت عنوان التعاون الدولي، فقط تضمن قسمين، الأول تحت عنوان المبادئ العامة ويضم المواد من 23–28 والقسم الثاني ويتعلق بالنصوص الخاصة ويضم المواد من 29–35 ، أما الفصل الخامس فيتضمن الاحكام الختامية ويضم المواد من 36 – 48 .

---

[3].. يونس عرب، المرجع السابق، ص16

1. عماد مجدي عبد الملك ، جرائم الكمبيوتر و الأنترنت ، دار المطبوعات الجامعية، الإسكندرية، 2011، ص175

شكل 1: البناء العام لاتفاقية بودابست 2001



أكدت مقدمة الاتفاقية على الحاجة إلى إتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر والأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الكمبيوتر وهي السرية confidentiality وسلامة المحتوى integrity وتوفر المعلومات والنظم availability ، كما أن المقدمة نجدها تلخص أهداف الاتفاقية بما يلي[83]:-

- السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوروبية .
- التأكيد على أهمية التعاون الاقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والأنترنت وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة جرائم الكمبيوتر والأنترنت .
- ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكمبيوتر وشبكات الكمبيوتر وأنشطة إساءة استخدام الكمبيوتر والشبكات، بما في ذلك تحديد الإطار الموضوعي لهذه الانشطة والإطار الإجرائي المتصل بالتحقيق والتحري والمقاضاة في ميدان جرائم الكمبيوتر على المستوى الوطني والدولي .

يضم الفصل الأول مادة واحدة (المادة 1) وهي التعريفات definitions وربما تكون هذه المادة من أهم المواد في ميدان اتفاقيات تقنية المعلومات84 بسبب الخلاف الكبير بشأن تعريف اصطلاحات الكمبيوتر تبعا لزاوية الرؤيا وهدف استخدام التعريف ، إلى جانب التباين بشأن المعايير والمقاييس التقنية وربما تكون لهذه المادة أهمية استثنائية لجهة توحيد التعريفات بعدما ظهر التناقض والتباين في تشريعات جرائم الكمبيوتر التي جرى سنها في أوروبا وأمريكا واستراليا وعدد من دول شرق آسيا، كما عرفت نظام الكمبيوتر computer system ، وعرفت هذه المادة معطيات الكمبيوتر computer data تعريفاً واسعاً يشمل الحقائق والمعلومات والمفاهيم بشكل مناسب لعمليات المعالجة في نظام الكمبيوتر.

أما الفصل الثاني من الاتفاقية والمعنون (المعايير المتعين اتباعها على المستوى الوطني – measures to be taken at the national level) تضمن أقساما ثلاث ، الأول حول التدابير الموضوعية أي القانون الجنائي الموضوعي، والتي تعنى بالسلوكيات التي يجب اعتبارها جريمة جنائية، والثاني حول التدابير الإجرائية، ويتناول التدابير التي تتخذ لإجراء تحقيقات أكثر فعالية فيما يتعلق بجرائم الكمبيوتر، ويجب التأكيد على أن هذه التدابير

---

1. المجلس الأوروبي ، المذكرة التفسيرية لاتفاقية بودابست 2001 النسخة المترجمة بالعربية، 2014/05/12 http://conventions.coe.int/Default.asp?pg=Treaty/Translations/TranslationsChart_en.htm#185،
2. هلالي عبد اللاه أحمد ،جرائم المعلوماتية و أساليب المواجهة و فقاً لاتفاقية بودابست،ط1، دار النهضة، القاهرة، 2007، ص30

الإجرائية يمكن استخدامها مع أية جرائم جنائية يشترك فيها نظام للكمبيوتر، والثالث حول الاختصاص، وبهذا الفصل تكون الاتفاقية قد قدمت الإطار القانوني للتدابير التشريعية الموضوعية والاجرائية المتعين اتخاذها لمواجهة جرائم الكمبيوتر والانترنت[85]، وهذا ما سيتناوله البحث بشيء من التفصيل.

الفصل الثالث تم تخصيصه للتعاون الدولي والحث على الأطراف أن تتعاون مع بعضها البعض، في تطبيق الأصول الدولية في المواد الجنائية، والمبادئ المتعلقة بالمساعدات القانونية المتبادلة، والمعلومات المقدمة طواعية، والمساعدة القانونية المتبادلة في حال عدم وجود وثائق دولية معمول بها، والسرية ووضع حد للاستخدام.

أما الفصل الرابع الأحكام الختامية .ويهتم هذا الفصل على وجه الخصوص بالدول غير الأوروبية كما ينص على سبل انضمام الدول غير الأعضاء إلى الاتفاقية.

الفرع الأول: القانون الجنائي الموضوعي

يعد موضوع القسم الأول من هذه الاتفاقية (المواد من 2 إلى 13) دليلاً ارشادياً لتحسن أو اصلاح وسائل منع وقمع الإجرام المعلوماتي Améliorer les moyens de prévenir et de réprimer la criminalité informatique، بتحديد أدنى القواعد العامة التي تسمح باتخاذ بعض التصرفات القانونية اتجاه هذه الجرائم ويسهل مكافحتها على المستوى الوطني والدولي، ويحدد قائمة تسمح بتجريم بعض الأفعال والتصرفات غير المشروعة التي ترتكب على بيئة معلوماتية، بعبارة أخرى حصر جرائم المعلوماتية بتحديد الحد الأدنى في بعض الأفعال غير المشروعة التي تعد من قبيل جرائم المعلوماتية.

فإذا كانت هذه الاتفاقية تنطبق على التصرفات التي توصف على أنها جرائم مرتكبة عن طريق تكنولوجيا المعلومات، فإن المذكرة التفسيرية حرصت على ايضاح أن الاتفاقية تستخدم تكنولوجيا محايدة Neutre أي التكنولوجيا الآنية والمستقبلية، كما ركزت المذكرة التفسيرية على ضرورة ارتكاب الجرائم المحصاة دون حق وذلك عندما نصت (يشترط في تجريم الأفعال في هذه الاتفاقية أن يكون القيام بالفعل دون حق (Sans droit)، كما أن كل الجرائم المدرجة يجب ان تكون مرتكبة بطريقة عمدية Facon Intentionnelle[86].

أولاً: الأفعال غير المشروعة

تناولت المواد من 2 إلى 10 الجرائم الواردة في هذه الاتفاقية

1. د طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، ص297
1. طارق ابراهيم الدسوقي عطية، المرجع نفسه، ص302

أ- **جرائم ضد سرية وسلامة و توافر البيانات و النظم المعلوماتي:** Infraction contre la confidentialité, L'intégrité et la disponibilité des données et systèmes informatique، إن الغرض من الجرائم التي تناولها هذا العنوان هو حماية سرية و سلامة و اتاحة أو تهيئة البيانات و نظم الحاسب للعمل أو التشغيل، وبالتالي يخرج من نطاق التجريم الأنشطة المشروعة و العادية و المرتبطة بتصميم الشبكات و كذلك الممارسات الاستثمارية أو التجارية المشروعة و العادية، و قد تناولتها[87] المواد من 2 إلى 6

- **الدخول غير القانوني (المادة2):** Accès Illégal والذي يعد الجريمة الرئيسية التي تهدد سرية وأمن وسلامة المعلومات وتوفرها وعلى ذلك فإن مجرد التدخل غير المصرح به بمعنى القرصنة Le piratage، أو الدخول غير المشروع في النظام يعتبر تصرفاً غير مشروع
- **الاعتراض غير القانوني (المادة3):** تهدف هذه المادة لحماية الحق في احترام نقل البيانات و أن هذه الجريمة تمثل انتهاكاً للحق في احترام الاتصالات مثل التصنت و التسجيل التقليدي للمحادثات و المراسلات بين بين الأشخاص.
- **الاعتراض على سلامة البيانات (المادة4):** الغرض من هذه المادة هو أن تكون بيانات وبرامج الحاسب مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمداً من اتلاف الأجهزة المادية و المنطقية المكونة للحاسب ومحو البيانات والبرامج.[88]
- **الاعتداء على سلامة النظام (المادة5):** تهدف هذه المادة إلى تجريم عرقلة الاستخدام الشرعي لنظام المعلومات، أو التأثير على سيرها العادي والتي تمنع او تبطئ بشكل ملموس سير عمل النظام.
- **إساءة استخدام أجهزة الحاسب (المادة6):** تشير هذه المادة أن الأعمال غير المشروعة التي تندرج تحت النوع أ من الجرائم المذكورة أعلاه تكون في الغالب عند حيازة و سائل الدخول كحصول المجرم على معدات التشويش أو أجهزة تحاليل الشبكات التي هي في الأصل تستعمل للتحقيق من إمكانية عمل الشبكات أو أجهزة مراقبة أمن الشبكات كما قد يكون جهاز الكمبيوتر نفسه أداة المزود بالأنترنت أداة لاختراق بعض المواقع أو الحسابات

---

[87]. هلالي عبد اللاه أحمد، المرجع السابق، ص 68

[88]ا. لمجلس الأوروبي ، المرجع السابق، ص21

الالكترونية[89]، كما تشمل الإنتاج المتعمد أو بيع أو شراء أو استيراد أو توزيع الأجهزة و الأدوات بهدف ارتكاب أي فعل المنصوص عليه في المواد 2 إلى 5 من هذه الأتفاقية.[90]

ب- **الجرائم المتصلة بالحاسب**: Infractions Informatiques وهي المادتين 7و8 والتي تتعلق بجرائم عادية يمكن في الغالب ان ترتكب عن طريق الحاسب الآلي:

- **التزوير المعلوماتي (المادة7)**: الغرض من هذه المادة في إنشاء جريمة موازية لجريمة تزوير المستندات الورقية كما تهدف إلى استكمال أوجه النقص[91] التي تعتري قانون العقوبات بالنسبة للتزوير التقليدي، و التزوير المعلوماتي يتكون من خلق Créer أو تعديل Modifier.
- **الغش المعلوماتي (المادة8)**: مع حدوث ثورة تكنولوجية تضاعفت إمكانية ارتكاب جرائم اقتصادية كالغش وبالأخص النصب ببطاقات الائتمان و المعاملات البنكية أو الودائع التي أصبحت هدفاً للنصب من خلال التلاعبات بمدخلات النظام بمعنى ادخال على النظام ببيانات غير صحيحة.

ت- **الجرائم المتصلة بالمضمون**: Infraction se rapportant au contenu هذه الجرائم المرتبطة بالمحتوى والتي تربط بإنتاج أو نشر غير المشروع للمواد الإباحية الطفولية عير النظم المعلوماتية.

- **الجرائم المتصلة بالمواد الاباحية (المادة9)**: تسعى هذه المادة إلى تدعيم الإجراءات التي تحمي الأطفال خاصة من الاستغلال الجنسي من خلال تحديث قانون العقوبات تشمل على استخدام الحاسب الآلي في اطار ارتكاب الجرائم الجنسية ضد الأطفال كما تجرم مختلف جوانب الإنتاج والحيازة والنشر للمواد الإباحية الطفولية.

ث- **الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية و الحقوق المجاورة**: Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes وهي الأفعال التي تعتبر عن انتهاكات واقعة على الملكية الفكرية و خاصة المؤلف من خلال المادة 10 من متخصصي النظام المعلوماتي وخصوصاً شبكة الانترنت والأفعال[92] هي: إن إعادة إنتاج وبث الأعمال المحمية عبر الأنترنت دون موافقة حائز الحق هو أمر غير شرعي وهذه الأعمال المحمية تشمل الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية.

---

[89]. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 319

[90]. عبد الله عبد الكريم عبد الله، المرجع السابق، ص 133

[91]. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 323

[92]. المجلس الأوروبي، المرجع السابق، ص66

ثانياً : تقرير العقوبات

أشارت المادة 13 من هذه الاتفاقية على ضرورة خضوع المنصوص عليها في المواد من 2 إلى 10 لعقوبات جزائية وبالنظر للالتزامات التي تفرضها هذه المواد فإنه يجب على الاطراف المتعاقدة استخلاص النتائج الخطيرة المترتبة على ارتكاب تلك الجرائم و إقرار عقوبات جزائية فعالة، مناسبة ورادعة تتضمن عقوبات سالبة للحرية.

وفي حالة الاشخاص الاعتباريين أن يخضعوا أيضاً لعقوبات فعالة ومناسبة ورادعة والتي يمكن أن تكون جزائية، مدنية أو ادارية، كما تركت نفس المادة المجال مفتوحاً لإمكانية فرض عقوبات أخرى أو إجراءات تتناسب مع خطورة الجرائم المرتكبة مثل قرار الحظر أو المصادرة.

الفرع الثاني: قانون الإجراءات (اتفاقية بودابست)

إن المواد في القسم الراهن نصت بعض الإجراءات التي يجب اتخاذها على الصعيد الوطني، والتي تخدم التحريات الجنائية التي ترتكب عن طريق المنظومة المعلوماتية، وجمع الادلة ذات الطابع الالكتروني.

فتكمن أحد أصحاب المشاكل في مجال مكافحة جرائم المعلوماتية في صعوبة تحديد هوية مرتكب الجريمة و مداها وتأثيرها والمشكلة الأخرى تكمن في ضياع البيانات الالكترونية التي يمكن نقلها أو تعديلها أو محوها في ثواني معدودة[93]، فمثلاً يستطيع الشخص الذي يتحكم في البيانات أن يستخدم المنظومة المعلوماتية بمحوها مدمراً بذلك جميع الأدلة التي يقوم عليها التحقيق الجنائي، لذا تعتبر في أغلب الأحيان السرعة والسرية من المكونات الأساسية لنجاح التحريات.

تُقر الاتفاقية إجراءات تقليدية مع المناخ التكنولوجي الحديث مثل التفتيش والمصادرة وبالتوازي وضعت إجراءات جديدة[94]، كالحفظ السريع للبيانات خلال مدة زمنية محدودة وذلك بهدف إتاحة الفرصة للحصول أو جمع البيانات التي تخدم التحريات أو الإجراءات الجنائية التي يجب القيام بها، والتي بموجبها يجري الإعداد والاتفاق على نظم حماية تسمح بالسيطرة على هذا المناخ التكنولوجي الجديد وتطوير سلطات إجرائية جديدة.

كما تشير هذا القسم إلى مجال تطبيق بنود هذه الاتفاقية من خلال المادة 14، حيث تلزم كل دولة طرف في الاتفاقية بإقرار الإجراءات التشريعية بما يسمح القانون الداخلي بها لخدمة التحريات والإجراءات الجنائية الخاصة على :

- الجرائم الجنائية المنصوص عليها في القسم الأول من الاتفاقية.
- جميع الجرائم الجنائية الأخرى التي ترتكب عن طريق المنظومة المعلوماتية.

---

1. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص496

94. المجلس الأوروبي، المرجع السابق، ص 68

- جمع الأدلة الالكترونية[95] لكل جريمة من أجل التحريات أو إجراءات جنائية معينة[96].

وتشير الاتفاقية بوضوح إلى أنه يجب ان تقر الأطراف بان القانون الداخلي يتضمن معلومات رقمية أو الكترونية قد تستخدم كأدلة[97] أما القضاء وذلك في إطار الجنائي أياً كان طبيعة الجريمة المطلوب متابعتها.

أولاً: الحفظ السريع للمعطيات المخزنة

إن الإجراءات التي تتضمنها المادة 16 و 17 تطبق على جميع البيانات المخزنة (بيانات خط السير أو بيانات المضمون) والتي تم جمعها وحفظها عن طريق أصحابها، أي أنها لا تطبق إلا عندما تكون بيانات المعلوماتية، موجودة آنفاً وفي طور التخزين.

والمقصود بحفظ البيانات[98] هو الاحتفاظ السابق بالمعلومات وتخزينها مع حمايتها من كل ما يمكن أن يفسدها أو يتلف نوعيتها أو حالتها الراهنة، فالحفظ هو عملية ضمان لسلامتها وجعلها بمأمن[99]، كما تشير المادة 14 من هذه الاتفاقية أنه يجب العمل بجميع الصلاحيات والإجراءات وذلك لخدمة التحريات والإجراءات الجنائية، فالاحتفاظ بالبيانات يعد صلاحية وإجراء قانوني جديد تماماً على القانون الداخلي[100]، فالأمر يتعلق بوسيلة جديدة لإجراء التحريات الهامة لمكافحة جرائم المعلوماتية وذلك للأسباب التالية:

- نظراً لقابلية البيانات المعلوماتية للتلاشي فإنه من السهل التلاعب بها وتعديلها، وكذلك من السهل فقدان العناصر التي تعد دليلاً على وقوع جريمة ولا سيما إذا كانت الممارسة المتبعة في المعالجة والتخزين تفتقد الدقة.
- إن جزء كبير من الإجرام المعلوماتي غالباً ما يرتكب من خلال انتقال الاتصال عن طريق المنظومة المعلوماتية، ومن الممكن أن تتضمن تلك الاتصالات محتوى غير مشروع.

ثانياً: تفتيش ومصادرة البيانات المعلوماتية

---

[95]. الدليل الالكتروني هو كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسب من إنجاز مهمة ما، عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات، دار الجامعة الجديدة، الاسكندرية، 2010 ، ص53

[96]. علماً أن القانون المدني الجزائري قد انتبه إلى مسألة حجية الدليل الرقمي والتوقيعات الالكترونية وقبولها من طرف القاضي في مادتيه 1/223 و 327 من قانون 10/05 المتعلق بالمنافسة، محمد فولان، الحماية القانونية لتكنولوجيات الإعلام، مجلة المحكمة العليا، الجزائر، العدد01، 2010، ص 41

[97]. المجلس الأوروبي، المرجع السابق، ص69

[1] الفرق بين حفظ البيانات وتوثيق البيانات فالتعبيرين لهما معنى متقارب ولكنه يختلف في مجال المعلوماتية فالتوثيق عبارة عن عملية تخزين للبيانات والاحتفاظ بها لفترة زمنية معينة، د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 501

[2]. المجلس الأوروبي، المرجع السابق، ص71

[3]. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 504

تهدف المادة 19 من هذه الاتفاقية إلى تحديث وتجانس التشريعات الداخلية الخاصة بالتفتيش ومصادرة البيانات المعلوماتية المخزنة للحصول على ادلة مرتبطة بتحريات وإجراءات جنائية معينة، وتنص جميع التشريعات الداخلية الخاصة بالإجراءات الجنائية على صلاحيات التفتيش والمصادرة للعناصر المادية.[101]

غير أنه فيما يتعلق بالبحث عن البيانات المعلوماتية، يتحتم وجود أحكام إجرائية إضافية حتى تضمن الحصول على البيانات المطلوبة بنفس فاعلية التفتيش ومصادرة الدعائم للمعلومات المادية ويرجع ذلك أن تتم قراءة المعطيات عن طريق جهاز معلوماتي ولكن لا يمكن مصادرتها ونقلها بنفس طريقة المستند الورقي، كما يمكن نقل الأجهزة الداعمة التي يتم عليها حفظ البيانات (قرص صلب، ديسك...إلخ)، بالإضافة لكون المنظومة المعلوماتية متصلة فيما بينها، فيكون من السهل الوصول إلى المعلومات المطلوبة من خلال هذه المنظومة في حالة عدم تخزين هذه المعلومات على جهاز الكمبيوتر موضوع أمر التفتيش، حيث تكون مخزنة في حافظة معلومات متصلة بصورة مباشرة بجهاز كمبيوتر آخر وعن بصورة غير مباشرة بواسطة نظام اتصالات كالأنترنت[102] ، عندما ألزمت الفقرة الأولى والثانية من نفس المادة الأطراف أن تخول لسلطاتها المختصة بمكافحة الجريمة المعلوماتية الحق في فحص والدخول على المعطيات سواء الموجودة في نظم معلومات أو جزء من هذه المنظومة مثل الأسطوانة ...إلخ[103].

كما تناولت الفقرة الثالثة السماح للسلطات المختصة بمصادرة البيانات أو الحصول عليها بطريقة مشابهة لها عن طريق نسخها بأي طريقة تقنية والتي لا تعرضها للإتلاف أو فقدانها أو جزء منها، إذا أخذنا بعين الاعتبار البعد الدولي لجرائم الإنترنت، يمكننا أن نستنتج أنه لا يمكن لدولة بمفردها أن تحقق النجاح في هذه المعركة، بل لا يتحقق ذلك إلا عن طريق التعاون على المستوى الدولي والاقليمي ولكننا نعلم أن التعاون يعتمد على الأنظمة القانونية للدول والتوفيق بين التشريعات الوطنية المختلفة، كما يجب على كل البلدان أن تضع إطارا قانونيا مناسبا، سواء على المستوى الوطني أو الدولي، بحيث يكون قادرا على توفير الأدوات التشريعية وأدوات التحقيق اللازمة لمكافحة جرائم الإنترنت مع الوضع في الاعتبار مدى تعقيدها.

المبحث الثاني: جهود المشرع الجزائري لمكافحة الجرائم المعلوماتية

عرف نظام المعلوماتية تطورا بطيئاً في الجزائر[104] بالرغم من الإمكانيات الاقتصادية والمالية والبشرية التي نزخر بها مقارنة بالكثير من دول العالم المتخلف، فالمشكل لم يكن يكمن في مجال نقص العتاد المعلوماتي بقدر ما هو

---

1. ومثال ذلك ما جاء في القسم الثالث "في الانتقال والتفتيش والقبض " من الكتاب الأول من قانون 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر55-165 المؤرخ في 08 يونيو 1965 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84، الجزائر، 24 ديسمبر 2006

[102]. نبيل صقر،موسوعة الفكر القانوني،جرائم الكمبيوتر و الأنترنت في التشريع الجزائري،دارالهلال للخدمات الإعلامية، طبعة2005 ، ص 160

[103]. المجلس الاوروبي، المرجع السابق، ص95

[104]. أحمد عمراني، نظام المعلومات في القانون الجزائري، المؤتمر السادس لجمعية المكتبات و المعلومات السعودية، الرياض، 2010، ص12

التخطيط العقلاني المساير للواقع إضافة على التأخر في صدور قوانين لاستغلال واعتماد النظم المعلوماتية[105] ماعدا شبكة الاتصالات التي وضعت لها قوانين واكبت التطور.

فالجزائر لم تعرف قوانين قبل سنة 2004 تطبق بشكل خاص على نظام المعلوماتية أو على تكنولوجيا الإعلام والاتصال ما عدا شبكة الاتصال السلكية واللاسلكية ووسائل الاعلام السمعية والبصرية، والواقع أن هناك العديد من التشريعات والاتفاقيات الدولية التي كانت تطبق في هذا المجال، منها الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات والمتضمن قانون الاجراءات الجزائية والأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني، وكذا قانون 2000-03 المؤرخ في 5 أوت 2000 والمتضمن القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية وكذا الامر رقم 03-05 المؤرخ في 19 يوليو سنة 2003 والمتعلق بحقوق والحقوق المجاورة.

أما الاتفاقيات الدولية فهناك جملة من هذه الاتفاقيات التي صادقت الجزائر عليها وأصبحت تعتبر من النظام القانوني الجزائري، نذكر منها اتفاقية باريس لحماية الملكية الصناعية، والاتفاقية العالمية حول حق المؤلف يوليو 1971 واتفاقية إنشاء المنظمة العالمية للفكرية الموقعة بستوكهولم 14 يوليو 1967 بالإضافة إلى بعض البروتوكولات المتعلقة بتكنولوجيا الإعلام والاتصال[106].

ولمسايرة التطور التكنولوجي كان لا بد للجزائر من إيجاد الإطار القانوني المناسب لحماية المنظومة المعلوماتية من السلوكيات الإجرامية المستحدثة من خلال:

- إدراجه لبعض الإجراءات الجزائية الخاصة بجرائم نظم المعلومات من خلاله لتعديليه لقانون الإجراءات الجزائية الأول 14/04 المؤرخ في 10 نوفمبر 2004 والثاني قانون 06-22 المؤرخ في 20 ديسمبر 2006 بتوسيع اختصاص بعض المحاكم المختصة واختصاص وكيل الجمهورية وقاضي التحقيق (المواد من 37-40 و329) وكذا توسيع صلاحيات الضبطية القضائية من خلال تمديد الاختصاص المحلي إلى كامل التراب الوطني (المادة16) وكذلك إمكانية تفتيش المحلات السكنية وغير السكنية في كل ساعة من ساعات الليل والنهار بإذن من وكيل الجمهورية (المادة47) مع أمكانية تفتيش المساكن دون حضور المشتبه فيه أو أصحاب السكن ودون الشهود (المادة 45)، مع إمكانية تمديد فترة التوقيف للنظر مرة واحدة في حالة التلبس (المادة 51).

---

[105]. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير حقوق، جامعة الحاج لخضر باتنة، الجزائر، 2012، ص 180

[106]. أحمد عماراني، المرجع السابق، ص14

أم من حيث أساليب التحريات الخاصة من اعتراض المراسلات الالكترونية (المادة 65 مكرر 5) والتسرب (المادة 65 مكرر11).[107]

- الأمر 06/03 المؤرخ في 2003/07/19 المتعلق بالعلامات المعدل والمتمم للأمر 57/66 المؤرخ في 1966/03/19 المتعلق بعلامات المصنع والعلامات التجارية والمعدل للأمر رقم 223/67 المؤرخ في 1967/10/19 المتضمن أحكام العلامات التجارية والعلامات التجارية هي كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات، وباعتبار أن كل برنامج من برامج الكمبيوتر يحمل اسماً خاصًا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجا أصحاب البرامج إلى وضع الاسم مقترنا به[108].
- الأمر 14/73 المؤرخ في 1973/04/03 المعدل والمتمم بمقتضى الأمر 10/97 المؤرخ في 1997/03/06 المعدل والمتمم بموجب الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة، وذلك عندما وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية وكذلك بتشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية (المادة 151 الأمر 10/97) إذ كان في السابق التعدي على الملكية الفكرية يخضع للمواد 394/390 من قانون العقوبات لكنها أخرجت بموجب الأمر 10/97 من مظلة قانون العقوبات وأصبح لها تجريم خاص إذ أن قانون العقوبات كان يقرر بموجب المادة 390 الغرامة كعقوبة للاعتداء على حق المؤلف بينما الأمر 10/97 يقرر عقوبتي الحبس والغرامة[109].
- بالإضافة إلى قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات وتلاه قانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وسنتعرض خلال هذا المبحث لكل قانون على حدا.

---

[107] محمد فولان، المرجع السابق، ص 43

[108] عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون و المعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص13

[109]. عطاء الله فشار، المرجع نفسه، ص 16

المطلب الأول :جرائم الحاسب الآلي في قانون العقوبات

إن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة في قانون العقوبات الجزائري على غرار قوانين العقوبات المقارن، فرض حلها البحث في الأوضاع القانونية القائمة ومدى ملاءمتها لمواجهة هذه المشاكل.

ولما كان القاضي الجزائي مقيدا عند نظره الدعوى الجنائية بمبدأ شرعية الجرائم والعقوبات فإنه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت هذه الأفعال مستهجنة وعلى مستوى عال من الخطورة الاجتماعية والاقتصادية، وكل ما يمكنه عمله هو محاولة تفسير النصوص القائمة طبقا لقواعد التفسير المسلم بها في القانون الجنائي، وأهمها مبدأ التفسير الضيق وحظر القياس.

وقد تطرق المشرع الجزائري على غرار الدول الأخرى مثل فرنسا[110] بتجريم أفعال المساس بأنظمة الحاسب الآلي وذلك نتيجة تأثر بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، مما دفع المشرع الجزائري[111] إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، والذي أفرد القسم "السابع مكرر" منه تحت عنوان "**المساس بأنظمة المعالجة الآلية للمعطيات، Des atteintes aux systèmes de traitement automatisé de données** " والذي تضمن 8 مواد من المادة 394 مكرر إلى 394 مكرر7، ونص على عدة جرائم هي[112]:

- الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك (394 مكرر فقرة1).
- الدخول أو البقاء المؤدي إلى تخريب نظام تشغيل المنظومة (394 مكرر3).
- إدخال أو إزالة أو تعديل بطريق الغش معطيات في نظام المعالجة الآلية (395 مكرر1).
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم (394 مكرر2).

---

[110]. في سنة 1994 تم تعديل قانون العقوبات الفرنسي حيث تم إضافة فصلاً ثالثا للباب الثاني تحت اسم "الاعتداءات على نظم المعالجة الآلية للمعطيات" "Des atteintes aux systèmes de traitement automatisé de données" و جاء من المادة 1/323 إلى 7/323 ، Clément ENDRELIN، المرجع السابق، ص76

2. جاء في عرض أسباب هذا التعديل: " أن التقدم التكنولوجي و انتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام مما دفع الكثير من الدول إلى النص على معاقبتها، وإن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية و أساليب المعالجة الآلية للمعطيات، و أن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، و سوف يُمكن لا محالة من مواجهة بعض أشكال الإجرام الجديد"، عائشة بن قارة مصطفى، المرجع السابق، ص27

3. نبيل صقر، المرجع السابق، ص128

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المتحصل عليها في هذا القسم (394 مكرر2).

في عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون رقم 06 – 23 المؤرخ في 20 ديسمبر 2006 حيث مسّ ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة[113] المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من قانون 04-15، وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الاعمار ومستويات التعليم نتيجة تبسيط وسائل تكنولوجيا المعلومات وانتشار الأنترنت كوسيلة نقل المعلومات حيث بلغ عدد مستخدمي الأنترنت ذات التدفق العالي وعبر الهاتف المحمول 11 مليون شخص لسنة 2012 [114].

الفرع الأول : صور الاعتداءات

تأخذ صور الاعتداء على النظام المعلوماتي في قانون العقوبات الجزائري صورتين أساسيتين هما[115] :

- الدخول والبقاء في منظومة معلوماتية
- المساس بمنظومة معلوماتية

كما تضمن قانون العقوبات صور أخرى للغش في حين أبقى خارج دائرة التجريم بعض الأفعال منها : المساس بحقوق الأشخاص عن طريق المعلوماتية، كجمع المعلومات حول شخص وتحويل المعلومات الاسمية عن مقصدها[116].

أولا: الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات Accès et maintien frauduleux dans un système de traitement automatisé des données.

نصت عليه المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن

---

[113]. مثال ذلك: " يعاقب على الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية بالحبس من ثلاث(3) أشهر إلى سنة (1) و بغرامة مالية من 000 50 إلى 000 200 دج طبقاً لقانون 06-23 بينما كانت العقوبة على نفس الجريمة من ثلاث أشهر إلى سنة بغرامة مالية من 000 50 إلى 000 100 في قانون 04-15، عائشة بن قارة مصطفى، المرجع السابق، ص29

[114]. بن حمادي يؤكد على عدد مستخدمي الأنترنت، يومية النهار، الجزائر، 1709، 2013/05/17، ص5

3. حمزة بن عقون، المرجع السابق، ص182

4. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة العاشرة، دار هومة، الجزائر، 2009، ص 445

الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج".

إذن فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، و يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

- **فعل الدخول L'accès** : لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، وإنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات[117]. ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[118].
- **فعل البقاء Le maintien**: يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، وقد يجتمعان. ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا. ومن أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورًا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي. ويكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والاطلاع فقط ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، والتي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض

1. أمال قارة، المرجع السابق، ص42
2. علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة، الاسكندرية، 1999، ص 121

الاجتماع المادي للجرائم وإذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضا وبصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة، وذلك بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له الحق السيطرة على النظام، ويقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج.[119]

أما عن الصورة المشددة لهذه الجريمة، نصت المادة 394 مكرر 3/2: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظمة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج"، على ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، ويتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه، ويكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة، ولا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب مثل هذا الشرط يكون غير معقول، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة. كما لا يشترط أن تكون تلك النتيجة مقصودة، أي على سبيل الخطأ غير ألعمدي، فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة العمدية الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتفاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

أ- **الركن المادي:** يتمثل الركن المادي لجريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية والذي يمتثل أساساً في النشاط الإجرامي بصورتيه البسيطة والمشددة في :

- الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات فعل البقاء.
- البقاء داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.
- محو أو تعديل المعطيات التي يحتويها النظام.

3. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائر ،دار هومة، الطبعة الثانية 2007، ص42

ب- **الركن المعنوي:** الولوج والتجول والبقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا تمّا عمداً، كما أن الركن المعنوي لهذه الجريمة تأخذ صورة القصد الجنائي بعنصريه العلم والإرادة.

فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصريه العلم والإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام[120].

ثانياً: المساس بمنظومة معلوماتية

يأخذ السلوك الإجرامي لهذه الجريمة إما الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات أو الاعتداء العمدي على المعطيات[121].

لم يورد المشرع الجزائري نصاً خاصاً بالاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات Atteintes volontaires au fonctionnement de STAD* واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام وقد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات والاعتداء على النظام على أساس ما اذا كان الاعتداء وسيلة أم غاية، فاذا كان مجرد وسيلة فان الفعل يشكل جريمة الاعتداء العمدي على النظام، أما اذا كان الاعتداء غاية فان الفعل يشكل جريمة الاعتداء العمدي على المعطيات122، يتمثل هذا السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات من أداء نشاطه العادي والمنتظر منه القيام به، وإما في فعل إفساد نشاط أو وظائف هذا النظام، ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية جهاز الحاسب الآلي نفسه، شبكات الاتصال، أجهزة النقل ...الخ، أما المعنوية مثل البرامج والمعطيات[123]. وتتمثل النشاطات غير المشروعة لهذه الجريمة:

---

[120]. علي عبد القادر قهوجي، المرجع السابق، ص 136

[121]. هيام حاجب، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر، 2008، ص47

* . **STAD** : Système de Traitement Automatisé des Données

4. هيام حاجب، المرجع نفسه، ص 48

5. عطاء الله فشار، المرجع السابق، ص27

- **التعطيل (العرقلة)**: تفترض وجود عمل إيجابي دون أن يشترط المشرع أن يتم التعطيل بوسيلة معينة سواء مادية أو معنوية و سواء اقترنت بالعنف أم لا، فأما عن الوسيلة المادية فمثلها كسر الأجهزة المادية للنظام أو تحطيم أسطوانة، أما عن الوسيلة المعنوية فهي التي تقع على الكيانات المنطقية للنظام كالبرامج والمعطيات. وذلك بإتباع إحدى التقنيات التالية: إدخال برنامج فيروسي، استخدام قنابل منطقية مؤقتة، جعل النظام يتباطأ في أدائه لوظائفه إلى غيرها من التقنيات.
- **الإفساد Fausser** : وهو كل فعل وإن كان لا يؤدي إلى التعطيل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها. والافساد من هذه الزاوية يقترب من التعييب الذي يعتبر ظرفا مشددا لجريمة الدخول والبقاء غير المشروع. والفارق بينهما يكمن في أن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون عمديا بينما يتطلب هذا الشرط بالنسبة لجريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات، ومن بين صور الإفساد أو التعييب نجد تقنية استخدام القنبلة المعلوماتية التي تدخل عن طريقها مجموعة معطيات تتكاثر داخل النظام تجعله غير صالح للاستعمال كاستخدام البرنامج المسمى بـ " حصان الطروادة " والذي يقوم بتغيير غير محسوس في البرامج أو المعطيات[124].

أما الاعتداءات العمدية على المعطيات فلق نص المشرع الجزائري عليها في المادة 394 مكرر2 في قانون العقوبات «يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها».

تأخذ الصورة الأولى الاعتداءات العمدية على المعطيات الموجودة داخل النظام، فالنشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية[125]:

- الإدخال L'intrusion.
- المحو 'effacement .
- التعديل Modification.

وأفعال الإدخال والمحو والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل وهذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد وهو المعطيات أو المعلومات التي تمت معالجتها آليا والتي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات، وليست المعلومات في ذاتها باعتبارها أحد عناصر

---

[124]. علي عبد القادر قهوجي، المرجع السابق، ص143

2. هيام حاجب، المرجع نفسه، ص 49

المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام وتشكل جزءا منه. لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام أو تلك التي دخلت، ولم يتخذ حيالها إجراءات المعالجة الآلية، أما تلك التي في طريقها إلى المعالجة حتى ولو لم تكن المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية، ويكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال.

تجدر الإشارة إلى أن الحماية الجنائية تشمل المعطيات طالما أنها تدخل في نظام المعالجة الآلية، أي طالما كان يحتويها ذلك النظام وكانت تكون وحدة واحدة مع عناصره ويترتب على ذلك أن الجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها وحتى ولو لفترة قصيرة، كما لو كانت مفرغة على قرص أو شريط ممغنط خارج النظام، فالحماية الجنائية تقتصر على المعطيات التي توجد داخل النظام أو تلك التي في طريقها إلى الدخول إليه، أو تلك التي دخلت بعد خروجها، ولا يشترط أن تقع أفعال الإدخال والمحو وتعديل المعطيات بطريق مباشر بل يمكن أن يتحقق ذلك بطريق غير مباشر سواء عن بعد أم بواسطة شخص ثالث.

- **الإدخال L'intrusion**: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، ويتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هاته الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، وكذلك الحامل الشرعي لبطاقة الائتمان والتي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب« فيروس...الخ» يضيف معطيات جديدة.
- **المحو L'effacement** : يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.
- **التعديل Modification**: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها وذلك برامج خبيثة[126] كالفيروسات[127] بصفة عامة، وهذه

1.البرامج الخبيثة Malware هي اختصار لكلمتين ، هي برامج يتم تضمينها أو إدراجها عمدًا في نظام الحاسوب لأغراض ضار، ويكيبيديا، البرامج الخبيثة، 2014/05/14، البرامج الخبيثة /http://ar.wikipedia.org/wiki

الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لأن كل تلك الأفعال لا تنطوي لا على إدخال ولا على تعديل بالمعنى السابق.

أما الصورة الثانية فهي جريمة المساس العمدي بالمعطيات خارج النظام التي وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها من خلال تجريمه السلوكيات التالية:

- نص المادة 394 مكرر 2 تستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة، كأن تخزن في أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.
- نص المادة 394 مكرر 2/2 يجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق... الخ.

أ- الركن المادي:

يعد مساساً بالأنظمة المعلوماتية هو إحدى النشاطات غير المشروعة الواردة والمتمثلة في الصورة التالية: التعطيل أو الإفساد او المحو أو التعديل أو الإدخال والتي لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي[128] بالإضافة إلى ما أوردته المادة 394 مكرر 2 ، تصميم أو البحث أو التجميع أو توفير أو نشر أو إتجار معلومات مختزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي وكذلك الحيازة أو الإفشاء أو استعمالها لأي غرض آخر.[129]

ب- الركن المعنوي:

2.فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما يشبهها من عمليات، ويكيبيديا، فيروس الحاسب، 2014/05/14، فيروس الحاسب http://ar.wikipedia.org/wiki

1. هيام حاجب، المرجع السابق، ص 48

2. حمزة بن عقون، المرجع السابق، ص185

إن الركن المعنوي إن هذه الجريمة جريمة عمدية، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء الغير مشروع داخل النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة[130].

أما الصورة الأولى من الاعتداءات العمدية على المعطيات الموجودة داخل النظام كجريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه الجرمي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أن ليس له الحق في القيام بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته، كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش ،لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وان كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا انه ليس عنصرا في الجريمة .

الصورة الثانية فهي جريمة المساس العمدي بالمعطيات خارج النظام فان هذا المساس يجب أن يكون عمدا وبطريق الغش أي بتوافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش.

الفرع الثاني : الجزاءات المقررة

طبقا للمادة 13 من اتفاقية بودابست فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات مالية للحرية، والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، كما توجد عقوبات تطبق على الشخص المعنوي بناءًا على تبني مبدأ مسالة الشخص المعنوي الواردة في المادة 12من الاتفاقية.

أولاً: العقوبات المطبقة على الشخص الطبيعي

أ- **العقوبات الأصلية** : من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات ،إذ نجد سلم خطورة يتضمن ثلاث درجات، جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.

- **الدخول والبقاء بالغش (الجريمة البسيطة)**: العقوبة المقررة هي 3 أشهر إلى سنة حبس و50000 دج إلى 100000 دج غرامة (المادة 394 مكرر) .

1. علي عبد القادر القهوجي، المرجع السابق، ص 136

- **الدخول والبقاء بالغش (الجريمة المشددة)**: تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر/02-03) .
- **الاعتداء العمدي على المعطيات**: طبقا لنص المادة 394 مكرر 2 فالعقوبة المقررة للاعتداء ألعمدي على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 2000000 دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، العقوبة المقررة هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000 دج إلى 5000000 دج.

بالإضافة إلى تشديد العقوبة في الحالات التالية:

- نصت المادة 394 مكرر /2-3 على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول والبقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة، ففي الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر، وفي الحالة الثانية تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج.
- نصت المادة 394 مكرر 3 على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام

ب- **العقوبة التكميلية**: نصت المادة 394 مكرر 3 قانون العقوبات على العقوبات التكميلية إلى جانب العقوبات الأصلية والمتمثلة في:

- **المصادرة**: وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.
- **إغلاق المواقع**: والأمر يتعلق بالمواقع (Le sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- **إغلاق المحل أو مكان الاستغلال**: إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها.

ثانياً: العقوبات المطبقة على الشخص المعنوي

مبدأ مساءلة الشخص المعنوي وارد في المادة 12 من اتفاقية بودابست، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه[131].

هذا مع ملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

كما تجدر الإشارة إلى أن المشرع الجزائري قد اقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات الذي ينص على أن: " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات و الجنح هي:

أ- العقوبة الاصلية:

الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة(394 مكرر 4).

ب- العقوبة التكميلية: واحدة أو أكثر من العقوبات الآتية[132]:

- حل الشخص المعنوي
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.

---

1. عطاء الله فشار، المرجع السابق، ص 33
2. المادة 18 مكرر ، قانون 04-15ا لمؤرخ في 10 نوفمبر 2004

– الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات ،وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

نشير بالذكر أن المشرع الجزائري لم يغفل عن معاقبة الاشتراك[133] حيث تنص المادة 394 مكرر 5 من قانون العقوبات : "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية ،يعاقب بالعقوبات المقررة بالجريمة ذاتها ".

إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو في اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات، كما أن المشرع ورغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.

أما عقوبة الشروع في الجريمة نصت عليه المادة 11 من اتفاقية بودابست وتبناه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص.

نصت المادة 394 مكرر 7 قانون العقوبات:" يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها ".

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ،إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر5 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي.[134]

---

2. هيام حاجب، المرجع السابق، ص 51

1. عطاء الله فشار، المرجع السابق، ص 35

المطلب الثاني : جرائم الحاسب الآلي قانون 09-04 المؤرخ في 05 أوت 2009

دفع القصور الذي عرفه قانون 04-15 والمعدل لقانون العقوبات الذي نص على حماية الجزائية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، بالمشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام والاتصال وخاصة الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، خاصة في ظل الثورة التي تعرفها في مجال استخدام الأنترنت، وذلك بوضع قانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من أجل تعزيز القواعد السابقة.

تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها.

كما أخذ المشرع في عين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة، لذلك تم اختيار عنوان القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حتى يكون النص مرتبطاً بتقنيات تشهد تطوراً مستمراً بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا، كما أن التركيز على المجالي الإعلام والاتصال بين مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الإجرام والوقاية منه[135].

يتضمن قانون 09-04 على ستة فصول نلخصها في :

نص الفصل الأول على الأحكام العامة التي تبين الأهداف المتوخاة من هذا القانون، وتحدد مفهوم مصطلح التقنية الواردة فيه وكذا مجال تطبيق أحكامه، حيث عرف الجرائم المرتكبة بتكنولوجيات الاعلام والاتصال على أنها هي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، أما المنظومة المعلوماتية على أنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المترابطة، ويقوم واحد منها أو أكثر بمعالجة آلية المعطيات تنفيذا لبرنامج معين، أما المعطيات فعرفها المشرع الجزائري على أنها أي عملية عرض وطرح للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، كما عرف الاتصالات الالكترونية على أنها أي تراسل أو ارسال أو استقبال علامات واشارات أو صور أو معلومات مختلفة بواسطة أي وسيلة الكترونية[136].

---

1. أحمد عمراني، المرجع السابق، ص15
2. المادة 1،2،3 من قانون 09-04 المؤرخ في 5 أوت 2009

وجسد الفصل الثاني أحكام خاصة بمراقبة الاتصالات الالكترونية، وقد روعي في هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية، وحدد الحالات التي يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الالكترونية، وقيدها بإذن مكتوب من السلطات القضائية المختصة.

أما الفصل الثالث فتضمن القواعد الإجرائية، وهذا بالنص على قواعد إجرائية خاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وذلك وفقاً للمعايير العالمية المعمول بها في هذا الشأن ومع ما تضنه قانون الإجراءات الجزائية من مبادئ عامة.

الفصل الرابع تطرق إلى التزامات المتعاملين في مجال الاتصالات الالكترونية، ولاسيما إلزامية حفظ المعطيات المتعلقة بحركة السير والتي من شأنها المساعدة في الكشف عن الجرائم ومرتكبيها[137]، حيث يهدف هذا القانون إعطاء مقدمي الخدمات دوراً إيجابياً ومساعداً للسلطات العمومية في مواجهة الجرائم والكشف عن مرتكبيها، حيث ألزم مقدمي الأنترنت على التدخل الفوري لسحب الفوري لسحب المحتويات التي بإمكانهم الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها القانون، وتخزينها أو جعل الدخول إليها غير ممكن، إضافة إلى وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول للموزعات التي تحتوي مخالفات للنظام العام والآداب العامة وإخطار المشتركين لديهم بوجودها.

أشار الفصل الخامس لوجود الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيات الاعلام والاتصال ومكافحته، إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من هذه الجرائم، وأحال على التنظيم تحديد كيفية تشكيل وتنظيم هذه الهيئة.

نص الفصل السادس على التعاون والمساعدة القضائية الدولية، إذ تناول قواعد الاختصاص القضائي والتعاون الدولي بوجه عام :

- فيما يخص الاختصاص القضائي فهو فضلاً عن قواعد الاختصاص العادية فقد تم توسيع اختصاص المحاكم الجزائية للنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال التي ترتكب من طرف الرعايا الأجانب عندما تكون المصالح الاستراتيجية للجزائر مستهدفة.

1. المواد 10،11،12 من نفس القانون

- فيما يتعلق بالتعاون الدولي فهو يقوم على مجوعة من المبادئ العامة في مجال التعاون الدولي لمكافحة هذا النوع من الجرائم خاصة ما يتعلق منها بالمساعدة وتبادل المعلومات، حيث تم اعتماد مبدأ التعاون على أساس المعاملة بالمثل[138].

الفرع الأول : القواعد الإجرائية

أولاً: التفتيش و الحجز

أجاز هذا القانون للجهات القضائية وضباط الشرطة القضائية الدخول والتفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، و كذلك المعطيات الآلية المخزنة فيها، مع إمكانية اللجوء مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، كما يسمح هذا القانون في المادتين 5 و 6 للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها[139]، وحجزها.

ثانياً: التعاون القضائي الدولي

تنص المادة 16 من نفس القانون على إمكانية تبادل المعلومات في الشكل الإلكتروني، أما الفقرة الثانية إمكانية استعمال وسائل الاتصال السريعة مثل البريد الإلكتروني والفاكس في حالة الاستعجال مع القيام بالإجراءات التحفظية اللازمة وذلك وفق مبدأ التعاون على أساس المعاملة بالمثل.

الفرع الثاني: القواعد الوقائية

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

أنشئت بموجب المادة 14 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومن مهامها:

- إدارة و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام الاتصال.

---

[138]. أحمد عمراني، المرجع السابق، ص17

1. عطاء الله فشار، المرجع السابق، ص 36

- المساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذا النوع من الجريمة، مع تفعيل التعاون القضائي والأمني الدولي.

ثانياً: مراقبة الاتصالات الالكترونية

نصت المادة 4 من قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها الحالات التي يسمح فيها باللجوء إلى المراقبة الالكترونية[140]:

- للوقاية من السلوكيات الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة، الدولة، بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد.
- في حالة توافر معلومات على احتمال القيام بالاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الالكترونية.
- في مجال تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

واكب المشرع الجزائري مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الالكترونية بما فيها الانترنت، خاصة التي تهدف إلى الحد من الاستخدام غير المشروع لها، وذلك مراعاة منه لما يشهده العالم من تطورات كبيرة في مجال الاعلام والاتصال خاصة الأنترنت.

ومن جهة أخرى إيماناً منه بأن الجزائر ليست بمعزل عن التطورات الإجرامية التي تحدث في العالم، خاصة في ظل التنامي المتسارع لاستعمال الانترنت، فكانت محاولات المشرع الجزائي الحد من هذه الظاهرة في استحداثه للقسم السابع مكرر من قانون العقوبات 04-15 وكذا قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته.

1. يوسف صغير، المرع السابق، ص 113

خاتمة

وفي الأخير بعد دراستنا لجرائم الحاسب الآلي يجب أن نسلم أننا أصبحنا نواجه واقعاً ملحاً على التدخل التشريعي لتنظيم التعاملات الإليكترونية بصفة عامة، قبل اصدار القوانين اللازمة لمواجهة الجرائم المعلوماتية، لأن المعاملات الإليكترونية اليوم أصبحت تغطي معظم التعاملات اليومية في مختلف المجالات.

ومنه فقد واكب المشرع الجزائري ولو بقدر قليل الحركية التشريعية التي فرضت نفسها عالميا، خاصة مع دخول الأنترنت في مختلف مناحي حياة المواكن الجزائري، فبعد الفراغ التشريعي الذي كانت تعاني منه الجزائر في هذا المجال سعت لسده في بادئ الأمر بتعديل قانون العقوبات وذلك بالقانون رقم 15/04 غير أن محدودية هذا القانون دفعت المشرع الجزائري إلى إصدار قانون خاص والمتمثل في قانون 04/09 والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ولم يكن هاذين القانونين الوحيدين في هذا المجال بل هناك محاولات أخرى خاصة في قوانين الملكية الفكرية مثل قانون حماية حق المؤلف والحقوق المجاورة، غير أن بالرغم من هذه المحاولات يبقى المشرع الجزائري بعيدا كل البعد عن التطور القانوني على المستوى العالمي من جهة، وتطور أساليب إرتكاب جريمة الحاسب الآلي من جهة أخرى، مما يستلزم مراجعة وتطوير القوانين وإصدار المزيد من القوانين لتقوية الترسانة القانونية في هذا المجال.

وبعد كل هذا نخلص الى النقاط التالية:

_ ضرورة اعادة النظر في قواعد الاختصاص القضائي لأن الفضاء السيبراني أو cyber space عبارة عن مسرح لارتكاب جرائم مستحدثة، ترتكب في عالم افتراضي غير ملموس ماديا لكن له وجودا حقيقياً، أهم خصائصه هي أنه يتجاوز حدود الزمان والمكان، وينذر بضرورة اعادة النظر في الكثير من القواعد والمسلمات القانونية مثل قواعد الاختصاص ومبدأ السيادة وغيره من المبادئ القانونية القائمة على المفهوم المادي للسلوك .

_ أظهر البحث غياب مفهوم عام متفق عليه بين الدول –حتى الأن – حول التعريف القانوني للنشاط الاجرامي المتعلق بالجريمة المعلوماتية واللأنماط المكونة لها من جهة، وكذا عدم كفاءة وملاءمة السلطات التي ينص عليها القانون بالنسبة للتحري واختراق نظم الكمبيوتر لأنها عادة ما تكون متعلقة بالضبط والتحري بالنسبة لوقائع مادية خاصة بالجرائم التقليدية وبالنتيجة فهي لا تتلاءم مع الوقائع " المعنوية" التي تتميز بها الجريمة المعلوماتية كاختراق المعلومات المبرمجة وتغييرها في الكمبيوتر من جهة أخرى .

_ السمة المميزة للكثير من الجرائم المعلوماتية هي أنها من النوع العابر للحدود .

_ بات من الضروري ابرام معاهدات للتسليم أو للمعاينة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي وان وجدت فانها غير كافية لمواجهة المتطلبات الخاصة .

_ لهذا يكون من الضروري الإسراع بسن قواعد إجرائية تتلاءم مع طبيعة الجريمة المعلوماتية حتى تكون القواعد الموضوعية المجرمة لها أكثر فعالية هذا من جهة، ومن جهة أخرى

فإنه لا بد من تكاثف الجهود الدولية والإقليمية في حقل جرائم المعلوماتية لتخطي العقبات التي تطرحها هذه الجرائم.

ومن هنا نصل إلى نهاية البحث كي نسجل أن الآلة في مواجهة الانسان فإما أن يفرض عليها إرادته، أو تطغى عليه صنيعته، وتفلت من سيطرته،

قائمة المراجع

المراجع:

1 أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة العاشرة، دار هومة، الجزائر، 2009.

2 أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الطبعة الثالثة، 2006 .

3 الهلال للخدمات الإعلامية، طبعة 2005 .

4 أحمد عمراني، نظام المعلومات في القانون الجزائري، المؤتمر السادس لجمعية المكتبات و المعلومات السعودية، الرياض، 2010.

5 أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائر ،دار هومة، الطبعة الثانية 2007.

6 جان فرنسوا هنروت، أهمية التعاون الدولي بين عناصر الشرطة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 جوان 2007.

7 جميل عبد الباقي الصغير ، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة ،2002.

8 حسين بن سعيد بن سيف الغفري، المنشاوي للبحوث و الدراسات، الجهود الدولية في مواجهة جرائم الأنترنت ،الرياض، 2007.

9 حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير حقوق، جامعة الحاج لخضر باتنة، الجزائر، 2012.

10 راسل تاينر، أهمية التعاون الدولي في منع جرائم الإنترنت، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19 06 2007 ، المملكة المغربية

11 سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، مذكرة دكتوراه ،جامعة عين شمس، 1997.

12 سفيان سوير، جرائم المعلوماتية ، مذكرة ماجستير ، جامعة أبو بكر بلقايد تلمسان ،الجزائر ،2010.

13 طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية.

14 عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات، دار الجامعة الجديدة، الاسكندرية، 2010.

15 عبد الفتاح البيومي الحجازي،مبادىء الاجراءات الجنائية في جرائم الكومبيوتر والانترنت،بهجات للكباعة والتجليد،مصر،2009.

16 عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية و الأنترنت دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، 2007.

17 عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون و المعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009.

18 علي جبار الحسناوي، جرائم الحاسوب و الأنترنت، دار اليازوي العلمية للنشر والتوزيع، عمان، 2009.

19 علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة، الاسكندرية، 1999.

20 عماد مجدي عبد الملك ، جرائم الكمبيوتر و الأنترنت ، دار المطبوعات الجامعية، الإسكندرية، 2011.

21 عواطف محمد عثمان عبد الحليم ،جرائم المعلوماتية ، مجلة العدل ، العدد الرابع و العشرون ،

22 غازي عبد الرحمن هيان الرشيد ، الحماية القانونية من جرائم المعلوماتية (الانترنت) ،مذكرة دكتوراه ، الجامعة الإسلامية، لبنان ،2004.

23 محمد فولان، الحماية القانونية لتكنولوجيات الإعلام، مجلة المحكمة العليا، الجزائر، العدد01، 2010.

24 نائلة عادل محمد قورة، جرائم الحاسب الإقتصادية دراسة نظرية وتطبيقية، ط1 ، دار النهضة العربية، القاهرة، 2003.

25 نبيل صقر،موسوعة الفكر القانوني،جرائم الكمبيوتر و الأنترنت في التشريع الجزائري،دار

26 نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير حقوق ، جامعة الحاج لخضر باتنة، الجزائر، 2012.

27 هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن،-الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 1992.

هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1995.

28 هلالي عبد اللاه أحمد ،جرائم المعلوماتية و أساليب المواجهة و فقاً لاتفاقية بودابست،ط1، دار النهضة، القاهرة، 2007.

29 هيام حاجب، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر، 2008.

30 يوسف صغير ، الجريمة المرتكبة عبر الأنترنت ، مذكرة ماجستير حقوق ، جامعة مولود معمري تيزي وزو، الجزائر، 2013.

31 يونس عرب ، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، 2-4 ابريل 2006، مسقط

القوانين:

1 القانون رقم 575 لسنة 2004 في 06/21 /2004 المتعلق بالثقة في الاقتصاد الرقمي .

2 قانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الجريدة الرسمية، 47، الصادر في 16 أوت 2009

3 القسم السابع تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من قانون 04-15 مؤرخ في 10 نوفمبر 2004 ، الجريدة الرسمية، العدد 71، 10 نوفمبر 2004

4 المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في الدورة الخامسة والعشرون المؤرخ في 15 نوفمبر 2000، موقع الأمم

المراجع الأجنبية:

الانجليزية:

1 André Lucas , le droit de l'informatique , Paris , PUF , 1987 .

2 Berrnard Standlar ،computer crime law

3 Parker(Donn B),Nycum(s)and Aura(s),Computer Abuse, Stanford

Research institute , 1973,

4 Suthreland (Eduin H) ,White collar criminality , Gers (Gilbert) in white collar criminal The offender in business the professions, , 1968

الفرنسية:

1_Clément ENDRELIN , Les moyens juridiques de lutte contre la cybercriminalité , Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen , 2011

2_Duleroy ,Les escrocs a l'informatique ,le nouvel économiste , octobre 2002

3_David Fayon, L'informatique, Vuibert, 1999

4_Rose Philipe, La criminalité informatique à l'horizon analyse prospective, 2005

المواقع:

البرامج الخبيثة http://ar.wikipedia.org/wiki

فيروس الحاسب http://ar.wikipedia.org/wiki

http://www.un.org/arabic/documentsالمتحدة، الدورة الخامسة والعشرون، 2014/05/14،

الفهرس