الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة وهران

كلية الحقوق

مذكرة لنيل شهادة الماجستير في القانون الجنائي

جرائم المساس بأنظمة المعالجة الآلية للمعطيات

من إعداد الطالبة :

جدي نسيمة

تحت إشراف الأستاذ :

العربي شحط عبد القادر

أعضاء لجنة المناقشة :

2014/03/19

الأستاذ : زهدور سهلي	**أستاذ محاضر (أ) جامعة وهران**	**رئيسا**
الأستاذ : العربي شحط عبد القادر	**أستاذ التعليم العالي جامعة وهران**	**مشرفا و مقررا**
الأستاذ : إخلف عبد القادر	**أستاذ محاضر (أ) جامعة وهران**	**مناقشا**
الأستاذ : فاصلة عبد اللطيف	**أستاذ محاضر (أ) جامعة وهران**	**مناقشا**

السنة الجامعية 2013 - 2014

إهـــداء

إلى والـدي العزيـزين

إلى إخوتي و أخواتي و أحفاد العائلة

إلى زملائي في العمل قضاة مجلس قضاء وهران و على

رأسهم السيد " مجاتي أحمد " رئيس مجلس قضاء وهران

و أخص بالذكر أيضا قضاة محكمة السانية

إلى دفعة الماجستير 2008 تخصص

قانون جنائي

شكر و تقدير

نقدم بالشكر الجزيل لكل من ساهم في تدريس طلبة الماجستير
سيما أساتذة تخصص القانون الجنائي الذين كان لنا شرف
التكوين أمامهم

نخص بالذكر الأستاذ المشرف العربي شحط عبد القادر الذي لم
يبخل علي أي طالب منا بالنصيحة و التوجيه

و نقدم الشكر الجزيل أيضا لأعضاء لجنة المناقشة لتخصيصهم
وقتهم للإطلاع وتقييم عملنا المتواضع و تصحيح أخطائنا و توجيهنا

المـــــــقـــــدمـــــــــة

شهد القرن العشرين ثورة أصطلح على تسميتها بثورة المعلومات الذي لعب فيها الحاسب الآلي الدور الرئيسي الذي ترافق مع تزايد الوعي لدى الشعوب لأهمية المعلومات بإعتبارها مصدرا للقوة و الثروة ، خاصة مع تعميم إستخدام شبكة الأنترنيت من طرف الجميع بصرف النظر عن عقائدهم و أيدلوجياتهم و إنتمائهم الطائفي أو العرقي بعد أن كان الهدف من إنشائها بداية هو الحاجة الحربية لجيش الولايات المتحدة الأمريكية.

كما أنعكس هذا التطور إيجابا على المجالات الإقتصادية و أوجد أيضا أنواعا جديدة من الجرائم أصطلح عليها بالجرائم المعلوماتية الأمر الذي إستدعى مراجعة كاملة للأحكام القانونية التقليدية التي أصبحت تقف عاجزة لمواجهة هذه الجرائم .

و ضمن طائفة الجرائم المعلوماتية المتعددة الصور و التي عجز فقهاء القانون عن حصرها نجد جرائم المساس بأنظمة المعالجة الآلية للمعطيات و التي بدورها جاءت كنتيجة للتطور التكنولوجي المذهل الذي أصبح يربط العالم بشبكة معلوماتية عنكبوتية إمتدت نحو كل أنحاء العالم ، و ربطت بين الشعوب و أصبحت وسيلة التعامل اليومي بين الأفراد و المؤسسات بمختلف الطبقات الإجتماعية التي أصبحت توفر الجهد و المسافات .

و لكن في ذات الوقت تتعرض المعلومات الموضوعة فيها لإنتهاكات بسبب إستخدامتها الغير مشروعة التي تسهل للمجرمين ارتكاب جرائمهم ، فهي جرائم تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية و تطال اعتداءاتهم معطيات الكمبيوتر المخزنة و المعلومات المنقولة عبر النظم و شبكات المعلومات .

و في بادئ الأمر خلال السبعينات من القرن الماضي مع شيوع إستخدام الكمبيوتر و قبل إنتشار إستعمال شبكة الأنترنيت ظهرت بعض أشكال التلاعب بأنظمة الكمبيوتر و البيانات المخزنة ، و طرحت للنقاش كظاهرة غير أخلاقية مستجدة . و في الثمانينات و

مع إنتشار الأنترنيت شاع إصطلاح (الهاكرز) كمقتحمين للنظم و ينشرون الفيروسات لتدمير الملفات ، بعدها إنتشرت الإعتداءات على النظم و تعدد أشكالها و ظهر إصطلاح جرائم الكمبيوتر و الإنترنيت و هي الظاهرة التي شهدت تناميا هائلا خلال التسعينات مع توسع إستعمال الانترنيت و التقنيات العالية التي أصبحت تسهل إرتكاب الجريمة و توسع شبكة المستخدمين التي أصبحت تشمل الملايين .

و تعد جرائم المساس بأنظمة المعالجة الآلية للمعطيات من أهم موضوعات البحث التي فرضت نفسها للدراسة و البحث ، كونها من الجرائم التي تمس بالفرد و الدولة بمؤسساتها العامة و الخاصة ، و ليس على المستوى الداخلي فحسب بل يمتد أثرها على المستوى الدولي مما جعل الدول تلجأ لإبرام إتفاقيات دولية ثنائية و مشتركة لمواجهة هذه الجرائم .

كما تسعى الدول من خلال تشريعاتها الداخلية لسن قوانين لتجريم هذا النوع من الإعتداءات و وضع عقوبات من شأنها حماية المجتمع منها . و الأمر لا يتوقف على صدور تشريع ثابت بشأن هذه الجرائم نظرا لما تتسم به من تطور و تغيير إذ تتنوع سبل إرتكاب الجريمة و تتعدد صورها مع تطور التكنولوجيا المعلوماتية ، و عليه وجب على المشرع بالمقابل أيضا الحرص على مواكبة النصوص التجريمية و العقابية لتشمل كل الأفعال المستحدثة ، و وضع إستراتيجية حماية جزائية للوقاية من هذه الجرائم .

و الواقع أن الولايات المتحدة الأمريكية و الدول الغربية كانت السباقة على الدول العربية في سن قانون يتعلق بهذا النوع من الجرائم حتى أن فرنسا و كندا تجاوزت مرحلة التشريع بخطوات إذ و منذ منتصف التسعينات من القرن الماضي شرعت في تأهيل الجانب البشري الذي يطبق هذه القوانين من قضاة و محققين و ضباط شرطة .

كذلك نذكر مساعي الإتحاد الأوروبي الذي كان يصدر التوصيات لسن القوانين المنظمة للمعلوماتية و التي تنوعت مواضيعها بين التجارة الإلكترونية و حماية المستهلك و غيرها و بلغ التعاون مداه بإبرام إتفاقية موحدة لمواجهة جرائم الغش المعلوماتي عام 2001 التي وقعت عليها أكثر من 12 دولة لتوحيد قواعد الإختصاص القضائي خاصة و القانون الواجب التطبيق .

و ظلت المحاولات العربية ضعيفة و مقتضبة في هذا الشأن منها صدور القانون العربي النموذجي و الإسترشادي لمكافحة جرائم الكمبيوتر و الأنترنيت كثمرة عمل بين وزراء العدل و الداخلية العرب بعد عقد إجتماع مشترك في 21 و 2002/05/22 أين تم إقراره ليبقى على الدول العربية أن تضمن محتواه في قوانينها الوطنية ، و الذي تم إقراره بوصفه منهجا إسترشاديا يلتزم به كل مشرع عربي.

و البحث في مفهوم هذه الجرائم و صورها و السبل المثلى للتعامل معها يخلق عدة إشكالات قانونية و عملية ، أولا لعدم إمكانية تطبيق النصوص القانونية الموجودة على كل الأفعال لعدم تناسبها معها و التي يتسع مجالها يوما بعد يوم .

و نظرا لكون هذه الجرائم مستحدثة فإن أول إشكال يطرح هو تحديد مفهوم المصطلحات الواردة في نصوص التجريم خاصة مع عدم تضمينها لتعاريف خاصة لصور الجرائم و المصطلحات الغير مألوفة في قانون العقوبات ، التي جاءت بها النصوص الجديدة الموضوعة حتى يتسنى فيما بعد تكييف الفعل على أنه من الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، و هذا ما يؤثر على عملية تكييف الوقائع و تحديد نطاق شمولية الجريمة لأفعال معينة ، خصوصا مع عدم كفاية النصوص القانونية السابقة الموضوعة و الإجرائية حاليا لمنع وقوع الجريمة و لردع المجرمين مما يولد الحاجة المستمرة لنصوص جديدة تتضمن كل جديد ، مع بيان خصائص هذه الجرائم و سمات مرتكبيها .

و بعد البحث في الجانب الموضوعي للجريمة تطرح عدة إشكالات من الناحية الإجرائية بداية من الإختصاص القضائي و القانون الواجب التطبيق بسبب أن آثار هذا النوع من الجرائم ممتد سواء داخل الدولة الواحدة مما يطرح إشكالا في الإختصاص المحلي لعدة محاكم . كما قد يتعدى أثرها حدود الدولة لإقليم دولة أخرى مما يثير إشكالات في تنازع الإختصاص سلبيا أو إيجابيا من جهة و إشكال نقص التعاون الدولي الذي من شأنه تسهيل إجراءات التحقيق و التحري عن هذه الجرائم.

و عند إنعقاد الإختصاص يواجه الجهة القضائية المختصة الإشكال الأهم و هو الحصول على الأدلة الإلكترونية ذات الطابع المعنوي التي تنصب على ذبذبات و برامج و

معطيات مخزنة غير ملموسة ، و هو ما يضع على كاهل القاضي مهمة صعبة لتقدير هذا الدليل و مشروعيته في ظل نظرية الإثبات و قانون الإجراءات الجزائية سيما المادة 212 منه .

سنحاول الإجابة عن هذه الأسئلة و غيرها خلال هذه الدراسة على ضوء القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات الجزائري الذي أضاف بموجبه المشرع القسم السابع مكرر بقانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات الذي تضمن 8 مواد من 394 مكرر إلى المادة 394 مكرر 7 و جرم فيه هذا النوع من الأفعال .

و من جهة أخرى نعتمد في دراسة الجانب الإجرائي على ما ورد في قانون الإجراءات الجزائية من قواعد عامة منظمة لجانب التحري و الإستدلال و التحقيق و النصوص التي خص بها المشرع هذا النوع من الجرائم ، مع الإشارة أيضا للنصوص الإجرائية الواردة بالقانون 04/09 المؤرخ في 2009/08/50 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال الذي تضمن إجراءات تتعلق بفئتين من الجرائم الواردة بالمادة الثانية منه و هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما هي محددة بقانون العقوبات و هي موضوع دراستنا و الفئة الثانية تشمل كل جريمة ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية ، و سنعتمد في سبيل ذلك المنهج التحليلي لما جاء في نصوص قانون العقوبات و قانون الإجراءات الجزائية الجزائري مع الإشارة في بعض العناصر للتشريعات المقارنة .

و إرتأينا تقسيم هذه الدراسة إلى ثلاثة فصول

في الفصل التمهيدي نتناول مفهوم نظام المعالجة الآلية للمعطيات و تمييزها عن باقي الجرائم المعلوماتية في ظل عدم وجود تعريف قانوني و نجيب عن إشكال مدى وجوب خضوع النظام لحماية فنية مسبقة ؟ ثم نبين أهم خصائص هذا الجرائم و أساليب إرتكابها و سيمات الجاني المعلوماتي و ما يميزه عن المجرم بالمفهوم التقليدي .

و أخيرا نتناول موضوع الحماية الجزائية التي وضعها المشرع لهذا النوع من الجرائم و هنا نتسائل عن مدى فاعليتها ؟

في الفصل الأول نعالج شرحا و تفصيلا صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كما جاءت في قانون العقوبات من حيث الركنين المادي و المعنوي .

و في الفصل الثاني نتعرض لمسألة الإختصاص و التحري في هذه الجرائم و مسألة الإثبات و تقدير الدليل و سبل الحصول عليه و أخيرا الجزاءات المقررة لها .

الفصل التمهيدي : الأحكام العامة لأنظمة المعالجة الآلية للمعطيات

يتمحور موضوع هذه الدراسة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات التي كما سلف الذكر إستحدثها المشرع الجزائري بموجب القانون رقم 2004-15 المؤرخ في 10 نوفمبر 2004 و الذي أضاف بموجبه القسم السابع مكرر بقانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات الذي تضمن ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 7 المعدل و المتمم بالقانون رقم 23/06 المؤرخ في 2006/12/20 .

و بداية و قبل التطرق لهذه الجرائم شرحا و تفصيلا من حيث أركانها نتناول في الفصل التمهيدي بيان مفهوم نظام المعالجة الآلية للمعطيات بعد تمييزها عن غيرها من الجرائم المعلوماتية التي ورد تعدادها في الإتفاقية الدولية للإجرام المعلوماتي ، و لعل الأمر بالدقة بحيث يختلط الأمر حتى القول أنهما مسميان لذات الشيء إلا أن الأمر غير ذلك فجرائم المساس بأنظمة المعالجة الألية للمعطيات كما سنأتي على بيان ذلك هي فئة من الجرائم المعلوماتية فهي جزء من كل .

و في ما يلي نتعرض لتعريف الجريمة المعلوماتية و تصنيفها و مفهوم نظام معالجة المعطيات ثم خصائص هذه الجرائم التي تميزها عن الجرائم الكلاسيكية هذا من جهة .

و لأن هذه الجرائم إرتبط ظهورها بتطور الثورة المعلوماتية و البحث في العلاقة بينهما يوجب البحث في دوافع إرتكاب هذا النوع من الجرائم خاصة و أنها في تزايد مستمر ، كما و نبين سمات المجرم المعلوماتي ، و أخيرا نعرض سبل الحماية الجزائية التي إتخذتها الدول على الصعيد الداخلي و في إطار التعاون الدولي .

المبحث الأول : ماهية نظام المعالجة الآلية للمعطيات

نعالج في المبحث الأول المقصود بنظام المعالجة الآلية للمعطيات الذي يتطلب بالضرورة تعريف الجريمة المعلوماتية بداية لأن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات هي قسم ينتمي لطائفة الجرائم المعلوماتية ، ثم نبين خصائص هذا النوع من الجرائم الذي يستهدف هذه الأنظمة ، و هنا يطرح إشكال مدى وجوب خضوع هذه الأنظمة لحماية حتى يكون الإعتداء عليها مجرما ؟ أو هل يشمل التجريم الإعتداءات الواقعة على الأنظمة سواء كانت محمية أو غير محمية ؟

المطلب الأول : تمييز الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات عن باقي الجرائم المعلوماتية

الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات هي قسم ينتمي للجرائم المعلوماتية التي تعددت تعريفاتها كما تعددت مسمياتها إذ يطلق عليها أيضا جرائم الكمبيوتر و الأنترنيت ، الجريمة الإلكترونية ، جرائم إساءة إستخدام المعلومات و هناك من الفقه من أطلق عليها إسم الجرائم المستحدثة أو جرائم الغش المعلوماتي[1] .

و فيما يلي من أهم تعريفات الفقهاء للجريمة المعلوماتية و التصنيفات التي أخذت بها بعض التشريعات المقارنة و إتفاقية بودابست لتعداد صور الجريمة المعلوماتية التي تعد جرائم المساس بأنظمة المعالجة الآلية للمعطيات إحدى فئاتها .

أولا : تعريف الجريمة المعلوماتية :

تعددت تعريفات الجريمة المعلوماتية فقها و طبعا لا يوجد تعريف دقيق متفق عليه نظرا لأنها ظاهرة إجرامية متغيرة و متطورة لا يمكن حصر صورها المتجددة . و إختلفت التعريفات أيضا بالنظر للمعيار المعتمد في ذلك ، إذ يوجد من عرفها بالنظر لمحل الجريمة أو وسيلة إرتكابها و من الفقه من اعتمد على معيار شخصي و عرفها

(1) أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، الجزء الأول ، دار هومة ، الطبعة الثالثة 2013 الصفحة 447 .

بالنظر لمميزات مرتكبيها و نذكر من التعريفات ما يلي :

" الجريمة المعلوماتية هي الإستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الإستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات"[1]

و عرفها خبراء المنظمة الأوروبية للتعاون و التنمية الإقتصادية على أنها : " كل سلوك غير مشروع أو غير مسموح به يرتبط بالمعالجة الآلية للمعطيات أو بنقلها "[2]

و عرفت أيضا أنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه." و عرفت كذلك أنها: "غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة و نقلها." [3]

و عرفها الفقه أنها :" الدخول الغير مشروع إلى الشبكات الخاصة و العبث بالبيانات الرقمية التي يحويها أو إتلافها أو محوها مما يلحق ضرر بالبيانات و المعلومات ذاتها و كذلك البرامج و الأجهزة التي يحويها "[4]

و ما يلاحظ من هذه التعريفات أنها تبقى غير دقيقة متغيرة في ظل عدم وجود تعريف قانوني يحصر صور الجريمة .

و من التعريفات أيضا تعريف المؤتمر العاشر للأمم المتحدة على أنها : " أي جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ."

و من التعريفات التي إعتمدت على المعيار الشخصي كتعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث و تبنته الوزارة في دليلها لعام 1979 على النحو الأتي :

---

(1) ممدوح عبد الحميد عبد المطلب بحث بعنوان جرائم إستخدام شبكة المعلومات العالمية (الجريمة عبر الأنترنيت من منظور أمني) ، ص 2 مأخوذ من الموقع الإلكتروني www.arablawinfo.com

(2) عبد الله حسين علي محمود بحث بعنوان إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات ص 02 مأخوذ من الموقع الإلكتروني www.arablawinfo.com

(3) علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، المكتبة القانونية القاهرة 1999 ، ص 20 .

(4) صالح أحمد البربري بحث بعنوان دور الشرطة في مكافحة جرائم الإنترنيت في إطار الإتفاقية الأوروبية الموقعة في بودابست في 2001/11/23 ص 4 و 5 مأخوذ من الموقع الإلكتروني www.arablawinfo.com

" هي جريمة تتطلب للقيام بها معرفة تقنية بالحاسبات تمكن الجاني من إرتكابه للفعل ."
و ما يؤخذ على هذا الإتجاه أن شرط المعرفة التقنية لدى الجاني ليس حتميـة واجبـة التوافر فقد ترتكب الجريمة من مجموعة تقسم فيها الأدوار حسب الكفاءة و يساهم بعضهم فيها رغم عدم معرفتهم الرفيعة بتقنيات الحاسوب ."
و ما يمكن ملاحظته من خلال التعريفات الفقهية العديدة التي حاولت وضع مفهوم للجريمة المعلوماتية أن الفقه أخذ إتجاهين إتجاه أخذ بمفهوم واسع و الثاني أخذ بمفهوم ضيق.

1- <u>المفهوم الواسع</u> : هذا الإتجاه أخذ به عدة فقهاء منهم تيادمان و دون باركر و الذين يوسعون مفهوم الجريمة المعلوماتية لتشمل كل اشكال السلوك غير المشروع الذي يرتكب بإستعمال الحاسب الآلي و تكون الأنظمة أداة لإرتكاب الجريمة أو كانت المعلوماتية هدفا لها و نذكر من هذه التعريفات :[1]

تعريف كلاوس تيادمان :" الجريمة المعلوماتية تشمل كافة أشكال السلوك الغير مشروع الذي يرتكب بإستخدام الحاسب."
و ما يؤخذ على هذا التعريف أنه بالغ العمومية و الإتساع إذ لم يبين خصوصية الجريمة و هذا يشابه تعريف ليسلي ديبالLesli d Ball أنها :" فعل إجرامي يستخدم الحاسب في إرتكابه كأداة رئيسية " [2]

تعريف Totty et Hardcastel :" هي تلك الجرائم التي تكون قد وقع في مراح إرتكابها بعض العمليات داخل نظام الحاسب الآلي و بعبارة أخرى هي تلك الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا ."

تعريف دون باركر :" كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية تربت عنه خسارة للمجني عليه أو مكسب يحققه الجاني ."

(1) آمال قارة مذكرة ماجستير بعنوان الجريمة المعلوماتية ، كلية الحقوق جامعة الجزائر 2001 ص 18.
(2) طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة الإسكندرية 2009 ص 45.

2 – <u>المفهوم الضيق</u> : يرى أصحاب هذا الإتجاه بإقصاء الأفعال التي يستخدم فيها الحاسوب للإعتداء على الغير أو الأموال و حصر مفهوم الجريمة في الجرائم الماسة بأنظمة المعلوماتية في حد ذاتها .

كما جاء في تعريف لمنظمة التعاون الإقتصادي : " كل سلوك غير مشروع أو غير مصرح به يتعلق بالمعالجة الألية للبيانات و نقلها ."

و هذا الإتجاه تزعمه الفقيه " فراري" الذي حصرها في الإعتداءات عن الكيان المنطقي للمعلوماتية بإعتبار الإعتداءات على العناصر المادية تطبق عليها النصوص الكلاسيكية.

<u>ثانيا : تصنيف الجرائم المعلوماتية</u>

من خلال دراستنا للتعاريف السالفة الذكر المتعددة لاحظنا إختلافا و تباينا في المعايير المعتمدة لتحديد عناصرها و مشتملاتها حتى أن مفرداتها غير متفق عليها مما جعل الإختلاف ينعكس أيضا على التشريعات إذ اختلفت القوانين المقارنة لدى تجريمها للجرائم المعلوماتية في تحديد صورها رغم الجهود الدولية و المحلية الداعية لتوحيد التشريعات الجنائية .

و المشرع الجزائري مثلا جرم في قانون العقوبات الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات و لها أربع صور سنأتي على تفصيلها بالفصل الأول من هذه الدراسة في حين وسعت تشريعات مقارنة من دائرة الأفعال التي تدخل تحت الجرائم المعلوماتية منها التزوير المعلوماتي ، السرقة ، تبيض الأموال التقليد و غيرها و هي من الجرائم التقليدية التي أصبحت معلوماتية متى تم إرتكابها بإستعمال الكمبيوتر و فيما يلي نذكر أهم تصنيفات التشريعات المقارنة للجريمة المعلوماتية و كذا التصنيف الذي وضعته إتفاقية بودابست .

1- <u>تصنيف الجرائم المعلوماتية في ظل إتفاقية بودابست</u> :

تضمنت إتفاقية بودابست للإجرام المعلوماتي الجرائم المعلوماتية سواء ما يقع على الأنظمة و المعلومات و هي موضوع دراستنا ، و كذا الجرائم التقليدية التي أعطتها وصف الجرائم المعلوماتية إذا إرتكبت من خلال شبكات رقمية ، و تضمنت الإتفاقية 48

مادة موزعة على أربع فصول أوردت بالمادة الأولى تعريفا للمصطلحات التقنية المتعلقة بموضوع الإتفاقية ثم نصت على صور الجريمة على النحو التالي :[1]

نصت المادة 2 على الدخول الغير مشروع إلى الشبكات و إنتهاك إجراءات الحماية بقصد الدخول على البيانات أو لأي غرض إجرامي آخر .

نصت المادة 3 على الإلتقاط المتعمد و غير المشروع للبيانات و المعلومات بإستخدام الوسائل الفنية المختلفة ، و ذلك أثناء إرسال هذه البيانات إلى المرسل إليه أو لدى المصدر أو داخل شبكة المعلومات ، و يدخل في ذلك أيضا الرسائل المرسلة بواسطة الأجهزة الكهرومغناطسية الصادرة عن شبكة معلومات و التي تحوي مثل هذه البيانات سواء بغرض إجرامي أو لمجرد الإتصال بين شبكة معلومات و شبكة أخرى.

نصت المادة 4 على الأفعال التي من شأنها الإضرار بالبيانات و هو فعل عمدي دون وجه حق للإضرار ، مسح ، إتلاف ، إفساد ، حذف البيانات و المعلومات .

نصت المادة 5 على الإضرار بنظام الشبكات فجرمت الإعاقة المتعمدة لمنع تشغيل نظام المعلومات عن طريق الدخول ، تحويل ، إرسال ، الإضرار ، مسح ، إتلاف إفساد أو حذف البيانات .

نصت المادة 6 على إساءة إستخدام المعطيات فنصت على وجوب تجريم :

أ. إنتاج ، بيع ، الحصول بغرض الإستخدام ، إستراد ، نشر ، الوضع تحت التصرف بأي شكل من الأشكال لأي أداة أو برنامج بطريقة تسمح بإرتكاب الجرائم المنصوص عليها بالمواد من 2 إلى 5 من هذه الإتفاقية ، أو أي كلمة مرور أو بيانات متشابهة تسمح بإرتكاب هذه الجرائم أو أي جرائم أخرى .

(1) صالح أحمد البربري ، المرجع السابق ، ص 2 و 3 .

ب. إمتلاك أحد الأدوات الموضحة آنفا بغرض إستخدامها لإرتكاب إحدى الجرائم المشار إليها بالمواد من 2 إلى 5 و يمكن النص في القوانين المحلية على أن مجرد إمتلاك بعض هذه الأدوات يكفي لقيام المسؤولية الجنائية .

نصت المادة 7 على جريمة تزوير المعلومات و يتعلق الأمر بالدخول ، إفساد ، إتلاف ، مسح و الحذف المتعمد للبيانات و إنشاء بيانات غير صحيحة لإستخدامها على أنها صحيحة .

نصت المادة 8 على النصب و الإحتيال المعلوماتي لإلحاق الضرر بممتلكات الغير عن طريق :

الدخول و إفساد و مسح البيانات .

أي شكل من أشكال الإعتداء على تشغيل شبكة المعلومات بطريق الإحتيال للحصول دون وجه حق على منفعة إقتصادية لنفسه أو للغير.

نصت المادة 09 على الجرائم المتعلقة بالدعارة بالنسبة للأطفال

نصت المادة 10 على الجرائم المتعلقة بالملكية الفكرية و الحقوق المرتبطة بها

للإشارة من الدول التي وقعت على الإتفاقية الولايات المتحدة الأمريكية ، اليابان، كندا ، جنوب إفريقيا و غيرها بمجموع 26 دولة من أصل 43 من أعضاء المجلس الأوروبي من بينها 12 دولة من الإتحاد الأوروبي و أشار مسؤولو مجلس أوروبا أن التوقيع على الاتفاقية مفتوح لسائر الدول ، و تدخل حيز التنفيذ عندما يصادق عليها خمس دول بينها ثلاث من أعضاء المجلس الأوروبي .[1]

2 - <u>التصنيف الأمريكي للجرائم المعلوماتية</u> : [2]

أ. في عام 2000 أقرت وزارة العدل الأمريكية تصنيف لجرائم الكمبيوتر بموجب قانون الكمبيوتر الفدرالي لدى مكاتب التحقيقات الفيدرالية كالآتي :

(1) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي الإسكندرية 2009 ص 277.

(2) عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، دار الكتب القانونية مصر 2007 ص 20 و 21.

- السطو على بيانات الكمبيوتر
- الإتجار بكلمة السر
- حقوق الطبع و القرصنة (البرامج ، الأفلام ، التسجيل الصوتي)
- سرقة الأسرار التجارية بإستخدام الكمبيوتر
-تزوير الماركات التجارية بإستخدام الكمبيوتر
- تزوير العملة بإستخدام الكمبيوتر
- الصور الجنسية الفاضحة و إستغلال الأطفال
- الإحتيال بواسطة شبكة الأنترنيت
- الإزعاج عن طريق شبكة الأنترنيت
- تهديدات القنابل بواسطة شبكة الأنترنيت
- الإتجار بالمتفجرات أو الأسلحة النارية أو المخدرات و غسيل الأموال عبر شبكة الإنترنيت .

ب. أما مكتب التحقيقات الفيدرالي الأمريكي (FBI) صنف الجرائم المعلوماتية في ديسمبر 2000 و قسمها لسبعة فئات :

- إقتحامات شبكات الهواتف العامة أو الخاصة بواسطة الكمبيوتر
- إقتحامات شبكة الكمبيوتر الرئيسية لأي جهة
- إنتهاكات السرية على بعض مواقع الأنترنيت
- إنتهاكات سلامة الشبكة المعلوماتية
- التجسس الصناعي
- برامج الكمبيوتر المسروقة
- البرامج الأخرى عندما يكون الكمبيوتر العامل الرئيسي في إقترافها .

و جدير بالذكر أن الولايات المتحدة الأمريكية أصدرت قانونا عاما يحمل رقم (100.99.474) رقمه التشريعي 1986/1213 لمواجهة جرائم الكمبيوتر و قد ورد في هذا التشريع جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية و إستنادا لذلك صدرت قوانين ولاتي تكساس و إلينوي في شأن جرائم الكمبيوتر .

3 – <u>تصنيف قانون العقوبات الفرنسي للجرائم المعلوماتية</u> :[1] إستحدث المشرع الفرنسي الجرائم المعلوماتية بموجب القانون 88/19 المتعلق بالغش المعلوماتي بناءا على إقتراح من النائب جاك قود فران (JACQUES GOD FRAIN) الذي تم إقراره في 1987/12/22 و الذي أصبح يعرف بقانون GOD FRAIN ثم لاحقا تم إدماج نصوصه في قانون العقوبات الجديد المواد من 323-1 إلى 323-7 الذي جرى تعديله في 1994/03/01 و الذي صنف جرائم الغش المعلوماتي إلى :

- الدخول أو البقاء غير المصرح به للنظام أو جزء منه
- الإتلاف المعلوماتي لمحتوى النظام الآلي لمعالجة البيانات
- إعاقة أو إفساد نظام معالجة آلية للمعطيات
- التزوير في وثيقة مبرمجة
- إستخدام وثيقة مبرمجة مزورة

و ما يلاحظ هنا أن المشرع الفرنسي جرم الإعتداء على أنظمة المعالجة الآلية بكل أشكاله ماعدا جريمة تزوير المستندات المعالجة آليا و إستعمالها فهذه الجريمة تحمي نتاج النظام و لا تعد إعتداءا على النظام ذاته ، و لاحقا قام المشرع الفرنسي بإلغاء المواد المتعلقة بالتزوير في وثيقة مبرمجة و إستخدامها مما يعني أنه أراد أن يدخل التزوير المعلوماتي ضمن نطاق التزوير التقليدي .

4 – <u>تصنيف الفقه للجرائم المعلوماتية</u>

بعد ما تم عرضه من تصنيفات الإتفاقيات الدولية و التشريعات المقارنة نأتي لتصنيف الفقه لفئات الجرائم المعلوماتية و التي قسمها لفئتين :

(1) طارق إبراهيم الدسوقي عطية ، المرجع السابق ص 227.

أ. <u>الجرائم الواقعة على النظام المعلوماتي</u> :

و هي الجرائم التي يكون موضوعا لها الإعتداء على البرامج و البيانات و هذه الفئة هي التي نص و عاقب عليها المشرع الجزائري تحت عنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و هي محل دراستنا .

ب . <u>الجرائم الواقعة بواسطة النظام المعلوماتي</u> :

و هي الجرائم التي تكون المعلوماتية وسيلة للإعتداء فيها و التي يستخدم فيها الحاسب الألي كأداة لإرتكاب الجريمة كالتزوير المعلوماتي ، السرقة ، التقليد ، النصب... و التي لا تعد جرائم معلوماتية بالمعنى الفني .

و بالنسبة للتشريع الجزائري فلم يعتبر هذه الجرائم من فئة الجرائم المعلوماتية و لم يخصها بنصوص خاصة و عليه يطبق على هذه الفئة النصوص الكلاسيكية في قانون العقوبات و القوانين الخاصة الملحقة به مثلا كجريمة التزوير المعلوماتي نطبق عليها المواد المتعلقة بالتزوير 214 و 229 من قانون العقوبات ، جريمة التقليد يطبق عليها المواد 151 و ما يليها من الأمر 03/08 المتعلق بحقوق المؤلف و الحقوق المجاورة ، الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال المنصوص عليها بالقانون 04/09.

المطلب الثاني : مفهوم نظام المعالجة الآلية للمعطيات

لدراسة جرائم المساس بأنظمة المعالجة الآلية للمعطيات لابد أولا من الإلمام بالمصطلحات و المفاهيم المتعلقة بالمجال المعلوماتي حتى يمكن فهم أركان الجريمة و سبل تحقق نتائجها.

و بالرجوع لقانون العقوبات الجزائري في المواد من 394 مكرر إلى 394 مكرر 7 فإنه لم يورد تعريفا لنظام المعالجة الآلية للمعطيات بأي نص ، و كذا فعل المشرع الفرنسي رغم إقتراح البرلمان الفرنسي لتعريف خلال مناقشة تعديل قانون تجريم هذا النوع من الإعتداءات . إلا أنه لم يتم الموافقة على تضمين هذا التعريف بنصوص التعديل بحجة أنه لا يمكن ربط التجريم في هذه الأنظمة بحالة تقنية متغيرة قد لا يشملها التعريف الموضوع لاحقا .

في حين ورد بالقانون04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال تعريف للمنظومة المعلوماتية بالمادة 2 فقرة ب على أنها :

" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ."

أما عن الإجتهاد القضائي الفرنسي فإنه أورد في قراراته كل مرة تحديد لمفاهيم عدة مصطلحات معلوماتية ، كما ورد تعريف في موسوعة (أنسيكلوبيديا يونيفارسال) بأن نظام المعالجة هو كل شيء مركب يتكون من عدة معطيات مرتبطة ببعضها بعدد معين من الروابط .[1]

و عرفه الفقيه خالد ممدوح إبراهيم على أنه : [2]

" مجموعة من العناصر المتداخلة و المتفاعلة مع بعضها البعض و التي تعمل على جمع البيانات و المعلومات و معالجتها و تخزينها و بثها و توزيعها بغرض دعم

(1) موقع الموسوعة wikipedia-org/wiki/universal

(2) خالد ممدوح إبراهيم ، التقاضي الإلكتروني ، دار الفكر الجامعي الإسكندرية 2009 ص 297.

صناعة القرارات و التنسيق و تأمين السيطرة على المنظومة إضافة لتحليل المشكلات للموضوعات المعقدة."

و من خلال هذا التعريف نستخلص أن لنظام المعالجة أربع نشاطات :

1- تأمين مدخلات البيانات فكل أنواع المعطيات توضع في النظام بواسطة وسائل إدخال مناسبة .

2- المعالجة : أي تحويل البيانات المدخلة من شكلها الأولي إلى نتائج و معلومات مفهومة و قابلة للإستخدام و من هذا المنطلق فالجزء المعالج بالجهاز (processing) يعتبر الأساس في نظام الكمبيوتر .

3- تأمين المخرجات : من المعلومات المطلوبة للمستخدمين لنقل المعلومات من وحدة المعالجة المركزية إلى وسيلة إخراج مناسبة .

4- التغذية الراجعة : إذ أن العديد من البيانات المخرجة من الحاسوب هي مدخلات ثانية لإعادة معالجتها لأغراض أخرى . [1]

و عرفه مجلس الشيوخ الفرنسي على أنه :

" نظام المعالجة الآلية للمعطيات هو كل مركب يتكون من وحدة أو مجموعة وحدات معالجة ، و التي تكون كل منها الذاكرة ، المعطيات ، أجهزة الإدخال و الإخراج ، أجهزة الربط التي تربط بينها مجموعة من العلاقات التي عن طريقها تم تحقيق نسخة معينة و هي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية"[2]

و ما يلاحظ على هذا التعريف انه أشار للعناصر المادية و المعنوية التي يتكون منها نظام المعالجة الآلية للمعطيات على سبيل المثال لا الحصر .

---

(1) خالد ممدوح إبراهيم ، التقاضي الإلكتروني ، المرجع السابق ص 298 .

(2) محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي ، دار الجامعة الجديدة الإسكندرية مصر 2007 ص 26.

كما تعرفه المادة 14/1 من القانون العربي النموذجي الموحد بأنه :" كل مجموعة مركبة من وحدة أو عدة وحدات الإدخال و الإخراج و الإتصال التي تساهم في الحصول على نتيجة معينة ." [1]

و نصت المادة الأولى من الفصل الأول الفقرة الأولى من الإتفاقية الدولية للإجرام المعلوماتي على تعريف للنظام المعلوماتي على أنه : " أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض ، أو التي هي ذات صلة بذلك و يقوم أحدها تنفيذا للبرنامج بعمل معالجة آلية للبيانات " و هو ذات المفهوم الذي أخذ به المشرع الجزائري السالف الذكر.

و جاء في المذكرة التفسيرية للإتفاقية أن المقصود بالنظام المعلوماتي هو جهاز يتكون من مكونات مادية و منطقية و ذلك بغرض المعالجة الآلية للبيانات الرقمية و هو يشتمل على وسائل للإدخال و إخراج و تخزين البيانات ، و هذا الجهاز قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة [2] و من خلال هذا التعريف نستشف أن لأنظمة المعالجة نوعين من المكونات مادية و غير مادية

أولا : المكونات المادية : لا يمكن تصور أنظمة المعالجة الآلية للمعطيات دون وجود جهاز إعلام آلي أو حاسوب بمكوناته المادية التي تتيح إستعمال الأنظمة و المعطيات لإجراء عمليات معالجتها آليا .

و لغة علم الحاسب هو علم الأعداد و تعني كلمة حاسب ناظمة آلية ، و من التعريفات التي أعطيت له أنه مجموعة من الأجهزة المتكاملة تعمل بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على نتائج معينة .

و يعرف أيضا أنه : " جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية و المنطقية للتعليمات المعطاة له بسرعات كبيرة تصل إلى عشرات الملايين من العمليات

(1) جباري عبد المجيد ، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة ، دار هومة للنشر و التوزيع الجزائر 2012 ص 109

(2) طارق إبراهيم الدسوقي عطية ، المرجع السابق ص 45 .

في الثانية بدرجة عالية من الدقة و لديه القدرة على التعامل مع كم هائل من البيانات و تخزينها و إسترجاعها عند الحاجة [1]

و يعرف الحاسب الآلي على أنه :" عبارة عن جهاز إلكتروني يتكون من مجموعة متداخلة من الأجزاء تعمل فيمـــا بينها لهدف مشترك و هو إخراج العمليـــات الحســـابية و المنطقية طبقا لبرنامج يتم وضعه مسبقا من خلال عدة عمليات و هي الإدخال ، المعالجة ، الإسترجاع و الإخراج "[2]

كما يعرف أيضا أنه : " آلة حاسبة إلكترونية تستقبل البيانات ثم تقوم عن طريق الإستعانة ببرامج معينة بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة [3]

و يعرف أيضا أنه : " جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات أو إخراج معلومات أو إجراء عمليـــات حســـابية أو منطقيـــة و يقوم بالكتابة على أجهزة الإخراج أو التخزين أين تم إدخال المعلومات بواسطة مشغل الحاسب و يمكن إعتباره آلة إلكترونية تستقبل البيانات لتقوم بالإستعانة ببرامج معينة بعملية تشغيلها للوصول للنتائج المطلوبة ."

و يتكون الحاسب الآلي من :[4]

1- <u>وحدات الإدخال</u> : و هي الوحدات التي يمكن من خلالها لشخص إدخال البيانات أو الأوامر التي لا يمكن للجاني إرتكاب جريمته دونها و التي يمكن بمقتضاها تغذية الحاسب الآلي بالمعلومات التي يريد تزويده بها أو تخزينها أو تعديل تلك المحفوظة

(1) خالد ممدوح إبراهيم ، التقاضي الإلكتروني ، المرجع السابق ، ص 291 و 292.

(2) أحمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي الإسكندرية ، الطبعة الثانية 2006 ، ص 27.

(3) علاء الدين محمد شحاتة ، رؤية أمنية للجرائم الناشئة عن إستخدام الحاسب الآلي ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة 2005 ص 25 .

(4) عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، المرجع السابق ص100 و ما بعدها .

على الجهاز و منها الفأرة ، مشغل الأقراص ، الماسح الضوئي ، مشغل الأسطوانات و لوحة المفاتيح و غيرها.

2- وحدات المعالجة المركزية : دور هذه الوحدات تلقي الأوامر عن طريق أجهزة الإدخال ثم معالجتها و إخراجها بالكيفية التي يرغبها مشغل الجهاز ، و هذه الوحدات تتمثل في وحدة الذاكرة الرئيسية و هي الوحدة التي تقوم بحفظ البيانات و النتائج بشكل مؤقت ، وحدة الحساب و المنطق و وحدات التحكم .

3- وحدات الإخراج : هي الوحدة التي من خلالها يتم إخراج النتائج و إظهارها بأشكال مختلفة مرئية و مطبوعة و منها الطابعات ، الشاشات ، مشغل الأقراص ، وحدات الأصوات و السماعات و غيرها.

4- وحدات التخزين : تعد من أهم الوحدات لإحتوائها على المعلومات و البرامج التي يستخدمها المستخدم في عمله و تمكنه من تخزين الملفات و برامج التشغيل المختلفة و منها الأقراص الصلبة ، المرنة ، أقراص الليزر ...

5- المودم : هي أجهزة تمكن الحاسبات من الإتصال ببعضها عبر خطوط معينة .

ثانيا المكونات الغير مادية : و هي أهم مكون لا قيمة للمكونات المادية دونها ، فهي روح الحاسب الآلي و تتمثل في البرامج و المعطيات .

- **البرامج :** يقصد بالبرامج بالمفهوم الضيق مجموعة من التعليمات ، فالبرنامج يرسل الأوامر إلى الجهاز لتنفيذها بناءا على توجيهات المستخدم [1]

و بالمفهوم الواسع يضم المفهوم إلى جانب التعليمات و الأوامر وصف البرنامج الكامل المفصل للعمليات بشكل شفوي ، خطي و غيره بغية تحديد مجموعة التعليمات المشكلة لبرامج الحاسب و صلة كل منها بالأخرى ، كما يتضمن المستندات الملحقة التي تهدف إلى تبسيط مفهوم البرامج و تطبيقاتها .

و هو ذات التعريف الذي أخذت به المنظمة العالمية للملكية الفكرية كالآتي :

---

(1) رشا علي الدين ، النظام القانوني لحماية البرمجيات بين نظرية تنازع القوانين و القانون الدولي الإتفاقي ، الطبعة الأولى ، مصر 2004 ص 80 .

" البرامج هي مجموعة من التعليمات التي تصبح بعد نقلها مقروءة من قبل الآلة لأداء أو إنجاز وظيفة أو مهمة أو نتيجة معينة عن طريق آلة قادرة على معالجة المعلومات."

و البرامج نوعان :[1]

1- برامج التشغيل : و تسمى كذلك برامج الإستغلال أو التنفيذ و هي التي تمكن الحاسب من أداء الوظيفة المحددة له ، و هي لهذا السبب تعتبر جزءا من الحاسب نفسه و يتولى الإشراف عليها برنامج مشرف أو مراقب لتنظيم أداء هذه البرامج بدورها .

2- برامج التطبيق : و تسمى برامج معالجة المعلومات و تقوم بتوجيه أقسام الحاسب الآلي ضمن النظام الذي وضع لها وفقا لأوامر البرامج التشغيلية المثبتة بالحاسب الآلي، أو بلوحات مستقلة يجري إدخالها في نظام الكمبيوتر فهي تجعل النظام يستخرج نتائج معينة مطلوبة من المستخدم .

- **المعطيات :** هي المعلومات و البيانات التي يتم تنظيمها و معالجتها داخل نظام المعالجة الآلية للمعطيات و تخزينها بغية إسترجاعها عند طلبها ، و المعطيات عبارة عن نبضات إلكترونية داخل الحاسب غير ملموسة [2]

و المعطيات عرفتها الإتفاقية الدولية للإجرام المعلوماتي في المادة الأولى من الفصل الأول فقرة ب على أنها : " عمليات عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر لما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها ."

و عرف الفقيه دون باركر المعلومات على أنها :

" مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل و الإتصال أو للتفسير و التأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية و هي تتميز بالمرونة بحيث يمكن تغييرها و تجزئتها و جمعها أو نقلها بوسائل و أشكال مختلفة."

---

(1) آمال قارة ، المرجع السابق ، ص23 .
(2) محمد خليفة ، المرجع السابق ص 25 .

و يميز بعض الفقه (مثل نائلة عادل محمد فريد فورة في المؤلف جرائم الحاسب الإقتصادية) بين المعلومات و البيانات فهذه الأخيرة تعبر عن الأرقام و الكلمات و الرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بينها و لم تخضع للتفسير أو الإستخدام، و تخلو من المعنى الظاهري احيانا ، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات [1]

فالبيانات تترجم data و المعلومات information .

و عن المشرع الجزائري لم يورد في قانون العقوبات تعريفا إنما عرف المعلومة بالمادة الثانية من القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال على أنها :

"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 ."

- **شبكات الإتصال :** و هي ذات طابع مادي تنقل المحتوى الغير مادي من المعطيات و يعمل على ربط الأجهزة و الأنظمة المعلوماتية المختلفة على المستوى المحلي أو الدولي التي تخضع لسلطة و تسيير العنصر البشري و لعل أهمها حاليا هو شبكة الأنترنيت .

المقصود بالأنترنيت : كلمة انترنيت (INTERNET) إختصار لمصطلحيين INTERCONNECTING-NETWORK و تعني الشبكة التي تربط مجموعة من أجهزة الكمبيوتر ببعضها البعض لتستطيع تبادل المعلومات ، و هي الشبكة التي أوجدها الجيش الأمريكي كوسيلة إتصال مستقلة و سريعة و إنطلق العمل بها رسميا بتاريخ 1969/01/02 ثم إنتشر هذا المشروع في منتصف السبعينات و تبنته هيئات التدريس في الجامعات لتبادل البيانات العلمية و الفنية و كان يسمى ARPA-NET و

(1) طارق إبراهيم الدسوقي عطية ، المرجع السابق ص 38

هو إختصار لـ " وكالة مشروعات البحوث المتقدمة ." [1]

إلا أن الإنتشار الحقيقي للأنترنيت كان عام 1980 و منذ ذلك التاريخ و هذه الشبكة في تطور و إنتشار و ما يساعد على ذلك عدم إنتمائها لأحد حيث يجري من خلالها تبادل المعلومات على المستوى العالمي بإستخدام الكتابة و الإتصالات الصوتية و المرئية .

و يعرف الإعتداء على أنظمة المعالجة الألية للمعطيات بأنه الإستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الإستخدام المتعمد الضار لأجهزته و ملفات البيانات .

المطلب الثالث : ضرورة خضوع نظام المعالجة الآلية للمعطيات لحماية فنية

مع خلق شبكات إتصال سلكية و لا سلكية أصبحت من خلالها الحواسيب في كل العالم متصلة بشبكة عالمية ، و أصبح تناقل المعلومات خلال أنظمة معالجة يفرض تأمين بقاء المعطيات سرية مما يجعل المتخصصين بهذا المجال في بحث دائم لإيجاد برامج تشفير لنقلها في سرية تامة .

و هنا يطرح إشكال بصدد دراسة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حول مدى وجوب توافر حماية فنية لأي نظام ليتمتع بالحماية الجزائية المنصوص عليها بقانون العقوبات ؟ أو هل يكفي الإعتداء على النظام بإحدى الصور المنصوص عليها في قانون العقوبات و التي سنأتي على دراستها بالفصل الأول دون أن يكون النظام محمي وجوبا مسبقا لتقوم الجريمة ؟

فقها إختلفت الآراء بهذا الشأن إذ يرى إتجاه بضرورة تقييد الحماية الجزائية بوجوب توافر عنصر الحماية الفنية بداية ، فوجب أن تخضع الأنظمة و المعطيات لنظام أمني إذ من غير المنطقي حماية معلومات تركها القائمون عليها مهملة و متاحة لأي كان .

و تطبيقا لهذا الرأي إذا صنفنا أنواع الأنظمة للأصناف الثلاث التالية :

---

(1) صالح أحمد البربري ، المرجع السابق ص 1 .

- أنظمة مفتوحة للجمهور .
- أنظمة قاصرة على أصحاب الحق فيها و لكنها دون حماية.
- أنظمة قاصرة على أصحابها و تتمتع بحماية فنية.

فإن الفئة الأخيرة فقط هي التي تتمتع بالحماية الجزائية لأنه من الطبيعي أن يعمل القائم على الأنظمة بوضع وسائل لحمايتها و القانون لا يحمي إلا الأشخاص الحرصين على أموالهم ، و فرض هذا الرأي من شأنه دفع مستعملي الأنظمة لإستخدام أنظمة الحماية و تطبيق الدور الوقائي .

أما الرأي الغالب في الفقه الفرنسي يرى وجوب خضوع النظام لحماية فنية ذلك أن وجوب الشرط لا يكون له سوى دور واحد هو إثبات سوء نية من قـــام بإنتهـاك النظـــام و الدخول إليه بطريقة غير مشروعة و يدخل ذلك في عبء إثبات القصد الجنائي [1]

و من جهة أخرى خضوع الأنظمة لنظام حماية أمني يسهل من إكتشاف أي إختراق و تعدي عليها ، و يثبت القصد الجنائي المتعمد لإرتكاب الجريمة و يسهل من إكتشاف الجريمة ، و التي تترك أثرا في هذه الحال كإلغاء كلمة السر أو تغييرها .

و في هذا الشأن لدى تعريف مجلس الشيوخ الفرنسي للنظام المعلوماتي أشار إلى أن النظام لابد ان يكون محمي بجهاز أمان و أن الأنظمة المحمية وحدها التي تحظى بالحماية الجزائية [2]

الرأي الثاني يري بوجوب تمتيع كل الأنظمة و المعطيات بالحماية الجزائية بغض النظر على إحتوائها على نظام أمان ، و هذا الإتجاه أخذت به محكمة الإستئناف في باريس في قرار لها صادر سنة 1994 أشارت في حيثياته أنه ليس من اللازم لقيام جريمة الدخول الغير شرعي أن يكون الفعل قد تم مخالفا لتدابير أمنية ، بل يكفي لقيام الجريمة أن يتم ذلك ضد إرادة المسؤول عن النظام .

---

(1) جباري عبد المجيد ، المرجع السابق ، ص 109 .

(2) محمد خليفة ، المرجع السابق ، ص 134 و 135

و على العكس من هذا تم بالمقابل إلغاء حكم لمحكمة باريس صادر بتاريخ 2002/02/13 في قضية شركة (طاتي) الذي جاء فيه أن عدم إحترام الشركة لقواعد تأمين المعطيات لا يشكل مبررا للمتهم للولوج بغير حق للنظام مع علمه بأن دخوله و بقائه كان عن طريق الغش ، و هو الحكم الذي ألغي بالقرار الصادر 2002/10/30 على أساس أنه لا يمكن محاسبة شخص على دخول نظام في متناول العامة لم يكن موضع حماية [1]

بالرجوع إلى قانون العقوبات الجزائري نجد أن المشرع الجزائري لم ينص على ضرورة أن تكون أنظمة المعالجة الآلية للمعطيات محمية فنيا لتتمتع بالحمايـة الجزائيـــة عند المساس بها ، بمعنى أنه إستبعد هذا الشرط كما أنه و من الناحية العملية فإن أغلب الأنظمة تتمتع بنظام حماية فنية إلا ما كان منها و منذ البداية موضوع للجمهور و وجود و عليه ما يستخلص من هذا أن كل الأنظمة تتمتع بالحماية الجزائية لنصوص قانون العقوبات الجزائري سواء كانت محمية بنظام أمني أم لا متى توافرت أركان الجريمة من ركن مادي و ركن معنوي .

(1) الملحق رقم 09 قرار صادر بتاريخ 2002/10/30 عن محكمة الإستئناف باريس الغرفة 12.

المبحث الثاني : خصائص الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات

المطلب الأول : خصائص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تعتبر جرائم المساس بأنظمة المعالجة الآلية للمعطيات من الجرائم المستترة التي تتم بسرعة و تتسم بالتطور في أساليب إرتكابها ، و هي أقل عنفا في التنفيذ ، و عابرة للحدود و يصعب إثباتها لعدم وجود أدلة مادية عليها ، كما يسهل إتلاف الأدلة الخاصة بها خاصة مع نقص الخبرة لدى الجهات القائمة على الضبط و عدم كفاية القوانين القائمة.

تعد هذه الجرائم و جل الجرائم المتعلقة بالمعلوماتية أكثر أنواع الإجرام المعاصر المثير للإشكالات القانونية إذ يتم بالمكر ، الحيلة و الدهاء و الغش في إستخدام تقنيات معلوماتية عالية الكفاءة و التي أصبحت سهولة إستخدامها و سرعة إنتشارها من الوسائل الأساسية لإرتكاب هذا النوع من الجرائم [1]

و هذا ما سينعكس بدوره على صعوبة إثبات الجريمة ، و يسهل إرتكابها و يسهل طمس معالمها ، إذ يستطيع الجاني إرتكاب الجريمة دون ترك أثر خارجي ملموس، إضافة لأن هذه الجرائم من الجرائم العابرة للحدود الوطنية غالبا إذ يتم الفعل من مكان لتحقق النتيجة على مسافات بعيدة دون أن يتمكن المجني عليه من معرفة مصدر الإعتداء .

و بما أن هذه الجرائم تقع على أمور معنوية المتمثلة في أنظمة معالجة و معطيات بإستخدام وسائل مستحدثة التي أوجدتها ثورة المعلومات الأمر الذي يجعل من هذه الجرائم تتميز بعدة خصائص تنفرد بها لا تتوافر بالجرائم بالمفهوم التقليدي سواء من حيث أسلوب و طرق إرتكابها أو مرتكبيها و منها ما يلي :

(1) محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات و الكمبيوتر ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة ، ص 25 .

1- هي جرائم عابرة للحدود ذات طابع دولي لا تعترف بالحدود إذ تقع بدولة ليمتد أثرها لدولة أخرى أو أكثر ، و لعل هذه الخاصية أهم خصائصها فمع وجود الشبكات المعلوماتية الغير مرئية الحدود فإن تبادل المعلومات يتم بين الأنظمة و بين الدول في ثواني مما ينعكس على تنفيذ الجريمة أيضا سرعة هائلة و يختفي أثرها بذات السرعة .

2- صعبة الإكتشاف لأنها لا تترك أثرا كونها معنويات و هو ما سنأتي على شرحه تفصيلا لدى التطرق لصعوبة الحصول على الأدلة الإلكترونية و إشكال صعوبة الإثبات في الفصل الثاني من هذه الدراسة .

3- لا يتصور أن ترتكب دون حاسب آلي عبر شبكات إتصال و أنظمة معلوماتية.

4- الجاني في هذه الجرائم على خبرة عالية في مجال الإعلام الآلي ، متمكن من إستعمال البرامج و أنظمة المعالجة و مواكب للتقنيات الجديدة .

5- هي جرائم خفية و مستترة في أغلبها فالضحية لا يلاحظها و الذي يمكن أن يكون متواجد في النظام أثناء وقوعها إلا أنه لا ينتبه لها إلا بعد حدوثها بسبب التعامل مع ذبذبات غير مرئية تكون غالبا في شكل فيروسات مدسوسة .

6- سرعة التطور في إرتكاب الجريمة فالتطور السريع للتكنولوجيا له إنعكاس مباشر على تطور و نشأة هذه الجرائم إذ يستفيد الجاني أيضا منه لتطوير خبراته الإجرامية و تبادلها مع غيره .

7- إنعدام العنف و الجهد العضلي إذ لا تتطلب مجهودا جسديا عنيفا لتنفيذها و التي يمكن أن ترتكب بمجرد الضغط على زر لإعطاء أمر لإتلاف النظام .

8- عدم وجود مفهوم مشترك لهذه الجريمة : [1] من خصائص هذا الجرائم عدم وجود مفهوم مشترك لماهية الجريمة و تعريف قانوني موحد لها ، و لعل السبب في ذلك يرجع لعدم وجود تنسيق دولي و عدم وجود معاهدات دولية ثنائية أو جماعية تبعا لإختلاف النظم القـــانونيـــة ، و لا شك أن ذلك يتطلب إيجاد وسائل مناسبة

(1) خالد ممدوح إبراهيم ، التقاضي الإلكتروني، المرجع السابق ص 326 .

لتشجيع الدول لمواجهة هذه الجرائم و العمل على سن تشريعات لمواجهتها و إبرام إتفاقيات لتبادل المعلومات و الخبرات و تسليم المجرمين .

و وقوع هذه الجرائم في بيئة المعالجة الآلية للمعطيات يستلزم التعامل مع بيانات مجمعة و مجهزة لدخول الحاسب بغرض معالجتها إلكترونيا بما يمكن المستخدم من إمكانية كتابتها في الحاسب الذي تتوافر فيه إمكانيات لتصحيحها ، تعديلها ، محوها ، تخزينها ، إسترجاعها و طباعتها ، و هذه العمليات وثيقة الصلة بإرتكاب الجرائم و كذلك التعامل مع مفردات جديدة كالبرامج و البيانات التي تشكل محلا للإعتداء [1]

المطلب الثاني : سمات الجاني في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

نظرا لما تتسم به هذه الجرائم من خصائص فإنها تتطلب مقدرة عقلية و ذهنية و درجة عالية من الذكاء لدى الجاني ، إذ لا يتطلب الأمر هنا قدرة جسدية و لا يميل الجاني لإستعمال العنف إنما يستعمل قدراته التقنية في إستعمال الحاسب الآلي و التحكم العالي في البرامج و التلاعب بها ، بغض النظر عن الدوافع و الأهداف المرجوة من الجريمة.

و عادة ما يكون الجاني من النوابغ يتميز بمستوى رفيع من الذكاء بما يمكنه من التغلب على العقبات و فك الشيفرات و كلمات المرور التي تواجهه أثناء إرتكاب الجريمة ، حتى يتمكن من إتلاف المعلومات أو التلاعب فيها و بالأنظمة التي تحويها مما يؤدي لتدميرها كليا أو جزئيا.

و ما يميز الجاني أيضا أنه متكيف إجتماعيا عكس الجناة بالمفهوم التقليدي كمرتكبي جرائم الإعتداء بالعنف الذين يظهرون كأعداء للمجتمع ، و هذا ما يزيد من خطورة الجاني الذي يبقى مخفيا كفرد صالح بالمجتمع و يطور أساليب متجددة لذلك .

(1) هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية القاهرة ، طبعة 1992 ص 15

هناك من الفقه من لخص سمات المجرم المعلوماتي في الآتي : [1]

1- المجرم المعلوماتي مجرم متخصص فقد ثبت في العديد من القضايا أن عددا من المجرمين لا يرتكبون إلا جرائم الكمبيوتر .

2- المجرم المعلوماتي مجرم عائد إلى الإجرام إنطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليه و تقديمه للمحاكمة في المرة السابقة .

3- المجرم المعلوماتي مجرم محترف ذلك أنه لا يسهل على الشخص العادي أن يرتكب هذه الجرائم إلا في حالات قليلة فالأمر يقتضي كثيرا من الدقة و التخصص في هذا المجال و ذلك لأجل التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر .

و يصنف الفقه المجرم المعلوماتي لعدة نماذج أهمها : [2]

1- القراصنة (les pirates) : و هم أنواع

- الهواة الهاكر (hackers) هم عادة شباب فضوليون يسعون للتسلية و لا يشكلون خطورة على الصناعات و أنظمة المعلوماتية.

- المحترفون الكراكر (crackers) و هم الصنف الأكثر خطورة الذين يحدثون أضرار كبيرة و قد يؤلفون أندية لتبادل المعلومات فيما بينهم و يسعون لتحقيق ضرر بالأنظمة.

2- المخادعون (fraudeurs) : هؤلاء يتمتعون بقدرات فنية عالية بإعتبارهم من الإخصائيين في المعلوماتية و من أصحاب الكفاءات ، و هم نوعان المخادع الداخلي و هو أخصائي في المعلوماتية يتمتع بقدرة تقنية عالية يسعى لإلحاق ضرر بالمؤسسة التي يعمل بها مستعملا الوسائل الموضوعة تحت تصرفه ، و نجد المخادع الخارجي و هذا يستفيد عادة من تواطؤ إرادي أو غير إرادي من ضحاياه يسعى لجمع أكبر قدر من المعلومات بالوسائل المتاحة له بواسطتهم .

---

(1) عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، المرجع السابق ص 80 .
(2) وليد عاكوم بحث بعنوان التحقيق في جرائم الحاسوب ص 2 مأخوذ من الموقع الإلكتروني www.arablawinfo.com

3- الجواسيس (espions) : و هم نوعان جواسيس الدولة و الخواص يتمتعون بكفاءة عالية من الصعب إكتشافهم ، هدفهم جمع المعلومات لصالح دولتهم أو لصالح الأشخاص أو المؤسسات التي يعملون لصالحها أو مؤسسات متنافسة فيما بينها .

4- الإرهابيون : و هم الأخطر إذ يقومون بتدمير المواقع و الصفحات الإلكترونية من خلال القيام بعمليات إستعراضية و تقنية لأغراض إنتقامية .

و يرى الأستاذ دون باركر أن المجرم المعلوماتي ينتمي لطائفة خاصة من المجرمين تقترب في سيماتها من جرائم ذوي الياقات البيضاء ، و إن كانت لا تتطابق معها فمن ناحية ينتمي المجرم المعلوماتي إلى وسط إجتماعي متميز على درجة من العلم و المعرفة كذوي الياقات البيضاء إلا أنه ليس من الضروري أن يرتكب جريمته من خلال مهنة معينة كهذه الفنة. [1]

و صنف الفقيه دون باركر المختص بالجريمة المعلوماتية بمعهد ستانفير أشكال ظهور الجاني إلى سبع فئات : [2]

1- الهواة

2- المهوسون : و هم الذين يرتكبون الجريمة بإستخدام العنف الذي من الصعب تصوره في المجال المعلوماتي .

3- الجريمة المنظمة : فالحاسوب و ما يتضمنه من أنظمة أصبح وسيلة في تنفيذ الجرائم كقاعدة البيانات التي تملكها عائلة (جيلبرتو رودريقيز) في كولومبيا المختصة في تجارة الكوكايين .

4- الحكومات الأجنبية : تستغل الأنظمة للجوسسة .

(1) طارق إبراهيم الدسوقي عطية ، المرجع السابق ،ص 175 .
(2) دون باركر ، جرائم الكمبيوتر و حماية المعلومات 1998 ، ص 114 و ما بعدها

5- النخبة: هم متخصصون في أجهزة الإعلام الآلي و أنظمته الذين يسود الإعتقاد لديهم أن سمات وظائفهم المرموقة و خبرتهم في إستعمال الأنظمة لأهداف شخصية أو للتنافس مما يؤدي بهم للتمادي في إستخدامها بطرق غير مشروعة تصل لحد إرتكابهم الجرائم.

6- المتطرفون : الذين يستخدمون الأنظمة لنشر أفكار بدافع أو لمذهب معين ديني أو سياسي أو إقتصادي مثل مجموعة (الألوية الحمراء) بإيطاليا .

7- المخربون : هم الذين يرتكبون الجريمة إرضاءا لرغباتهم .

و إرتباط هذا النوع من الجرائم بالحاسب الآلي لا يجعل الجرائم مميزة عن الجرائم التقليدية بل يترك أثره على الجاني أيضا كما بينا و يعد الأستاذ باركر واحد من أهم الباحثين في الجريمة المعلوماتية بصفة عامة و الذي يرمز إلى سمات المجرم في هذا المجال بكلمة skram و تعني :

المهارة (skills)، المعرفة (knowleg) ، الوسيلة (resources) ، السلطة (authority) ، الباعث (motives) .

1- المهارة : المهارة هي أبرز سمات المجرم المعلوماتي التي يكتسبها عن طريق الدراسة المتخصصة ، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الإجتماعي مع الآخرين ، إلا أن هذا لا يعني بالضرورة أن يكون على قدر كبير من العلم إذ أثبت الواقع العملي أن بعض من أخطر المجرمين المعلوماتيين لم يتلقوا المهارة الكافية عن طريق التعلم .

2- المعرفة : تتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها و إمكانات نجاحها أو إحتمال فشلها ، فالمجرم المعلوماتي يمكن أن يكون له تصور كامل عن الجريمة لأنه يرتكبها داخل نظام يعرف كل تفاصيله و يمكنه تطبيق جريمته على أنظمة مماثلة .

3- الوسيلة : هي الإمكانيات التي يتزود بها الجاني لإتمام جريمته ، و عادة في هذا المجال الوسائل المادية المستعملة في التلاعب بالأنظمة بسيطة قد لا تتعدى حاسوب متصل بشبكة معلوماتية إضافة لمهارات الجاني الذهنية و هي الوسيلة الأهم .

4- السلطة : هي الحقوق و المزايا التي يتمتع بها الجاني ، فقد يكون شيفرة خاصة للدخول للنظام التي تعطي الجاني مزايا فتح الملفات ، تعديلها ، محوها ... أو قد يكون حق إستعمال الحاسوب و إجراء معاملات ، و قد يستخدم الجاني سلطة غير مخولة له كشيفرة خاصة بشخص آخر .

5- الباعث : قد لا يختلف الباعث في هذه الجرائم عن الجرائم التقليدية فقد يكون الرغبة في تحقيق ربح مادي بطريق غير شرعي و هذا يظل الباعث الأول في إرتكاب أغلب الجرائم ثم يأتي بعده الرغبة في قهر أنظمة الحاسب و تخطي حواجز الحماية الموضوعة ، و أخيرا قد يكون الباعث هو الإنتقام من رب العمل أو أحد الزملاء مثلا.

و في مقابل ذكر صفات الجاني ففيما يتعلق بالمجني عليه في هذا النوع من الجرائم لا يمكن حصره في فئات معينة فيستحيل تحديد صفات ضحايا هذه الجرائم بميزات معينة ، إذ يمكن أن يكون شخصا طبيعيا أو معنويا و يمكن أن يمارس أي نشاط دون تحديد إقتصادي ، إجتماعي ، سياسي أو عسكري ، غير أن القاسم المشترك بينهم جميعا هو وقوعهم ضحية لجريمة ماسة بالمعطيات و الأنظمة المعلوماتية .

المطلب الثالث : أساليب إرتكاب الجرائم الماسة بأنظمة المعالجة الألية للمعطيات

سنبين في الفصل الأول لاحقا تفصيلا صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، و نبين الركن المادي المكون لكل جريمة ، غير أن تحقق هذا الركن يتم بأسلوب معين في تنفيذه ، و الأساليب المعتمدة من الجاني في هذه الجرائم هي أساليب تقنية في غالب الأحيان تبدو معقدة عادة ، و يمكن حصرها في نوعين من الإعتداءات منطقية و مادية.

أولا : الإعتداءات المنطقية (attaques logiques)

تشمل هذه الإعتداءات البرامج و البيانات و المعطيات المخزنة في الحواسيب و هي عديدة نذكر فيما يلي أمثلة عن هذه الإعتداءات :

1- القنبلة المعلوماتية (bombe informatique) : و هو برنامج يعده مصمم معلوماتي و يثبته على أن يعمل بعد إنقضاء مدة محددة على إستعمال النظام بهدف تدميره أو تعطيله أو محو بياناته و هي نوعان :

- القنبلة المنطقية (logic bomb) : و هي برنامج ينفذ في لحظة محددة يتم وضعه في شبكة للمعلومات يحدد هدفها في ظرف معين بغرض تسهيل تنفيذ عمل غير مشروع ، مثلا يوضع برنامج للبحث في نظام و إزالة حرف معين من السجلات المخزنة و عليه يتم حذف كل مستفيد من النظام تم حذف هذا الحرف من إسمه .

- القنبلة الزمنية (time bomb): ينطلق عملها في زمن أو تاريخ محدد أي موعد بذاته محدد مسبقا في برنامج القنبلة ، و من امثلتها قضية حادثة شركة أوميغا أن قام موظف بدافع الإنتقام بوضع برنامج لإتلاف بيانات الشركة التي طرد منها ليتم ذلك بعد ست أشهر من مغادرته .[1] و فيروس shernoble شرنوبيل و هو فيروس ينشط كل يوم 26 من كل شهر و يزداد تدميرا شهر أفريل إخترعه (شن ينج) و هو تايواني الجنسية ، يستهدف هذا الفيروس القرص الصلب للجهاز و يدمر البيانات الموجودة بحيث لا تظهر على الشاشة ، كما يوهم المستخدم أنه ألغى التقسيمات الموجودة على القرص الصلب مما يدفعه لإعادة تهيئته و محو ما فيه ، و أخذ الفيروس تسميته من حادثة إنفجار في مفاعل تشرنوبيل النووي بأوكرانيا عام 1986.

(1) الملحق رقم 08 نماذج من الإعتداءات على أنظمة المعالجة الألية للمعطيات .

أيضا ما حدث في جامعة مونماوث في الولايات المتحدة الأمريكية إذ تم وضع قنبلة إستهدفت نظام البريد الإلكتروني للجامعة الذي ترتبط به أعمال و أنشطة على درجة عالية من الأهمية ، كالتسجيل و تبادل الأبحاث و حتى دفع الرسوم ، فإنهار النظام و قدرت الخسائر بعشرات الألاف من الدولارات و تم معرفة الفاعل الذي حاول تبرير ذلك بأنه لم يقصد التخريب و النتيجة التي تحققت . [1]

2- برنامج الدودة (worm-ver) : هو برنامج يستغل أي فجوة كي ينتقل من جهاز حاسوب لآخر و يتكاثر أثناء ذلك كالبكتيريا و ينتج نسخ منه ليشغل أكبر مساحة في الشبكة للتقليل من كفاءة الجهاز ، و أحيانا يتعدى ذلك للتخريب الفعلي للملفات الموجودة و البرامج و أنظمة التشغيل .[2] إذ يعمل على التشويش على البرامج المعلوماتية و يشل قدرتها على تبادل المعلومات .

3- الفيروس (virus) : هو برنامج يشبه الجراثيم التي تهاجم جسم الإنسان إذ يتكاثر لهدف ضار هو تدمير الأنظمة المعلوماتية ، يتميز بالقدرة الهائلة على الإختراق و الإنتشار و التدمير بكيفية لا يمكن معها إسترجاع الملفات إذ يتم مسحها نهائيا و يملأ مكانها بالنفايات ، إذ يعمل على نسخ نفسه في البرنامج الذي يصيبه و يتحكم به كما يميز البرامج المصابة بالعدوى بتحكم بعد إصابتها مرة أخرى ، و لدرء مخاطر الفيروسات يتم صنع البرامج المضادة للفيروسات (anti-virus) و رغم ذلك تضل الفيروسات تتسلل ببرامج مقرصنة .

و أنواع الفيروسات كثيرة و متنوعة الأهداف منها : [3]

- فيروس قطاع التشغيل : و هو من أخطر الأنواع إذ يقوم بزرع نفسه في قطاع التشغيل أو الإقلاع (البدء) مما يمنع المستخدم من تشغيل الجهاز .

---

(1) محمود أحمد عبابنة ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر و التوزيع عمان ، الطبعة الأولى 2009 ص 104 .

(2) نصرون وردية ، الغش المعلوماتي ، المجلة القضائية العدد 1 سنة 2002 ص 109 .

(3) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، المرجع السابق ، ص 429.

- فيروس الملفات : و يسمى أيضا بفيروسات البرامج و هي التي تربط نفسها بالتطبيقات و الملفات التنفيذية و تتكاثر بتنشيط التطبيق المصاب و تقوم بإصابة ملفات جديدة .

- الفيروسات المتعددة : تصيب كلا من قطاعي التشغيل و الملفات و هي الأسرع في التكاثر.

-الفيروسات الطفيلية : تربط نفسها ببعض الملفات حتى تتكاثر و تضيف عدة سطور للملف المصاب فكلما عمل الملف تكاثر الفيروس .

- الفيروسات المرافقة : لا تهاجم إلا الملفات التنفيذية فكلما عمل هذا الملف في التشغيل عمل بدوره الملف الملوث .

- الفيروسات الإستبدالية : هنا يبحث الفيروس عن ملف و يستبدله بملف من ذات الحجم ملوث و يدمر الأصلي ليبدو أنه موجود إلا أنه لا يعمل .

- فيروس الماكرو : يؤثر خاصة على برامج ميكروسوفت أوفيس غالبا يعدل الأمر (حفظ) ليشغل نفسه تلقائيا بعد ذلك .

- الفيروسات المتحولة : هي التي تتبدل أوامرها كلما إنتقلت من جهاز لآخر عادة هي فيروسات رديئة سهلة الإزالة .

4- حصان دروادة (cheval de troie) : سمي بهذا الإسم نسبة للأسطورة اليونانية الشهيرة التي تروي قصة الحصان الخشبي الذي تم تقديمه كهدية و عربون سلام ، و الذي كان يحوي بداخله غزاة دخلوا المدينة و إستولوا عليها ، و كبرنامج فإنه يتضمن وظائف يعرفها الجاني فقط تبدأ بالعمل عند الدخول للنظام دون علم المستعمل الشرعي.

و هو برنامج خادع خفي يظهر كبرنامج عادي يؤدي مهام مؤلوفة بينما يكون بصفة خفية ينفذ أوامر و تعليمات تؤدي عند إعادة التشغيل لأضرار غير متوقعة و مثال ذلك في الولايات المتحدة الأمريكية وجد برنامج عرف بإسم (zoxoon) يبدو عند بداية تشغيله أنه ألعاب تسلية إلا أنه يقوم بذات الوقت بمحو أقراص النظام ، أيضا برنامج (filer) الذي يبدو ظاهريا كبرنامج لتنظيم الملفات في حين يقوم في الحقيقة بمحوها

و عادة ما توجد برامج أحصنة طروادة في برامج العمال كبرامج معالجة النصوص و الجداول للتلاعب برواتبهم و مستحقاتهم و تعطي نتائج غير صحيحة و هي بخلاف الفيروسات لا تنسخ نفسها و هي بالغة الصعوبة لإكتشافها .

و مثالها أيضا ما حدث سنة 1989 عندما تم إرسال 000 20 شريطا يحتوي ظاهريا على برامج معلومات حول مرض السيدا إلى كافة أنحاء العالم ، و تضمن عبارة في بنود الإستعمال أنه في حال عدم دفع الثمن لإستعماله تتخذ إجراءات ضد اللوجسيال و هي عبارة لا يمكن التنبه لها من كل المستخدمين ، و ما حدث عند الإستعمال المباشر أن البرنامج يقوم بتخريب كل المعلومات المخزنة على الكمبيوتر و هذا هو معنى عبارة إجراءات تتخذ ضد اللوجسيال .

5 – الفخ أو الخبيئة (trap) [1] و هي نقطة دخول أو منفذ يجهز مسبقا في نظام معلوماتي من قبل مصممه يسمح له لاحقا بإنزال برامج خاصة من شأنها أن تعيق سير عمل هذا النظام المعلوماتي و أن تدخل إليه عناصر إعاقة لتطبيقاته .

6 – الخداع (mystification) : يهدف للإيقاع بمستعمل مرخص له بالإستعمال من أجل الإستيلاء على المعلومات التي تسمح له بالنفاذ لها كإسمه أو كلمة المرور الخاص به و غير ذلك.

7- التسلل (faufilement) هو الدخول وراء المستعمل المرخص له و تخطي نقطة مراقبة الدخول .

8- سلامي (salami) تسمح هذه التقنية بأخذ معلومات مجزئة أو مشتتة من نظام معلوماتي معين و من ثمة العمل على تجميعها تدريجيا .

---

(1) وليد عاكوم ، المرجع السابق ، ص 4 .

ثانيا : الإعتداءات المادية (attaques physiques)[1]

1- الإعتراض المتعمد للبيانات (interception) و يقصد به رصد الإشارات الكهرومغناطسية في الأنظمة المعلوماتية و تحليلها بغية إستخراج المعلومات المفهومة أو المقروءة منها.

2- التشويش (brouillage) و يهدف لإعاقة تشغيل النظام مما يؤثر على سرعته و سلامة معلوماته .

3- التخريب : يضع المعلومات الموجودة بالنظام خارج الخدمة .

4- التنصت (ecoute) : يتم بالتمركز داخل نظام معين و تسجيل و حفظ المعلومات المعالجة فيه و البيانات المتبادلة فيما بين الأنظمة المعلوماتية .

5- التجسس : يهدف للحصول على معلومات إستراتيجية عسكرية ، سياسية أو إقتصادية لها طابع سري .

6- التفخيخ (piegeage)[2] : و يحصل عندما يعمد المعتدي إلى إدخال وظائف خفية في مرحلة تصميم أو تصنيع أو نقل أو صيانة النظم .

(1) منير محمد الجنبيهي ، أمن المعلومات الإلكترونية ، دار الفكر الجامعي الإسكندرية 2005 ص 36.
(2) وليد عاكوم ، المرجع السابق ص 5.

المبحث الثالث : الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات

بعد التعرف على ماهية أنظمة المعالجة الآلية للمعطيات و دراسة خصائص هذه الجرائم التي تبين و دون شك خطورتها و جسامة آثارها ، مما يدفع بنا للتساؤل حول أهمية الحماية الجزائية في هذا النوع من الجرائم ، مع وجوب دراسة دوافع إرتكاب هذه الجرائم مقارنة بالجرائم التقليدية و بواعث حماية هذه الأنظمة .

و أخيرا نعرض أهم إجراءات الحماية الجزائية التي تبنتها الدول سواء على مستوى التشريع الداخلي أو في إيطار التعاون الدولي .

المطلب الأول : دوافع إرتكاب الجرائم الماسة بأنظمة المعالجة الألية للمعطيات

لكل جريمة باعث على إرتكابها و هو الغرض أو الغاية التي يهدف الجاني لتحقيقها ، و فيما يلي نحاول البحث في الدافع لإرتكاب هذا النوع من الجرائم ذات الطبيعة الخاصة و البحث في أهدافها و هل تختلف عن أهداف الجرائم التقليدية ؟

و يمكن تقسيم دوافع إرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى دوافع شخصية و دوافع خارجية .

أولا : الدوافع الشخصية و تنقسم لمادية و ذهنية :

1- الدوافع المادية : يعتبر السعي لتحقيق الكسب المالي من بين أكثر الدوافع لإرتكاب أغلب الجرائم بصفة عامة و ليس دافعا لإرتكاب الجرائم الماسة بأنظمة المعالجة وحدها و بالأخص في هذه الجرائم فإن هدف تحقيق الكسب المالي يحتل المرتبة الأولى نظرا لما تتيحه تقنيات المعلوماتية من الربح الكبير الممكن تحقيقه بجهد بسيط .

و أشار دون باركر في دراسة له أن 43 بالمئة من جرائم الغش المعلوماتي المعلن عنها أرتكبت من أجل الحصول على المال ، و وفقا لعدة دراسات فإن القطاع المالي يعد أكثر القطاعات إستهدافا من هذه الجرائم لأنها تعتمد بشكل أساسي على الأنظمة الإلكترونية كالبنوك ، كما أن شركات التأمين تعد من القطاعات المستهدفة لعمليات النصب و الإحتيال كما حدث لشركة (أكويتي فنذنغ) بلوس أنجلس الأمريكية التي تمكن

مستخدموها من خلال خرق نظامها من خلق عملاء وهميين مؤمن عليهم و تم بيع 46000 بوليصة تأمين .[1]

و مثال ذلك في دراسة مقارنة في فرنسا سنة 1986 قيم عائد إرتكاب سرقة مع حمل سلاح بـ 000 70 فرنك فرنسي في حين عائد جريمة الغش المعلوماتي قدر بـ 000 670 فرنك فرنسي .

و هناك فئة من مرتكبي هذه الجرائم تكون الديون المالية هي الدافع لإرتكاب الجريمة و إستخدام أي وسيلة متاحة لتسديدها .

2- الدوافع الذهنية : هنا يكون دافع الجاني هو إثبات الذات في مجال التقنيات المعلوماتية بقهرها مهما كانت معقدة ، أكثر من الرغبة في الحصول على الربح ، فيبحث الجاني عن نقاط الضعف في النظام و يستغلها في إختراقه و التلاعب بمعطياته.

و هذا الدافع عادة لا ينبني على خطورة إجرامية فالجاني عادة ليس من معتادي الإجرام بل يرغب في تحدي النظام بمحاولة إختراقه و مثال ذلك ما حدث لوزارة الدفاع الأمريكية التي تقوم بتغيير أنظمة الترميز يوميا للحفاظ على الأمن ، بالمقابل يوجد متسابقون لخرق هذه الأنظمة لإظهار تفوقهم و دليل ذلك كا قام به أحد الهواة في أوروبا الذي تمكن من حل تشفير أحد مراكز البنتاغون و عبث بها .[2]

ثانيا: الدوافع الخارجية :

في بعض الأحيان يكون الدافع لإرتكاب الجريمة هو نتاج تأثر الجاني بعوامل خارجية أثناء تواجده في بيئة لمعالجة المعطيات و عليه يؤول الأمر لإرتكاب الجريمة إما بدافع الإنتقام ، التعاون ، التواطؤ مع شخص آخر أثر عليه أو إضرارا بالغير أو أن يرتكبها تحت التهديد مثلا .

(1) محمود أحمد عبابنة ، المرجع السابق ص 24
(2) محمود أحمد عبابنة ، المرجع السابق ص 25

و مثال ذلك أن يعمد موظف بعد طرده لتدمير أنظمة المؤسسة التي كان يعمل بها بدافع الإنتقام و إضرار برب عمله ، أو أن يرتكب عامل الجريمة بسبب ضغط العمل و توتر علاقة العمل بينه و بين رب عمله .

و قد تكون الدوافع سياسية إذ يتم تسخير شبكات المعلوماتية يوميا من قبل أجهزة المخابرات و الأفراد أيضا الذين يسعون لخرق الأجهزة الأمنية الحكومية مثال ذلك أن إستطاع ثلاث إخوة من قرية "كفر قاسم" بفلسطين إختراق نظام الموساد علما أنهم فاقدي البصر و تمكنوا من التصنت على المكالمات و تقديم معلومات إلى السلطة الفلسطينية ، كذلك تعطيل الموساد لموقع حزب الله نهاية عام 2000 عند إنطلاق الانتفاضة . [1]

المطلب الثاني : بواعث حماية أنظمة المعالجة الآلية للمعطيات

من الضروري نظرا لخصوصيات هذا النوع من الجرائم و خطورتها و آثارها الوخيمة بسط وسائل الحماية على النظم المعلوماتية لأن ذلك من شأنه تحقيق أمن المعلومات المتعلقة بأسرار أفراد المجتمع و تأمين إستثماراتهم التي تعتمد بصفة مباشرة على تكنولوجيات المعلومات ، ففرض حماية من شأنه تشجيع الإبتكار و دفع التطور العلمي و التقني و رقي المجتمع لتحقيق أهداف الدولة الإقتصادية التعليمية و غيرها .

و فيما يلي نعرض أهمية وجود نظام حماية و أهم الأسباب التي جعلت من الدول تبرم إتفاقيات دولية تصدر من خلالها توصيات ، لسن قوانين داخلية تهدف لوضع حماية جزائية من هذه الإعتداءات .

أولا : أهمية وجود نظام حماية : تظهر من جانبين

1- **على المستوى الشخصي :** وجود نظام حماية يكفل حماية المعلومات الشخصية و أسرار الأفراد و حياتهم الخاصة من الخطر التي أصبحت كلها محفوظة في شكل أنظمة معلوماتية مجمعة و محفوظة ، ومع وجود خطر إستعمالها بشكل سلبي فيجب

---

(1) محمود أحمد عبابنة ، المرجع السابق ص 26

2- **على المستوى الموضوعي :** حماية النظم المعلوماتية يشجع الأفراد على الإبتكار و الإثراء العلمي ليكفل تقدم الدول على كل الأصعدة دون خوف من إختراق القراصنة لنشاطهم خصوصا مع تنامي حجم الإستثمارات و بالموازاة معها إستعمال الأنظمة المعلوماتية في كل الميادين التنموية .

ثانيا : قصور الحماية الفنية لأنظمة المعالجة الآلية للمعطيات

سبق و طرحنا إشكالا في المبحث الأول حول مدى ضرورة خضوع النظام لحماية فنية حتى تتمتع بالحماية الجزائية ، و خلصنا إلى أنه فيما يتعلق بقانون العقوبات الجزائري لم يشترط صراحة وجوب توافرها ، و عليه فالقانون يكفل الحماية لكل الأنظمة و لو لم تكن خاضعة لنظام حماية .

إلا أنه واقعيا رغم التطور الذي نعيشه في مجال إبتكار برامج و أجهزة أمان متطورة و متجددة يتم تزويد الأنظمة بها لحمايتها ، إلا أن هذا لا يحول دون وقوعها ضحية لهذه الجرائم ، مما يجعلها غير كافية فالجاني المعلوماتي حاليا أصبح مواكبا لكل تطور في هذه الأنظمة و يجد له الطريق لتجاوزه و خرقه .

فالمجرم المعلوماتي و كما سلف و بينا خلال دراستنا لسماته هو مجرم ذكي له قدرة على التحكم في تقنيات الحاسوب و إستخدام أنظمته ، و كلما أستحدثت أنظمة أمنية جديدة فإنه يطور وسائل بالمقابل لإختراقها .

و عليه فالأنظمة لا يجب حمايتها بطرق فنية فقط إذ أنها عرضة للإعتداءات رغم ذلك و التي يجب التصدي لها بوضع حماية جزائية رادعة للحد منها .

ثالثا : بواعث إقتصادية

ازدهرت صناعة المعلوماتية في أوائل السبعينات و أصبحت مصدرا هاما لإستثمار الأموال التي أصبحت تدر ثروة ، كما أصبح هذا النوع من الصناعة مقياسا لتطور الدول و مصدر لقوتها السياسية و العسكرية ، و يؤكد علماء الإقتصاد أن الإستثمار في مجال نظام المعلومات و البرمجيات تعد إستثمار المستقبل إذ أن صناعة البرمجيات قد ساهمت بأكثر من ترليون دولار في حركة التجارة عام 1998 [1] فالإعتماد على أجهزة الإعلام الآلي في الأعمال يوفر الوقت من جهة و يقصر المسافات ، إلا أنه يضاعف خطر

تعرض المعلومات المتعلقة بكل هذه المعاملات لإعتداءات ، خاصة و أن كل المؤسسات المالية الضخمة و البنوك و الشركات تعتمد كليا على برامج و أنظمة متصلة بشبكات معلوماتية في تسيير معاملاتها .

و ورد في تقرير للمركز الوطني للبيانات في الولايات المتحدة الأمريكية في بحث نشر سنة 1999 أنجزه (برنالدود ستاندير) أن الخسائر الناتجة عن الجرائم المعلوماتية بلغت 000 810 دولار في الشهر ، و في تقرير نشرته المجموعة الإقتصادية الأوروبية أحصت الخسائر بـ 5،64 مليون أورو [2]

و نظرا لأهمية الجانب المعلوماتي في الجانب الإقتصادي لكل دولة و الخسائر التي تتكبدها جراء التعدي على أنظمتها ، وجب على كل دولة وضع خطة لإقرار حماية جزائية من هذه الجرائم التي أصبحت أضرارها جسيمة مقارنة بالأضرار التي تخلفها الجرائم التقليدية .

المطلب الثالث : وسائل الحماية من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

سبق و بينا الدوافع التي تدعو لإيجاد حماية جزائية للأنظمة من الإعتداءات التي تتعرض لها الأنظمة فما دور هذه الحماية؟ و ما الشكل القانوني الذي تأخذه ؟

أولا : دور الحماية الجزائية

إن وضع نصوص قانونية تجرم الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات يوفر لها الحماية تتخذ شكلين وقائي و عقابي ردعي ، فعند تجريم قانون العقوبات

(1) رشا علي الدين ، المرجع السابق ص 80 .
(2) أحمد خليفة الملط ، المرجع السابق ، ص 96 .

لسلوك كان مباحا و وضع عقوبة مشددة له على قدر خطورة الفعل و جسامته يجعل من متعود إرتكاب هذا النوع من الإعتداءات و قبل الإقدام على فعله أن يفكر في عواقب ذلك ، و في العقوبة التي ستوقع عليه في حال تم إدانته عنها خاصة و أن الجاني في هذا النوع من الجرائم كما وضحنا سابقا من المتفوقين فكريا ، متكيفون إجتماعيا و عليه و على الأغلب يكونون مرموقين إجتماعيا و ذوي مكانة ، قد يفكرون أكثر من مرة لدى مواجهة نظام قانوني متشدد قبل الإقدام على إرتكاب جريمة و التضحية بمكانتهم بالمجتمع .

و بهذا الشكل فالنصوص القانونية لها دور وقائي لمنع الجريمة قبل وقوعها إذ تقف حائلا دون إرتكابها .

و يكون للحماية الجزائية دورا ردعيا إذا ما تم تبني عقوبة مشددة تردع الجاني المحكوم عليه من إرتكابها ثانية ، و رادعة لغيره خشية توقيع ذات العقوبة عليه ، فيتخلى الجاني عن أفكاره لإرتكاب الجريمة للعواقب التي قد تنجر عليها مقارنة بالفائدة المرجوة منها.

ثانيا :الحماية الجزائية على المستوى الدولي

بعد تنامي هذا النوع من الجرائم و نظرا لطبيعتها الدولية و آثارها الممتدة العابرة للحدود أدركت الدول أن إيجاد نظام قانوني داخلي غير كافي لمواجهة الجريمة إذ تعجز كل دولة منفردة على التصدي لها ، مما دفع المجتمع الدولي للسعي لتوحيد الجهود لمكافحتها و إبرام إتفاقيات تعاون و لإصدار توصيات نذكر منها :

1- منظمة الأمم المتحدة [1] : أصدرت منظمة الأمم المتحدة عدة توصيات خلال مؤتمراتها المنعقدة بإستمرار لمواجهة هذه الظاهرة الإجرامية منها المؤتمر السابع ميلانو بإيطاليا 1985 المتعلق بمنع الجريمة و معاملة المجرمين الذي أكدت فيه على ضرورة الإستفادة من التكنولوجيا في مواجهة هذه الجرائم التي تهدف لإختراق أنظمة الحاسب الآلي و البيانات المخزنة فيه .

(1) محمود أحمد عبابنة ، المرجع السابق ص 156

و في سنة 1990 في المؤتمر الثامن هافانا بكوبا أصدرت المنظمة التوصيات التالية :

- تحديث القوانين الجنائية الوطنية .
- تحسين أمن الحاسب الآلي و التدابير المنعية .
- إعتماد إجراءات تدريب كافية للموظفين و الوكلات المسؤولة عن منع الجريمة الإقتصادية و الجرائم المتعلقة بالحاسب الآلي و التحري و الإدعاء فيها .
- تلقين مبادء الحاسب الآلي كجزء من مفردات مقررات الإتصالات و المعلومات .
- إعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم .
- زيادة التعاون الدولي من أجل مكافحة هذه الجرائم .

و في المؤتمر العاشر المنعقد في بودابست بالمجر عام 2000 تم إصدار توصية على وجوب العمل على إتخاذ تدابير للحد من القرصنة الإلكترونية .

2- <u>المجلس الأوروبي</u> : للمجلس الأوروبي إتفاقيتين بارزتين الأولى إتفاقية الجرائم المعلوماتية وقعت عليها 32 دولة و تم المصادقة عليها من 9 دول و دخلت حيز النفاذ إعتبارا من أول يوليو 2004 و تعتبر الإتفاقية الوحيدة الملزمة و تضمنت النص على الجرائم التالية :

- الجرائم المرتكبة ضد سرية و تكامل و توافر البيانات أو نظم الكمبيوتر (التدخل ، الإختراق ، التعدي على أجهزة الكمبيوتر) الجرائم المتصلة بالمحتوى .
- الجرائم التي تتضمن إنتهاكا لحقوق الملكية الفكرية و ما يتصل بها .[1]

الثانية هي إتفاقية بودابست الموقعة 2001/11/23 التي إعتبرت قفزة نوعية في مجال التعاون الدولي لمحاربة الجرائم المعلوماتية و جاء في المذكرة التفسيرية لهذه الإتفاقية مايلي : [2]

---

(1) طارق إبراهيم الدسوقي عطية ، المرجع السابق ، ص 334 .
(2) هلالي عبد الله أحمد ، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست ، دار النهضة العربية القاهرة 2003 ص 23 .

" هناك سمة بارزة في تكنولوجيا المعلومات تتمثل في الأثر الذي أحدثته و ما زالت تحدثه في تطوير تكنولوجيا الإتصالات عن بعد ، فمثلا يكفي أن يتم إدخال البيانات إلى شبكة معينة من خلال عنوان المرسل إليه حتى تصبح متوافرة لأي شخص يريد الدخول إليها ."

و على ذلك يجب على القانون الجنائي أن يواكب التطورات التكنولوجية التي تقدم فرصا واسعة لإساءة إستخدام إمكانيات الفضاء المعلوماتي ، و أن يعمل على ردع هذه الأفعال و جاء في مقدمة الإتفاقية ما يلي :

" الدول الأعضاء بالإتحاد الأوربي و الدول الأخرى الموقعة و إعتقادا منها بضرورة إنتهاج سياسة جنائية مشتركة لحماية المجتمع من الجرائم الإلكترونية بصفة أساسية و على الأخص تبني التشريعات الملائمة لتحسين التعاون الدولي .

و إحساسا منها بالمتغيرات التي طرأت على الأنظمة الرقمية و بوحدة الهدف و العولمة الدائمة لشبكات المعلومات و إهتماما منها بالمخاطر التي تمثلها شبكات المعلومات و الإتصالات الإلكترونية و إستغلالها لإرتكاب جرائم جنائية.

و إعترافا منها بضرورة قيام تعاون بين الدول و المشروعات الصناعية الخاصة من أجل مكافحة جرائم الإنترنيت ، و الحاجة الملحة لحماية المصالح المشروعة و المرتبطة بتطور التقنيات و المعلومات .

و تقديرا منها أن مكافحة جرائم الإنترنيت تتطلب تعاونا دوليا في المجال الجنائي بشكل متزايد و سريع و فعال .

و إعتقادا منها بضرورة و أهمية الإتفاقية الحالية لمعاقبة الأفعال التي تضر بالثقة و تسئ إلى أداء نظم شبكات المعلومات و الأدوات الخاصة بها و البيانات أو الإستخدام الإحتيالي لمثل هذه الشبكات و البيانات و ذلك للتأكيد على تجريم هذه الأفعال و السلوكيات وفقا لما ورد في هذه الإتفاقية ، و تبني السلطات الكافية التي تسمح بالمقاومة الفعالة ضد هذه الجرائم و تسهيل إكتشافها و ملاحقتها سواء على المستوى المحلي أو الدولي ، و العمل على إيجاد وسائل ملموسة سريعة و فعالة في مجال التعاون الدولي .

و إيمانا منها أيضا بحماية البيانات الشخصية التي وردت في إتفاقية المجلس الأوروبي عام 1981 لحماية الأشخاص بشأن معالجة البيانات الشخصية .

و تأكيدا على أن الإتفاقية تهدف لإستكمال الإتفاقيات السابقة و لتفعيل إجراءات التحقيق بشأن جرائم المعلومات و البيانات .

و دعما للمبادرات الحديثة التي تهدف إلى تحسين التفاهم و التعاون الدولي و مقاومة الجرائم الإلكترونية ."

و تحوي هذه الإتفاقية على 48 مادة موزعة على ثلاث أبواب :

الباب الأول يتضمن المصطلحات

الباب الثاني الإجراءات الواجب إتخاذها (القانون العقابي الموضوعي ، القانون الإجرائي ، الإختصاص القضائي)

الباب الثالث يتعلق بالتعاون الدولي إذ نصت المادة 23 على المبادئ العامة المتعلقة بالتعاون الدولي بغرض التحقيقات و الإجراءات المتعلقة بالجرائم المعلوماتية و الحصول على الأدلة في الشكل الإلكتروني .

و نصت المادة 24 على شروط تسليم المجرمين

فيما نصت المادة 25 على المساعدة لإجراء تحقيقات طارئة التي يمكن طلبها بأي وسيلة من وسائل الإتصالات السريعة كالفاكس أو البريد الإلكتروني و إمكانية الرفض طبقا للمادة 27 إذ إتخذت الجريمة طابعا سياسيا أو فيه مساس بالسيادة أو الأمن .

كما تضمنت الإتفاقية جانب آخر من التعاون إنصب حول تدريب أعوان الأمن لإكتساب خبرات في النوع من الجرائم ، و في الجزائر أعدت عدة برامج في مدارس الأمن و الدرك لهذا النوع من الجرائم و تم إرسال عدة دفعات من القضاة للإستفادة من تكوين بالولايات المتحدة الأمريكية .

3- **القانون الجنائي العربي الموحد :** هو قانون نموذجي تم إعتماده من مجلس وزراء العدل العرب بموجب القرار رقم 229 سنة 1996 لمواجهة جرائم معطيات الحاسب الآلي الذي نص على الإعتداءات في نظام المعالجة المعلوماتية و عاقبت المادة 464

منه على الدخول بطريق الغش إلى نظام المعالجة الآلية للمعطيات و عرقلة أو إفساد نظام التشغيل و تغيير المعلومات داخل النظام .

ثالثا : الحماية الجزائية على المستوى الداخلي

على غرار باقي الدول و تطبيقا للتوصيات الدولية التي شددت على وجوب النص في القوانين الداخلية و تجريم هذا النوع من الإعتداءات كذلك فعل المشرع الجزائري بتعديله لقانون العقوبات بموجب الأمر 15/04 المؤرخ 2004/11/10 المعدل و المتمم بالأمر رقم 155/06 و الذي أفرد القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات الذي يحوي ثماني مواد من 394 مكرر إلى 394 مكرر 7 أو ما يسمى بجرائم الغش المعلوماتي [1]

و جاء في عرض أسباب هذا التعديل مايلي : "إن التقدم التكنولوجي و إنتشار وسائل الإتصال الحديثة أدى إلى إبراز أشكال جديدة للإجرام مما دفع بالكثير من الدول إلى النص على معاقبتها ، و إن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلومـــاتيـة و أساليب المعالجة الآلية للمعطيات ، و أن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات ، و سوف يمكن لا محالة من مواجهة بعض أشكـــال الإجرام الجديد ".

إضافة للجانب الإجرائي إذ نص المشرع على إجراءات للوقاية من الجريمة و مكافحتها بالقانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، الذي تضمن في الفصل السادس النص على التعاون و المساعدة القضائية الدولية فيما يتعلق بهذه الجرائم .

و الجدير بالذكر أنه بموجب القانون السالف الذكر الفصل الخامس منه تم إستحداث ما يسمى :" الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحته" في إنتظار تحديد تشكيل هيئتها و كيفيات تسييرها عن طريق التنظيم طبقا للمادة 13 من هذا القانون .

---

(1) أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، المرجع السابق ، ص 447

و نصت المادة 14 على المهام التي تتولها هذه الهيئة خصوصا و هي :

أ- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحته .

ب- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الإتصال بما في ذلك تجميع المعلومات و إنجاز الخبرات القضائية .

ج- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و تحديد مكان تواجدهم .

و للإشارة لم يتم تنصيب هذا الهيئة حتى إعداد الدراسة .

الفصل الأول : صور المساس بأنظمة المعالجة الآلية للمعطيات

تعتبر فرنسا من بين أولى الدول التي أصدرت تشريعا خاصا في مجال الجرائم المعلوماتية بموجب قانونين الأول صدر بتاريخ 1978/01/05 حول المعلوماتية و الحريات ، و الثاني هو قانون (god frain) المؤرخ 1988/01/05 حول الغش المعلوماتي الذي جرم من خلاله الإعتداءات الماسة بالأنظمة المعلوماتية .

و على سبيل المثال أيضا أصدرت الولايات المتحدة الأمريكية عام 1998 قانون الغش في الكمبيوتر و قانون سرية المخابرات الإلكترونية و إستحدث بموجبه 2000 جهاز خاص تابع لـ (أف بي أي) خاص بمكافحة جرائم الإنترنيت .

و إستحدث المشرع الجزائري هذه الجريمة بصورها بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 الذي أضاف بموجبه القسم السابع مكرر بقانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات الذي تضمن 8 مواد و التي سندرس منها المواد من 394 مكرر إلى المادة 394 مكرر 2 التي تنص على صور الجريمة المتعددة و التي يمكن تصنيفها إلى أربع فئات نتناولها تفصيلا .

و سنعرض بداية في المبحث الأول جريمة الدخول أو البقاء الغير الشرعي في نظام المعالجة الآلية للمعطيات البسيط و هي الصورة التي نص عليها قانون العقوبات بالمادة 394 مكرر في الفقرة الأولى .

و يليه المبحث الثاني الذي يأخذ بالدراسة جريمة الإتلاف الغير العمدي أو الدخول أو البقاء الغير الشرعي المؤدي إلى الحذف أو التغيير أو التخريب و هي الصورة التي نص عليها المشرع بالمادة 394 مكرر في فقرتيها الثانية و الثالثة من قانون العقوبات.

أما في المبحث الثالث فنعالج جريمة المساس العمدي بالمعطيات أو التلاعب بالمعطيات و هي الصورة المنصوص عليها بالمادة 394 مكرر 1 من قانون العقوبات. و أخيرا يتضمن المبحث الرابع دراسة جريمة التعامل بالمعطيات الغير مشروعة و هي الصورة المنصوص عليها بالمادة 394 مكرر 2 من قانون العقوبات على أن يتضمن كل مبحث بيان كل من الركن المادي في المطلب الأول و الركن المعنوي في المطلب الثاني.

المبحث الأول : جريمة الدخول أو البقاء الغير الشرعي في نظام المعالجة الآلية للمعطيات البسيط

و هي الصورة التي نص عليها قانون العقوبات بالمادة 394 مكرر الفقرة الاولى التي تقابلها المادة 323 فقرة 1 من قانون العقوبات الفرنسي و المادة 2 من الإتفاقية الدولية للإجرام المعلوماتي و تنص المادة الآنفة الذكر على :

" يعاقب بالحبس من ثلاث أشهر إلى سنة و بغرامة من 000 50 دج إلى 000 200 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك "

و هي أبسط صور هذه الجرائم التي تتحقق بمجرد الدخول أو البقاء الغير مشروع فما المقصود بذلك ؟

المطلب الأول : الركن المادي لجريمة الدخول أو البقاء الغير الشرعي في نظام معالجة آلية للمعطيات

أولا الدخول :

يعني الدخول كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي و يتحقق بالوصول إلى المعلومات و البيانات المخزونة داخل نظام معين دون رضا المسؤول عنه من شخص غير مرخص له بإستخدامه . [1]

و لغويا يترجم الدخول بـ (acces) لأنه يدل على النقاد و الإحتراف إلى مكان غير مادي بينهما (entree) يقصد به الدخول لمكان مادي ، و عليه لا يقصد بالدخول الدخول بالمعنى المادي إنما الدخول كظاهرة معنوية كأفكار و عمليات ذهنية في نظام معالجة .

(1) خالد ممدوح إبراهيم ، أمن المستندات الإلكترونية ، الدار الجامعية الإسكندرية 2008 ص 148 .

و يستخلص من التعريف السالف الذكر أن الدخول الغير الشرعي هو سلوك إيجابي و لم يحدد المشرع وسيلة معينة لذلك ، إنما تتحقق الجريمة في كل حالة يكون فيها الدخول مخالفا لشروط الدخول التي نص عليها القانون أو الإتفاق أو بمخالفة إرادة من له الحق في السيطرة على النظام الذي تم الدخول له ، مثلا كوضع نظام للدفع لقاء الدخول في حين يعمد الجاني لإيجاد وسيلة للإستفادة من النظام دون الدفع على خلاف إرادة مالكه .

و نذكر من أكثر التقنيات المستعملة الدخول :

– إستخدام البرامج المخصصة لتخطي أنظمة الحماية الفنية في الحالات الطارئة إذ على الرغم من ضرورة تزويد الحاسبات بأنظمة حماية للحيلولة دون الإتصال غير المشروع بالبرامج و البيانات المخزنة إلا أن إدارة و تشغيل هذه الحواسيب تقتضي وجود نوع من البرامج يمكن إستخدامها لتخطي حواجز الحماية في الحالات الطارئة ، و في حالة إختلال وظائف الحاسب أو توقفه عن العمل و أشهرها برنامج يسمى (superzap) إلا أن هذا النوع من الأنظمة إذا ما وقع في أيدي غير مصرح لها بإستخدامه فإن هذا يسمح لها بالتغلغل في منظومة الحاسب الآلي و لو كان محمي [1].

– أبواب المصيدة (trap-doors) و يقصد بها الفواصل التي يتعمد واضعي البرامج تركها أثناء إعداده لتستخدم في إضافة ما يحلو لهم لاحقا .

– إستعمال ما يرمى بصناديق القمامة دون حذفه نهائيا .

- طريقة المختصرات (raccourci) تتم بإستغلال نقاط ضعف بالنظام للدخول إليه.

- طريقة القناع : بأن يقنع القرصان البرنامج أنه شخص مرخص له بالدخول .

و يتحقق الدخول من أي شخص مهما كانت صفته سواء كان يعمل في مجال معالجة النظام أم لا و متى وضع صاحب النظام قيودا للدخول أو لم يضعها و عليه يتم الدخول بمجرد فتح جهاز الكمبيوتر و إستعمال النظام مباشرة أو بفك رمز المرور أو إدخاله

---

(1) آمال قارة ، المرجع السابق ، ص42 .

لفتح النظام و الولوج إليه و مخالفة كافة الإجراءات الأمنية و يستوي في ذلك أن يكون الدخول بدافع و هدف معين أو لمجرد الفضول .

و بهذا المفهوم وجب النظر في جريمة الدخول الغير مشروع كظاهرة معنوية و ليس الدخول بالمعنى المادي كما و تتحقق جريمة الدخول بغض النظر عن مجال أو تخصص الموقع أو النظام المعلوماتي المستهدف ، سواء تضمن معلومات شخصية أو عامة و سواء تعلق بهيئة عامة أو حتى أسرار الدولة و دون إشتراط صفة معينة بالجاني كما سلف الذكر و هو ما يستشف من نص المادة " ... كل من دخل ..." بمعنى يكفي آلا يكون من أولئك الذين لهم الحق في الدخول للنظام .

و مجرد الدخول معاقب عليه حتى و لو لم يترتب عليه ضرر للمجني عليه أو فائدة للجاني فما هو منصوص و معاقب عليه هو مجرد الدخول الغير مشروع ، كما و يتحقق فعل الدخول طبقا للمادة سواء تم الولوج للنظام كلية أو لجزء منه إذ وردت بالمادة عبارة " كل من دخل ... عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات " .

و بهذا المفهوم يتحقق الدخول أيضا إذا كان مرخصا للجاني الدخول لجزء معين من النظام و تجاوزه لجزء آخر [1] لذلك يخرج من نطاق الجريمة قيام الجاني بالدخول إلى برنامج منعزل عن نظام معالجة المعطيات الذي حظر عليه الدخول إليه .

ومعنى أن يكون الدخول غير مشروع أو كما إصطلح عليه قانون العقوبات الجزائري بعبارة " ... عن طريق الغش ..." أن يكون دخولا غير مصرح به فهو في هذه الحال يتوقف على إرادة الشخص أو الهيئة المسؤولة على منح التصريح بإعتبارهما من يملكان السيطرة على النظام بالإدارة و التنظيم .

و قد عرفته المادة 2 من الإتفاقية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعطيات بأنه " كل شخص طبيعي أو معنوي أو كل سلطة عامة أو كل مؤسسة

(1) عبد الفتاح بيومي حجازي ، الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية المعلوماتية) دار الفكر الجامعي الإسكندرية 2008 ص 83 .

أو جهاز يكون له سلطة التصرف في نظام الحاسب الآلي التابع لهم ، و تقرير مضمونه أو محتواه ، و كيفية تنظيمه و الهدف منه ". [1]

و من خلال نص هذه المادة يكون الدخول غير مصرح به إذا لم يستوفي شروط الدخول للنظام ككلمة السر أو الإشتراك بالعضوية أو دفع مبلغ مالي أو كان الموقع محمي و ممنوع من الدخول على الإطلاق أو كما سبق و أن ذكرنا أن يتجاوز الجاني الجزء المصرح به إلى آخر أو تجاوز الهدف الذي سمح للجاني به و تجاوز مهمته إلى أجزاء أخرى من النظام لأداء مهمة أخرى .

ثانيا : البقاء

و يقصد بالبقاء الغير الشرعي في نظام الآلية للمعطيات التواجد في النظام ضد إرادة من له الحق في السماح بالبقاء ، و قد يقترن البقاء بالدخول غير الشرعي منذ البداية كما يتحقق مع دخول شرعي مصرح به إذا إستمر البقاء لغير المدة المحددة و هذا ما يعرف بتجاوز التصريح فتجريم كل منهما غير مرتبط بالآخر.

كما يتضح الهدف من تجريم البقاء بالنسبة للجاني الذي لم يقصد الدخول عن طريق الغش للنظام و مع ذلك يبقى داخل النظام و تنصرف إرادته إلى ذلك و الذي كان يمكن أن يغادر النظام . [2]

و مما سبق يتضح أن سلوك الجاني في هذه الجريمة هو سلوك سلبي إذ رغم علمه بعدم أحقيته إلا أنه يتعمد البقاء في النظام ككل أو في جزء منه و يرفض الخروج منه إذ يشمل هذا الحكم الدخول و البقاء على حد سواء حسب المادة 394 مكرر من قانون العقوبات .

و مثال ذلك إستعمال الجاني لخدمة معينة كالأنترنيت أو خدمات الهاتف لمدة تطول عن تلك التي دفع مقابلها بإستخدام الغش أو وسائل غير مشروعة.

---

(1) محمد خليفة ، المرجع السابق ، ص 62 .

(2) عبد الفتاح بيومي حجازي ، الجريمة في عصر العولمة ، المرجع السابق ، ص 83 .

كما قد تجتمع الجريمتين في آن واحد بأن يتم الدخول عن طريق الغش إلى نظام معلوماتي معين ثم بقاء الجاني فيه و رفضه المغادرة قبل تصفح محتواه و الإطلاع عليه فتتوافر أركـــان الجرمتين معا فصيـاغة المشرع لنص المـــادة 394 مكرر من قـانون العقوبات جعلت من الدخول و البقاء جريمتين منفصلتين إذ تنص كل من يدخل **أو** يبقى " و ليس " كل من يدخل **و** يبقى " و عليه فالأمر لا يتعلق بحريمة واحدة و إنما وصفين مستقلين جريمة الدخول الغير مشروع و ثانيا جريمة البقاء الغير مشروع .

و هنا يجب التأكد من أن كل جريمة سواء الدخول أو البقاء تقع مستقلة عن الأخرى لكل منهما سلوكها المجرم الخاص بها ، ذلك أن المشرع ذكر مصطلحين مختلفين و خير بينهما ، فجريمة الدخول وقتية في حين جريمة البقاء مستمرة .

و بالتالي يمكن متابعة الشخص الذي يقوم بالدخول لنظام معلوماتي معين عن طريق الغش و البقاء فيه عن تهمتين على أساس التعدد الفعلي للجرائم . [1]

و يمكن وصف الجريمتين أنهما جريمة سلوك مجرد تقع و تكتمل بمجرد إنتهاء السلوك (الدخول أو البقاء) دون أن يشترط المشرع تحقق نتيجة معينة. [2]

و لعل الفصل بين الجرمين يطرح إشكالا متى تكون نهاية جريمة الدخول و متى تبدأ جريمة البقاء عند القول بتوافرهما معا ؟

لقد تعددت الآراء الفقهية بهذا الشأن إذ ذهب رأي إلى أن جريمة الدخول تتحقق منذ لحظة الدخول الفعلي للبرنامج الذي يفترض لحظة قصيرة بعدها نحن بصدد البقاء داخل النظام إلا أن هذا الرأي لا يتسم بالدقة .

و ذهب رأي آخر لتحديد تلك اللحظة منذ الوقت الذي يعلم فيه الجاني أن بقاءه غير مشروع ، و هذا الرأي يغفل من جهة الدخول الغير مشروع في حد ذاته منذ البداية إضافة لصعوبة إثبات لحظة العلم لتحديد بداية النشاط الإجرامي .

---

(1) سي الحاج أحمد مدير التكوين بوزارة العدل ، محاضرة بعنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ملقاة على قضاة التكوين التخصصي في قانون الأعمال الدفعة السابعة 2008 ص 11 .

(2) جميل عبد الباقي ، جرائم التكنولوجيا الحديثة ، دار النهضة العربية ص 28 .

و يرى إتجاه ثالث أن جريمة البقاء تبدأ من لحظة إنذار الجاني أن تواجده غير مشروع و تعمد عدم الإنسحاب منه ، إلا أن ما يؤخذ على هذا الرأي أن إمكانية إنذار الجاني غير متوافرة في كل الأنظمة المعلوماتية التي تتعرض للدخول و البقاء .

و حسب رأينا فإن الأصح أن جريمة الدخول تبدأ من اللحظة التي يدخل فيها الجاني النظام و تبدأ جريمة البقاء من اللحظة التي يبدأ فيها الجاني بالتجول و الإطلاع على النظام رغم علمه أنه ليس له الحق في ذلك أو أن يستمر في التجول بعد المدة المحددة له بداية .

فإذا دخل الجاني و ظل ساكنا فإن الفعل المجرم هنا هو الدخول غير المشروع ، أما إذا بدأ بالتجول يتابع عن جنحتين هما الدخول و البقاء الغير مشروع في النظام

و تكمن اهمية التفريق بينهما خاصة في مسألة الإختصاص و التقادم و قد إتفق الفقة على أن جريمة الدخول جريمة وقتية و جريمة البقاء جريمة مستمرة ذات أثر ممتد.[1]

المطلب الثاني : الركن المعنوي لجريمة الدخول أو البقاء الغير الشرعي في نظام معالجة آلية للمعطيات

جريمة الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات هي جريمة عمدية تقوم على قصد جنائي عام و لا تتطلب قصدا خاصا ، إذ لا تحتاج لترتب عنها نتيجة أو أثر خاص للتحقق الجريمة و لو كان الهدف هو فضول الجاني للدخول أو لإثبات قدراته في هذا المجال .

و يتحقق القصد العام بتوافر عنصري العلم و الإرادة إذ يجب أن يعلم الجاني أنه لا يحق له الدخول للنظام كما لا يحق له البقاء فيه ، و يعلم أن قيامه بذلك مخالف لإرادة من له الحق في السيطرة على النظام إذ لم يمنحه إذنا أو تصريحا بذلك ، و رغم ذلك تتجه إرادته للدخول أو البقاء مخالفا بذلك القانون .

---

(1) علي عبد القادر القهوجي ، المرجع السابق ، ص 26 .

أولا : العلم

يجب أن يعلم الجاني بأنه لا حق له بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات و أن الطريقة التي تم بها ذلك غير مشروعة لكونه لا يملك تصريحا من مالك النظام أو ممن له الحق في السيطرة أن تسيير النظام .

و لهذا يرى جانب من الفقه أن الدخول يكون مشروعا من كان بطريق الصدفة أو السهو أو الخطأ و على الشخص الذي دخل بهذه الطريقة أن ينسحب فورا فإذا لم ينسحب منذ هذه اللحظة توافر في حقه القصد الجنائي . [1]

كذلك الشأن إذا بقي الشخص في النظام و إستعمله دون أن ينتبه أن بقاءه غير مصرح أو أنه تجاوز حدود ما صرح له به سهوا و لا يتوافر في حقه القصد الجنائي إلا من لحظة علمه و كذلك إذا إعتقد الشخص أنه مسموح له بذلك و قام بالدخول أو البقاء ظنا أنه مصرح له بذلك أو أخطأ في حدود التصريح الممنوح له .

ثانيا : الإرادة

وجوب توافر عنصر الإرادة عنصر الإرادة يعني إتجاه إرادة الجاني إلى إرتكاب الركن المادي للجريمة بالدخول إلى نظام المعالجة الآلية للمعطيات و البقاء فيه رغم علمه بعد مشروعية هذا ، فإذا فعل ذلك خطأ لا تقوم الجريمة لكن شريطة مغادرة النظام فورا .

و لا تشمل الإرادة أن يهدف الجاني لنتيجة معينة بل يكفي توجه إرادته لدخول و خرق الحماية التي تحيط به ، مثلا الدخول دون الحصول على إذن أو إستعمال التحايل للحصول على كلمة السر و لا محل للإعتداد بالباعث ، كما لو تعمد الجاني الدخول لإثبات قدراته على خرق نظام الحماية أو على سبيل الفضول متى إتجهت إرادته للدخول أو البقاء رغم علمه بعدم مشروعية ذلك ، و من هنا يمكن إستخلاص نية الغش من سلوك الجاني الواضح .

---

(1) علي عبد القادر القهوجي ، المرجع السابق ، ص 54 .

كما و يتوافر القصد حتى بالنسبة للجاني المرخص له بالدخول للنظام إذا كانت الرخصة مقيدة بحيز معين كجزء من النظام و رغم علمه بذلك تتجه إرادته للدخول لأجزاء أخرى و البقاء فيها ، و قد يكون القيد زمني كالموظف الذي يستمر في إستعمال النظام خارج أوقات العمل المرخص بها .

و تجدر الإشارة أن جريمتي الدخول أو البقاء الغير الشرعي بصورته البسيطة مثلتا بالجزائر من سنة 2005 حتى أفريل 2010 نسبة 29 بالمئة من صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات . [1]

و بعد بيان مفهوم جريمتي الدخول أو البقاء في صورتها البسيطة سنتطرق بالمبحث التالي للصورة المشددة لهما التي من شأنها أن تؤدي إلى الحذف أو التغيير أو تخريب المعطيات الموجودة بالنظام و هي الجريمة التي يطلق عليها تسمية جريمة الإتلاف الغير عمدي للمعطيات .

(1) دراسة لمختار الأخضري مدير الشؤون الجزائية و إجراءات العفو وزارة العدل بعنوان الإطار القانوني لمواجهة جرائم المعلوماتية و جرائم الفضاء الإفتراضي ، نشرة القضاة ، العدد 66 لسنة 2011 ص 68 .

المبحث الثاني : جريمة الإتلاف الغير العمدي للمعطيات (الدخول أو البقاء الغير الشرعي المؤدي إلى الحذف أو التغيير أو التخريب)

و هي الصورة التي نصت عليها المادة 394 مكرر من قانون العقوبات في فقرتيها الثانية و الثالثة على النحو التالي :

" ... تضاعف العقوبة إذ ترتب على الدخول أو البقاء الغير مشروع حذف أو تغيير لمعطيات المنظومة .

و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 000 50 دج إلى 000 300 دج . "

و يستخلص من المادة أنها تتضمن صورة مشددة لجنحتي الدخول و البقاء الغير الشرعي متى ترتبت عليه نتيجة معينة تتمثل في إتلاف المنظومة إما بالحذف أو التغيير أو التخريب ، على ألا يكون بصورة عمدية و هذا ما سيأتي بيانه على مطلبين الركن المادي ثم الركن المعنوي .

المطلب الأول : الركن المادي لجريمة الإتلاف الغير عمدي للمعطيات

تتطلب جريمة الدخول أو البقاء الغير شرعي في صورتها المشددة زيادة على ما ذكرناه بالمبحث الأول أن يترتب على ذلك نتيجة معينة هي إتلاف المنظومة في ثلاث صور حددت على سبيل الحصر و المتمثلة في الحذف ، تغيير المعطيات و تخريب النظام ، و عليه يستخلص أن الركن المادي للصورة المشددة و التي نطلق عليها جريمة الإتلاف الغير عمدي للمعطيات ثلاث عناصر :

1 – السلوك الإجرامي

2 – النتيجة

3 – العلاقة السببية

أولا : السلوك الإجرامي :

تضمنت الفقرة الثانية من المادة 394 مكرر من قانون العقوبات ظرف تشديد يتحقق متى توافرت نتيجة معينة لنكون أمام الصورة المشددة من الجريمة و عليه وجب بداية توافر الصورة البسيطة لجريمة الدخول أو البقاء الغير الشرعي على النحو السالف الذكر بالمبحث الأول لذا لا داعي لإعادة شرحها .

ثانيا : النتيجة :

تتطلب هذه الجريمة أن يترتب على الدخول أو البقاء في نظام المعالجة الآلية للمعطيات إحدى النتائج الثلاث و هي المحددة على سبيل الحصر بالمادة 394 مكرر من قانون العقوبات و هي :

أ – حذف المعطيات و يتم ذلك بإزالتها كلية عن طريق المحو أو الإلغاء .

ب – تغيير المعطيات و هو المساس بالحالة الأصلية بحيث لا تبقى على ما كانت عليه بالقيام بعمليات عشوائية غير مدروسة .

ج – تخريب نظام التشغيل بجعله غير قابل للإستعمال و أداء ما وضع من أجله كما و لا يؤدي وظيفته .

ثالثا : العلاقة السببية :

يكفي لتتحقق الجريمة أن تكون هناك علاقة سببية بين الدخول أو البقاء الغير شرعي و بين النتيجة التي تحققت و هي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات [1] ، فلا بد من وجود علاقة سببية فإن حدثت إحدى هذه النتائج نتيجة فعل آخر فلا نكون أمام هذه الصورة المشددة من الجريمة بل البسيطة لتحقق فعل الدخول أو البقاء فقط ، فإذا أثبت الجاني إنتفاء العلاقة السببية بين فعله و النتيجة التي تحققت لم تقم الجريمة كتدخل عامل آخر ، حادث مفاجئ أو قوة قاهرة .

(1) جميل عبد الباقي الصغير ، القانون الجنائي و التكنولوجيا الحديثة ، الكتاب الأول (الجرائم الناشئة عن إستخدام الحاسب الآلي) دار النهضة العربية القاهرة ، 1992 ص 20 .

المطلب الثاني : الركن المعنوي لجريمة الإتلاف الغير عمدي للمعطيات

بداية و فيما يتعلق بالسلوك الإجرامي المتمثل في الدخول أو البقاء الغير الشرعي يتطلب توافر قصد جنائي عام على النحو الذي سبق بيانه في المبحث الأول من هذا الفصل بأن يعلم الجاني أن دخوله أو بقاءه غير مشروع و أن تتجه إرادته إلى إرتكاب هذا السلوك الإجرامي .

غير أن النتيجة المتمثلة في إتلاف النظام فلا يشترط فيها القصد العمدي فهذه الجريمة هي من الجرائم الغير عمدية لا بد أن تتحقق النتيجة فيها بغير قصد من الجاني عن طريق الخطأ دون سوء نية .

فإن كان للجاني نية الغش و قصد إحداث هذه النتيجة نكون أمام جريمة أخرى هي المساس العمدي أو التلاعب العمدي بالمعطيات و التي سنأتي إليها بالدراسة في المبحثين اللاحقين .

و قد احتل هذا النوع من الجرائم نسبة 34 بالمئة من مجموع القضايا التي طرحت أمام القضاء الجزائري من 2005 إلى أفريل 2010 [1]

(1) مختار الأخضري ، المرجع السابق ،ص 68 .

المبحث الثالث : جريمة المساس العمدي بالمعطيات

و هي ما يسمى أيضا بجريمة التلاعب بمعطيات أنظمة المعالجة الآلية للمعطيات و هي الجريمة المنصوص عليها بالمادة 394 مكرر1 من قانون العقوبات على النحو الآتي :

" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة مالية من 000 500 دج إلى 000 000 4 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها "

و أول ما يفهم من المادة السالفة الذكر أن المشرع الجزائري جرم المساس بالمعطيات التي يتضمنها النظام بإحدى الوسائل التي سنأتي عليها بالشرح في المطلب الأول دون أن يجرم الإعتداء أو المساس بالنظام في حد ذاته .

و قد وضع الفقه معيار للتفرقة بين الإعتداء على المعطيات و الإعتداء على النظام على أساس ما إذا كان الإعتداء وسيلة أم غاية ، فإذا كان الإعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الإعتداء العمدي على النظام أما إذا كان الإعتداء غاية فإن الفعل يشكل جريمة الإعتداء العمدي على المعطيات . [1]

و قد خالف في ذلك القانون الجزائري الإتفاقية الدولية للإجرامي المعلوماتي التي جاءت بالنص على ضرورة تجريم العمليات المرتكبة عن قصد بخصوص الإعاقة دون وجه حق لعمل منظومة الكمبيوتر من خلال أحكام المادتين 5 و 8 منها ، و هو ما أخذ به المشرع الفرنسي و نص في المادة 323 الفقرة الثانية من قانون العقوبات على تجريم الإعتداء العمدي على سير نظام المعالجة الآلية للمعطيات و إعاقتها و إفسادها على النحو الآتي :

"كل من عطل أو أفسد نشاط أو وظائف نظام المعالجة الآلية للمعطيات يعاقب بالحبس حتى ثلاث سنوات و بغرامة حتى 000 45 أورو "

---

(1) فشار عطا الله ، بحث مقدم إلى الملتقى المغاربي حول القانون و المعلوماتية عقد بأكاديمية الدراسات العليا بليبيا أكتوبر 2009 ، ص مأخوذ من الموقع الإلكتروني www.arablawinfo.com

و للإشارة بإختصار نبين المفاهيم التي وردت بالقانون الفرنسي المتعلقة بالإعتداء على النظام قبل التطرق للصورة المنصوص عليها بالقانون الجزائري المتعلقة بالإعتداء على المعطيات الواردة بالنظام .

1 – التعطيل :

تعطيل النظام أو توقيفه هو إعاقة النظام المعلوماتي بأي وسيلة كانت بإدخال فيروس على البرنامج أو تعديل كلمة السر أو قد ينصب على أداء وظيفة النظام بجعله يتباطئ [1] و عليه و يفترض في التعطيل أنه سلوك إيجابي الذي لم يشترط فيه المشرع وسيلة معينة فقد تكون الوسيلة مادية قد تقترن بالعنف إذا وقعت على الأجهزة المادية للنظام أو منعت الوصول إليها ككسرها أو تحطيمها أو قطع شبكة الإتصال ، و قد تكون الوسيلة معنوية إذا ما وقعت على الكيان المنطقي للبرامج و المعطيات كإدخال فيروس أو قنبلة منطقية ، جعل النظام يتباطئ ، التلاعب في المدخلات ...

و يستوى أن يكون التعطيل مؤقتا أو دائما فقد يؤدي للتوقف الدائم للنظام عند بدء تشغيله أو مؤقتا منقطعا على فترات كالناتج عن إدخال فيروس .

و لا يشترط في التعطيل أن يتم بفعل إيجابي من الجاني بأن يصدر عنه نشاط يؤدي لتوقيف النظام بل قد يتم بفعل إمتناع الجاني عن القيام بما هو مفروض عليه من واجب تشغيل النظام وفقا للقواعد الموضوعة مما يؤدي لتوقفه .

2 – الإفساد : (fausser)

هو التعييب بشكل لا يعطل النظام إنما يجعله غير سليم يشكل يعطي نتائج غير تلك التي كان يجب الحصول عليها ، و يستوي في ذلك أن يشمل كل النظام أو جزء منه و هو من الأفعال الإيجابية العمدية و من وسائله إستعمال الفيروسات ، إدخال بيانات محرفة أو تغيير مسار نظام التشغيل الأصلي أو إدخال تعديلات غير مرخص بها على البرامج الأصلية المستخدمة الذي يظهر بشكل برنامج معد لهدف معين إلا أن الهدف المضمر هو محو البيانات مثلا.

---

(1) علي عبد القادر القهوجي ، المرجع السابق ، ص 56 .

و إن كان يمكن التمييز من الناحية النظرية بين التعطيل و الإفساد إلا أنهما كثيرا ما يتطابقان من الناحية العملية لوحدة الوسائل التي تحققهما من فيروسات و قنابل و تقارب النتائج بينهما .

و عدم إدراج المشرع الجزائري لصور هذا التجريم المتعلق بأنظمة المعالجة قد يطرح إشكال إفلات الإعتداءات على سير النظام من العقاب و يمكن تفسير ذلك بالتشابه بين الجرمتين بإعتبار الإعتداء على المعطيات يؤدي إلى إفساد النظام أو تعطيله ، لكن هذا لا يتحقق بالضرورة .

و بناءا على المادة 394 مكرر 1 السالفة الذكر ندرس فيما يلي الأفعال التي تعد مساسا بالمعطيات و هي ثلاث ثم ندرس القصد الجنائي بإعتبارها من الجرائم العمدية .

المطلب الأول : الركن المادي لجريمة المساس العمدي بالمعطيات.

الركن المادي لجنحة المساس بالمعطيات أو التلاعب بها يتحقق بإتيان الجاني لفعل من الصور الثلاث التالية :

1 – الإدخال

2- المحو أو الإزالة

3 – التعديل

و هي الصور المنصوص عليها بالمادة 394 مكرر 1 من قانون العقوبات السالفة الذكر و المنصوص عليها بالمواد 3 ، 4 ، 8 من الإتفاقية الدولية للإجرام المعلوماتي و تقابلها المادة 323 الفقرة الثالثة من قانون العقوبات الفرنسي الجديد .

و لا يشترط الركن المادي توافر الصور الثلاث بل يكفي أن يقوم الجاني بإدخال معطيات مغلوطة جديدة لم تكن موجودة أو محو معطيات موجودة أو تعديل أخرى كانت موجودة أصلا يحتويها النظام ، فغاية الأمر أن يرد الأمر على معطيات بإحدى الصور الثلاث التي سنأتي على شرحها تفصيلا و التي تشكل جزءا من النظام .

و كل هذه الأفعال تؤدي إلى تغيير في الحالة التي كانت عليها المعطيات محل الإعتداء و تؤدي إلى المساس بسلامتها و تكاملها .

و عليه و بهذا المفهوم لا تتحقق الجريمة بالنسبة للمعطيات التي لم تتم معالجتها بعد في نظام معين و لم تدخله بعد ، إذ تتمتع المعالجة بالحماية متى بدأت و متى تضمنت المعطيات بنظام معين يخضع لحماية كالمعطيات المحفوظة على روابط تخزين كالأقراص أو الوسائط خارج النظام ، و هنا بهذه الصورة يفتح المجال لدراسة توافر الجريمة التامة و الشروع فيها .

و هذه الصورة إصطلح عليها بعض الفقه بالقرصنة المعلوماتية فهذه الجريمة لا تستهدف النظام بل يستهدف فيها الجاني الوصول للمعلومات الموجودة أو إختراق النظام لإدخال معلومات لم تكن موجودة أو لمحو و تعديل المتضمنة .

و لا يشترط في هذه الجريمة أن تتم بطريقة مباشرة من الجاني فقد تتم عن بعد و هذه هي الصورة المثالية للقرصنة أو بتدخل شخص آخر .

و تجدر الإشارة إلى أن المشرع المصري الذي تناول جريمة إتلاف المعطيات إشترط أن يكون محل الجريمة أموال ثابتة أو منقولة و بذلك يكون قد أعطى منحى آخر لهذه الجريمة لا تماثل محل الجريمة في القانون الجزائري الذي يجرم فعل الإعتداء على المعلومة في حد ذاته و ليس الإعتداء الذي يهدف لإتلاف أموال [1]

أولا : الإدخال .(l intrusion)

يتحقق الإدخال بإضافة معطيات جديدة على الدعامة الأساسية للنظام سواء كانت خالية أم توجد عليها معطيات من قبل [2] و هنا يستوى أن يقوم بفعل الإدخال شخص أجنبي لا يحق له التواجد و إستعمال النظام و أن يكون من المصرح لهم بإستعمال النظام إلا أنه يعمد لإدخال معطيات خاطئة تخرج عن الإستعمال المنوط بمهامه .

(1) لمزيد من التفصيل بالنسبة لهذه الجريمة أنظر أحمد خليفة الملط ، المرجع السابق، ص 518.
(2) عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 92

و يسهل إرتكاب هذه الصورة عند التشغيل الأولي لأي نظام معالجة عند إدخال المعطيات لحفظها في المراحل الأولى للتشغيل أين يقبل النظام أي معلومـات صحيحـة أو مغلوطة و يعمل على حفظها و مثال ذلك حـالة إدخال فيروس الهدف منـه إضـافة معلومات جديدة لم تكن موجودة و هذا النوع من الفيروسات يصطلح عليه بفيروس حصان طروادة و القنابل المعلوماتية .

أيضا أصحاب البطاقات الممغنطة لبطاقات السحب و الإئتمان سواء كان الحامل شرعي أو الغير الذي يعمد لسحب مبلغ بإستعمال الرقم السري أكبر من الموجود بالحساب أو تسديد مبلغ أكبر من المحدد و يتحقق الإدخال بأي إستعمال تعسفي للبطاقة فيما عدا السرقة أو التزوير أو الفقد فهنا نكون أمام جرائم أخرى محلها البطاقة و ليس المعطيات التي تم التلاعب بها و كانت البطاقة وسيلة لذلك .

و من الأمثلة العملية حدث في ألمانيا الشرقية أن قام مستخدم بمكتب القوى العاملة مختص بتوزيع الإعانات على العاملين بتحويل مبلغ 000 500 مارك لحسابه في شكل مرتبات بإزالة الرقم الأول للمبالغ المحولة .

كما توجد طريقة يطلق عليها إسم (بلوف) تتمثل في إستخدام النظام من أجل طبع فواتير مصطنعة يقوم العملاء بتسديدها ، أيضا في حالة أخرى قام المدعو فلادمييير بوريليت و هو مهاجر روسي بإدخال فواتير وهمية لا حصر لها و تحويل ما تم تسديده لحساب شركات وهمية إصطنعها أيضا .[1]

و يعد إصطناع المعلومات هو الصورة الأكثر سهولة سيما في المنشآت المالية خاصة من المسؤول عن القسم المعلوماتي الذي يمكنه خلق مستخدمين غير موجودين أو عدم حذف المصروفين من مناصب عملهم و تحويل حقوقهم المالية إلى حساب الجاني أو لحساب فتح خصيصا لهذا الغرض و هي المعطيات التي لم تكن موجودة [2]

(1) أحمد خليفة الملط ، المرجع السابق ، ص 182 .
(2) محمد أمين الشوابكة ، جرائم الحاسوب و الإنترنت (الجريمة المعلوماتية) مكتبة دار الثقافة للنشر و التوزيع عمان الأردن ، 2004 ص 232.

ثانيا : المحو (l effacement)

يقصد بالمحو :" إقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق ضغط خصائص أخرى فوقها أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة ".

و عملية المحو هي عملية لاحقة على إدخال المعطيات فلمحو يفترض الوجود السابق لعملية الإدخال .

و يعرف أيضا أنه إزالة المعطيات أو جزء منها المثبتة على النظام أو نقلها أو تخزينها في منطقة خاصة فالمحو هو إزالة كل أثر للمعطيات داخل النظام عن طريق برنامج الدودة أو فيروس .

و يقصد بالفيروس " برنامج يتم إعداده من قبل شخص على درجة متقدمة من العلم بالبرمجة بإستخدام تقنيات متطورة يكون من خصائصه الإنتقال إلى أنظمة الحاسب الآلي و التكاثر فيه الأمر الذي يؤدي لتدمير البرامج و المعطيات المخزنة . " [1]

و إنقسم الفقه بشأن المحو إلى رأيين ، الأول يرى أن فعل المحو يتحقق إذا تم إزالة المعلومة نهائيا أو بإخفائها بحيث لا يمكن الوصول إليها دون أن يتم محوها فعليا بحيث لا يبقى لها أثر بالنظام .

في حين يتجه الرأي الثاني إلى أن إخفاء المعطيات دون محوها لا يشكل صورة المحو.

و حسب رأينا الرأي الأول هو الأصوب بإعتبار أن نقل المعلومات من النظام الذي كانت به لمنطقة محجوبة يحقق صورة الجريمة المتمثل في محو المعلومة ، و كونها لا تزال موجودة بمنطقة أخرى من عدمه سيام بإعتبار الجاني حرم صاحب النظام من المعطيات إما بإزالتها نهائيا أو بأخذها و الإحتفاظ بها بمنطقة أخرى أو بإحدى وسائط التخزين المعروفة .

(1) محمود أحمد عبابنة ، المرجع السابق ص 100 و 101 .

و لعل هذا ما قصده المشرع الجزائري من خلال صياغة نص المادة الذي لم ينص على كيفية محددة للمحو كما لم يتضمن شرحا لمفاهيم صور الجرائم بل إقتصر على تعدادها ، و عليه يتحقق المحو بأي صورة كانت حسب رأينا ، فيكفي أن تخفي المعطيات من المنظومة التي أدخلت إليها بصفة شرعية بداية لنكون أمام محو سواء تم الإحتفاظ بها من قبل الجاني أو أزال مباشرة نهائيا .

و من أمثلة الجرائم التي أرتكبت عن طريق المحو قيام شخصين بإختلاس مبلغ قدره 61 000 دولار مرسلة من شركات التأمين إلى إحدى المراكز الجامعية الأمريكية و التي جعلاها غير قابلة للتحصيل ، كما تم الكشف في مدينة دالاس الأمريكية عن أربعة من موظفي البلدية قاموا بمحو 271 مخالفة مدنية مقابل 300 16 دولار . [1]

ثالثا : التعديل (la modification)

يقصد بالتعديل تغيير المعطيات الموجودة داخل النظام و إستبدالها باخرى جزئيا أو كليا ، كذلك يتم التلاعب بالمعطيات عن طريق إستبدالها أو التلاعب بالبرنامج بإمداده بمعطيات مغايرة عن تلك التي صمم لأجلها [2] مما يؤدي لنتائج مغايرة عن تلك المنتظرة .

و يعرف التعديل أيضا بأنه تغيير لحالة المعطيات الموجودة دون تغيير الطبيعة الممغنطة لها أو هو كل تغيير غير مشروع للمعلومات و البرامج يتم عن طريق إستخدام إحدى وظائف الكمبيوتر و يتحقق فعل التغيير عن طريق برامج غريبة تتلاعب بالمعطيات .

و كقاعدة يتم تعديل المعطيات بإستعمال الفيروسات و القنابل المعلوماتية التي يصنعها شخص على درجة عالية من الذكاء و ذو قدرة عالية و تحكم بالتقنيات المعلوماتية و هو الملقبون بـ " المجرمين ذوي الياقات البيضاء " كفيروس الدودة الذي يمكن له في مرحلة متقدمة ليس تعديل النظام فقط بل قد يصل لتعطيل النظام أو فيروس موريس

(1) أحمد خليفة الملط ، المرجع السابق ، ص 183 .
(2) عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 95 .

نسبة لمصممه هو طالب كان يعد لرسالة دكتوراه و أساء إستخدام البرنامج الذي خرج عن السيطرة و تخلل حواسيب القوات المسلحة الأمريكية و غزى 6200 جهاز إعلام آلي ، أيضا نجد القنابل الموقوتة التي يرتبط بدأ تشغيلها بواقعة أو كلمة محددة أو تاريخ أو ساعة معينة متى قام بها المستخدم نشط البرنامج لتغيير محتوى المعطيات و هي الوسائل التي تحقق الجريمة في صورة المحو السالفة الذكر أو التعديل ، و بهذا المفهوم يخرج من هذه الصور نسخ المعلومات الموجودة و نقلها إذ لا تنطوي هذه الأعمال على إدخال و لا تعديل .

و تجدر الإشارة أنه فيما يتعلق بالتعديل فإن التوصية الصادرة عن المجلس الأوروبي المتعلقة بالجرائم المعلوماتية فرقت بين التعديلات التي تؤدي لنتائج سلبية ، و تلك التي تساعد على تحسين أي من مكنونات النظام إذ طالبت التوصية بإدراج الأولى ضمن القائمة الآساسية للجرائم المعلوماتية ، أما ذات الأثار الإيجابية ضمن القائمة الإختيارية .

غير أن معظم التشريعات لم تأخذ بالتوصية عند تجريمها للجرائم المعلوماتية و منها التشريع الجزائري الذي قام بتجريم صورة التعديل على مطلقها دون النظر لآثارها أو ما يترتب عليه من آثار إيجابية أو سلبية ، و يكفي تغيير المعطيات داخل النظام جزئيا أو كليا و بأي شكل لتحقق الجريمة .[1]

المطلب الثاني : الركن المعنوي لجريمة المساس العمدي بالمعطيات

جريمة التلاعب بالمعطيات تتطلب قصد جنائي عام و هو ما يستشف من نص المادة 394 مكرر 1 : " كل من أدخل أزال عدل بطريق الغش " فمصطلح الغش يدل على ضرورة توفر قصد جنائي عام بعنصريه ، و عليه يجب أن تتجه إرادة الجاني إلى إرتكاب السلوك الإجرامي بإحدى الصور على النحو السالف بيانه إما بإدخال معطيات داخل نظام المعالجة الآلية للمعطيات أو إزالة المعطيات الموجودة به أو تعديلها مع وجوب علمه أنه غير مسموح له بذلك أو أن ذلك يتجاوز حدود صلاحياته ، أو أنه يعلم

(1) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ،المرجع السابق ، ص 418 .

أن فعله سيؤدي حتما لنتيجة معينة هي إزالة المعلومة أو تغييرها أو تعديلها رغما عن علم صاحب الحق في هذه المعطيات أو من له حق السيطرة عليها .

و لا يشترط في القصد أن يكون معين بمعطيات معينة إذ يتحقق إذ قصد الجاني الدخول لمحو معطيات ثم تم محو أخرى و لو تم التلاعب بمعطيات عشوائيا دون تهديد هدف معين إذ يحمي قانون العقوبات كل المعطيات دون الحاجة لتحديدها .

و لا تتطلب المادة 394 مكرر 1 قصد خاص إنما يكفي توافر قصد عام إذ لا تشترط نية الإلحاق الضرر بالغير و لا يشترط أن يتصرف الجاني بنية إلحاق الضرر إذ تقوم الجريمة متى قصد الجاني التلاعب بالمعطيات المتضمنة بنظام المعالجة الآلية للمعطيات.

و شكلت صورة التلاعب في المعطيات 21 بالمئة من القضايا التي طرحت أمام القضاء الجزائري من 2005 إلى أفريل 2010 [1]

(1) مختار الأخضري ، المرجع السابق ص 68 .

المبحث الرابع : جرائم التعامل في معطيات غير مشروعة

و هي الجريمة المنصوص عليها بالمادة 394 مكرر 2 من قانون العقوبات الجزائري على النحو الآتي :

" يعاقب بالحبس من شهرين إلى ثلاث سنوات و بغرامة 000 000 1 دج إلى 000 000 10 دج كل من يقوم عمدا و عن طريق الغش بما يأتي :

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أو ترتكب بها الجرائم المنصوص عليها في هذا القسم .

2- حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من أحدى الجرائم المنصوص عليها في هذا القسم "

و في هذه المادة عمد المشرع لتجريم مجموعة من الأفعال التي تمس بالمعطيات في حد ذاتها على خلاف الجرائم السالفة الذكر التي تعلقت بالمعطيات الموجودة داخل نظام المعالجة الآلية و خص المعطيات التي تصلح لأن ترتكب بها إحدى الجرائم التي تمس سريتها سلامتها او وفرتها هذا من جهة ، كما جرم ثانيا التعامل بالمعطيات المتحصل عليها من جريمة و خص هذه الأخيرة أن تكون من إحدى الجرائم المنصوص عليها بهذا القسم و هي تلك التي سبق و فصلنا فيها.

و في ذات السياق أشارت إتفاقية بودابست لسنة 2001 في مذكرة تفسيرية إلى الهدف من تجريم هذه الأفعال بـ :

"جرائم المعطيات يتطلب إرتكابها حيازة وسائل الولوج كأدوات القرصنة أو أي أدوات أخرى و أن هناك دافعا قويا للحصول على هذه الوسائل لأغراض إجرامية ، مما يؤدي إلى خلق نوع من السوق السوداء لإنتاج و توزيع مثل هذه الأدوات ، و أنه و من أجل وقاية أكثر فعالية من هذه المخاطر فإنه يجب على قانون العقوبات أن يحظر الأفعال راجحة الخطورة من المنبع قبل إرتكاب الجرائم المشار إليها بالمواد 2 إلى 5 " [1]

(1) محمد خليفة ، المرجع السابق ، ص 62 .

و ما يستشف من المادة 394 مكرر 2 من قانون العقوبات أن المشرع جرم فئتين من التعامل بالمعطيات لهدفين إثنين :

الأول تجريم التعامل في المعطيات التي يمكن أن ترتكب بها جريمة الهدف من وقائي لمنع حدوث الجريمة .

الثاني تجريم التعامل في المعطيات المتحصل عليها من جريمة و الهدف منه الحد قدر الإمكان من الآثار و النتائج المترتبة على الجريمة الأولى التي سبق إرتكابها للتضييق من دائرة الجناة المتعاملين بطريقة غير مشروعة فيها .

المطلب الأول : الركن المادي لجريمة التعامل في المعطيات غير المشروعة

بقراءة المادة 394 مكرر 2 من قانون العقوبات فإن الركن المادي لهذه الجريمة يتمثل في مجموعة من الأفعال مذكورة على سبيل الحصر .

و ما يلاحظ أوليا أنه طبقا للقواعد العامة المتعلقة بالمساهمة المنصوص عليها بقانون العقوبات فإن الأفعال المجرمة بهذه الفئة لا تتعدى كونها من أعمال الإشتراك طبقا للمادة 42 من قانون العقوبات .

فهي ليست مساهمة مباشرة في الجريمة إنما أعمال مساعدة و معاونة جعل منها المشرع جريمة كاملة و تامة بنص خاص و عليه أصبحت فعل مجرم مستقل عن الجريمة الأصلية ، و الفائدة من ذلك تكمن في إمكانية عقاب أفعال المساعدة في غياب الجريمة الأصلية [1]

و سندرس الركن المادي لهذه الفئة من الجرائم في نقطتين :

1 – محل الجريمة

2 – السلوك المجرم : المتمثل في فئتين

- التعامل في معطيات صالحة لإرتكاب جريمة

(1) سي الحاج أحمد ، المرجع السابق ، ص 25 .

- التعامل في معطيات متحصلة من جريمة

أولا : محل الجريمة

محل الجريمة طبقا للمادة 394 مكرر 2 من قانون العقوبات إما :

1- معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية .

2- معطيات متحصل عليها من إحدى الجرائم المنصوص عليها بالمواد من 394 مكرر و 394 مكرر 1

و بهذا التعداد فإن المشرع هدف لتوسيع دائرة التجريم إذ شمل بالحماية المعطيات مهما كانت حالتها ، إذ لم تقتصر على تلك الموجودة بنظام المعالجة الآلية كالجرائم السابقة بل وسع المجال إلى مختلف المعطيات مهما كانت حالتها مخزنة ، مرسلة ، معالجة على إعتبار إمكانية إرتكاب جرائم حتى بإستعمال معطيات موجودة على وسائط تخزين خارجية .

كما لم يخص المشرع بالتجريم المعطيات المعدة لإرتكاب جريمة بالتحديد بل يكفي أن تكون صالحة أو قابلة لأن ترتكب بها جريمة و هذا ما نصت عليه المادة 394 مكرر 2 بالفقرة الأولى بعبارة " ...يمكن **أو** ترتكب بها الجرائم ..." .

و هو ذات المفهوم الوارد بالمادة 6 من إتفاقية الإجرام المعلوماتي التي جعلت محلا لهذه الجريمة كل جهاز يشمل برنامج حاسب آلي تم تصميمه أو تطويعه أساسا لغرض إرتكاب إحدى الجرائم المنصوص عليها بالمادتين 2 و 5 .

و التي تقابلها المادة 323 من قانون العقوبات الفرنسي التي تنص على أن التعاملات المجرم يمكن أن تقع أيضا على تجهيزات أو أدوات أو على برنامج معلوماتي أو على كل معطيات مصممة أو معدة لإرتكاب واحدة أو أكثر من جرائم الدخول أو البقاء الغير مصرح بهما أو إعاقة أو إفساد أنظمة المعالجة الآلية للمعطيات أو التلاعب بالمعطيات.

و عليه فالمشرع الجزائري حصر نطاق هذه الجريمة بالمعطيات التي تكون قابلة لإرتكاب جريمة أو يكفي أن تكون صالحة لذلك أو المتحصل عليها من جريمة ، في حين المشرع الفرنسي توسع في محل الجريمة ليشمل كل الوسائل التي يمكن إستخدامها في

إرتكاب الجرائم سواء ذات طبيعة مادية أو غير مادية المعدة و المصممة لإرتكاب واحدة أو أكثر من الجرائم الماسة بالمعطيات .

ثانيا : السلوك المجرم

1 – التعامل في معطيات صالحة لإرتكاب جريمة

و هي الجريمة المنصوص عليها بالفقرة الأولى من المادة 394 مكرر 2 من قانون العقوبات و ورد فيها أفعال على سبيل الحصر و التي تشمل كافة أشكال التعامل على المعطيات السابقة لعملية إستعمالها في إرتكاب جريمة و المتمثلة في ست أفعال (التصميم – البحث – التجميع – التوفير – النشر – الإتجار)

أ – التصميم : يعني إيجاد و خلق معطيات صالحة لإرتكاب جريمة و هذا العمل يقوم به المتخصصون كالمبرمجين و مصممي البرامج مثلا تصميم فيروس ، برامج خبيثة ، برامج إختراق و قرصنة و عادة مرتكبي هذه الجرائم يكونون على كفاءة و دراية عالية بالبرمجة و مختصين بالإعلام الآلي .

ب – البحث : البحث في تصميم المعطيات و إعدادتها .

ج – التجميع : جمع المعطيات التي يمكن إستخدامها لإرتكاب جريمة أخرى من المذكورة بالفصل و يفترض أنها معلومات تشكل خطرا.

د – التوفير : ورد بالنص الفرنسي عبارة (met a disposition) و الترجمة الحرفية لها هي "الوضع تحت التصرف" و هو ذات المصطلح الوارد في إتفاقية بودابست و هو المعنى الأدق و الأكثر ملائمة و عليه يقصد بالتوفير وضع المعطيات الممكن إستخدامها في إرتكاب جريمة تحت تصرف الغير و إتاحتها لمن يريد إستخدامها

ه – النشر : هو إذاعة المعطيات و التمكين من الإطلاع عليها بأي وسيلة من وسائل النشر و هو من أخطر الأفعال لأنه من شأنه نقل المعلومات لأكبر عدد من الأشخاص في وقت واحد قياسي.

و – الإتجار : مصطلح الإتجار يشير مباشرة للمقابل لقاء الحصول على المعطيات من أجل إستخدامها و قد يكون المقابل نقدي أو عيني أو خدماتي .

للإشارة لم تنص إتفاقية بودابست أو المشرع الفرنسي للإتجار كسلوك مجرم للتعامل في المعطيات بل إكتفت الإتفاقية بالبيع و الإستيراد و إكتفى المشرع الفرنسي بالاستيراد.

2 – التعامل في معطيات متحصلة من جريمة :

و هي الجريمة المنصوص عليها بالفقرة الثانية من المادة 394 مكرر 2 من قانون العقوبات و هي الجريمة التي تتحقق بأربع سلوكات ذكرت على سبيل الحصر المتمثلة في (الحيازة – الإفشاء- النشر – الإستعمال) .

أ – الحيازة :

الحيازة هي السيطرة الواقعية و الإرادية للحائز على المنقول تخوله مكنة الإنتفاع به أو تعديل كيانه أو تحطيمه أو نقله ، فهي السيطرة من الشخص على الشيء التي تستند لسبب قانوني

و في هذه الحال المعطيات هي منقولات معنوية التي تخول الحائز الإنتفاع به أو تعديل كيانه أو تحطيمه أو نقله فهي سيطرة إرادية و تامة على الشيء و التي قد تكون غير مشروعة .

و الحيازة في قانون العقوبات ليست حقا عينيا كالقانون المدني فقد تكون حيازة الجاني مشروعة أو غير مشروعة و فيما يتعلق بجريمة التعامل بالمعطيات فيفترض في الحيازة أنها غير مشروعة يسيطر من خلالها الجاني على المعطيات بالشكل الذي يمكنه من خلاله تعديلها ، إستعمالها ، إزالتها ، الإنتفاع بها و إستغلالها و لو كانت هذه الإستفادة محدودة .

ب – الإفشاء :

يقصد بالإفشاء نقل المعطيات من حيازة الشخص الذي تحصل عليها بطريقة غير مشروعة إلى غيره و من يقوم بذلك ليس مؤتمنا على المعطيات فقد لا يكون ملزما قانونا بكتمانها التي قام بإفشائها إنما تحصل عليها أيضا بطريقة غير مشروعة و نشرها .

ج – النشر :

سبق و تطرقنا للنشر بصدد التعامل في المعطيات الصالحة لإرتكاب جريمة و هي صورة مشتركة بين هذه الأخيرة و التعامل في معطيات متحصلة من جريمة و هو ذات المفهوم بإختلاف المحل و المقصود منه إذاعة المعطيات و التمكين من الإطلاع عليها بأي وسيلة من وسائل النشر .

د – الإستعمال : هو إستخدام و إستعمال المعطيات و يشمل الإستعمال كل المعطيات و مهما كان الهدف منه مهما كانت كيفيته إذ ورد بالمادة عبارة " ...أو إستعمال لأي غرض كان..." كل ما في الأمر أن يتم إستعمال معطيات تم التحصل عليها من إرتكاب جريمة أخرى بطريقة غير مشروعة [1] و هو أخطر الأفعال .

و كما سلف الذكر مجرد توافر إحدى الصور جرمها المشرع و جعل منها جريمة قائمة بذاتها و دون أن يشترط ترتب نتيجة معينة أو ضرر معين سواء على المعطيات أو النظام .

المطلب الثاني : الركن المعنوي لجريمة التعامل في معطيات غير مشروعة

جريمة التعامل في المعطيات غير المشروعة هي جريمة عمدية لا بد من توافر عنصري القصد الجنائي من علم و إرادة ، و عليه يجب أن يعلم الجاني أنه يتعامل بمعطيات غير مشروعة التي من شأنها أن تستعمل في إرتكاب جرائم بالنسبة للصورة الأولى .

أو يعلم أنه يتعامل بمعطيات متحصل عليها من جريمة بالنسبة للصورة الثانية .

و رغم ذلك تتجه إرادته لإرتكاب إحدى السلوكات المنصوص عليها بالمادة السالفة الذكر ، و هنا يطرح الإشكال هل تتطلب جريمة التعامل بمعطيات غير مشروعة قصد جنائي خاص أم يكفي قيام القصد الجنائي العام ؟

ذهب جانب من الفقه إلى أن الصورة الأولى تتطلب قصد خاص إذ لا يمكن مسألة الجاني إلا إذا كان له قصد في الإعداد لإستعمال هذه المعطيات في جريمة أخرى .

---

(1) محمد خليفة ، المرجع السابق ، ص 200 إلى 206 .

و حسب رأينا يكفي توافر القصد العام إذ لم تنص المادة 394 مكرر 2 على وجوب توافر قصد خاص حتى فيما يتعلق بالصورة الأولى إذ نصت المادة على إمكانية إستعمال المعطيات و لم تشترط أن تستعمل فعلا لتقوم الجريمة .

و تجدر الإشارة لأن المشرع على خلاف الجرائم السابقة نص على العمد و الغش معا رغم أن باقي الجرائم أيضا عمدية و لعل هذا راجع للتأكيد على العمديـة لأن المعطيـات التي ترد عليها الجريمة ليست معدة كمبدأ لإرتكاب جريمة بل يرد عليها تعامل يجعل منها غير مشروعة و إستعمالها " عن طريق الغش " و بصفة " عمدية " هو ما يضفي عليها وصف التجريم .

و الغش يكمن في العلم بطبيعة هذه المعطيات و صفتها الغير مشروعة و مع ذلك يقوم الجاني بالتعامل فيها [1]

و شكلت صورة التلاعب في المعطيات الغير مشروعة 13 بالمئة من القضايا التي طرحت أمام القضاء الجزائري من 2005 إلى أفريل 2010 [2]

بعد بيان صور المساس بأنظمة المعالجة الآلية للمعطيات و تفصيل أركانها من حيث الركن المادي و المعنوي طبقا لما ورد بمواد قانون العقوبات و ما تناوله الفقه شرحا للمفاهيم الواردة به ، ننتقل في الفصل الثاني لسبل قمع هذه الجرائم و مسألة الإختصاص و التحري فيها ، طرق الإثبات و التحري و الجزاءات المقررة لها .

(1) محمد خليفة ، المرجع السابق ، ص 218.
(2) مختار الأخضري المرجع السابق ، ص 68.

الفصل الثاني : قمع الجرائم الماسة بانظمة المعالجة الآلية للمعطيات

سبق و تطرقنا في الفصل الأول إلى بيان صور الجرائم الماسة بانظمة المعالجة الآلية للمعطيات و فصلنا في أركانها كما وردت في قانون العقوبات الجزائري ، و قارناها بنصوص قانون العقوبات الفرنسي .

و نظرا لخصوصية هذه الجرائم و إتسامها بميزات سبق بيانها في الفصل التمهيدي مقارنة بباقي الجرائم إضافة لأنها جرائم ذات طابع دولي ، و مسايرة لهذا النوع من الجرائم التي تطرح إشكاليات متزايدة يوما بعد يوم تسعى التشريعات الوطنية لإيجاد حلول لها بسن نصوص جديدة موضوعية تنص على جرائم جديدة ، و نصوص إجرائية تنظم إختصاص الهيئات القضائية ، المتابعة و أشكال جمع الأدلة الإلكترونية و قيمتها القانونية بالنظر للأدلة الأخرى .

و على المستوى الدولي أصبحت هذه الجرائم تخرج عن النطاق الوطني و لم تعد تضع إعتبارا للحدود الجغرافية بعد أن أصبح العالم متصل بشبكة عنكبوتية واحدة تصل لأبعد نقطة فيها في لحظات زمنية معدودة .

و لعل الرادع الأكبر الواجب على الدول إعتماده لقمع هذه الجرائم هو توسيع الجهود في مجال التعاون الدولي فيما يتعلق بهذه الجرائم و خصها بقواعد إجرائية فعالة.

و هذا ما أخذ به المشرع الجزائري الذي إعتمد توصيات الإتفاقية الدولية للإجرام المعلوماتي ، و إستحدث موادا تنص على هذه الجرائم و تعاقب على الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، و أخرى تنص على قواعد إجرائية .

و سنحاول في هذا الفصل دراسة وسائل قمع هذه الجرائم فنتناول في مبحث أول مسألة الاختصاص و التحري ، و هنا يطرح إشكال القانون الواجب التطبيق في ظل الواقع الإفتراضي الذي ترتكب فيه هذه الجرائم التي لا تتعلق بواقع و حيز مادي محدد و بالتبعية يطرح هذا إشكال الإختصاص القضائي ثم أساليب التحري و التحقيق فيها .

أما في المبحث الثاني نعالج إشكالية الإثبات من حيث إجراءات الحصول على الدليل الإلكتروني و خصوصية و تقدير قيمته في ظل قانون الإجراءات الجزائية الجزائري .

و أخيرا و في المبحث الثالث نتعرض إلى الجزاء المقرر لهذه الجرائم بالنسبة للشخص الطبيعي ثم الشخص المعنوي ، و كذا الجزاء المقرر للإتفاق الجنائي و الشروع .

المبحث الأول : الإختصاص و التحري في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

يطرح القانون الواجب التطبيق و الجهة القضائية المختصة بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات عدة إشكالات ذلك أن غالبية هذه الجرائم ترتكب من قبل أشخاص من خارج حدود الدولة ، أو أنها تمر عبر شبكات معلوماتية و أنظمة من خارج الحدود حتى عندما يرتكبها شخص من دولة على نظام الدولة نفسها [1] هذه الجرائم التي تقتضي السرعة في التحري و التحقيق فيها خشية ضياع الدليل .

و لما كانت هذه الجرائم تتميز بطبيعة خاصة فإنه يتوجب لمواجهتها تأهيل نوع خاص من رجال الضبطية و القضاة من نيابة و تحقيق و حكم ، خاصة مع إستحداث الأقطاب الجزائية المتخصصة .

و هنا يطرح إشكال القانون الواجب التطبيق و الجهة القضائية المختصة في التحقيق و الفصل و كذا إشكالية تطبيق أساليب التحري المنصوص عليها في قانون الإجراءات الجزائية على هذه الجرائم .

المطلب الأول : القانون الواجب التطبيق بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

نصت المادة 22 من القانون العربي النموذجي لمكافحة جرائم الكمبيوتر و الأنترنيت على أنه : " تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا ارتكبت كلها أو جزء منها داخل حدودها ، كما تختص محاكمها بنظر الدعوى المترتبة عن تلك الجرائم ، و على الدول العربية عقد إتفاقات لتبني المعيار الأول في حالة تنازع الإختصاص بين الدول .

(1) يوسف عرب ، جرائم الكمبيوتر و الإنترنيت ورقة عمل مقدمة إلى مؤتمر الأمن العربي تنظيم المركز العربي للدراسات و البحوث الجنائية أبوظبي 2002 ، ص 18

كما يسري التشريع الجنائي للدولة على الجرائم المعلوماتية التي تقع خارج الحدود إذا كانت مخلة بأمنها وفقا للقواعد العامة المنصوص عليها في قانون العقوبات[1]

أولا : الجرائم المرتكبة فى الإقليم الجزائري :

و نص المشرع الجزائري في المادة الثالثة من قانون العقوبات على أنه :

" يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية"

و عليه يطبق القانون الجزائري سواء كانت الجريمة مرتكبة من مواطن جزائري أو أجنبي متى تم إرتكابها داخل إقليم الجمهورية الجزائرية ، و هنا يطرح إشكال عند إرتكاب أحد الأعمال المكونة للركن المادي في الجزائر و الباقي في دولة أخرى؟

هذا الإشكال أجابت عليه المادة 586 من قانون الإجراءات الجزائية التي تنص أنه تعتبر مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر تطبيقا لمبدأ إقليمية القوانين الذي أساسه سيادة الدولة على إقليمها تطبيقا للمادة 12 فقرة 2 من الدستور الجزائري التي تنص على أن إقليم الدولة يتكون من المجال البري و الجوي و البحري .

- فالمجال البري هو المساحة الأرضية التي تباشر الدولة عليها سيادتها و تنظم و تقوم فيها بالخدمات العامة .

-أما المجال البحري هو المنطقة الواقعة بين شاطئ الدولة و البحر العام و التي تلزم لتحقيق اغراض دفاعية و صحية و إقتصادية مع العلم أن سيادة الدولة تمتد من شاطئها مسافة البحر الإقليمي 12 ميل .

- أما المجال الجوي هو الفضاء الذي يعلو إقليمها الأرضي و بحرها الإقليمي .

كما يطبق القانون الجزائري على الجنايات و الجنح التي ترتكب في ميناء بحرية جزائرية و على ظهر باخرة أجنبية أو طائرات أجنبية هبطت بالجزائر بعد وقوع الجريمة .

(1) عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر و الأنترنيت ، دار الفكر الجامعي الإسكندرية ، 2006 ص 49

و على هذا الأساس يطبق القانون الجزائري متى ارتكبت الجريمة على إقليم الدولة الجزائرية ، كما نصت المادة 585 على انه يطبق قانون العقوبات الجزائري على كل من كان في إقليم الجمهورية شريكا في جناية او جنحة مرتكبة بالخارج بشرطين :

- أن يكون الفعل معاقب عليه بالجزائر و البلد الذي ارتكب فيه الفعل .

- أن تكون الواقعة موصوفة بجناية أو جنحة و ثبت ارتكابها بقرار نهائي من جهات قضائية أجنبية .

ثانيا : الجرائم المرتكبة خارج الإقليم الجزائري من جزائريين

و نظرا لكون المشرع الجزائري قد اخذ بمبدأ الشخصية كأساس لتطبيق قانون العقوبات الجزائري على الجرائم المرتكبة خارج الإقليم الجزائري على كل حامل للجنسية الجزائرية طبقا للمواد 582 و 583 من قانون الإجراءات الجزائية شرط:

- أن تكون الواقعة تشكل جناية أو جنحة في التشريع الوطني و تشريع الدولة التي ارتكبت فيها.

- أن يكون المتهم جزائريا وقت ارتكاب الجريمة .

- أن يعود المتهم للجزائر.

- ألا يكون المتهم قد حكم عليه نهائيا في الخارج تطبيقا لمبدأ عدم جواز محاكمة متهم من أجل ذات الواقعة مرتين.

ثالثا : الجرائم الماسة بالمصالح الأساسية للدولة :

نصت المادة 588 من قانون الإجراءات الجزائية على تطبيق القانون الجزائري طبقا لمبدأ العينية متى وجد مساس بالمصالح الأساسية للدولة على كل أجنبي او جزائري يرتكب خارج الإقليم جريمة تمس بالدولة ، و مبرر ذلك وجوب الدفاع عن سيادة الدولة.

و زيادة على المادة السالفة الذكر ورد النص بالمادة 15 من القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال النص على إختصاص المحاكم الجزائرية بالنظر في القضايا المتعلقة بجرائم المساس بأنظمة المعالجة الألية للمعطيات (كإحدى فئات الجرائم المتصلة بتكنولويات الإعلم و الإتصال) المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها

أجنبيا و يستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني .

غير أن الصعوبة تظهر في أن تحديد مكان ارتكاب الجريمة ليس سهلا فقد يقوم الجاني مثلا بإستعمال جهاز محمول مزود بخدمة الإنترنيت لإختراق نظم عدة دول في وقت واحد .

و بالعودة لصور الجريمة التي تم عرضها بالفصل السابق نجد أن الدخول أو البقاء الغير مشروع بصورته البسيطة أو المشددة ، أو المساس بالمعطيات و التعامل بمعطيات غير مشروعة متى تم بالجزائر فإن المشرع اعتبر أنها جرائم مرتكبة في الجزائر أو متى تحققت الجريمة في الجزائر ، و كذا إذا بدا تنفيذها في الجزائر و تحقق أثرها في دولة أخرى فيطبق القانون الجزائري تطبيقا لأحد المبادئ الشخصية ، العينية أو الإقليمية .

غير أن تطبيق هذه المبادئ يقتضي وجود تعاون دولي فعال ، و تخوف الدول في العصر الراهن من الإعتداء على خصوصية و سرية المعلومات بهدف التجسس و غير ذلك أصبح هاجس يحول دون الحصول على المعلومات اللازمة لإثبات الجريمة عند وقوعها و تحديد أدلتها و فاعليتها لمباشرة المتابعة الجزائية .

و ما يؤكد ذلك نص القانون السالف الذكر في المادة 18 تحت عنوان القيود الواردة على طلبات المساعدة القضائية الدولية على رفض تنفيذ أي طلب إذا كان من شأنه المساس بالسيدة الوطنية أو النظام العام .

و يستجاب للطلب المقيد بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم إستعمالها في غير ما هو موضح في الطلب .

لذلك نادى البعض بضرورة إنشاء وحدات خاصة بمكافحة الجريمة المعلوماتية بواسطة الحاسب الآلي و الأنترنيت أسوة بجهات البحث الجنائي الوطنية و الدولية " الأنتربول " لإثبات الجريمة عند وقوعها و تحديد أدلتها و فاعليتها ، و هو ما يعني كذلك إيجاد صيغة ملائمة للتعاون الدولي و تبادل الخبرات و المعلومات حول هذا النوع من الجرائم و مرتكبيها و سبل مكافحتها.

و من العراقيل التي تفرضها هذه الجرائم أيضا عدم وجود نموذج قانوني واحد متفق عليه ، فالتشريعات الجنائية للدول غير متطابقة فالجريمة التي تضر بمصالح دولة معينة قد ترتكب في دولة أخرى و تعد فعلا مباحا ، و عليه لا يمكن لهذه الأخيرة بسط سلطان المتابعة عليه .

المطلب الثاني : الإختصاص القضائي

الإختصاص هو مباشرة سلطة المتابعة و التحقيق و الحكم في الجريمة وفقا للقواعد التي رسمها القانون و الحدود التي تبناها المشرع لهذه السلطات أثناء ممارسة مهامها .

و نصت المادة 22 من إتفاقية بودابست على أنه لكل طرف إتخاذ الإجراءات التشريعية و غيرها التي يراها لازمة كي يحدد إختصاصه و بالنسبة لكل جريمة تقع وفقا لما هو وارد بالمواد من 2 إلى 11 من الإتفاقية عندما تقع الجريمة :

- داخل النطاق المحلي للدولة .
- على ظهر سفينة تحمل علم الدولة .
- على متن طائرة مسجلة بهذه الدولة .
- بواسطة أحد رعاياها إذا كانت الجريمة معاقبا عليها جنائيا في المكان الذي إرتكبت فيه إو إذا كانت الجريمة لا تدخل في أي إختصاص مكاني لأي دولة .

و لكل طرف أي يحتفظ لنفسه بحق عدم تطبيق قواعد الإختصاص إلا بشروط خاصة المنصوص عليها في الفقرة الأولى .

(1) عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، المرجع السابق ، ص 187 .

أولا : القاعدة العامة في الإختصاص

حدد المشرع الجزائري معايير الإختصاص المحلي في قانون الإجراءات الجزائية في المواد 37 ، 40 و 329 .

1 – الإختصاص المحلي لوكيل الجمهورية :

بالنسبة لوكيل الجمهورية تنص المادة 37 فقرة أولى من قانون الإجراءات الجزائية على أن الإختصاص المحلي له يتحدد بمكان وقوع الجريمة أو بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى و لو حصل هذا القبض لسبب آخر .

2 – الإختصاص المحلي لقاضي التحقيق :

و أما بالنسبة لقاضي التحقيق تنص المادة 40 الفقرة الأولى على أن إختصاصه المحلي يتحدد بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى و لو كان هذا القبض قد حصل لسبب آخر.

و عن ضباط الشرطة القضائية طبقا للمادة 1/16 من قانون الإجراءات الجزائية فإنهم يمارسون إختصاصهم المحلي في حدود الدائرة التي يباشرون فيها وظائفهم المعتادة ، و في حالات الإستعجال لهم مباشرة مهامهم في كافة إختصاص المجلس القضائي الملحقين به أو كافة الإقليم الوطني بناءا على أمر من القاضي المختص و بعد إطلاع وكيل الجمهورية التابعين له .

3 – الإختصاص المحلي لجهات الحكم :

و أما فيما يخص جهات الحكم في مواد الجنح فتنص المادة 329 على أنه تختص محليا بالنظر في الجنحة المحكمة محل إرتكاب الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم و لو كان هذا القبض قد وقع لسبب آخر .

كما تختص محكمة محل حبس المحكوم عليه إستثناءا طبقا لأحكام المواد 552 و 553 من قانون الإجراءات الجزائية إذا كان المحكوم محبوسا بحكم نهائي أولا عليه بعقوبة سالبة للحرية بنظر القضايا المنسوبة إليه فيما يخرج عن المواد 37 ، 40 و 329 من

قانون الإجراءات الجزائية ، كما تختص المحكمة في نظر الجنح و المخالفات الغير قابلة للتجزئة أو المرتبطة .

و يرجع الإختصاص للمحكمة التي ارتكبت في نطاق دائرتها المخالفة أو المحكمة الموجودة في بلد إقامة مرتكب المخالفة بالنظر في تلك المخالفة .

و نوعيا بالنسبة للأحداث فإن قسم الأحداث المختص إقليميا هو المحكمة التي ارتكبت الجريمة بدائرة إختصاصها أو بها محل إقامة الحدث أو والديه أو وصيه ، أو محكمة المكان الذي عثر فيه على الحدث أو المكان الذي أودع به الحدث سواء بصفة مؤقتة أو نهائية طبقا لأحكام المادة 451 من قانون الإجراءات الجزائية في فقرتها الثالثة .

و عن معيار مكان وقوع الجريمة فهو يختلف حسب طبيعة الجريمة إذ يتحدد بالنسبة للجريمة الوقتية بالمكان الذي وقع فيه تنفيذ الفعل ، و بالنسبة للجريمة المستمرة يتحدد المكان بكل مكان قامت فيه حالة إستمرار الفعل ، و بالنسبة للجرائم المتتابعة يعتبر مكان إرتكاب الجريمة كل مكان تقع فيه أحد الأفعال.

و مثال ذلك نشر فيروس ثم يتحقق إتلاف لمعطيات بنظام معين إذ تم تنشيطه بمكان و تحققت النتيجة بمكان أخر أو أكثر . فالإختصاص ينعقد بمكان إرتكاب السلوك أو النتيجة على حد سواء ، فنكون أمام جرائم متعددة بعدد المرات التي إنتشر فيها الفيروس مع مراعاة مبدأ عدم جواز متابعة المتهم عن ذات الجريمة مرتين بأن يتابع الشخص على نشر فيروس واحد بكل المحاكم التي تحققت النتيجة بها و هنا تكون الجهة المختصة هي الجهة التي تحال عليها أول حالة .

أما عن محل إقامة المتهم فالعبرة بالمحل الذي كان يقيم فيه المتهم وقت اتخاذ إجراءات المتابعة بغض النظر عن التغييرات التي تحدث به [1]

(1) جيلالي بغدادي ، التحقيق دراسة مقارنة و تطبيقية ، الديوان الوطني للأشغال التربوية ، الطبعة الأولى 1999 ص 108 .

و مثال التعاون الدولي البناء في مجال الإختصاص ما أقدمت عليه دول الإتحاد الأوروبي من إعتبارها دولة واحدة و إقليم واحد لحل مشكلة المحكمة المختصة بنظر الدعاوى الجنائية الناتجة عن كافة الجرائم المعلوماتية [1]

ثانيا : تمديد الإختصاص

بعد صدور المرسوم التنفيذي رقم 348/06 المؤرخ 2006/10/05 المتضمن تمديد الإختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و جهات التحقيق ، و تم إستحداث ما يعرف بالأقطاب الجزائية المتخصصة لمحاكم (قسنطينة ، ورقلة ، وهران ، سيدي أمحمد) المتخصصـــة للفصل في نـوع خـاص من الجرائـــم المحددة على سبيل الحصر منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و التي حددت المواد من 2 إلى 5 مجال تمديد الإختصاص فيها على النحو التالي :

- محكمة سيدي محمد : يمتد فيها الإختصاص المحلي إلى محاكم المجالس القضائية للجزائر ، الشلف ، الأغواط ، البليدة ، البويرة ، تيزي وزو ، الجلفة المدية ، المسيلة ، بومرداس ، تيبازة و عين الدفلى .

- محكمة قسنطينة : يمتد فيها الإختصاص المحلي إلى محاكم مجالس قسنطينة ، أم البواقي ، باتنة ، بجاية ، بسكرة ، تبسة ، جيجل ، سطيف ، سكيكدة ، عنابة ، قالمة ، برج بوعريريج ، الطارف ، الوادي ، خنشلة ، سوق أهراس و المسيلة.

- محكمة ورقلة : يمتد فيها الإختصاص المحلي إلى محاكم المجالس القضائية لورقلة ، أدرار ، تمنراست ، إيليزي ، تندوف و غرداية .

- محكمة وهران : يمتد فيها الإختصاص المحلي إلى محاكم المجالس القضائية لوهران، بشار ، تلمسان ، تيارت ، سعيدة ، سيدي بلعباس ، مستغانم ، معسكر ، البيض ، تسمسيلت ، النعامة ، عين تموشنت ، غليزان .

---

(1) عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت، المرجع السابق ، ص 88 .

و نصت المادة 6 من ذات المرسوم أنه يعود لرئيس المجلس القضائي الذي يقع بدائرة إختصاصه المحكمة التي تم تمديد إختصاصها للفصل بموجب أمر في الإشكالات التي قد يثيرها تطبيق أحكام المرسوم ، دون أن يكون هذا الأمر قابلا لأي طعن .

و تضمنت المواد 40 مكرر إلى 40 مكرر 5 الإجراءات أمام الأقطاب الجزائية، إذ يجب على وكيل الجمهورية الذي وقعت بدائرة إختصاصه إحدى هذه الجرائم أن يرسل نسخة من ملف الإجراءات فورا إلى النائب العام لدى المجلس القضائي التابعة له المحكمة ذات الإختصاص الموسع الذي يحيلها لها لتتخلى الجهة الأصلية عن الملف .

و تجدر الإشارة إلى أنه يجوز للنائب العام طلب ملف الإجراءات في اي مرحلة من مراحل الدعوى ، فإن كان الملف على مستوى قاضي التحقيق عليه أن يصدر أمرا بالتخلي لفائدة قاضي التحقيق بالمحكمة ذات الإختصاص الموسع ، و في هذه الحال يتلقى ضباط الشرطة القضائية التعليمات و الإنابات مباشرة من هذا الأخير.

و جاء هذا المرسوم تبعا لتعديل قانون العقوبات بموجب القانون 14/04 المؤرخ 10 نوفمبر2004 الذي نص في المادة 37 فقرة 2 و 40 فقرة 2 و 329 فقرة أخيرة على جواز تمديد الإختصاص المحلي لوكيل الجمهورية أو قاضي التحقيق أو المحكمة إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

و تجدر الملاحظة أنه لم يتم تعديل المادة 451 من قانون الإجراءات الجزائية المتعلقة بإختصاص قسم الأحداث على غرار باقي المواد و لعل مرد ذلك أن قانون الإجراءات الجزائية مكن وكيل الجمهورية في القضايا المتشعبة كهذه الجرائم أن يقدم طلب إفتتاحي واحد للأحداث و البالغين لقاضي التحقيق طبقا للمادة 452 فقرة أخيرة و لكن لم يتم النص على تمديد الإختصاص إذا تعلق الأمر بأحداث فقط .

المطلب الثالث : التحري و التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

عند الحديث عن البحث و التحري عن الجريمة المعلوماتية عامة و الجرائم الماسة بأنظمة المعالجة الألية للمعطيات يرى جانب من الفقه أنه يصعب تطبيق قواعد البحث و الضبط في هذا الفضاء المعنوي الذي تقع فيه هذه الجرائم ، في غياب نقاط المراقبة و عدم ذكر الأسماء و التشفير مما يصعب من تحديد شخصية مرتكب الجريمة و يعقد من عمل الضبطية و القضاة ، غير أنه يوجد جانب من الفقه إعتبر هذا الرأي غير صحيح لحد ما للأسباب التالية : [1]

- إذا لم يمتد أثر الجريمة لخارج الدولة يستطيع المحقق إتخاذ أي إجراء من شأنه الكشف عن الجريمة دون عقبات .

- عدم معرفة المرسل خلال الشبكة هو أمر نسبي حيث يترك الفاعل أثرا أثناء تنقله يسمح بالوصول إليه .

- الطابع الدولي للجريمة لا يمثل عقبة في إجراء التحقيق.

و قد تم إبداء هذه الملاحظات عند إنعقاد قمة واشنطن في ديسمبر 1997 للدول الثماني التي وضعت عشر مبادئ لمقاومة الجرائم المعلوماتية .

في فرنسا صدر قانون قود فران (God frain) بتاريخ 1997/01/05 لمكافحة الجرائم التقليدية و الحديثة الخاصة بالمعلومات كالفيروسات و القنابل المنطقية ، حصان طروادة ، برامج التجسس و القرصنة .

في الولايات المتحدة الأمريكية صدر قانون في 1998/05/15 يلزم بالكشف عن هوية المستخدمين مما يسهل تتبع أي خرق.

---

(1) صالح أحمد البربري ، المرجع السابق ، ص 4 و 5 .

و رغم أن الكشف عن هوية مرتكب الجريمة ما زال يواجه الكثير من الصعوبات إلا أن الدول تعمل على إستحداث إجراءات جديدة تسهل من البحث و التحري للكشف عن الجريمة لاحقا مثل القانون الصادر 1986/09/30 في فرنسا الذي يوجب في مادته الثالثة و الأربعين على جميع مؤدي خدمات الإتصال للجمهور تحديد هوية الناشر على مواقعهم تحت طائلة عقوبة الغرامة المنصوص عليها بالمادة 76 فقرة 2 من نفس القانون.

في فرنسا أيضا في إطار تحديد شخصية المشتركين بشبكات المعلومات تم التعاون بين مؤدي الخدمة و رجال الشرطة و النيابة خلال التحقيقات طبقا للمادة 642 فقرة 1 من قانون العقوبات التي طبقت لأول مرة في مارس 1994 و يستلزم هذا الإجراء على مؤدي الخدمة أن يكون قادرا على تقديم بيانات شخصية عن زبائنه المشتركين بشبكات معلوماتية التي يجب أن يطلبها منهم مسبقا ، و هذا الإجراء معمول به و معتمد عليه مع كمتعاملي الهاتف النقال بعد تحديث بيانات كل المشتركين و توقيف تشغيل كل الخطوط التي رفض مستعملوها الكشف عن هويتهم .

و من الإجراءات التي تم إعتمادها من الكثير من الدول حاليا هو حفظ بيانات الإتصالات حتى يمكن الرجوع إليها خلال التحقيق و التحري لفترة معتبرة إذ أن هذا النوع من الجرائم قد يمتد أثره لفترة زمنية دون أن يتم إكتشافها كالقنابل الوقتية أين يتم حفظ البيانات عن المستخدم ، وقت بداية و نهاية الإتصال و موقعه ، المعلومات التي طلبها و تحصل عليها ... و هي الآثار التي يمكن الإعتماد عليها في حال إرتكاب جريمة خاصة مع كثافة المستخدمين ففي فرنسا يلزم المتعملون الهاتفيون بحفظ البيانات لمدة عامل كامل و باقي المعلومات على الشبكات لمدة لا تقل عن ثلاث أشهر تحت طائلة توقيع جزاء على المخالف .

و عن المشرع الجزائري نص على إلتزامات مقدمي الخدمات بموجب القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال في الفصل الرابع منه و ألزمهم في المادة 10 على

تقديم المساعدة لسلطات التحري القضائية لجمع و تسجيل المعطيات و محتوى الإتصالات التي يتعين عليهم حفظها طبقا للمادة 11 من ذات القانون .

و تلزم المادة 11 مقدمي الخدمات حفظ البيانات لمدة سنة من تاريخ التسجيل و تشمل المعطيات التي تسمح بالتعرف على مستعمل الخدمة ، المعطيات المتعلقة بالتجهيزات ، الخصائص التقنية من تاريخ و وقت و مدة كل إتصال ، المعطيات التي تسمح بالتعرف على المرسل و المرسل إليه ...

و الدليل الإلكتروني هو ما يستمد من أعمال التحري و التحقيق التي تختلف في كيفياتها و طبيعتها عن الإستدلال في الجرائم التقليدية التي تعرض على القاضي لتمحيصها و تقديرها .

و عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بصفة خاصة مثل باقي الجرائم المعلوماتية تصطدم بصعوبات عند مرورها بمرحلة التحري و التحقيق و كقاعدة عامة أخذ المشرع الجزائري بحرية الإثبات في المادة الجزائية إذ تنص المادة 212 من قانون الإجراءات الجزائية على أنه :

" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي نص فيها القانون على غير ذلك. "

و مهمة البحث و التحري و جمع الأدلة تناط بداية بالضبطية القضائية طبقا لأحكام المادة 12 من قانون الإجراءات الجزائية و بعد فتح تحقيق تطبق أحكام المادة 13 من قانون الإجراءات الجزائية .

و تجدر الإشارة أنه فيما يتعلق بالضبطية القضائية ورد في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر و الإنترنيت في نص المادة الرابعة و العشرون على أنه يكون المأمور المختص بالضبط القضائي مختصا في البحث في هذه الجرائم بأن يكون مؤهلا للطبيعة الخاصة لهذه الجرائم .

و تأكيدا على عمل رجال الشرطة تناول القسم الثاني من الإتفاقية الأوروبية في نص المادة 14 على ترك لكل طرف إتخاذ الإجراءات القانونية التي يراها ضرورية للتطبيق

الإجراءات المنوه عنها لأغراض التحقيق في الجرائم الواردة بالمواد 2 إلى 11 و كافة الجرائم الأخرى التي ترتكب بإستخدام شبكة المعلومات و جمع الأدلة الإلكترونية .

كما منح المشرع الجزائري إختصاصات غير عادية إذا تعلق الأمر بهذه الجرائم بشروط خاصة و عليه نتناول تبعا الإختصاصات العادية في التحري و التحقيق ثم الإختصاصات الغير عادية ، و اخيرا نشير للإجراءات التحفظية التي يمكن اتخاذها أثناء التحقيق .

أولا : الإختصاصات العادية

1 – الإنتقال و المعاينة

المعاينة في اللغة نظر الشيء و مشاهدته ، و في الإصطلاح الجنائي رؤية محل إرتكاب الوقائع الجنائية و إثبات حالتها بالشكل الذي تركها عليها الجاني عقب إرتكاب الجريمة كما تنصرف إلى فحص و إثبات ما يوجد من آثار .[1]

يجوز لقاضي التحقيق طبقا للمادة 79 من قانون الإجراءات الجزائية الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة ، و يخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته مستعينا بكاتب التحقيق و يجب أن يتم ذلك في حضور المتهم .

و يقصد بالمعاينة فحص مكان أو شيء أو شخص له علاقة بالجريمة و إثبات حالته و المعاينة من إجراءات التحقيق و الإستدلال الجوازية شأنها في ذلك شأن كافة إجراءات التحقيق ، و الإشكال الذي يطرح عند تطبيق هذا الإجراء على الجرائم المـاسة بآنظمة المعالجة الآلية للمعطيات هو مدى ملائمة مسرح هذه الجرائم للمعاينة ؟ ومدى جدوى الإجراء بالنسبة لهذه الجرائم التي لا تترك أثرا ماديا ؟

يفرق الفقه بين حالتين بهذا الخصوص : [2]

(1) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، المرجع السابق ، ص 147 .

(2) عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون ، دراسة مقارنة ، الطبعة الثانية ، ص 338 .

إذا ما تمت معاينة المكونات المادية للحاسب الألي و بما أنها محسوسة فإنها لا تثير صعوبة مادية لمعاينتها و التحفظ على الأدلة المادية و وضعها في أحراز مختومة و ضبطها للرجوع إليها .

أما إذا وقعت الجريمة على مكون غير مادي كإتلاف معطيات بفيروس هنا يصطدم المحقق بإشكال عدم وجود آثار للجريمة لمعاينتها و عدم إمكانية حصر عدد المترددين على مسرح الجريمة .

و تبعا لذلك لا بد أن تتم المعاينة من قاضي التحقيق أو من عناصر الضبطية ممن إستفادوا من تكوين أو بالإستعانة بذوي خبرة فنية في مجال الإعلام الآلي بما يمكنهم من إسترجاع المعلومات و التعامل مع حفظ الأدلة الإلكترونية و ما تبقى من آثارها .

في فرنسا على سبيل المثال تم إستحداث خلية شرطة متخصصة تشرف على تنفيذ المهمات التي يعهد بها لهم وكلاء الجمهورية أو قضاة التحقيق تتكون من 13 شرطي تلقو تدريبا متخصصا إلى جانب إختصاصهم الأساسي في مجال التكنولوجيا الحديثة يقومون بمرافقة المحققين أثناء التفتيش لفحص كل جهاز و نقل و نسخ كل معلومة من القرص الصلب و بيانات البريد الإلكتروني ثم ينجزون تقرير يرسل للقاضي المختص[1]

أما عن المعدات و البرامج فهم يستخدمون برامج لإستعادة المعلومات من على الأسطوانات حتى التالفة منها بإستعمال البرامج العالية الكفاءة الموضوعة تحت تصرفهم لتسهيل عملهم .

و لسرعة فقد هذا النوع من الأدلة و إمكانية تعديلها نصت المادة 16 من إتاقية بودابست على انه :" يجوز لكل طرف إتخاذ كل إجراء قانوني يسمح بطريق السرعة لحفظ المعلومات الإلكترونية و على الأخص إذا وجد سبب يدعو للإعتقاد أن تلك المعلومات عرضة للفقد أو التعديل ."

(1) صالح أحمد البربري ، المرجع السابق ص 8 .

فتكليف عناصر ضبطية غير متخصصين من شأنه أن يكون له آثار وخيمة كما حدث بالولايات المتحدة الأمريكية أين تعرضت إحدى الشركات الخاصة للقرصنة ، فطلبت منها دائرة الشرطة توقيف تشغيل جهاز الإعلام الآلي لتتمكن من وضعه تحت المراقبة و ما حدث أن دائرة الشرطة تسببت بذلك في إتلاف كل ما إستلمته من البرامج و الملفات [1] للإشارة بالنسبة للجزائر تم إستحداث فرق متخصصة بالضبطية بهذه الجرائم إذ نجد على مستوى الدرك مركز محاربة جرائم الأعلام الآلي و على مستوى الشرطة فوج مكافحة الجرائم الإقتصادية و المالية و الإعلام الآلي و الأنترنيت .

و ما يميز هذه الجرائم أن المشرع اجاز المعاينة في أي ساعة لاي محل كان بعد اخذ إذن وكيل الجمهورية المختص على إمتداد التراب الوطني ، و يجوز لقاضي التحقيق القيام بذلك أو أمر ضابط شرطة قضائية طبقا للمادة 40 مكرر 2 من قانون الإجراءات الجزائية .

و تكمن أهمية الإنتقال و المعاينة في إعطاء صورة لجهة التحقيق و المحاكمة عن موقع الجريمة و آثارها لإعطاء تصور عن كيفية حدوثها و إستخلاص الأدلة.

2 – <u>التفتيش</u> :

و التفتيش من إجراءات التحقيق التي تنطوي على مساس بحرية الأشخاص و حرمة ممتلكاتهم و مساكنهم الهدف منه البحث عن الأدلة متى وجدت قرائن على حيازة الخاضع لهذا الإجراء لها .

و أول فكرة تتبادر للذهن المجرم بعد ارتكاب الجريمة هو طمس معالمها و إزالة كل أثر قد يكشف عن شخصيته ، و قد يتطلب ذلك تفكيرا و وقتا ، و التفتيش هو الوسيلة لإثبات الأدلة المادية . [2]

(1) محمد أو العلا عقيدة بحث بعنوان التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية ، ص 4 مأخوذ من الموقع الإلكتروني www.arablawinfo.com

(2) أحسن بوسقيعة ، التحقيق القضائي ، دار هومة ، الطبعة الخامسة 2000 ، ص 87 .

و التفتيش من الإجراءات التي أوصت إتفاقية بودابست التشريعات الداخلية بالنص عليه بالمادة 19 منها و السماح بأن يشمل التفتيش كل شبكات المعلومات و البيانات المخزنة عليها و كل أجهزة تخزين المعلومات و أوصت على إتخاذ كل الإجراءات التي من شأنها تسهيل التفتيش و سرعته على النطاق المحلي و نصت المادة 20 على وجوب الترخيص من السلطات بهذا الإجراء و تحديد مضمونه.

و من التشريعات نجد القليل الذي نص على قواعد خاصة لتفتيش مكونات الحاسبات الآلية بصفة خاصة فقانون الإجراءات الجنائي اليوناني في مادته 251 و القانون الجنائي الكندي في مادته 478 و القانون الأنجليزي الصادر 1990 كلها نصت صراحة على تفتيش مكونات الحاسب المادية و المعنوية [1].

و يعرف التفتيش فقها على أنه :" البحث عن الحقيقة في مستودع سرها حيثما تكون مع الشخص أو في منزله ، و الحقيقة تتمثل في ثبوت أو إنتفاء إرتكاب شخص معين لجريمة وقعت بالفعل و أتهم هذا الشخص بإرتكابها على أساس من الجدية التي تؤديها أمارات قوية ." [2]

و يقصد بالتفتيش بمدلوله القانوني بالنسبة لهذه الجرائم إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للمعطيات بما تشمله من مدخلات و تخزين و مخرجات لأجل البحث فيها عن أفعال غير مشروعة مرتكبة تشكل جناية أو جنحة و التوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة و نسبتها إلى المتهم. [3]

(1) طارق إبراهيم الدسوقي عطية ، المرجع السابق ص 380 .
(2) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، المرجع السابق ، ص 182 .
(3) هلالي عبد الله أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، دار النهضة العربية 2006 ص 73 .

و يتم تفتيش المكونات المادية للكمبيوتر بحثا عن كل ما يتصل بالجريمة و يفيد وقوعها للكشف عنها و عن مرتكبيها ، و هنا جواز تفتيش هذه المكونات يتوقف على طبيعة المكان الموجودة فيه ، ما إذا كان مسكن المتهم أو الغير و في أي ساعة و بصفة عامة تخضع إجراءات التفتيش هنا لذات الضمانات المنصوص عليها في قانون الإجراءات الجزائية التي سنأتي على ذكرها .

أما عن تفتيش المكونات المعنوية فهو مسألة تثير عدة إشكالات تتعلق بمحل التفتيش الذي يقع على معنويات و ليس ماديات، و كأصل يهدف التفتيش للحصول على دليل مادي و المشرع الجزائري أجاز التفتيش عن أي شيء و لم يحدد الطبيعة المادية كشرط ، و عليه يطبق التفتيش على هذا النوع من المكونات المعنوية من برامج و معطيات مخزنة لعدم وجود قيد على ذلك ، إضافة لوسائط الحفظ و التخزين و الوحدات المركزية و كل ما يتعلق بالحاسب الآلي .

و لتفتيش البيانات المخزنة آليا يتطلب ذلك عون مؤهل للتعامل بالبرامج و حفظ الملفات و فك الشيفرات و كلمات المرور للتمكن من الحصول على الأدلة و حفظها .

و بهذا المفهوم فالتفتيش فيما يتعلق بهذه الجرائم ليس له مسرح جريمة محدد إذ يمكن التفتيش على ذات الشبكة من غير الحاسوب المستعمل في إرتكاب الجريمة ، إذ يمكن للجاني أن يستعمل حاسوب من أي مقهى أنترنيت بنظام معين و عليه يمكن البحث عن آثار إستخدام نظام معين من أي حاسوب آخر منصل بذات الشبكة .

و هذا ما يعرف بالتفتيش على الخط مباشرة و هو ما تم إعتماده في فرنسا في قضية (forum 51) فوروم التي تم فيها نشر صور مخلة بالأداب على الإنترنيت ، فقام رجال الشرطة بمدينة ريامز بتنسيق عملية واسعة في 27 مقاطعة بإستخدام 220 شرطي لإجراء 21 تفتيش في ذات الوقت لتجنب إختفاء عناصر الإثبات [1]

(1) صالح أحمد البربري ، المرجع السابق ، ص 9 .

- تفتيش مسكن المتهم : حرصا من الدستور على ضمان حرمة المساكن لا بد أن يتم التفتيش بناءا على أمر مكتوب من السلطات القضائية و خص قانون إجراءات التفتيش بالمواد 45 إلى 47 من قانون الإجراءات الجزائية .

إذ وجب أولا أن يحضر المتهم عملية التفتيش كقاعدة ، إلا أن المادة 45 فقرة 7 أعفت ضابط الشرطة القضائية من وجوب توافر هذا الشرط إذا كان التفتيش متعلق بجريمة المساس بأنظمة المعالجة الآلية للمعطيات و عليه لا يكون حضور المتهم إلزاميا ، كما أعفت المادة 47 فقرة 4 بخصوص هذه الجريمة من القيد الزمني للتفتيش فيجوز القيام به في أي ساعة من ساعات النهار أو الليل بناءا على إذن مسبق من وكيل الجمهورية أو قاضي التحقيق المختص مع وجوب إحترام السر المهني طبقا للمادة 45 فقرة 3 من قانون الإجراءات الجزائية.

- ضوابط التفتيش : قبل أن يأمر القاضي المختص بالتفتيش عليه مراعاة توافر عدة شروط أهمها :

- وقوع جريمة من الجرائم الماسة بأنظمة المعالجة الألية للمعطيات .

- تورط شخص أو أكثر في إرتكابها المراد تفتيش مسكنهم أو اشتركوا في ذلك ، حيث تتوافر دلائل كافية تدعو للإعتقاد بأنهم ساهموا في إرتكاب الجريمة و أن التفتيش سيؤدي لحجز الأدلة على ذلك .

- توافر قرائن قوية على وجود أدلة تفيد في كشف الحقيقة لدى شخص أو في مكان معين سواء كانت أداة إرتكاب الجريمة أو متحصلة منها .

- أن يشمل التفتيش المكونات المادية و المعنوية للحاسب الآلي .

- تفتيش حاسب آلي متصل بشبكة :

و بخصوص التفتيش يطرح أيضا إشكال مدى جواز تفتيش حاسوب متصل بشبكة؟ و هنا توجد عدة إحتمالات :

- إما أن يكون الجهاز متصل بآخر مملوك لغير المتهم بذات الدولة بإختصاص محكمة أخرى فهل يمكن تفتيش بيانات و سجلات هذا الأخير ؟

- و إما أن يكون جهاز الكمبيوتر متصل بأخر خارج إقليم الدولة ؟

فمثلا القانون الإجرائي الهولندي أجاز بنص صريح في مادته 125 القسم الخامس على جواز تمديد التفتيش إلى نظم معلوماتية موجودة في موقع آخر شرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة مع مراعاة بعض القيود ، كما أجازت نفس المادة التفتيش في نظم موجودة بدولة أخرى شرط أن يكون التدخل مؤقت و أن تكون البيانات لازمة لإظهار الحقيقة .

أما بالنسبة لقانون الإجراءات الجزائري فقد ورد النص على الحالة الأولى فإذا كان الحاسوب الثاني المتصل بالأول المراد تفتيشه موجود على التراب الوطني أجاز ذلك شرط أن يكون قد صدر أمر من وكيل الجمهورية أو قاضي التحقيق بتفتيش مفتوح يمتد على مستوى التراب الوطني بكامله طبقا للمادة 47 من قانون الإجراءات الجزائية في فقرتها الآخيرة .

إضافة لنص القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال في الفصل الثالث المعنون القواعد الإجرائية لتفتيش المنظومات المعلوماتية في المادة الخامسة على أنه :

" يجوز للسلطات القضائية المختصة و كذلك ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش و لو عن بعد إلى :

أ- منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها .

ب-منظومة تخزين معلوماتي .

في الحالة المنصوص عليها في الفقرة أ من هذه المادة إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها ، إنطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها إنطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول

عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل ."

و من المشاكل التي تواجه عملية جمع الأدلة حالة إمتداد التفتيش إلى خارج الإقليم الجغرافي للدولة لدولة أخرى و هو ما يسمى بالولوج أو التفتيش عبر الحدود و قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها و حدودها الإقليمية . [1]

و لعل المخرج في هذا الإشكال هو تفعيل آليات التعاون الدولي الذي من شأنه كما ذكرنا سابقا لتسهيل إجراءات البحث و التحري بعقد إتفاقيات تبادل معلومات بين الدول ، و هو ما ضمنه المجلس الأوروبي في إحدى تقاريره الذي ورد فيه أن التفتيش بالإختراق المباشر يعتبر إنتهاكا لسيادة الدولة الأخرى ما لم توجد إتفاقية دولية في هذا الشأن ، و رغم ذلك أجازت المادة 32 من الإتفاقية الأوربية في صيغتها النهائية إمكانية الدخول بغرض التفتيش و الضبط في أجهزة و شبكات تابعة لدولة أخرى دون إذنها في حالتين :

- إذا تعلق الأمر بمعلومات أو بيانات متاحة للجمهور .
- إذا رضي صاحب أو حائز هذه البيانات بالتفتيش .

و هذا ما حدث بالفعل بين دولتي ألمانيا و سويسرا بعد أن تبين وجود إتصال بين حاسب في ألمانيا تم تخريب من خلاله بيانات بآخر في سويسرا ، و عندما أرادت سلطات التحقيق الألمانية الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة بين الدولتين .

و بهذا الصدد لم تنظم الجزائر إلى يومنا لأي معاهدة أو إتفاقية خاصة بالتعاون في مجال الجرائم المعلوماتية رغم نص المادة 16 من القانون 04/09 على أنه :

(1) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، المرجع السابق ، ص 205 .

" يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني ."

و يمكن في حالة الإستعجال طبقا لذات المادة و مع مراعاة الإتفاقيات الدولية و مبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية إذا وردت عن طريق وسائل الإتصال السريعة بقدر ما توفره من شروط أمن كافية للتأكد من صحتها.

3 – التوقيف للنظر :

يعرف التوقيف للنظر بأنه إجراء بوليسي يأمر به ضابط الشرطة القضائية بوضع شخص يراد التحفظ عليه فيوقفه في مركز الشرطة أو الدرك لمدة 48 ساعة كلما دعته مقتضيات التحقيق لذلك [1] و كان يطلق عليه قبل تعديل 08/01 لقانون الإجراءات الجزائية بالحجز تحت المراقبة .

و إن كان التوقيف للنظر من متطلبات البحث و التحري الذي يأمر به ضابط الشرطة القضائية للوصول للحقيقة و نظرا لتعرض الإجراء للحرية الفردية فقد أحاطه المشرع بعدة ضمانات .

فطبقا للمادتين 47 و 48 من الدستور الجزائري لا يمكن أن يتابع أحد و لا يوقف و لا يحتجز إلا في الحالات المحددة قانونا و فقا للإجراءات التي نص عليها القانون على أن لا تتجاوز المدة 48 ساعة .

و طبقا للمواد 51 ، 63 ، 64 و 65 من قانون الإجراءات الجزائية لا يجوز أن تتجاوز مدة التوقيف للنظر 48 ساعة ، و ان الأشخاص الذين لا توجد أي دلائل ضدهم لا يجوز توقيفهم فوق المدة الكافية لأخذ أقوالهم ، و لأن إجراء التوقيف للنظر إجراء خطير يمس بحرية الأشخاص لا بد أن يأمر به ضابط شرطة قضائية تحت إشراف وكيل الجمهورية ، و لا تمدد المدة إلا بأمر منه.

(1) عبد الله أوهايبية ، شرح قانون الإجراءات الجزائية الجزائري ، التحري و التحقيق ، دار هومة 2004 ص 239 .

و بالنسبة للجرائم محل الدراسة لا يتم التمديد إلا مرة واحدة مع وجوب تقديم المتهم خلال 48 ساعة بعد تحرير محضر يتضمن الوقائع إضافة لمدة إستجوابه و أوقات الراحة و ساعة التقديم أو إطلاق سراحه مع توقيع الموقوف أو الإشارة لذلك في حال إمتناعه و التي يجب أن تدون في السجل الخاص الذي يلزم ضابط الشرطة القضائية بإمساكه تحت طائلة قانون العقوبات في مادته 110 مكرر .

و أورد القانون عدة ضمانات و حقوق للموقوف منها أن يتم الوقف في أماكن لائقة مخصصة لهذا الغرض تخضع دوريا لمراقبة وكيل الجمهورية ، و عرضه على الطبيب للتأكد من عدم المساس بسلامته الجسدية و إرفاق شهادة طبية بملف الإجراءات قبل تقديمه أمام السيد وكيل الجمهورية طبقا للمادة 51 مكرر 1 فقرة 2 ، إضافة لتمكينه من حقه في الإتصال بعائلته و السماح بزيارته طبقا للمادة 51 مكرر 1 الفقرة الأولى .

و كما سلف الذكر بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يمكن تمديد الوقف للنظر مرة واحدة بإذن مكتوب من وكيل الجمهورية ، أما باقي القواعد و الإجراءات التي تحكم الوقف للنظر فهي مشتركة بين هذه الجرائم و غيرها .

ثانيا : الإختصاصات الغير عادية

إستحدث القانون رقم 22/06 المشار إليه آنفا أساليب التحري و التحقيق تخص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و تتمثل في :

- المراقبة و التتبع .
- إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور.
- التسرب .

1 – المراقبة و التتبع :

يمكن لضباط الشرطة القضائية بعد تعديل القانون 22/06 للمادة 16 مكرر من قانون الإجراءات الجزائية تمديد الإختصاص بموافقة وكيل الجمهورية بكامل التراب الوطني لتنفيذ عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحتمل على الإشتباه فيهم بإرتكابهم هذه الجرائم ، أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من إرتكاب هذه الجرائم أو أشياء ستستعمل في إرتكابها .

2 – إعتراض المراسلات و تسجيل الأصوات و إلتقاط صور

نص المشرع الجزائري على جواز اللجوء لهذا الإجراء بالفصل الرابع من الكتاب الأول الباب الثاني في جرائم محددة على سبيل الحصر و هي المخدرات ، الجريمة المنظمة العابرة للحدود الوطنية ، جرائم تبييض الأموال ، جرائم الإرهاب ، الجرائم المتعلقة بالصرف و الجرائم محل الدراسة الماسة بانظمة المعالجة الألية للمعطيات .

و مرجع هذا الحصر هو خطورة هذه الجرائم و مساس هذه الإجراءات بحرمة حياة الأشخاص الخاصة التي كفلها الدستور في مادته 39 الفقرة الثانية التي تنص على سرية المراسلات و الاتصالات الخاصة بكل أنواعها مضمونة .

و قد أثير إشكال إمكانية التنصت على المحادثات الهاتفية إذ لم ترد في نصوص قانون الإجراءات الجزائية ، إذ يتعلق الأمر بمسألة بالغة الأهمية لكونها تشكل إنتهاكا لجريمة المراسلات التي كفلها الدستور بنص المادة 2/39 بقولها :" سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة ." [1]

و ممن أيد جواز ذلك إستند لنص المادة 68 من قانون الإجراءات الجزائية التي تتيح لقاضي التحقيق القيام بكل الإجراءات التي يراها ضرورية للكشف عن الحقيقة .

في فرنسا أيضا أثير هذا الإشكال و قضت محكمة النقض الفرنسية بشرعية أمر أصدره قاضي التحقيق بالتنصت على محادثات هاتفية و هو ما أكدته المادة 08 من الإتفاقية الأوروبية التي تحضر كل تدخل من جانب السلطات في الحياة الخاصة إلا بنص القانون و لضرورة الوقاية من الجرائم . [2]

(1) أحسن بوسقيعة ، التحقيق القضائي المرجع السابق ، ص 93 .
(2) أحسن بوسقيعة ، التحقيق القضائي ، المرجع السابق ص 89 .

حل هذا الإشكال بصدور القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال الذي حددت المادة الرابعة منه الحالات التي تسمح باللجوء إلى مراقبة الإتصالات الإلكترونية الواردة بالمادة 3 من ذات القانون بوضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها، و ورد ضمن الحالات المسموح اللجوء فيها بهذا الإجراء بالبند ب من المادة 4 و هي حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني .

و هذه الفقرة حددت مجال الإذن بنوع معين من الجرائم إلا أن الفقرة ج سمحت بهذا الإجراء كلما تطلبته مقتضيات التحريات و التحقيقات القضائية بالنسبة لكل الجرائم عندما يكون من الصعب الوصول إلى نتيجة دون اللجوء للمراقبة الإلكترونية ، على أن لا يتم هذا الإجراء دون إذن مكتوب من السلطة القضائية المختصة .

أما إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور فقد أجازه القانون في المادة 65 مكرر 5 من قانون الإجراءات الجزائية لوكيل الجمهورية أن يأذن بـ :

- إعتراض المراسلات التي تتم عن طريق وسائل سلكية و لا سلكية .
- وضع الترتيبات التقنية دون موافقة المعنيين من أجل إلتقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

و يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها و لو خارج المواعيد المحددة في المادة 47 من قانون الإجراءات الجزائية و بغير علم أو رضا الأشخاص الذين لهم الحق طبقا للمادة 65 مكرر 5 فقرة 4 .

العمليات المأذون بها تتم تحت الإشراف و المراقبة المستمرة لوكيل الجمهورية أو قاضي التحقيق بعد فتح تحقيق طبقا للمادة 65 مكرر 5 فقرة 5 و 6 والتي حددت البيانات الواجب توافرها في الإذن و الذي يسلم لمدة أقصاها 4 أربع أشهر قابلة للتجديد.

و طبقا للمادة 65 مكرر 8 يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية أو قاضي التحقيق أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية .

و إذا اكتشفت جرائم أخرى غير تلك التي ورد ذكرها بإذن القاضي المختص فهذا لا يعد سببا لبطلان الإجراءات طبقا للمادة 65 مكرر 6 فقرة 2 .

و بعد إنتهاء الإجراء يحرر ضابط الشرطة القضائية محضرا يذكر فيه تاريخ و ساعة بداية العملية و إنتهائها ، و يصف و ينسخ المراسلات و الصور و المحادثات المسجلة و المفيدة في إظهار الحقيقة في محضر يودع بملف الإجراءات ، كما تترجم المكالمات إذا كانت بغير العربي و يستعان بمترجم إذا لزم الأمر .

3 – التسرب

و هو إجراء تم إستحداثه بالفصل الخامس من الكتاب الأول الباب الثاني من قانون الإجراءات الجزائية بالمواد 65 مكرر 11 إلى 18 الذي أجاز المشرع اللجوء له في فئة الجرائم السالفة الذكر .

و تنص المادة 65 مكرر 11 أنه عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته بمباشرة عملية التسرب.

و ورد تعريف إجراء التسرب بالمادة 65 مكرر 12 على أنه قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية مراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.

و عليه التسرب هو تقنية تسمح بالإختراق و التوغل داخل جماعة إجرامية بهدف جمع أكبر قدر ممكن من المعطيات و البيانات حول الجرائم و تمكن من تقدير الإمكانيات المادية و البشرية المستعملة.

و لان هذه العملية على قدر من الخطورة وجب إختيار ضابط شرطة قضائية ممن توافر فيهم مواصفات خاصة كالقدرة على التأقلم و التكييف في الوسط الإجرامي ، و على

سبيل الأمان يتم زرع أكثر من موظف دون أن يعلم أحدهم بالآخر و تسمى هذه العملية بالتقاطع و هدفها التأكد من مصداقية المعلومات المقدمة من عناصر مختلفين .

و لا يجوز القيام بالإجراء قبل الحصول على إذن مكتوب يشار فيه للجريمة و هوية الضابط المنفذ للعملية على ألا يتجاوز مدة أربع أشهر قابلة للتجديد ، كما يجوز للقاضي توقيف العملية في أي وقت يراه مناسبا طبقا للمادة 65 مكرر 15 من قانون الإجراءات الجزائية إذ تتم العملية منذ بدايتها تحت إشرافه طبقا للمادة 65 مكرر 11 .

و حماية للمتسرب و ضمانا لسلامته لا يمكن أن يعتبر أي من الأعمال التي يرتكبها بمناسبة القيام بالمهمة المسندة إليه تحريضا على إرتكاب جرائم ، كما و لا يسأل عن إخفاء هويته و له إستعمال هوية مستعارة كما لا يسأل عما يرتكبه من جرائم طبقا للمواد 65 مكرر 12 ، 14 .

كما نص المشرع على أحكام جزائية بالمادة 65 مكرر 16 توقع على كل من يكشف عن هوية المتسرب فيعاقب بالحبس من عامين إلى خمس سنوات و غرامة من 50000 دج إلى 000 200 دج .

و إذا تسبب الكشف في أعمال عنف أو ضرب عليه أو زوجه أو أبناءه أو أصوله تكون العقوبة هي الحبس من 5 سنوات إلى 10 سنوات و غرامة من 000 200 دج إلى 000 500 دج غرامة نافذة .

و إذا تسبب الكشف في وفاة أحد هؤلاء الأشخاص تكون العقوبة هي الحبس من عشر إلى عشرين سنة و غرامة من 000 500 دج إلى 000 000 1 دج .

و عند إنتهاء المهمة أو توقيفها من القاضي المختص يقوم المكلف بالمهمة بإنجاز تقرير يتضمن كل المعلومات التي توصل لها دون الإشارة لهوية المنجز و يودع ملف الإجراءات رفقة الإذن الأولي ، و لا يمكن بأي حال من الأحوال الإشارة لهوية المتسرب خلال كل مراحل الدعوى إذ أن الضابط المنسق وحده من يمكن سماعه كشاهد تحت مسؤوليته الشخصية طبقا للمادة 65 مكرر 18 من قانون الإجراءات الجزائية .

ثالثا : الإجراءات التحفظية :

نصت المادة 40 مكرر 5 من قانون الإجراءات الجزائية على أنه يجوز لقاضي التحقيق تلقائيا أو بناءا على طلب النيابة العامة طوال مدة التحقيق أن يأمر بإتخاذ كل إجراء تحفظي أو تدبير أمن زيادة على حجز الأموال المتحصل عليها من الجريمة أو التي أستعملت في إرتكابها .

كما نصت المواد 40 مكرر 2 و 3 ، 44 ، 47 من قانون الإجراءات الجزائية على جواز إجراء حجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناءا على إذن مسبق من وكيل الجمهورية المختص ، كما يمكن لقاضي التحقيق القيام بذلك على إمتداد التراب الوطني أو يأمر ضابط الشرطة القضائية للقيام بذلك .

المبحث الثاني : مسألة الإثبات في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تتميز الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كالجرائم المعلوماتية بصفة عامة بصعوبة إثباتها لما تتميز به من خصائص نتعرض لها بالمطلب الأول كونها تتعلق في غالبها بمعنويات يسهل محو أثرها و تدميرها ، مما يطرح بالتبعية إشكالا في الإجراءات المتبعة للحصول على الدليل الإلكتروني بإعتماد أساليب التحري و التحقيق السالفة الذكر و جردها و الحفاظ عليها بملف الدعوى .

فالدليل الإلكتروني يعد الوسيلة لإثبات الجرائم التي ترتكب بوسائل معلوماتية و التي تقع إما بتحريف البيانات المعالجة آليا عن طريق أجهزة الإعلام الآلي أثناء إدخال البيانات أو تخزينها أو أخراجها و للوصول إلى الأدلة على ذلك فإن الأمر يحتاج إلى أدلة علمية تثبت وقوعها و إسنادها .

و بعد إستخلاص الدليل الإلكتروني الغير محسوس يطرح إشكال تقدير قيمته في ضوء قانون الإجراءات الجزائية ، و نص المادة 212 منه و مبدأ حرية القاضي في تكوين إقتناعه ، فعلى الرغم من أنه يتمتع بالحرية في تكوين عقيدته من أي دليل إلا أنه ملزم بتسبيب حكمه و بيان الأدلة التي إستمد منها قناعته ، فليس معنى الحرية أن نطلق له العنان لكي يقتنع بما يحلو له ، إنما هو حر في إستخلاص الحقيقة من مصدر مشروع فهناك طرق للإثبات نص عليها قانون الإجراءات الجزائية التي تعد مشروعة و يجوز له استخلاص الحقيقة منها. [1]

و عليه نتناول في هذا المبحث في المطلب الأول خصوصية الدليل الإلكتروني نعرض فيه مميزاته و خصائصه ، ثم إجراءات الحصول على الدليل الإلكتروني ، و أخيرا و في المطلب الثالث نتناول إشكالية الدليل الإلكتروني و تقديره في ظل قانون الإجراءات الجزائية بإعتبار أن النظام السائد في الجزائر في الإثبات هو نظام مختلط يحتل موقعا وسطا بين نظام حرية الإثبات و الإثبات المقيد الذي يقوم على تحديد المشرع سلفا لأدلة الإثبات التي يجب على القاضي الإستناد عليها لإصدار حكمه في الدعوى .

(1) رمسيس بهنام ، الإجراءات الجنائية تأصيلا و تحليلا ، منشأة المعارف ، طبعة 1984 ص 698

المطلب الأول : خصوصية الدليل الإلكتروني

لم ينص المشرع الجزائري على خصوصية معينة بالنسبة للأدلة المعلوماتية المستمدة من الحواسيب الآلية مما يترتب عنه صعوبات عملية في تقدير هذه الأدلة مرجعها الخصوصيات المميزة لها و أهم ما تتميز به الأدلة المعلوماتية :

أولا : عدم مرئية الدليل :

تتميز الجرائم الماسة بأنظمة المعالجة الألية للمعطيات أنها لا تتعلق بوثائق أو مستندات مادية ، فمحل الجريمة كما سبق البيان في الفصل الأول معطيات و نظام معالجة معلوماتي ، و سبق و تطرقنا لمفهوم نظام المعالجة الآلية للمعطيات و عليه فإن الجاني يعتمد على العبث بذبذبات غير مرئية و برامج تنتج آثارها في أجزاء من الثانية ، لتتحقق الجريمة بإتلاف معطيات أو تغييرها أو محوها أو نشر فيروس مثلا في زمن قياسي .

فإثبات الأمور المادية التي تترك أثارا ملحوظة يكون سهلا بعكس إثبات المعنوية بالنظر لأنها لا تترك أثرا يدل و يكشف عنها ، ذلك أن أغلب المعلومات و البيانات التي يتم تداولها عبر الحاسبات الألية من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز و نبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن قرائتها إلا من خلال هذه الحاسبات الآلية . [1]

و عليه تتحقق نتيجة هذه الجرائم دون التمكن من رؤية الدليل مع إمكانية طمس معالمها في ثواني إذ يمكن للجاني فعل ذلك حتى في ظل حضور عناصر الضبطية الغير متخصصين و الذي قد يحقق ذلك بمجرد الضغط على زر .

فالتحقيق في مثل هذه الجرائم يتطلب معرفة واسعة و إحاطة بالتكنولوجيا الحديثة في مجال الإعلام الآلي ، فغالبية هذه الجرائم يتم إكتشافها صدفة .

(1) علي محمود علي حمودة بحث بعنوان الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي ، ص 16 مأخوذ من الموقع الإلكتروني www.arablawinfo.com

و أشارت بعض الدراسات أنه لا يتم إكتشاف إلا نسبة 1 بالمئة من الجرائم المرتكبة و ما يتم الإبلاغ عنه يمثل نسبة 15 بالمئة من نسبة الواحد بالمئة السابقة ، و القضايا التي طرحت أمام القضاء فإن أدلة الإدانة فيها كانت غير كافية. (1)

و عمليا لا يسعى الضحية للتبليغ خاصة إذا تعلق الأمر بمؤسسة مالية خوفا من فقدان ثقة الزبائن الذين سيعمدون لسحب أموالهم لدى إنتشار معلومة إختراق أنظمتها .

و هو ما يعرف بالرقم الأسود (chiffre noir) حيث لا يعلم عدد ضحايا هذه الجرائم ففي إحدى الوقائع الشهيرة تعرض بنك marchant bank city في بريطانيا لنقل 8 مليون جنيه من أحد أرصدته إلى رقم حساب في سويسرا و قد تم القبض على الفاعل أثناء محاولته سحب المبلغ ، و لكن البنك بدل الإدعاء ضد الفاعل قام بدفع مبلغ مليون جنيه للجاني شرط عدم الإعلان عن جريمته و إعلام البنك بالآلية التي تمكن بواسطته من إختراق نظام الحاسوب المركزي الأمني (2)

و في دراسة مسحية تمت من قبل لجنة تدعى " لجنة التدقيق" في إنجلترا في شأن الإحتيال المعلوماتي و إساءة إستعمال الحاسب شملت 6000 مؤسسة تجارية و شركات قطاع خاص ، تبين أن ما يقرب نصف حالات التعدي على الأنظمة قد اكتشفت مصادفة و التي كبدتها خسائرا قدرت بـ 5،2 مليون جنيه إسترليني (3)

و لعل سعي المؤسسات لوضع أجهزة للرقابة و التدقيق يمكن أن يعول عليه في كشف هذه الجرائم خاصة بالمؤسسات المالية و الحكومية التي تعد عرضة لهذه الجرائم ، و من ثمة إظهار الدليل الخفي و يفترض أن يكون الجهاز المكلف بهذه المهمة جهاز تقني ذو كفاءة بهذا المجال مواكب لأحدث الطرق التي يواكبها المجرمون أيضا ، بما يمكن من إكتشاف الجريمة مبكرا .

الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لا تترك آثار مادية لأنها تستهدف معنويات المتمثلة بالمعطيات الموجودة داخل النظام ، و كلها معنويات و عليه يصعب

(1) محمد خليفة ، المرجع السابق ، ص 62 .
(2) عبد الله حسين علي محمود ، المرجع السابق ص 3
(3) عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، المرجع السابق ، ص 107 .

ثانيا :إنعدام آثار الجريمة

إكتشافها حتى مع التبليغ عنها على خلاف الجرائم التقليدية الواقعة على الأموال و الأشخاص التي تترك آثار تنصب مباشرة على محل الجريمة ، كآثار الكسر أو الإقتحام في السرقة و آثار التحطيم ، جثة الضحية بجريمة القتل و الإصابات و الرضوض في أعمال التعدي على سلامة الأشخاص .

و حتى مع إعتماد إجراءات المراجعة اليومية أو الأسبوعية أو الشهرية للمعاملات بالمؤسسات خاصة المالية منها قد لا تكتشف الجريمة ، فالجاني في هذا المجال كما بينا في الفصل التمهيدي شخص على درجة عالية من الذكاء ، إذ يعتمد لإرتكاب الجريمة بطريقة تبدو بها الهوامش المتغيرة طفيفة لا يمكن ملاحظتها ، أو إذا لوحظت لا يكترث لها خاصة كما ذكرنا مع تخوف المؤسسات من فقدان ثقة الزبائن الذين يعمدون لعدم التبليغ عن ذلك و البحث فيه .

و هذه الجرائم عبارة عن معطيات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحواسيب و لأنها لا تترك أثرا خارجيا تكون صعبة الإكتشاف ، و ما يزيد من هذه الصعوبة عدم وجود آثر كتابي لما يجري خلال تنفيذها من عمليات تتم بواسطة نقل المعلومات و إمكانية إرتكابها عبر الدول بإستخدام شبكات الإتصال دون تحمل عناء الإنتقال . [1]

و ذهب رأي في الفقه لعدم إطلاق هذه الخاصية معللين ذلك أن تغيير المعطيات يعد أثرا على إرتكاب الجريمة و صعوبة إثباتها يكمن في عدم ثبوت وسيلة الإرتكاب و ليس الأثر.[2]

و إنعدام آثار الجريمة يأتي نتيجة حتمية لخاصية عدم مرئية الدليل الذي هو عبارة عن ذبذبات غير مرئية ، و إن تحولت إلى معطيات مرئية أحيانا ما تكون مشفرة أو مرمزة لا يمكن قرائتها ، و عليه يمكن للجاني طمس الدليل كاملا بحيث يستحيل ملاحقته أو كشف هويته .

(1) و (2) طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة الإسكندرية 2009 ص 171 و 172 .

و لعل مرجع الصعوبة في عدم إمكانية تتبع الدليل هو عدم إمكانية تتبع الطريق العكسي لمرور المعطيات بالنظام بعد إرتكاب الجريمة فلو تم محو المعطيات أو تغييرها لا يمكن معرفة الفاعل أو إعادة الحال لما كان عليه ، كما يستحيل معرفة هدف الجريمة من آثارها و إن وجدت ، و أن أمكن إسترجاع معلومات فيجب أن يقوم بذلك متخصص على قدر عالي من التدريب على مثل هذه المهام .

و قد يرجع السبب في إفتقاد الآثار التقليدية لهذه الجرائم أن بعض العمليات تتم دون أن تتوقف على الرجوع لوثائق أو مستندات للنقل منها [1] كما لو كان البرنامج معد سلفا و مخزن على حاسب و تتوافر أمام المتعامل عدة خيارات و بالنقر على إحداها لتكتمل الحلقة المطلوب تنفيذها .

و من الأسباب التي تساهم في تعذر الحصول على آثار تقليدية لهذه الجرائم محو الجاني بنفسه للأدلة التي تدينه و تدميرها في وقت قصير و بسهولة في ثواني معدودة إذ قد يتمكن من ذلك بالموازاة مع إرتكاب الجريمة و أثناء تشغيل الوسائل الإلكترونية نفسها .

ثالثا : صعوبة إستخلاص الدليل

يقصد بالدليل العلمي النتيجة التي تسفر عنها التجارب العلمية لتعزيز دليل مسبق تقدمه سواء للإثبات أو لنفي الواقعة التي يثور الشك بشأنها [2]

مسألة فنية بحتة تتطلب ندب خبير من المحكمة ، فإجراء تجارب و إستعمال وسائل الإعلام الآلي بتقنيات عالية لا يتمكن منها القضاة أو عناصر الضبطية الذين تبقى خبرتهم محدودة بمجال الإعلام الآلي لا يرقى للتخصص ، و يتم ندب الخبير من قـــاض التحقيق من تلقاء نفسه أو بناءا على طلب الأطراف طبقا للمادة 143 من قانون الإجراءات الجزائية .

(1) عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، المرجع السابق ، ص 123 .
(2) عفيفي كامل عفيفي ، المرجع السابق، ص 336 .

و تطبيق هذا التعريف على الجرائم محل الدراسة يجعل من عملية استخلاص الدليل

و تكليف خبير بالكشف عن الأدلة في كل مرة تعلق فيها الأمر بهذه الجرائم يغيب دور القاضي في البحث و التحري عن الأدلة إذ يلعب الخبير الدور المطلق في استخلاص الأدلة .

و لصعوبة إستخلاص الدليل في مثل هذه الجرائم يري المختصون في جرائم الحاسب الآلي أن هذا الجهاز و ما يقع عليه من جرائم يعد تحديا لرجال الأمن الذي تنحصر معلوماتهم في قانون العقوبات بصورته التقليدية فلن يكونوا قادرين على التعامل مع الجريمة المعلوماتية التي تقع بطرق تقنية عالية. [1]

فالجاني في هذه الجرائم من المجرمين المحترفين الذين يستخدمون قدراتهم العقلية لإنجاح تخطيطهم و يحيطون أنفسهم بتدابير أمنية وقائية تزيد من صعوبة كشف الجريمة فقد يستعملون التشفير لجعل الأدلة رمزا لا يمكن لغيرهم فهمه و هذا ما يجعل الوصول إليها في غاية الصعوبة [2]

(1) الدكتور عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، المرجع السابق ، ص 107 .

(2) علي محمود علي حمودة ، المرجع السابق ، ص 18 .

المطلب الثاني : إجراءات الحصول على الدليل الإلكتروني

إن إجراءات الحصول على الدليل الإلكتروني لا تختلف في مدلولها القانوني على إجراءات الحصول على الأدلة بالمفهوم التقليدي مع مراعاة خصوصية الدليل لما يتمتع به من الخصائص السالفة الذكر ، التي توجد عقبات في الحصول على الدليل و حجزه و تحريزه و حفظه في ملف الدعوى بإستعمال أساليب التحري و التحقيق التي سبق و درسناها ، المتمثلة في الطرق العادية من معاينة و تفتيش و خبرة و غير عادية و هي تلك التي خص بها المشرع هذا النوع من الجرائم من تسرب و و إعتراض تسجيلات و إلتقاط صور على النحو السالف الذكر ، و بالإستعانة بأساليب التحقيق من إستجواب شهادة و خبرة يمكن لقاضي التحقيق إستكمال اجراءات التحقيق و الحصول على الدليل

أولا : الإستجواب

و الإستجواب هو إجراء من إجراءات التحقيق القضائي يختص به قاضي التحقيق طبقا للمادة 100 من قانون الإجراءات الجزائية التي تعرفه على أنه إجراء بمقتضاه يتحقق قاضي التحقيق من شخصية المتهم و يناقشه تفصيلا في التهمة المتابع بها و يطالبه بالرد على الأدلة القائمة ضده إما بتفنيدها أو التسليم بها التي تؤدي لإعتراف المتهم ، و القانون الجزائري لم يعرف الإستجواب بل حدد شروطه .

أما الفقه فقد عرفه بأنه : " مجابهة المتهم بالأدلة القائمة ضده و مناقشته فيها مناقشة تفصيلية تتيح له إن إستطاع تفنيدها و قد تحمله طواعية و إختيارا على الإعتراف بالتهمة "[1].

و يهدف الإستجواب لهدفين الأول إثبات شخصية المتهم و مناقشته تفصيلا في الإتهام الموجه له ، و الثاني تحقيق حقوق الدفاع فمناقشة المتهم للأدلة قد يؤدي لإعترافه كما تفتح له المجال لإثبات برائته ، لذلك فالإستجواب ذو طبيعة مختلطة فهو وسيلة إثبات و دفاع في نفس الوقت .

---

(1) نبيل مدحت سالم ، شرح قانون الإجراءات الجنائية ، ص 381 .

و إستجواب المتهم فيما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تحكمه القواعد العامة إلا أن الفرق يكمن في وجوب أن يكون المحقق مؤهلا للتحقيق في هذا النوع من الجرائم و يكون مستوعبا لمفرداتها فالمجرم المعلوماتي خبير في الحاسوب و إستخدام تقنياته .

و الإستجواب يتم خلاله التحقيق في الأدلة الموجودة ضد المتهم و التي يقدمها لصالحه حتى الوصول لثبوت الجريمة و الإحالة للمحاكمة أو صدور أمر بألا وجه للمتابعة ، و هو إجراء أحاطه المشرع بالعديد من الضمانات كحق المتهم في إلتزام الصمت تحت طائلة البطلان و أن سكوته لا يجب أن يؤخذ كقرينة على ثبوت التهمـــة ضده ، قرينـــة البراءة ، حق الإستعانة بمحامي طبقا للمادة 100 من قانون الإجراءات الجزائية التي تنص : " ... فإذا أراد المتهم أن يدلي بأقواله تلقاها قاضي التحقيق منه على الفور ، كما ينبغي للقاضي أن يوجه المتهم بأنه له الحق في إختيار محام عنه فإن لم يختر له محاميا عين له القاضي محاميا من تلقاء نفسه " و حق هذا الأخير في الإطلاع على الملف طبقا للمادة 105 من قانون الإجراءات الجزائية و إستدعاءه بكتاب موصى عليه قبل يومين على الاقل من الإستجواب و تمكينه من الإطلاع على الملف 24 ساعة على الأقل إضافة لمراعاة المواد من 91 إلى 95 في تحرير محضر الإستجواب .

مع مراعاة مقتضيات المادة 100 الآنفة الذكر في حالة الإستعجال الناجمة عن وجود شاهد في خطر الموت أو وجود أمارات على وشك الإختفاء و يجب الإشارة لحالة الإستعجال في المحضر .

و بشأن الإستجواب يجب التفرقة بين إعتراف المتهم و بين أقواله إذ يجب أن يكون الإعتراف صريحا واضح الدلالة بأن يقر بإرتكاب الفعل المسند إليه ، كما و يشترط في الإعتراف أن يكون من متهم مميز متمتع بكامل قواه العقلية و أن يكون قضائيا صريحا و أن يكون من المتهم على نفسه لا على الغير ، فإقراره ببعض الوقائع لا يعتبر إعترافا بالمعنى المقصود في قانون الإجراءات الجزائية و يبقى للقاضي إستخلاص الأدلة بالطرق الأخرى المتاحة إستعانة بالقرائن أو الشهادة أو الخبرة.

ثانيا : الخبرة

يقصد بالخبرة المهارة الكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص مدة زمنية معتبرة أو نتيجة دراسات خاصة تلقاها الخبير أو نتيجة الإثنين معا و يطلق على ذوي هذه المهارات " الخبراء " ، و يقصد بالخبرة القضائية إجراء التحقيق الذي يعهد به القاضي إلى شخص مختص تتعلق بواقعة يستلزم بحثها أو تقديرها إبداء رأي بعلم معين لا يتوافر بشخص عادى ، و مايميز الخبرة عن غيرها من إجراءات التحقيق أنها تتطلب رأيا من خبير فني يتطلب أن يتوافر فيه معارف علمية أو فنية لا تتوافر لدى المحقق أو القاضي [1]

يمكن لقاضي التحقيق أيضا بصدد جمع الأدلة الإستعانة بإجراء الخبرة ، و الخبرة هي الوسيلة الفنية لتحديد التفسير العلمي للأدلة و أجاز المشرع اللجوء لهذا الإجراء بموجب المادة 143 من قانون الإجراءات الجزائية في فقرتها الأولى التي تنص على أنه يجوز لكل جهة قضائية تتولى التحقيق أو الحكم إذا تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناءا على طلب النيابة أو الخصوم أو من تلقاء نفسها.

و بالنظر لخصوصيات الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن إجراء الخبرة يعد ضروري لأنها جرائم ذات طابع فني من حيث أسلوب إرتكابها أو طرق الكشف عنها ، نظرا لأن أجهزة الكمبيوتر و الشبكات المتصلة بها على أنواعها و نماذجها المتعددة و التقنيات المتصلة بها تنتمي إلى تخصصات علمية و فنية دقيقة و متطورة و سريعة قد يصعب حتى على المتخصص فيها مجاراتها ، و على القاضي إختيار الخبراء ذوي الإختصاص بدقة و من بين المتمكنين علميا بهذا المجال .

(1) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، المرجع السابق ، ص 283

و لقاضي التحقيق كأصل أن يختار خبير من بين الخبراء المسجلين في جدول المجلس القضائي ، و له أن يختار ندب خبير من غير المعتمدين بقرار مسبب بعد أن يؤدي اليمين كما يجوز أن يتعدد الخبراء طبقا للمادة 147 من قانون الإجراءات الجزائية .

و على القاضي أيضا تحديد المهمة الموكلة للخبير الذي تم ندبه بدقة طبقا للمادة 146 من قانون الإجراءات الجزائية ، و لعل أهم النقاط الواجب أن تشملها الخبرة بيان تركيب الحاسب و أنظمة تشغيله و الشبكة المرتبطة به ، وسائط الإتصال به و الموضع المحتمل للأدلة و الشكل و الهيئة التي تكون عليها ، إمكانية نقل الأدلة لوسائط تخزين خارجية حتى يمكن الرجوع لها دون إتلافها و حتى لا يتم تدميرها لاحقا وإمكانية تجسيد الادلة في صورة مادية بنقلها من الدعائم الممغنطة إلى نسخ ورقية حتى يمكن الإطلاع عليها من القاضي مباشرة و ضمها للملف دون الحاجة لإعادة تشغيل النظام .

و رغم ما يناط بالخبير من مهام حيث أجاز له القانون تلقى أي تصريح مفيد من الغير يبقى الخبير مجرد مساعد للقاضي ، تنحصر مهمته في إنارة القاضي بخصوص مسآلة فنية ، و لا يجوز له بأي حال من الأحوال أن يحل محل القاضي أو ينوب عنه. [1]

ثالثا : الشهادة

يجوز طبقا للمادة 88 من قانون الإجراءات الجزائية لقاضي التحقيق سماع كل شخص يرى فائدة من سماع شهادته سواء كان شاهد نفي أو إثبات بعد استدعائه بكتاب عادي أو موصى عليه أو بالطريق الإداري أو بواسطة أحد أعوان القوة العمومية.

و الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام القضاء بشأن جريمة معينة سواء تعلق الأمر بإثبات إسناد الجريمة للمتهم أو إثبات برائته ، و للشهادة في مجال الإجراءات أهمية بالغة لأن الجريمة ليست تصرفا قانونيا و لكنها عمل غير مشروع بجتهد الجاني في التكتم عند إرتكابه و يحرص على إخفائه عن الناس .

---

(1) أحسن بوسقيعة ، التحقيق القضائي ، المرجع السابق ، ص 116 .

و يمكن أن يكون الشاهد في هذا النوع من الجرائم الذي يمكن سماعه لتحصيل الدليل من مشغلي الحاسب الآلي و ذوي الخبرة بمعداته و إستخدامه و خبراء البرمجة و محللي البرامج و أنظمة المعالجة و كذا مهندسي الصيانة الذين قد يساعدون القاضي أثناء الإدلاء بشهادتهم في الكشف عن الشيفرات و كلمات السر و تحليل الأدلة الموجودة و إعطاء رأيهم بالمستندات الموجودة أو التي تم طبعها و المعلومات التي تم إسترجاعها مما يمكن من الحصول على أدلة جديدة و هذا ما يطلق عليه بالشاهد الخبير ، كما يطلق عليه فقها إسم الشاهد المعلوماتي .

و الشاهد المعلوماتي عدة طوائف أهمها : [1]

1- القائم على تشغيل الحاسب الآلي : و هو المسؤول عن تشغيل جهاز الحاسب الآلي و المعدات المتصلة به و يجب أن يكون له خبرة كبيرة في تشغيل الجهاز و إدخال البيانات.

2 - المبرمجون : و هم فئتان

- مخططو برامج التطبيقات : و هم الذين يقومون بتحويل خصائص و مواصفات النظام المطلوب إلى برامج دقيقة موثقة لتحقيق هذه المواصفات .

- مخططو برامج النظم : يقومون بإختيار و تعديل و تصحيح برامج الحاسب الداخلية التي تتحكم بوحداته و وسائط التخزين .

3 – المحللون : المحلل هو الذي يحلل الخطوات و يجمع البيانات و يدرسها و يحلل النظام أين يقسمه لوحدات منفصلة و يستنتج العلاقات الوظيفية منها و يتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط التدفق .

4 – مهندسو الصيانة و الإتصالات و هم المسؤولون عن أعمال صيانة الحاسب الآلي و الشبكات المتصلة به .

5 – مديرو النظم هم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية .

---

(1) عبد الله حسين علي محمود ، المرجع السابق ، ص 15 و 16

و هناك من القوانين من حصرت فئات الشاهد المعلوماتي كقانون ولاية كاليفورنيا الأمريكية على النحو الآتي : [1]

محلل النظم الذي صمم و أوجد برامج الكمبيوتر ، المبرمج ، المشغل ، طاقم عمليات البيانات ، أمناء مكتبة الأشرطة ، مهندس الصيانة ، موظفو المدخلات و المخرجات و المسؤولون عن معالجتها ، مبرمجو الصيانة ، المستخدم النهائي .

والهدف من وراء كل إجراءات التحري و التحقيق التي يقوم بها رجال الضبطية القضائية و قاضي التحقيق هو ضبط الأدلة و جمعها في أحراز و تحرير نسخ منها و محاضر ضبط بشأنها و ضمها لملف الإجراءات ، و بما أن الجرائم محل الدراسة هي ماسة بمعطيات و أنظمة معالجة فجمع الأدلة فيها بالدرجة الأولى لا يتعلق بضبط عتاد الحاسب الآلي و ملحقاته من شاشة و أسلاك و وحدات تشغيل إنما ما تتضمنه من برامج و معلومات يمكن إستخلاصها و حفظها على مخرجات أو وسائط تخزين خارجية كالأقراص المضغوطة و البرنامج المطبوع و القصد من هذه الإجراءات حماية الأدلة المضبوطة من التلف و العبث فيها أو تغييرها للمحافظة على الدليل. [2]

و لتحقيق ذلك ينبغي مراعاة عدة قواعد و إرشادات فنية أبرزها : [3]

- العناية البالغة بطريقة إعداد النظام و آثاره كالسجلات الإلكترونية لمعرفة مواقع الإتصال و الجهاز الذي أستعمل للولوج للنظام .

- التحفظ على الحاسب و الأجهزة المتصلة به و ملحقاته و تسجيل وقت و تاريخ و مكان إلتقاط كل صورة .

- إثبات حالة التوصيلات لإجراء عمليات المقارنة و التحليل اللاحقة .

- عدم نقل أي معلومة حتى التأكد من سلامة العملية .

- التحفظ على المعلومات الموجودة حتى تلك الموجودة بسلة المهملات .

---

(1) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، المرجع السابق ، ص264 .

(2) مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الأولى ، مطابع الشرطة القاهرة مصر ، 2009 ص 347 .

(3) عبد الله حسين علي محمود المرجع السابق ص 5 و 6 .

- التحفظ على مخرجات الجهاز .

و يتم إستخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهات التحقيق و تبقى تحت تصرفها إلى حين إنتهاء المحاكمة ، و يرى البعض بضرورة حفظ نسخة أخرى على مستوى المحكمة خشية تلف أو ضياع النسخة الوحيدة الموضوعة تحت تصرف جهة التحقيق أو الحكم. [1]

و نص القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال في المادة 06 على قواعد حجز المعطيات المعلوماتية التي تنص على إمكانية نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و وضعها في أحراز طبقا لما هو مقرر في قانون الإجراءات الجزائية كما سلف الذكر .

و يجوز في هذه الحال إستعمال كل الوسائل التقنية الضرورية لتشكيل و إعادة تشكيل المعطيات لجعلها قابلة للإستغلال أثناء التحقيق شرط عدم المساس بمحتواها .

و تنص المادة 07 على أنه إذا إستحال إجراء الحجز على سلطات التحقيق ضمان منع الوصول إلى المعطيات أو نسخها و يمكن للسلطة التي تباشر التحقيق طبقا للمادة 8 إذا كانت المعطيات المعنية بالإجراء ذات محتوى مجرم منع الإطلاع عليها.

(1) محمد أبو العلا عقيدة ، المرجع السابق ص 12 .

المطلب الثالث : إشكالية قبول الدليل الإلكتروني و تقديره في ظل قانون الإجراءات الجزائية

نظرا للخصوصيات التي تتميز بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و بالتبعية الطبيعة الخاصة للدليل الإلكتروني المتحصل عليه تبعا للإجراءات التي سبق عرضها ، و مع صعوبة الحصول على الدليل يثار الإشكال حول قيمة هذا الدليل و مدى مصداقيته في التعبير عن الجريمة التي تتم بطريقة معنوية و تمس بمعنويات ، المتمثلة في المعطيات الموجودة بنظام عبارة عن ذبذبات متنقلة في شبكات معلوماتية .

فهل تصلح هذه الأدلة كأدوات إثبات خلال الدعوى العمومية ، و مدى الثقة التي يمكن أن تعطى لها و للنتائج المتحصل عليها بعد البحث و التحري للحصول على الدليل ، خاصة مع سهولة العبث بها و التلاعب فيها و حتى تغييرها في ثواني من الخبراء .

بالرجوع للقواعد العامة في قانون الإجراءات الجزائية الجزائري أخذ المشرع بنظام مختلط في الإثبات إذ نص بداية كقاعدة بالمادة 212 من قانون الإجراءات الجزائية على مبدأ حرية الإثبات فيجوز إثبات كل الجرائم بأي طريق من طرق الإثبات ، و للقاضي الحرية في تكوين إقتناعه من أي دليل على أن يسبب حكمه.

و إستثناءا أخذ المشرع الجزائري بالإثبات المقيد إلا بوجود نص خاص ، و بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لم ينص على وجود إتباع طريق معين في إثباتها و عليه تخضع لحرية الإثبات طبقا للمادة 212 من قانون الإجراءات الجزائية.

بعض التشريعات المقارنة نصت على هذا النوع من الأدلة بصفة خاصة و ذهب بعضها للنص على قبول البيانات المسجلة على الدعائم الممغنطة أو المخزنة داخل نظام المعالجة الآلية للمعطيات كأدلة يقوم عليها الإثبات الجنائي [1]

(1) هلالي عبد الله أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي المرجع السابق ، ص 212 .

و في الولايات المتحدة الأمريكية صدرت قوانين بهذا الشأن في بعض الولايات ففي ولاية كاليفورنيا سنة 1983 صدر تشريع نص على أن النسخ المستخرجة من البيانات التي يحتويها الحاسب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات ، و في ولاية أيوا صدر قانون للحاسب الآلي سنة 1984 نص على أن مخرجات الحاسب الآلي تكون مقبولة كأدلة إثبات للبرامج و البيانات المخزونة فيه.[1]

أما بالنسبة للقانون الجزائري فالقاضي يخضع الدليل الإلكتروني كغيره من الأدلة لسلطته التقديرية ، و يعود له التمحيص في مدى إعتباره دليلا منطقيا كافيا للإثبات ، و إذا إستمد منه قناعته عليه تسبيب ذلك في الحكم تسبيب إعتماده على هذا الدليل و يدرس حجية هذه الأدلة العلمية كطريق إثبات طبقا للمادة 212 من قانون الإجراءات الجزائية .

و يتقيد القاضي في ممارسته لحريته في الإقتناع لقيود خاصة أملتها إعتبارات تتعلق بضمان حق المتهم في الدفاع و أهم هذه القيود ما يلي :

- أن تكون عقيدة القاضي أستمدت من أدلة طرحت بالجلسة .
- يجب أن يكون إقتناع القاضي مبنيا على دليل مستمد من إجراء صحيح .
- يجب أن يكون إقتناع القاضي مبنيا على أدلة مستساغة عقلا .
- أن يكون إقتناع القاضي مبنيا على اليقين .
- ألا يؤسس القاضي إقتناعه على قرينة واحدة أو إستدلال واحد .[2]

و قد أثيرت في فرنسا مشكلة محاضر المخالفات التي تحرر عقب عملية المراقبة الإلكترونية للسيارات و إنتهى القضاء إلى عدم إعتبار محاضر المخالفات حجة بذاتها إلا إذا أثبت فيها محرره وقائع تدخل في إختصاصه يكون قد شاهدها أو سمعها أو تحقق منها بنفسه. [3]

(1) هلالي عبد الله أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، دار النهضة العربية 1997 ص 54
(2) العربي شحط عبد القادر و نبيل صقر ، الإثبات في المواد الجزائية في ضوء الفقه و الإجتهاد القضائي ، دار الهدى عين مليلة الجزائر 2006 ص 28 و 29 .
(3) جميل عبد الباقي الصغير ، الجوانب الإجرائية المتعلقة بالأنترنيت ، دار النهضة ، القاهرة 1998 ص 29 .

و يطرح الإشكال أيضا بشأن هذه الأدلة المخزنة على مخرجات كوسائط التخزين خاصة في الأنظمة الأنجلو أمريكية التي تأخذ بمبدأ الإثبات بالشهادة و عليه فإعتماد مستندات مطبوعة من مخرجات عبارة عن إشارات ممغنطة يعد إشكال هل يؤخذ بها أو لا ؟ إذ لا يمكن للمحلفين في هذه الأنظمة و القاضي مشاطرة هذه الأدلة و وضع أيدهم عليها و هذا يجعلها أدلة ثانوية و ليست أصلية [1] في حين لا يطرح إشكال في التشريعات التي تأخذ بالنظام اللاتيني حيث يسود مبدأ حرية القاضي في الإقتناع.

و في أنجلترا ينص قانون الإثبات الجنائي في مادته 69 على أن الناتج من الوسائل الإلكترونية لا يقبل كدليل إذا تبين وجود سبب معقول يدعو إلى الإعتقاد بأن هذا الناتج غير دقيق أو أن بياناته غير سليمة أو يجب كذلك أن يكون الحاسب الناتج منه المخرج الإلكتروني [2]

و لأن الدعاوى التي تتعلق بهذه الجرائم محدودة نسبيا لعزوف الضحايا عن تقديم شكاوى من أجلها كما بينا سابقا ، و نظرا لصعوبة الحصول على الدليل فإن تصادف القاضي مع إحدى هذه الدعاوى يضع على كاهله عبء التعامل مع هذه الأدلة الفريدة التي يتعامل معها بخلفية التشكيك ، إذ يمكن أن تكون قد تعرضت للتحريف و التغيير و هنا يفترض من القاضي إعتماد أدلة تتوافرها بها شروط معينة لتعزيز مصداقيتها كدليل و منها :

1 – أن تكون أدلة ثابتة و منطقية : أي أن تدرج ملف الدعوى دلائل يقينية و ليس تلك التي تبقى مجرد تخمين ، و عليه يجب إدراج الأدلة التي تؤدي على الأغلب بعد مناقشتها لإثبات الجريمة أو نفيها بطريقة علمية واضحة مؤسسة ، و هذا يتطلب أن يكون القاضي على دراية بهذه الأدلة و متحكما في تقنيات الإعلام الآلي بما يمكنه من مناقشة الأدلة المتحصلة من أجهزة الحواسيب و المخزنة بالوسائط المستعملة بهذا المجال .

---

(1) هشام محمد فريد رستم ، قانون العقوبات و المخاطر التقنية للمعلومات ، المكتبة الحديثة 1992 ، ص 173
(2) هلالي عبد الله أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، المرجع السابق ، ص 72 .

2 – مناقشة الدليل : توجب المادة 212 من قانون الإجراءات الجزائية في فقرتها الثانية على القاضي أن يبني حكمه إلا على الأدلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه .

و عليه متى تضمن ملف الدعوى أدلة إلكترونية وجب تبعا للفقرة السالفة الذكر تناولها بالمناقشات بعد طبعها و الإطلاع عليها بإحدى الوسائل المتاحة تطبيقا لمبدأ شفوية المرافعات ، و بعد غلق باب المناقشات و المرافعات و لدى نظر القاضي في الدعوى يجب أن يبني حكمه على تلك الأدلة التي تمت مناقشاتها بالجلسة .

3 – مشروعية الدليل : من البديهي أن يكون الدليل المتحصل عليه من الوسائل الإلكترونية تم وفقا لإجراءات قانونية مشروعة و إلا كانت أدلة باطلة لا يمكن بناء حكم بالإدانة عليها ، كعدم الحصول على إذن مسبق من القاضي المختص لإلتقاط صور أو قبل عملية التسرب أو وضع أجهزة التسجيلات ثم يتم تقديم ما تم العثور عليه كدليل و لو كان قاطعا لا يجوز مناقشته كدليل إثبات و يجب إستبعاده .

و من الأدلة المتحصل عليها بطرق غير شرعية تلك التي كانت نتيجة تعذيب أو إكراه مادي أو معنوي لفك الشيفرة أو كلمة السر المتحصل عليها بإستخدام التدليس أو الغش أو الخديعة .

و رغم توفر التقنيات الحديثة و الوسائل لإستخلاص الأدلة إلا أن المشرع الجزائري لم يقيد سلطة القاضي في إختيار و تقدير قيمة أي من هذه الأدلة و لم يضع شروط أو معايير لذلك و لم يقيد سلطة القاضي في الإقتناع من أي دليل ، لكن هذا يزيد من أهمية دور القاضي و صعوبة المهمة الموكلة له في إستخلاص الدليل القاطع من أدلة غير ثابتة و غير مستقرة غير بينة المعالم يحوطها الشك .

و هنا لا ننسى أن المشرع أتاح للقاضي في كافة مراحل الدعوى إمكانية اللجوء للخبراء كلما إعترضته مسألة فنية فيمكنه الإستعانة بذوي الإختصاص في هذا المجال للإجابة عن الإشكالات التقنية ، التي تتطلب إستخدام وسائل علمية حديثة لإعطاء نتائج و الإجابة عنها ، و من الهيئات التي يمكن اللجوء إليها مخبر الشرطة العلمية الذي يوجد به مخبر الأدلة المعلوماتية الذي يستخدم تقنيات عالية لإستخلاص الأدلة الجنائية من الأدلة

الإلكترونية كنظام إسترجاع المعطيات ، و معهد الإجرام و الأدلة الجنائية التابع لقسم الشرطة القضائية لقيادة الدرك الوطني و الذي له عدة أقسام من بينها القسم الإلكتروني المعلوماتي .

و عن نتائج الخبرة تخضع بدورها للسلطة التقديرية للقاضي طبقا للمادة 213 من قانون الإجراءات الجزائرية

مع الإشارة لوجوب أن تتطور طرق إستخلاص الدليل مواكبة مع نشأة جرائم جديدة كل يوم سهل من إنتشارها توافر التقنيات العلمية التي زادت من تعقيد إرتكابها و عقدت أيضا من الوصول إليها و تحصيل الأدلة خاصة مع إختفاء آثارها بسرعة و التي أصبحت طرق الإثبات التقليدية عقيمة معها إذ أصبحت الطرق العلمية و الفنية أصبحت الوحيدة المناسبة لإثبات هذا النوع من الجرائم.

و إذا كانت الكفة تميل للخبرة العلمية لإثبات هذه الجرائم فهذا يزيد من دور القاضي في إظهار مواطن الضعف و القوة في النتائج المتوصل لها ، و البحث في إسنادها للمتهم ليحول الحقيقة العلمية لحقيقة قضائية ثابتة بدليل قاطع .

المبحث الثالث : الجزاءات المقررة للجرائم الماسة بنظام المعالجة الآلية للمعطيات

تضمنت المادة 13 من الإتفاقية الدولية المتعلقة بالإجرام المعلوماتي على توصية فيما يتعلق بالجزاء الواجب النص عليها لهذا النوع من الجرائم إذ اكدت على ضرورة وضع عقوبات فعالة متناسبة و داعية للعدول عنها و تشمل الحرمان من الحرية بالنسبة للجرائم المنصوص عليها بالمواد من 2 إلى 11 من الإتفاقية تماشيا مع خطورة هذه الجرائم.

المطلب الأول : الجزاء المقرر للشخص الطبيعي

نتناول في هذا المطلب العقوبات الأصلية و العقوبات التكميلية ثم ظروف تشديد العقوبة

أولا : العقوبات الأصلية

من خلال الإطلاع على المواد النصوص العقابية الخاصة بهذا النوع من الجرائم يلاحظ أن المشرع الجزائري اعتمد سلما تصاعديا للعقوبات حسب خطورة الجريمة و التي يمكن تقسيمها إلى ثلاث فئات :

- جريمة الدخول أو البقاء الغير شرعي البسيط .
- جريمة الدخول أو البقاء الغير شرعي في صورتها المشددة.
- جريمة المساس العمدي بالمعطيات و التعامل في المعطيات الغير مشروعة

و تم تحيين العقوبات طبقا لأحكام المادة 60 من القانون 23/06 المؤرخ 2006/12/20 المعدل و المتمم لقانون العقوبات .

1 – جريمة الدخول أو البقاء الغير شرعي في صورتها البسيطة

عاقب قانون العقوبات الفرنسي علة هذه الجريمة بالمادة 323-1 فقرة 1 بالحبس مدة سنتين و 30 000 أورو غرامة ، تقابلها المادة 394 مكرر فقرة 1 من قانون العقوبات الجزائري التي نصت على تطبيق عقوبة من ثلاث أشهر إلى سنة و غرامة من 50 000 دج إلى 200 000 دج

2 - جريمة الدخول أو البقاء الغير شرعي في صورتها المشددة

نصت المادة 232-1 من قانون العقوبات الفرنسي في فقرتها الثانية على عقوبة هذه الصورة التي يجب أن ينتج عنها محو أو تغيير أو تعييب للنظام برفع العقوبة لثلاث سنوات حبس و 45 000 أورو ، في حين المشرع الجزائري نص على مضاعفة العقوبة الواردة بالفقرة الأولى إذا ترتب عن الدخول أو البقاء الغير شرعي حذف أو تغيير للمعطيات بنص المادة 394 مكرر في فقرتها الثانية .

و طبقا للفقرة الثالثة من ذات المادة إذا أدى الدخول أو البقاء إلى تخريب نظام إشتغال المنظومة تكون العقوبة من ستة أشهر إلى سنتين حبس و غرامة من 50 000 دج إلى 300 000 دج ، بالمقابل نصت المادة 232-1 فقرة 3 في هذه الحال تصبح العقوبة خمس سنوات و 75 000 أورو .

3 – جريمة المساس العمدي بالمعطيات و التعامل بمعطيات غير مشروعة

عاقبت عليها المادة 323-2 الفقرة الثانية من قانون العقوبات الفرنسي بعقوبة ثلاث سنوات حبس و 75 000 أورو غرامة ، أما قانون العقوبات الجزائري في المادة 394 مكرر 1 العقوبة المقرر للإعتداء العمدي على المعطيات الموجودة داخل النظام بالإدخال ، الإزالة أو التعديل بالحبس من ستة أشهر إلى ثلاث سنوات و غرامة من 500 000 دج إلى 4 000 000 دج .

أما العقوبة المقررة لإستخدام المعطيات في إرتكاب الجرائم الماسة بالأنظمة و كذا حيازة و إفشاء أو نشر أو إستعمال المعطيات المتحصل عليها من إحدى الجرائم هي الحبس من شهرين إلى ثلاث سنوات و غرامة 1 000 000 دج إلى 10 000 000 دج و هي العقوبة المنصوص عليها بالمادة 394 مكرر 2

ثانيا : العقوبات التكميلية

و تنطبق على كل صور الجرائم و نص قانون العقوبات الفرنسي على مجموعة من العقوبات بنص المادة 323 في فقرتها الخامسة .

و للإشارة قبل تعديل 1992 تضمن قانون العقوبات عقوبة تكميلية واحدة هي المصادرة الجوازية للوسائل المستعملة في إرتكاب الجريمة المعلوماتية ، و بعد التعديل نص على عدة عقوبات تكميلية بالمادة السالفة الذكر و التي يمكن إجمالها في مايلي :

_ الحرمان من الحقوق السياسية و المدنية و العائلية لمدة لا تتجاوز خمس سنوات و ذلك طبقا للمادة 131 من ذات القانون .

- الحرمان من حق تولي الوظائف العامة أو أي نشاط مهني أو إجتماعي تكون الجريمة قد إرتكبت بسببه او بمناسبته .

- مصادرة الاشياء التي إستخدمت أو كان من شأنها أن تستخدم في إرتكاب الجريمة.

- غلق المؤسسة أو المؤسسات التي ساهمت في إرتكاب الجريمة مدة لا تتجاوز خمس سنوات.

- الإستبعاد من التعامل في الأسواق العامة مدة لا تتجاوز 5 سنوات .

- نشر الحكم طبقا للشروط المنصوص عليها في المادة 131 فقرة 35 .

و فيما يتعلق بقانون العقوبات الجزائري نص أيضا على عقوبات تكميلية التي تطبق على كافة صور المساس بانظمة المعالجة الآلية للمعطيات و هي العقوبات المنصوص عليها بالمادة 394 مكرر 6 على النحو التالي :

" مع الإحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقب عليها وفقا لهذا القسم .

علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد إرتكبت بعلم مالكها"

و من نص هذه المادة يمكن حصر العقوبات التكميلية في :

1 – المصادرة : كما عرفتها المادة 15 في فقرتها الأولى من قانون العقوبات هي : " الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة ، أو ما يعادل قيمتها عند الإقتضاء ."

و تشمل المصادرة فيما يتعلق بهذه الجرائم الأجهزة و البرامج و الوسائل المستعملة في إرتكاب الجريمة مع مراعاة حقوق الغير الحسن النية .

و بذلك تكون المصادرة بالنسبة لهذه الجرائم عقوبة وجوبية إذ أن المادة السالفة الذكر لم تخيير القاضي بين الحكم بها أو عدمه فليست له سلطة تقديرية في ذلك ، على أنه يجب أن تكون الأشياء التي يحكم بمصادرتها قد إستخدمت في إرتكاب الجريمة طبقا للمادة 394 مكرر 6 من قانون العقوبات التي عددت محل المصادرة على سبيل المثال و ليس الحصر إذ ورد بها عبارة (... و الوسائل المستخدمة ...) التي تستوعب أي شيء و تجعله قابل للمصادرة ، مع التأكيد على عدم الإخلال بحقوق الغير حسن النية ذلك أنه لا يتوافر لديه القصد الجنائي و الذي يجهل أن وسائله أستعملت في إرتكاب جريمة و الذي لو علم لحال دون ذلك .

2 – إغلاق المواقع : يتعلق الأمر بالواقع التي تكون محلا لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

3 – إغلاق المحل أو مكان الإستغلال : شرط أن تكون الجريمة قد ارتكبت بعلم مالك المكان الذي سمح من خلاله بالدخول غير المصرح به لمختلف الأنظمة و سمح بالتلاعب بالمعطيات مثل مقاهي الأنترنيت و هنا وجب التأكد و إثبات ركن العلم لدى هذا الأخير إذ يمكن أن يكون غير مرتكب الجريمة و عليه لا تطبق عليه العقوبة التكميلية بعد إدانة الجاني .

و بالنسبة لمدة الغلق لم تحددها المادة 394 مكرر 6 من قانون العقوبات و عليه يمكن أن تكون مؤبدة أو مؤقتة كما نصت على ذلك المادة 26 من قانون العقوبات :" يجوز أن يؤمر بغلق المؤسسة نهائيا أو مؤقتا في الحالات المنصوص عليها في القانون ."

ثالثا : الظروف المشددة

نصت المادة 394 مكرر في فقرتها الثانية و الثالثة على تشديد العقوبة في جريمتي الدخول أو البقاء الغير شرعي إذا ما تحقق ظرف معين .

أولا إذا ما ترتب عليه حذف أو تغيير في المعطيات فتضاعف العقوبة المنصوص عليها بالفقرة الأولى .

و ثانيا إذا ما ترتب عليه تخريب نظام إشتغال المنظومة ترفع العقوبة إلى " من ستة أشهر إلى سنتين و غرامة من 000 50 إلى 000 300 دج .

و الظرف المشدد هو ظرف مادي يجب إثبات وجود علاقة سببية بينه و بين الجريمة الأصلية و النتيجة للقول بتوافره و تشديد العقوبة .

كما نصت المادة 394 مكرر 3 على ظرف تشديد آخر بقولها :

" تضاعف العقوبات المنصوص عليها في هذا القسم إذ إستهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد "

و هنا ظرف التشديد يتعلق بمركز المجني عليه فمتى كانت الضحية المستهدفة إحدى الهيئات المنصوص عليها بالمادة تكون العقوبة المقررة هي ضعف العقوبة المنصوص عليها لكل جريمة طبقا للمواد السالفة الذكر .

المطلب الثاني : الجزاء المقرر للشخص المعنوي

نص المشرع الجزائري و الفرنسي على مسآلة الشخص المعنوي و تطبيق عقوبات خاصة به تطبيقا للتوصية الواردة بالمادة 12 من الإتفاقية الدولية للإجرام المعلوماتي التي نصت على وجوب أن يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا ، كما يسأل عن الجريمة التامة أو الشروع فيها شرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي و بواسطة أحد أعضائه أو ممثليه .

مع تجدر الملاحظة إلى أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

و بالنسبة لقانون العقوبات الفرنسي نص في المادة 6/323 على جواز مساءلة الشخص المعنوي و تتحدد المسؤولية حسب أحكام المادة 2/21 من ذات القانون و يسأل بصفته فاعلا أو شريكا كما يسأل عن الجريمة التامة و تلك التي تقف عند حد الشروع طبقا للمادة 2/122 .

و نصت كذلك الفقرة 3 و 2 من المادة 121 على أن المسؤولية الجزائية للأشخاص الإعتباريين لا تخل بمسؤولية الشخص الطبيعي كفاعل أو شريك متى توافرت شروطها

أولا : العقوبات الأصلية

نصت المادة 323 من قانون العقوبات الفرنسي في فقرتها السادسة أن العقوبات التي تطبق على الشخص المعنوى و هي :

- الغرامة .
- العقوبات المقررة بالمادة 131 فقرة 33 .
- المنع من مزاولة النشاط الذي بمناسبته إرتكبت الجريمة.
- مصادرة الأشياء التي إستعملت في إرتكاب الجريمة .
- الغلق لمدة خمس سنوات أو أكثر فيما يتعلق بالمؤسسات التي ساهمت في إرتكاب الجرائم.
- المنع من المشاركة في الأسواق العمومية لمدة خمس سنوات .
- نشر الحكم .

و عن المشرع الجزائري فإنه أخذ بمبدأ مسؤولية الشخص المعنوي عامة المستقلة عن مسؤولية الشخص الطبيعي بعد تعديل قانون العقوبات بموجب القانون 23/06 المؤرخ 2006/12/20 في المادة 18 مكرر التي عددها فيها العقوبات المطبقة على الشخص المعنوي .

و بالنسبة للعقوبات المطبقة على الشخص المعنوي في حال إرتكابه أحد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فقد نصت عليها المادة 394 مكرر 4 من قانون العقوبات على النحو الآتي :

" يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي"

و يشترط تبعا لذلك لتقرير مسؤولية الشخص المعنوي ثلاث شروط :

- يشترط في الشخص المعنوي أن يكون عاما أو خاصا بإستثناء الدولة .
- يجب أن ترتكب الجريمة لصالح الشخص المعنوي.
- يجب أن ترتكب الجريمة من طرف عضو أو ممثل الشخص المعنوي دون أن تؤثر على مسؤولية الشخص الطبيعي.

ثانيا : العقوبات التكميلية

و هي ذات العقوبات التكميلية المطبقة على الشخص الطبيعي على الشخص الطبيعي و المنصوص عليها بالمادة 394 مكرر 6 التي جاءت شاملة و التي سبق و أن تناولنها بالشرح بالمطلب السابق الخاص بالجزاءات المطبقة على الشخص الطبيعي التي نصت:

" مع الإحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكا ."

المطلب الثالث : الجزاءات المقررة للإتفاق الجنائي و الشروع

أولا : الجزاء المقرر للإتفاق الجنائي

يقصد بداية بالإتفاق الجنائي إتجاه إرادة شخصين أو أكثر لإرتكاب جناية و جنحة أو أي من الأعمال المنفذة أو المسهلة لإرتكابها ، و نصت على وجوب تجريمه المادة 11 من الإتفاقية الدولية للإجرام المعلوماتي على النحو الآتي : " يجب على كل طرف ان يتبنى الإجراءات التشريعية و أية إجراءات أخرى يرى أنها ضرورية لتجريم (تبعا لقانونه الداخلي) كل إشتراك إذا تم عمدا بغرض إرتكاب إحدى الجرائم المشار لها بالمواد 2 – 10 من الإتفاقية الحالية بنية إرتكاب تلك الجريمة "

و تبين المذكرة التفسيرية هدف وضع هذه المادة هو إنشاء جرائم تكميلية ترتبط بالإشتراك في الجرائم المعرفة بواسطة هذه الإتفاقية بغرض إرتكابها [1]

و هو ما أخذ به المشرع الفرنسي بالمادة 4/323 التي تعاقب على المساهمة في إرتكاب الأفعال المادية التحضيرية التي تهدف إلى إرتكاب إحدى الجرائم المنصوص عليها بالمواد 1/323 إلى 3/323 أي جرائم الإعتداء على نظم المعالجة الآلية للمعطيات .

و عليه فالمشرع خرج عن القواعد العامة التي تقتضي عدم العقاب إلا على الجرائم التامة إذ عاقب على مجرد الإتفاق على إرتكاب الأعمال التحضيرية المسهلة لإرتكاب الجرائم ، و لعل مبرر ذلك سعي المشرع لإيجاد نوع من الحماية و الوقاية من الجرائم و لمواجهة القرصنة المعلوماتية .

و تبنى المشرع مبدأ معاقبة الإتفاق الجنائي بنص المادة 394 مكرر 5 على النحو التالي : " كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها "

---

(1) طارق إبراهيم الدسوقي عطية ، المرجع السابق ص 207 .

و ما يلاحظ بداية أن المشرع الجزائري خص الإتفاق المتعلق بهذه الجرائم بنص خاص على الرغم من نص قانون العقوبات بالمادة 176 على جمعية الأشرار التي تؤلف للإعداد لإرتكاب جنايات أو جنح ، و لعل مرجع ذلك أن هذا النص محدود المجال فيما يتعلق بالجنح إذ خص بالذكر الإعداد لإرتكاب الجنح المعاقب عليها بخمس سنوات على الأقل و عليه لا يمكن أن يشمل حكم المادة 176 من قانون العقوبات كل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي تقل فيها عقوبات بعض الصور عن هذا الحد .

و لعل الحكمة من تجريم الإتفاق الجنائي و النص عليه بنص خاص هو ان هذه الجرائم عادة ما ترتكب في شكل مجموعات تم تكوينها لهذا الغرض ، و رغبة من المشرع في توسيع نطاق التجريم نص على تجريم الأفعال التحضيرية التي تسبق البدء في التنفيذ إذا تم في إيطار إتفاقي و عليه و بمفهوم المخالفة تخرج الأعمال التحضيرية المرتكبة من شخص واحد عن إطار التجريم .

و يعاقب المشرع الجزائري طبقا للمادة 394 مكرر 5 بنفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تطبق عقوبة الجريمة الأشد .

و يشترط إنطلاقا من المادة 394 مكرر 5 للعقاب على الإتفاق الجنائي مايلي :

1- إشتراط المشاركة في مجموعة أو إتفاق :

و يستوى هنا أن يكون أعضاء الإتفاق شركة ، مؤسسة أو شخص معنوي أو جماعة يكفي فيها أن يعرف مجموعة من الأشخاص الطبيعية شخصين فأكثر بعضهم البعض و إتفقوا على إرتكاب جريمة أو أكثر .

2- الهدف : يجب أن يكون الغرض من تكوين الجماعة هو الإعداد لإرتكاب جريمة أو أكثر من الجرائم الماسة بنظام المعالجة الآلية للمعطيات ، و عليه لا يعاقب على الإتفاق الذي يهدف لإرتكاب جريمة التقليد مثلا المعاقب عليها بنص حق المؤلف و الحقوق المجاورة .

3 – تجسيد التحضير بفعل مادي : كتبادل المعلومات الضرورية لإرتكاب الجريمة فهو من الأفعال الإيجابية و ليس مجرد الإنضمام فهذا الأخير يجب أن يظهر للوجود بسلوك معين .

4 – القصد الجنائي : يجب توافر العلم لدى كل فرد في المجموعة بأنه عضو في جماعة إجرامية و أن تتجه إرادته إلى تحقيق نشاط إجرامي معين المتمثل في العمل التحضيري ، و لا يشترط أن يكون كل فرد عالما بنشاط الآخر و تعتبر كل مشاركة في الإتفاق أو المجموعة معاقب عليها بنفس العقوبة المقررة للجريمة المراد إرتكابها متى توافرت الشروط السابقة الذكر و تطبق عليها العقوبات الأصلية و التكميلية التي سبق و تقدم بيانها .

ثانيا : الجزاء المقرر للشروع في إرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

نصت إتفاقية بودابست للإجرام المعلوماتي في الفصل الخامس للمسؤولية و الجزاءات على الشروع في المادة 11 في فقرتها الثانية كالآتي :" يجب على كل طرف ان يتبنى الإجراءات التشريعية و أية إجراءات أخرى يرى أنها ضرورية لتجريم (تبعا لقانونه الداخلي) كل شروع عمدي لإرتكاب إحدى الجرائم المشار لها بالمواد من 3 إلى 5 و7 إلى 9 من الإتفاقية الحالية " .

و تبين المذكرة التفسيرية أن هدف وضع هذه المادة هو إنشاء جرائم تكميلية ترتبط بالشروع في الجرائم المعرفة بواسطة هذه الإتفاقية [1]

عاقب التشريع الفرنسي بالمادة 323 الفقرة السابعة من قانون العقوبات على الشروع في إرتكاب الجرائم الماسة بالأنظمة المعلوماتية بالعقوبة ذاتها المقررة للجريمة في صورتها الكاملة تطبيقا لما أوصت به الإتفاقية الدولية للإجرام المعلوماتي في مادتها الحادية عشر.

و هو ما أخذ به المشرع الجزائري بالمادة 394 مكرر 7 من قانون العقوبات التي تنص: " يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "

و بما أن كل الجرائم في هذا القسم ذات وصف جنحي فإنه لا يعاقب على الشروع طبقا للقواعد العامة إلا بنص خاص ، و من خلال نص هذه المادة يلاحظ أن المشرع

(1) طارق إبراهيم الدسوقي عطية ، المرجع السابق ص 199 .

الجزائري وسع دائرة الجرائم لتشمل الشروع في كل الجرائم الواردة بالقسم بما فيها الإتفاق الجنائي المنصوص عليه بالمادة 394 مكرر 5 على خلاف المشرع الفرنسي الذي إستثنى الإتفاق لأن التحضير للجرائم الذي يتم في إيطار إتفاق يشكل في حد ذاته محاولة أو عمل تحضيري و القول بالمعاقبة على الشروع فيه يطرح إشكال الشروع في الشروع .

و رجوعا للقواعد العامة تنص المادة 30 من قانون العقوبات على أن كل المحاولات لإرتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة لإرتكابها تعتبر كالجناية نفسها ، إذا لم يوقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى و لو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها ."

و طبقا للمادة 31 من قانون العقوبات لا يعاقب على الشروع في مادة الجنح إلا بنص خاص ، و فيما يتعلق بهذه الجرائم النص هو المادة 394 مكرر 7 من قانون العقوبات.

و الإشكال الذي يطرح بشأن الشروع هو التمييز بين الأعمال التي تعد تحضيرية و تلك التي تعد بدأ في التنفيذ لأن هذا التمييز ذو أهمية و التي تظهر في أن الأعمال التحضيرية كقاعدة غير معاقب عليها إذ تعد مجرد أفكار أما الأفعال التي تشكل بدأ في التنفيذ فمعاقب عنها .

فيما يتعلق بالشروع يعد بدأ في التنفيذ الجريمة المعلوماتية هو إتيان أي عرقلة مادية مثل الدخول للقاعة أين توجد الوسائل بهدف إرتكاب جريمة يعد من الأعمال التحضيرية و في اللحظة التي تصبح فيها العملية الفكرية مجسدة كالدخول للنظام فهذا بمثابة بدأ في التنفيذ .

و تبقى عملية التفريق بين الأعمال التحضيرية و أعمال البدأ في التنفيذ جد صعبة و لعل هذا ما دفع المشرع لتجريم الإتفاق لنكون أمام جريمة مستقلة منذ بداية الأعمال التحضيرية لإرتكاب أي جريمة .

الخـــاتمـــــة

حاولنا قدر الإمكان من خلال هذه الدراسة عرض بعض الأحكام المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات ذلك أنه لا يمكن الإلمام بها نظرا لخصائصها المتغيرة و المرتبطة إرتباطا وثيقا بالتطور التكنولوجي المستمر .

وخلاصة ما يمكن قوله بخصوص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أنها تعد تهديدا مباشرا و غير مباشر لتقدم البشرية ، إذ ينفذها أشخاص على درجة عالية من الذكاء يستعملون التكنولوجيا لغرض الإضرار بالمجتمع و ليس لخدمته.

و هي جرائم على قدر عالي من التعقيد يزداد كلما تطورت التكنولوجيا أكثر إذ أن هذا التطور سلاح ذو حدين يستفيد منه الجاني أيضا لتطوير وسائل إرتكاب الجرائم و إتخاذ صور جديدة منها ، مما يجعل متابعة الجرائم و التحقيق فيها لا يخلو من العراقيل و العقبات المادية و القانونية ، هذا الذي يفرض تكوين فئة معينة من رجال القانون متمكنين من المادة التي يبحثون فيها لجمع الآلة و الحفاظ عليها و تتبع آثار الجريمة التي تكاد تنعدم مما يحتم بحثا إحترافيا .

و ما لاحظناه من خلال هذه الدراسة قصور النصوص القانونية لإيجاد حماية جزائية في هذا النوع من الجرائم إذ أن بعض الدول لم تجرم هذا النوع من الأفعال إلا مؤخرا ، كالمشرع الجزائري الذي جرمها بموجب القانون 15/04 المعدل و المتمم لقانون العقوبات ، و هو التعديل الذي جاء مقتضبا من حيث صور الجريمة المعلوماتية المجرمة كما لم يتضمن مفاهيم لصور الجريمة أو محلها سيما مفهوم أنظمة المعالجة الآلية و المعطيات ، إضافة للنقص في جانب النصوص الإجرائية أيضا إذ وجب أن يكون لهذا النوع من الجرائم نصوص خاصة و إختصاصات موسعة للبحث و التحري عن الأدلة ذات الطبيعة الخاصة .

و كمحاولة و لو متأخرة أصدر المشرع الجزائري القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات

الإعلام و الإتصال لتنظيم الجانب الإجرائي خاصة مع صعوبة الإثبات في هذه الجرائم بإستعمال الإجراءات التقليدية المنصوص عليها بقانون الإجراءات الجزائية نظرا لإرتكاب هذه الجرائم في بيئة إلكترونية تفوق فيها الخسائر خسائر أي جريمة أخرى الأمر الذي من شأنه تهديد إستقرار كل المعاملات .

و يمكن تلخيص النتائج المتوصل لها من هذه الدراسة فيما يلي :

قصور النصوص التشريعية الخاصة بهذه الجرائم من الناحية الموضوعية مما يرتب ضعف الحماية الجزائية للفرد و المجتمع من هذه الجرائم ، و أيضا من الناحية الإجرائية مما ينعكس سلبا على إجراءات التحري ، المتابعة ، التحقيق و المحاكمة و البحث عن الدليل في ظل جرائم صعبة الإثبات لا اثر لها .

طبيعة هذه الجرائم و إرتباطها بمستوى رفيع من التكنولوجيا المعلوماتية يحتم تأهيل بشري بذات المستوى ، سواء من رجال الضبطية أو القضاة في مراحل التحقيق أو المحاكمة ، و هي الجرائم التي غيب فيها دور القاضي في البحث عن الادلة نسبيا و أصبح الخبير المعلوماتي هو من يلعب الدور الرئيسي في إيجاد الدليل .

صعوبة الحصول على الدليل الإلكتروني من حيث طبيعته و دور الوسائل التقنية في ذلك ، و قيمة الدليل المتحصل عليه بإستعمال هذه الطرق ، و تقديره من طرف القاضي في ظل مبدا الإقتناع الحر للقاضي و حريته في تكوين عقيدته من أي دليل طبقا للمادة 212 من قانون الإجراءات الجزائية و الذي و رغم مساهمته المحدودة في إستخلاص الدليل يبقى له التقدير النهائي للدليل ما إذا كان كافيا لإدانة المتهم أو إستبعاده أو إعمال قاعدة تفسير الشك لصالح المتهم .

و من خلال النقائص المسجلة بعد هذه الدراسة يمكن أن نخلص لمجموعة من التوصيات و الإقتراحات المتعلقة بهذه الجرائم :

وجوب وضع تعريفات للمصطلحات المتعلقة بهذه الجرائم ليس بالشكل الذي يحصر صورها المتجددة إنما بشكل يعطي خطوط عريضة عن مكوناتها و المفاهيم المتداولة فيها .

السعي لإبرام إتفاقيات للتعاون الدولي لتسهيل تبادل المعلومات حول المجرمين و الجرائم للحد منها خاصة و أنها عابرة للحدود لا تترك أثرا ، فمن شأن التعجيل في إتخاذ تدابير التحري أن يحقق الحصول على أكبر قدر ممكن من الأدلة قبل طمسها .

تحيين النصوص التشريعية الموضوعية و الإجرائية مواكبة مع تطور وسائل إرتكاب الجرائم و تعدد صورها بعد أن ثبت قصور الحماية الفنية .

السعي لتوحيد نصوص التجريم الداخلي لتسهيل إجراءات المتابعة للأفعال المرتكبة بالخارج لتكون مجرمة فيها أيضا .

تكوين رجال القضاء و مساعديه تكوين خاص بتقنيات الكمبيوتر و وسائل إرتكاب هذه الجرائم من رجال الضبطية القضائية و قضاة خاصة قضاة الأقطاب الجزائية المتخصصة ذات الإختصاص الموسع ، مع وجوب برمجة دورات تكوينية مستمرة لمواكبة كل ما هو جديد بالتنسيق مع الخبراء في مجال الكمبيوتر و الإعلام الآلي .

إحداث أدلة إثبات جديدة و أساليب تحقيق خاصة تتناسب مع طبيعة هذه الجرائم.

دعوة الدول المتقدمة لتقديم المساعدة لنظيراتها التي تحتاجها لتمكينها من مكافحة هذه الجرائم عن طريق توفير برامج تدريب و مساعدة فنية .

و هناك من الدول من طبق بعضا من هذه التوصيات ، ففي فرنسا تم الإعداد لتأهيل الجانب البشري لمواجهة هذا النوع من الجرائم من قضاة و محققين و ضباط شرطة قضائية منذ منتصف التسعينات من القرن الماضي .

و من التوصيات التي أصدرها مجلس الدولة الفرنسي في مؤتمر عقد في سبتمبر 1997 عن الأنترنيت و الشبكات الرقمية :

التشديد على تعريف شخصيـــة المستخدمين فعلى من ينشر بيـــانـــات على الجمهور و بصفة شخصية أن يكشف عن هويته ، و بالنسبة للمواقع المهنية يجب الإشارة إلى المسؤول عن الموقع و مؤدي الخدمة الذي إن لزم الأمر عليه أن يمد المحققين بالبيانات عن الإتصالات التي يجب حفظها لمدة سنة على الأقل و وضع عقوبة للبيانات المزيفة .

وضع تشريعات من شأنها السماح لمؤدي الخدمة للإحتفاظ بعينات من بيانات المتعاملين و السماح لرجال الأمن إصدار توجيهات لمؤدي الخدمة لحفظ البيانات ذات المصدر الأجنبي مع فحص الموضوع طبقا للقانون المحلي بعد صدور أمر قضائي .

تأمين الوسائل التي تسمح بالحفظ السريع للمعلومات و الكشف السريع عن أكبر كمية من المعلومات تنفيذا لأي أمر قضائي محلي أو دولي و إمداد الدولة الطالبة بالمعلومات الكافية في أقرب الآجال ما لم يكن في ذلك مخالفة لسيادة الدولة و أمنها [1]

و أبرز خطوة قام بها الإتحاد الأوروبي في إطار التعاون الدولي لمواجهة هذه الجرائم عام 2001 هي إبرام إتفاقية بودابيت للإجرام المعلوماتي التي وقعت عليها أكثر من إثني عشر دولة أوربية لحل مشكلة الإختصاص القضائي و القانون الواجب التطبيق .

و على المستوى العربي صدر القانون العربي النموذجي لمكافحة جرائم الكمبيوتر و الأنترنيت و هو ثمرة عمل مشترك بين وزراء العدل العرب و وزراء الداخلية بعد عقد إجتماع مشترك في 21 و 2002/05/22 أين تم إقرار المشروع .

و عن المشرع الجزائري فقد أقر حماية جزائية لأنظمة المعالجة الآلية للمعطيات بموجب تعديل قانون العقوبات 15/04 إذ جرم عدة صور من الإعتداءات عليها عالجناها بالفصل الأول من هذه الدراسة ، و الذي كفل الأنظمة بالحماية الجزائية سواء كانت خاضعة لحماية فنية مسبقة أو دونها ، و هنا حسب رأينا كان الأجدر بالمشرع تشديد العقوبة إذا ما تم المساس بأنظمة محمية مسبقا لأن هذا عادة ما يتم على يد مجرم خطير على درجة من الكفاءة و الذكاء .

أيضا لا بد من تشديد العقوبة لإعتبارات شخصية في الجاني كأن يكون قد إرتكب الجريمة بمناسبة تأدية مهام وظيفته أو بمناسبتها ، إذ يكون بذلك قد خان الثقة التي وضعها فيه رب عمله مستغلا وظيفته لإرتكاب الجريمة الذي لم يكن له ذلك لولاها.

(1) صالح أحمد البربري ، المرجع السابق ص 20 .

كما جرم المشرع الجزائري الإتفاق الجنائي بهدف إرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، و وضع عقوبات خاصة أيضا بالشخص الطبيعي و المعنوي لقمعها .

و هذه الجرائم و مع إتساع مفهومها و تطورها يوما بعد يوم هذا يفرض على المشرع تحديث النصوص التشريعية الموضوعية و الإجرائية لمكافحتها إذ أنها ليست كباقي الجرائم نظرا لخصوصيات الجريمة و لخصوصيات الجاني فيها و لآثارها الجسيمة ، كما يجب تكثيف الجهود على مستوى التعاون الدولي لمواجهة هذه الجريمة العابرة للحدود .

تمت بحمد الله

قائمة المراجع

1- المؤلفات :

أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، الجزء الأول ، دار هومة ، الطبعة الثالثة 2011 .

أحسن بوسقيعة ، التحقيق القضائي ، دار هومة ، الطبعة الخامسة ، 2006 .

أحمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي الإسكندرية ، الطبعة الثانية ، 2006 .

العربي شحط عبد القادر و نبيل صقر ، الإثبات في المواد الجزائية في ضوء الفقه و الإجتهاد القضائي ، دار الهدى عين مليلة الجزائر ، 2006 .

جباري عبد المجيد ، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة ، دار هومة للنشر و التوزيع الجزائر 2012 .

جميل عبد الباقي الصغير ، القانون الجنائي و التكنولوجيا الحديثة ، الكتاب الأول (الجرائم الناشئة عن إستخدام الحاسب الآلي) دار النهضة العربية القاهرة ، 1992 .

جميل عبد الباقي الصغير ، الجوانب الإجرائية المتعلقة بالأنترنيت ، دار النهضة العربية القاهرة ، 1998 .

جميل عبد الباقي الصغير ، جرائم التكنولوجيا الحديثة ، دار النهضة العربية ، 1998 .

جيلالي بغدادي ، التحقيق دراسة مقارنة و تطبيقية ، الديوان الوطني للأشغال التربوية ، الطبعة الأولى 1999 .

خالد ممدوح إبراهيم ، أمن المستندات الإلكترونية ، الدار الجامعية الإسكندرية 2008 .

خالد ممدوح إبراهيم ، التقاضي الإلكتروني ، دار الفكر الجامعي الإسكندرية 2009 .

خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي الإسكندرية 2009 .

دون باركر ، جرائم الكمبيوتر و حماية المعلومات ، 1998 .

رمسيس بهنام ، الإجراءات الجنائية تأصيلا و تحليلا ، منشأة المعارف ، طبعة، 1984 .

رشا علي الدين ، النظام القانوني لحماية البرمجيات بين نظرية تنازع القوانين و القانون الدولي الإتفاقي ، الطبعة الأولى ، مصر ، 2004 .

طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة الإسكندرية ، 2009 .

عبد الله أوهايبية ، شرح قانون الإجراءات الجزائية الجزائري ، التحري و التحقيق ، دار هومة ، 2004 .

عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر و الأنترنيت ، دار الفكر الجامعي الإسكندرية ، 2006 .

عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، دار الكتب القانونية مصر، 2007 .

عبد الفتاح بيومي حجازي ، الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية المعلوماتية) دار الفكر الجامعي الإسكندرية ، 2008 .

عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون ، دراسة مقارنة ، الطبعة الثانية 2003.

علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، المكتبة القانونية القاهرة 1999 .

محمد أمين الشوابكة ، جرائم الحاسوب و الإنترنت (الجريمة المعلوماتية) مكتبة دار الثقافة للنشر و التوزيع عمان الأردن ، 2004 .

محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي ، دار الجامعة الجديدة الإسكندرية مصر ، 2007 .

محمود أحمد عبابنة ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر و التوزيع عمان ، الطبعة الأولى ، 2009 .

مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الأولى ، مطابع الشرطة القاهرة مصر ، 2009 .

منير محمد الجنبيهي ، أمن المعلومات الإلكترونية ، دار الفكر الجامعي الإسكندرية 2005 .

هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية القاهرة ، طبعة 1992 .

هشام محمد فريد رستم ، قانون العقوبات و المخاطر التقنية للمعلومات ، المكتبة الحديثة 1992 .

هلالي عبد الله أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، دار النهضة العربية ، طبعة 1997 .

هلالي عبد الله أحمد ، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست ، دار النهضة العربية القاهرة 2003 .

هلالي عبد الله أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، دار النهضة العربية 2006 .

2 - مجلات و نشرات

المجلة القضائية ، العدد 1 سنة 2002 ، دراسة لنصرون وردية بعنوان الغش المعلوماتي .

نشرة القضاة ، دراسة للأستاذ مختار الأخضري مدير الشؤون الجزائية و إجراءات العفو وزارة العدل بعنوان الإطار القانوني لمواجهة جرائم المعلوماتية و جرائم الفضاء الإفتراضي ، العدد 66 لسنة 2011 .

3 – المذكرات و البحوث و العلمية

آمال قارة مذكرة ماجستير بعنوان الجريمة المعلوماتية ، كلية الحقوق جامعة الجزائر 2001 .

سي الحاج أحمد مدير التكوين بوزارة العدل ، محاضرة بعنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعطياة ، ملقاة على قضاة التكوين التخصصي في قانون الأعمال الدفعة السابعة 2008 .

صالح أحمد البربري بحث بعنوان دور الشرطة في مكافحة جرائم الإنترنيت في إطار الإتفاقية الأوروبية الموقعة في بودابست في 2001/11/23 ص 4 و 5 مأخوذ من الموقع الإلكتروني WWW .ARABLAWINFO.COM

عبد الله حسين علي محمود بحث بعنوان إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات مأخوذ من الموقع الإلكتروني WWW .ARABLAWINFO.COM

علاء الدين محمد شحاتة ، رؤية أمنية للجرائم الناشئة عن إستخدام الحاسب الآلي ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة 2005 .

علي محمود علي حمودة بحث بعنوان الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي مأخوذ من الموقع الإلكترونيWWW .ARABLAWINFO.COM .

فشار عطا الله ، بحث مقدم إلى الملتقى المغاربي حول القانون و المعلوماتية عقد بأكاديمية الدراسات العليا بليبيا أكتوبر 2009 ، مؤخوذ من الموقع الإلكتروني WWW .ARABLAWINFO.COM .

محمد أبو العلا عقيدة ، مقال حول التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية القانون ، الصفحة 12 ، مؤخوذ من الموقع الإلكتروني ، الدليل الإلكتروني للقانون العربيWWW .ARABLAWINFO.COM

محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات و الكمبيوتر ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة .

ممدوح عبد الحميد عبد المطلب بحث بعنوان جرائم إستخدام شبكة المعلومات العالمية (الجريمة عبر الأنترنيت من منظور أمني) ، مأخوذ من الموقع الإلكتروني WWW .ARABLAWINFO.COM .

وليد عاكوم بحث بعنوان التحقيق في جرائم الحاسوب مأخوذ من الموقع الإلكتروني .WWW .ARABLAWINFO.COM

يوسف عرب ، جرائم الكمبيوتر و الإنترنيت ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 تنظيم المركز العربي للدراسات و البحوث الجنائية أبوظبي .

النصوص التشريعية

المرسوم الرئاسي رقم 96-438 المؤرخ 1997/12/07 المتضمن الدستور المعدل و المتمم بموجب القانون 02-03 المؤرخ 2002/04/10 و القانون 19-08 المؤرخ 2008/11/15 .

الأمر رقم 155/66 المؤرخ في 18 صفر عام 1386 هـ الموافق لـ 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري المعدل و المتمم .

الأمر رقم 156/66 المؤرخ في 18 صفر عام 1386 هـ الموافق لـ 08 يونيو 1966 المتضمن قانون العقوبات الجزائري المعدل و المتمم

المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق

القانون 04/09 المؤرخ في 2009/08/50 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال

الفهرس :

المقدمة.....01

الفصل التمهيدي : الأحكام العامة لأنظمة المعالجة الآلية للمعطيات 06

المبحث الأول : ماهية نظام المعالجة الآلية للمعطيات 07

المطلب الأول : تمييز الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات عن باقي الجرائم المعلوماتية 07

أولا : تعريف الجريمة المعلومات..... 07

ثانيا : تصنيف الجرائم المعلوماتية 10

1- تصنيف الجرائم المعلوماتية في ظل إتفاقية بودابست 10

2 - التصنيف الأمريكي للجرائم المعلوماتية..... 12

3 - تصنيف قانون العقوبات الفرنسي للجرائم المعلوماتية 14

4 - تصنيف الفقه للجرائم المعلوماتية 14

المطلب الثاني : مفهوم نظام المعالجة الآلية للمعطيات 16

المطلب الثالث : ضرورة خضوع نظام المعالجة الآلية للمعطيات لحماية فنية 23

المبحث الثاني : خصائص الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات... 26

المطلب الأول : خصائص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات 26

المطلب الثاني : سيمات الجاني في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.....28

المطلب الثالث : أساليب إرتكاب الجريمة..... 32

أولا : الإعتداءات المنطقية 33

ثانيا : الإعتداءات المادية 37

المبحث الثالث : الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات 38
المطلب الأول : دوافع إرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... 38
أولا : الدوافع الشخصية 38
ثانيا : الدوافع الخارجية 39
المطلب الثاني : بواعث حماية أنظمة المعالجة الآلية للمعطيات 40
أولا : أهمية وجود نظام حماية 40
ثانيا : قصور الحماية الفنية لأنظمة المعالجة الآلية للمعطيات 41
ثالثا : بواعث إقتصادية..... 41
المطلب الثالث : وسائل الحماية الجزائية من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات..... 41
أولا : دور الحماية الجزائية..... 42
ثانيا :الحماية الجزائية على المستوى الدولي..... 43
ثالثا : الحماية الجزائية على المستوى الداخلي.....,..... 47

الفصل الاول : صور المساس بانظمة المعالجة الآلية للمعطيات.....49
المبحث الأول : جريمة الدخول أو البقاء الغير شرعى فى نظام المعالجة الألية البسيط.....51
المطلب الأول : الركن المادي للجريمة 51
أولا الدخول 51
ثانيا : البقاء.....54
المطلب الثاني : الركن المعنوي للجريمة 56
أولا : العلم.....57
ثانيا : الإرادة.....57
المبحث الثانى : جريمة الإتلاف الغير عمدي للمعطيات (الدخول أو البقاء المؤدي إلى الحذف أو التغيير أو التخريب).....59

المطلب الأول : الركن المادي للجريمة 59

أولا : السلوك الإجرامي 60

ثانيا : النتيجة.....60

ثالثا : العلاقة السببية.....60

المطلب الثاني : الركن المعنوي للجريمة 61

المبحث الثالث : جريمة المساس العمدي بالمعطيات (التلاعب بالمعطيات).....62

المطلب الأول : الركن المادي للجريمة 64

أولا : الإدخال 65

ثانيا : المحو 67

ثالثا : التعديل.....68

المطلب الثاني : الركن المعنوي للجريمة 69

المبحث الرابع : جريمة التعامل في المعطيات غير المشروعة 71

المطلب الأول : الركن المادي للجريمة 72

أولا : محل الجريمة 73

ثانيا : السلوك المجرم.....74

المطلب الثاني : الركن المعنوي للجريمة 76

الفصل الثاني : قمع الجرائم الماسة بانظمة المعالجة الآلية للمعطيات.....78

المبحث الأول : الإختصاص و التحري في هذه الجرائم 80

المطلب الأول : القانون الواجب التطبيق بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات 80

أولا : الجرائم المرتكبة في الإقليم الجزائري 81

ثانيا : الجرائم المرتكبة خارج الإقليم الجزائري من جزائريين 82

ثالثا : الجرائم الماسة بالمصالح الأساسية للدولة.....82
المطلب الثاني : الإختصاص القضائي 84
أولا : القاعدة العامة في الإختصاص.....85
ثانيا : تمديد الإختصاص 87
المطلب الثالث:التحري و التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.....89
أولا : الإختصاصات العادية 92
ثانيا : الإختصاصات الغير عادية.....101
ثالثا : الإجراءات التحفظية 106

المبحث الثاني : مسألة الإثبات في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.....107
المطلب الأول : خصوصية الدليل الإلكتروني.....108
أولا : عدم مرئية الدليل 108
ثانيا :إنعدام آثار الجريمة.....110
ثالثا : صعوبة إستخلاص الدليل 111
المطلب الثاني : إجراءات الحصول على الدليل الإلكتروني 113
أولا : الإستجواب.....113
ثانيا : الخبرة.....115
ثالثا : الشهادة.....116
المطلب الثالث :إشكالية قبول الدليل الإلكتروني و تقديره في ظل قانون الإجراءات الجزائية.....122

المبحث الثالث : الجزاءات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات
.....125

المطلب الأول : الجزاء المقرر للشخص الطبيعي.....125
أولا العقوبات الأصلية 125
ثانيا العقوبات التكميلية 126
ثالثا الظروف المشددة 128
المطلب الثاني : الجزاء المقرر للشخص المعنوي.....129
أولا العقوبات الأصلية 130
ثانيا العقوبات التكميلية 131
المطلب الثالث : الجزاء المقرر للإتفاق الجنائي و الشروع.....131
أولا : الجزاء المقرر للإتفاق الجنائي.....131
ثانيا : الجزاء المقرر للشروع في إرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات 134
الخاتمة.....136
قائمة المراجع 141
الفهرس 146
قائمة الملاحق 151
الملاحق .

قائمة الملاحق

الملحق الأول : الإتفاقية الدولية الخاصة بالإجرام السيبيري المبرمة ببودابست في 2001/11/23 مترجمة .

الملحق الثاني : القانون العربي الإسترشادي لمكافحة جرائم أنظمة المعلومات و ما في حكمها صادر عن جامعة الدول العربية .

الملحق الثالث : مشروع القانون الإتحادي في شأن مكافحة جرائم تقنية أنظمة المعلومات لسنة 2004 .

الملحق الرابع : مقرارات و توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 4-9 تشرين أول 1994 البرازيل ريودي جانيرو بشأن جرائم الكمبيوتر .

الملحق الخامس : القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال .

الملحق السادس : إحصائيات حول قضايا المساس بأنظمة المعالجة الآلية للمعطيات التي طرحت على المحاكم و عدد الأشخاص المتابعين إلى غاية 2010/04/30 (نشرة القضاة العدد 66 سنة 2011) .

الملحق السابع : القرار الصادر عن مؤتمر الأمم المتحدة الثمن لمنع الجريمة ، قرار بشأن الجرائم ذات الصلة بالكمبيوتر هافانا 1990 .

الملحق الثامن : حالات عملية شهيرة من واقع الملفات القضائية .

الملحق التاسع : حكم فاصل في قضية طاتي صادر عن محكمة باريس بتاريخ 2002/10/30 .

الملاحق

الملحق الأول

الاتفاقية الخاصة بالإجرام السيبيري بودابست 2001/11/23

تمهيد

إن الدول الأعضاء بالمجلس الأوروبي و غيرها من الدول الأخرى الموقعة على هذه الإتفاقية الخاصة بالإجرام السيبيري؛

- اهتماما من جانبها بأن المجلس الأوروبي هدفه تحقيق الوحدة الكبرى بين أعضائه؛
- و اعترافا منها بقيمة رعاية التعاون مع الدول الأخرى أطراف هذه الاتفاقية؛
- و اقتناعا منها بضرورة الحاجة لإتباع سياسة جنائية مشتركة تهدف، في المقام الأول، إلى حماية المجتمع من الإجرام السيبيري و ذلك من خلال إقرار التشريع الملائم و رعاية التعاون الدولي و دعمه،
- و إدراكا منها بعمق التغيير التي أحدثتها عمليات الترقيم والتقارب و استمرار عولمة شبكات الكومبيوتر؛
- و انشغالا من جانبها بالمخاطر الخاصة باحتمال استخدام شبكات الكومبيوتر و المعلومات الالكترونية أيضا في ارتكاب جرائم يعاقب عليها القانون و احتمال تخزين الأدلة المتعلقة بمثل هذه الجرائم و نقلها عبر هذه الشبكات؛
- و اعترافا منها بضرورة الحاجة إلى التعاون بين الدول و الصناعة الخاصة في مكافحة الإجرام السيبيري و ضرورة حماية المصالح الشرعية خلال عملتي الاستخدام و التطوير لتكنولوجيا المعلومات في شتى صورتها؛
- و إيمانا منها بأن المكافحة الفعالة للإجرام السيبيري تستلزم زيادة، و سرعة، و تفعيل التعاون الدولي في الأمور الجنائية تفعيلا جيدا؛
- و اقتناعا من جانبها بأن الاتفاقية الحالية أمرا حتميا و ضرورية لردع الأعمال الموجهة ضد سرية منظومات الكومبيوتر، و الشبكات، و بيانات الكومبيوتر،و تكاملها و سلامتها، و توافرها، و كذلك أيضا ضد إساءة استخدام مثل هذه المنظومات، و البيانات عن طريق إصدار النصوص القانونية بتأثيم مثل هذا السلوك كما هو مبين بهذه الاتفاقية، و إقرار السلطات المختصة بمكافحة مثل هذه الجرائم بفعالية من خلال تسهيل كشفها، و التحقيق و البحث فيها، و الفصل فيها قضائيا على الصعيدين المحلي الداخلي... و الدولي، وكذلك عن طريق توفير الإجراءات الخاصة بسرعة تحقيق التعاون الدولي و مصداقيته؛
- و حرصا من جانبها على ضرورة ضمان وجود توازن ملائم بين مصالح تنفيذ القانون و احترام حقوق الإنسان الأساسية كما هو منصوص عليه باتفاقية المجلس الأوروبي لعام 1950 الخاصة بحماية حقوق الإنسان و الحريات الأساسية، فإن الاتفاقية الدولية للأمم المتحدة لعام 1966 الخاصة بالحقوق المدنية والسياسية و المعاهدات الدولية لحقوق الإنسان التي يتم تطبيقها و العمل بها تؤكد على حرية الفرد في التعبير عن رأيه دون أي تدخل من أحد، و كذلك أيضا الحق في حرية التعبير بما في ذلك حرية البحث، و التلقي، و إفشاء المعلومات و الأفكار في شتى المجالات، بغض النظر عن الحدود و الحقوق المتعلقة باحترام الخصوصية،
- و حرصا من جانبها أيضا على حق حماية البيانات و المعلومات الشخصية، مثلما تم التباحث و التشاور بشأن ذلك، مثلا، بموجب اتفاقية المجلس الأوروبي لعام 1981 الخاصة بحماية الفرد بالنسبة للمعالجة الآلية للبيانات الشخصية للفرد؛
- و اهتماما من جانبها باتفاقية الأمم المتحدة لعام 1989 الخاصة بحقوق الطفل و اتفاقية منظمة العمل الدولية لعام 1999 الخاصة بأسوأ الصور لعمل الأطفال؛

- و أخذا على عاتقها، فإن اتفاقيات المجلس الأوروبي الحالية و الخاصة بالتعاون في المجال الجنائي، و كذلك أيضا المعاهدات المماثلة الموجودة بين الدول الأعضاء بالمجلس الأوروبي و الدول الأخرى، و تركيزا من جانبها على أن الاتفاقية الحالية الغرض منها استكمال تلك الاتفاقيات لإجراء عمليات البحث الجنائي و الإجراءات الجنائية المتعلقة بالجرائم الخاصة بمنظومات و بيانات الكومبيوتر و جعلها أكثر فعالية حتى يمكن تجميع الأدلة للجريمة في شكل الكتروني؛
- و ترحيبا من جانبها بعمليات التطوير الحالية التي تدفع بالتفاهم و التعاون الدوليين إلى المزيد من التقدم في مكافحة الإجرام السيبيري، بما في ذلك الإجراءات التي تتخذها الأمم المتحدة، و منظمة التعاون الاقتصادي و التنمية، و الاتحاد الأوروبي، و مجموعة الدول الصناعية الثمانية؛
- و إحياء لتوصيات لجنة الوزراء لرقم R (85)10 الخاصة بالتطبيق العملي للاتفاقية الأوروبية بشأن تبادل المساعدات في الشن الجنائية فيما يتعلق بالإدانة القضائية الخاصة باعتراض الاتصالات السلكية و اللاسلكية، و رقم R (88) 2، الخاصة بالسرقة و انتحال مؤلفات الآخرين أو اختراعاتهم أو أفكارهم (السرقة الأدبية) و استخدامها بدون ترخيص في مجال حق النشر و الطبع وحقوق الجيرة، و رقم R (87) 15 التي تنص على الاستعانة بالبيانات الشخصية في قطاع الشرطة، و رقم R (95) 4 الخاصة بحماية البيانات الشخصية في مجال الخدمات المتعلقة بالاتصالات السلكية و اللاسلكية، و تشير بصفة خاصة للخدمات التلفونية، و كذلك أيضا رقم R (89) 9 الخاصة بتوفيـــر و تقديم الإرشادات للهيئات التشريعية الوطنية فيما يتعلق بتعريف جرائم معينة تتعلق بالكومبيوتـــر، و رقم R (95) 13 الخاصة بالمشكلات المتعلقة بقانون الإجراءات الجنائية و التي لها علاقة بتكنولوجيا المعلومات.
- عقب النظر في القرار رقم 1 الذي أقره وزراء العدل الأوروبيين في مؤتمرهم في مؤتمرهم الواحد و العشرين (ببراغ- في 10-11 يونيو 1997) ، و الذي أوصى بقيام لجنة الوزراء بدعم العمل الخاص بالإجرام السيبيري و الذي تتولى اللجنة الأوروبية القيام به و تنفيذه فيما يتعلق بالمشكلات الخاصة بالجريمة و ذلك لجعل نصوص القوانين الجنائية المحلية أكثر قربا من بعضها البعض و التمكن من استخدام الوسائل الفعالة للتحقيق و البحث في مثل هذه الجرائم و كذلك أيضا بالنسبة للقرار رقم 3 الذي تم إقراره و التصديق عليه بالمؤتمر الثاني لوزراء العدل الأوروبيين (بلندن، يومي 8-9 يونيو 2000)، و الذي شجع أطراف المفاوضات على متابعة جهودها بغرض إيجاد الحلول الملائمة حتى يتمكن أكبر عدد ممكن من الدول أن يصبح أطرافا في الاتفاقية، و أقر بضرورة الحاجة إلى منظومة تعون دولي تتسم بالمرونة و الفعالية و تأخذ على عاتقها على النحو الملائم النصوص المحددة الخاصة بمكافحة الإجرام السيبيري.
- و عقب النظر أيضا لخطة العمل التي أقرها رؤساء دول و حكومات الدول الأعضاء بالمجلس الأوروبي بمناسبة عقد القمة الثانية لهم (في استراسبورج، يومي 10-11 أكتوبر 1997)لإيجاد حلول و ردود متشتركة لتطوير تكنولوجيا المعلومات الحديثة في شتى صورها وفقا للمعايير و القيم الخاصة بالمجلس الأوروبي ،
- فقد تم الاتفاق من جانبهم على ما يلـــــــــي:

الفصل الأول

مادة 1- تعاريف خاصة بأغراض هذه الاتفاقيـــــــــــــة

أ- يقصد " بمنظومة الكومبيوتر " أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو التي ذات صلة بذلك، و يقوم أحدها أو أكثر من واحد منها، تبعا للبرنامج، بعمل معالجة آلية للبيانات.

ب- يقصد " ببيانات الكومبيوتر " أية عمليات عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكومبيوتر، بما في ذلك البرنامج المناسب لجعل منظومة الكومبيوتر تؤدي وظائفها.

ج- يقصد "بجهاز الخدمـــة"

1- أي كيان عام أو خاص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال بواسطة منظومة الكمبيوتر،

2- أي كيان آخر يقوم بمعالجة أو تخزين بيانات الكومبيوتر نيابة عن خدمة الاتصالات أو مستخدمي مثل هذه الخدمة.

د- "خط سير البيانات" ، و يقصد بها البيانات المتعلقة بالاتصال عن طريق منظومة الكومبيوتر و التي تنتجها منظومة الكومبيوتر، و قد تقوم بتشكيل جزء في حلقة أو سلسلة اتصالات، توضح مصدر الاتصالات، و الوجهة المرسلة إليها، و الطريق الذي تسلكه، ووقت و تاريخ، وحجم، و مدة، و نوع الخدمة الأساسية.

الفصل الثاني:الإجراءات الواجب اتخاذها على الصعيد الوطني:

القسم الأول- القانون الجنائي الأساسي:

الباب الأول- الجرائم التي تمس سرية، و أمن و سلامة و توافر ببيانات الكومبيوتر و منظوماته.

مادة 2- الدخول الغير مشروع

تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا قانونيا أو تشريعيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، عند ارتكابها عن قصد، و ذلك من حيث الدخول على منظومة الكومبيوتر كليا أو على أي جزء منها دون وجه حق، و قد يلزم على الدولة الطرف بالاتفاقية إدراك أن الجريمة ترتكب عن طريق مخالفة الإجراءات الأمنية، بقصد الحصول على بيانات الكومبيوتر أو بقصد آخر غير شريف، أو فيما يتعلق بمنظومة الكومبيوتر المتصلة بمنظومة كومبيوتر أخرى.

مادة 3- الاعتراض الغير مشروع

يقوم كل طرف من الدول الأطراف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا قانونيا أو تشريعيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، عند ارتكابها عن قصد، و ذلك من حيث اعتراض خط سير البيانات دون وجه حق، و يتم ذلك باستخدام الوسائل الفنية، لقطع عمليات البث و الإرسال الغير عمومية لبيانات الكومبيوتر إلى- أو من، أو داخل- منظومة الكومبيوتر، بما في ذلك ما ينبعث من منظومة الكومبيوتر من موجات كهرومغناطيسية تحمل معها هذه البيانات. و قد يلزم على طرف الاتفاقية إدراك أن الجريمة ترتكب بقصد غير شريف، أو فيما يتعلق بمنظومة الكومبيوتر المتصلة بمنظومة كومبيوتر أخرى.

مادة 4- التدخل في البيانات:

1 - تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا لإصدار نصا قانونيا أو تشريعيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، عند ارتكابها عن قصد، و ذلك من حيث إتلاف، أو إلغاء، أو إفساد، أو تغيير، أو تدمير البيانات الموجودة بالكومبيوتر دون وجه حق.

2- يمكن لأي طرف من أطراف الاتفاقية الاحتفاظ بالحف في المطالبة بأن السلوك الموضح بالفقرة 1 قد ينتج عنه أضرارا فادحة و جسيمة.

مادة 5- التدخل الغير مشروع في المنظومة:

تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها عند ارتكابها عن قصد، و ذلك من حيث الإعاقة الخطيرة، دون وجه حق، لعمل منظومة الكومبيوتر عن طريق تزويد جهاز الكومبيوتر ببرامج و معلومات و إرسالها أو بثها، أو إتلاف، أو إفساد، أو تبديل، أو تدمير البيانات الموجودة بالكومبيوتر.

مادة 6- إساءة استخدام الأجهزة:

1- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها عند ارتكابها عن قصد، دون وجه حق و ذلك من حيث:

أ) الإنتاج، أو البيع، و الحصول بغرض الاستخدام، أو الجلب أو بالأحرى توفيـــــــــــــــــــــــــر:

*1-*جهاز يشمل برنامج كومبيوتر، يتم تصميمه أو تطويعه أساسا بغرض ارتكاب أية من الجرائم التي ورد نصا بشأنها في المواد من 2-5.

2- كلمة السر الخاصة بالكومبيوتر، أو الكود الشفري للدخول، أو بيانات مماثلة يمكن من خلالها القدرة على الدخول على منظومة الكومبيوتر بأكملها أو على أي جزء منها، و ذلك بقصد استخدام الجهاز في الأغراض الخاصة بارتكاب أية من الجرائم الواردة بالمواد من 2-5 .

ب) حيازة إحدى القطع المشار إليها بالفقرة أ (1) أو (2) بعاليه بقصد استخدامه في الأغراض الخاصة بارتكاب أية من الجرائم التي وردت بالمواد من 2-5 و يجوز لإحدى الدول الأطراف بالاتفاقية المطالبة قانونا بحيازة عدد من هذه القطع أو الأشياء قبل الوقوع تحت طائلة المسائلة الجنائية.

*2-*لن يتم تفسير هذه المادة على أنها توقع عقوبة المسائلة الجنائية في حالة الإنتاج، أو البيع أو الحصول بغرض الاستخدام، أو الجلب، أو التوزيع، أو بالأحرى التوفير، أو الحيازة المنوه عنها بالفقرة 1 من هذه المادة ليس لغرض ارتكاب جريمة من الجرائم المنصوص عليها وفقا للمواد من 2-5 من هذه الاتفاقية بقدر ما هو الحال بالنسبة لحق التفويض قانونا بتجربة أو اختبار منظومة الكمبيوتر أو حمايتها.

3- يجوز لكل دولة طرف بالاتفاقية الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشرط ألا يكون هذا التحفظ متعلقا بعمليات بيع، أو توزيع، أو بالأحرى توفير هذه القطع أو الأجزاء أو الأشياء المشار إليها بالفقرتين (أ)، (2) من هذه المادة.

الباب الثاني: الجرائم المتعلقة بالكومبيوتر

مادة 7- جريمة التزوير المتعلقة بالكومبيوتر:

تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، عند ارتكابها عن قصد ، و بدون وجه حق، و ذلك من حيث تزويد الكومبيوتر ببرامج خاصة بمعلومات و بيانات، أو تبديل أو تغيير، أو إلغاء، أو تدمير المعلومات و البيانات الخاصة بالكومبيوتر مما ينتج عنه وجود معلومات و بيانات غير صحيحة بقصد دراستها أو الاهتمام بها أو العمل بها لأغراض قانونية كما لو كانت صحيحة، بغض النظر عما إذا كانت هذه البرامج و البيانات أو المعلومات مقرؤه و مفهومة وواضحة بشكل مباشر من عدمه، و يجوز للدولة الطرف بالاتفاقية أن تشترط وجود نية التدليس، أو وجود قصد مماثل غير شريف، و ذلك قبل البدء في اتخاذ الإجراءات الخاصة بالمسائلة الجنائية.

مادة 8- جريمة التدليس المتعلقة بالكومبيوتر

تقوم كل دولة طرف بالاتفاقية إقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها عند ارتكابها عن قصد، و بدون وجه حق، و ذلك من حيث إحداث خسائر بممتلكات الغير عن طريق:

أ- أية عمليات إدخال برامج تشغيل على الكومبيوتر أو تزويده بمعلومات أو بيانات، أو تبديلها أو تغييرها، أو إلغائها أو تدميرها.

ب- أي نوع من التدخل في طبيعة عمل منظومة الكومبيوتر، بقصد يشوبه التدليس و عدم الأمانة أو بقصد غير شريف للحصول و بدون وجه حق، على منفعة أو فائدة إلكترونية لصالح الشخص ذاته أو لصالح الغير.

الباب الثالث: الجرائم المتعلقة بالرغبة الإشباعية

مادة 9- الجرائم المتعلقة بالأعمال الإباحية و صور الأطفال الفاضحة

*1-*تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها عند ارتكابها عن قصد، و بدون وجه حق من حيث ممارسة السلوكيات التالية:

*أ-*إنتاج صور الأطفال الفاضحة بغرض توزيعها عبر منظومة الكومبيوتر.

*ب-*عرض أو توفير صور الأطفال الفاضحة عبر منظومة الكومبيوتر.

ج-توزيع أو بث صور الأطفال الفاضحة عبر منظومة الكومبيوتر.

*د-*الحصول على صور الأطفال الفاضحة عبر منظومة الكومبيوتر لصالح الشخص ذاته أو لصالح الغير.

*ه-*اقتناء صور الأطفال الفاضحة داخل منظومة الكومبيوتر أو بحجرة تخزين بيانات الكومبيوتر.

2- بالنسبة للغرض من الفقرة 1 بعاليه، تشمل العبارة " صور الأطفال الفاضحة" على المواد الفاضحة التي توضح بالتصوير المرئي:

*أ-*أحد القصر منشغلا بارتكاب فعل أو سلوك جنسي واضح.

*ب-*شخص يبدو واضحا أنه قاصر منشغلا بارتكاب فعل أو سلوك جنسي واضح.

*ج-*صور واقعية و حقيقية تبين وجود أحد القصر منشغلا بارتكاب فعل أو سلوك جنسي واضح.

3- بالنسبة للغرض من الفقرة 2 بعاليه، فإن اصطلاح "قاصر" يشمل جميع من هم دون الثامنة عشر، إلا أنه يجوز لأية دولة طرف بالاتفاقية أن تشترط حدا عمريا أو سنيا أقل، بما لا يقل عن السادسة عشرة.

4- يجوز لكل دولة طرف بالاتفاقية أن تحتفظ بالحق في عدم تطبيق الفقرتين الفرعيتين "د، ، "ه" من الفقرة 1 و الفقرتين الفرعيتين "ب"، "ج" من الفقرة "2" كليا أو جزئيا.

الباب الرابع: الجرائم المتعلقة بالانتهاكات الخاصة بحقوق الطبع و النشر و الحقوق المتعلقة بها

مادة 10- الجرائم المتعلقة بالانتهاكات الخاصة بحقوق الطبع و النشر و الحقوق المتعلقة بها

1- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، و ذلك من حيث مخالفة أو انتهاك حقوق الطبع و النشر، كما هو محددا وفقا للقانون الخاص بهذه الدولة الطرف بالاتفاقية، وفقا للالتزامات التي قد تتعهد بها بموجب وثيقة باريس الصادرة في 24 يوليو 1971 التي تثقل و تؤكد اتفاقية **برن الخاصة بحماية الأعمال** الأدبية و الفنية، و الاتفاقية الخاصة بالنواحي التجارية لحقوق الملكية الفكرية، و معاهدة المنظمة العالمية للملكية الفكرية الخاصة بحقوق الطبع و النشر باستثناء أية حقوق أدبية و أخلاقية تم التباحث و التشاور بشأنها

من خلال هذه الاتفاقيات، حيث أن مثل هذه الأفعال ترتكب طواعية و بمحض إرادة مرتكبيها، على الصعيد التجاري، و بواسطة منظومة كومبيوتر .

2- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها من حيث مخالفة أو انتهاك الحقوق المتعلقة بذلك؛ كما هو محدد بموجب القانون الخاص بتلك الدولة الطرف في الاتفاقية، ووفقا للالتزامات التي قد تتعهد بها بموجب الاتفاقية الدولية لحماية الممثلين و منتجي أجهزة الحاكي (الفونوغراف) و الهيئات الإذاعية (اتفاقية روما) و الاتفاقية الخاصة بالنواحي التجارية لحقوق الملكية الفكرية، و معاهدة المنظمة العالمية للملكية الفكرية الخاصة بالأعمال الإبداعية، و التمثيل، و أجهزة الحاكي (الفونوغراف)، باستثناء أية حقوق أدبية و أخلاقية تم التباحث و التشاور بشأنها من خلال تلك الاتفاقيات حيث أن مثل هذه الأفعال ترتكب طواعية و بمحض إرادة مرتكبيها و على الصعيد التجاري، و بواسطة منظومة كومبيوتر.

3- يجوز لكل دولة طرف بالاتفاقية الاحتفاظ بالحق في عدم توقيع المسائلة الجنائية بموجب الفقرتين 1، 2 من هذه المادة في ظروف محددة بشرط أن تتوافر الوسائل العلاجية الفعالة الأخرى، و ألا يخل هذا التحفظ بالالتزامات الدولية من قبل الدولة الطرف بالاتفاقية المعلنة بالاتفاقيات الدولية المشار إليها بالفقريتين 1 ، 2 من هذه المادة.

الباب الخامس: المسائلة القانونية و العقوبات الإضافية المساعدة

مادة 11- الشروع، و المساعدة، و التحريض

1- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، عند ارتكاب عن قصد، من حيث المساعدة، أو التحريض على ارتكاب أية جريمة من الجرائم المنصوص عليه وفقا للمواد من 2-10 الخاصة بالاتفاقية الحالية، و ذلك بقصد ارتكاب مثل هذه الجريمة.

2- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، عند ارتكاب عن قصد، و ذلك من حيث الشروع في ارتكاب أية جريمة من الجرائم المنصوص عليها وفقا للمواد من 3 و حتى 5، 7، 8، 9- 1 (أ)، (ب)، الخاصة بهذه الاتفاقية.

3- يجوز لكل دولة طرف بالاتفاقية الاحتفاظ بالحق في عدم تطبيق الفقرة 2- كليا أو جزء منها من هذه المادة.

مادة 12- المسائلة القانونية الاعتبارية (للشخص الاعتباري)

*1-*تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، و ذلك لضمان إمكانية وقوع رجال القانون تحت طائلة القانون بسبب جريمة منصوص عليها وفقا لهذه الاتفاقية، و التي يرتكبها أي شخص طبيعي من أجل منفعة أو استفادة خاصة بهم، و ذلك من حيث قيامه بفعل ذلك سواء بمفرده أو كونه أحد أفراد جماعة تابعة لرجال القانون، و الذي يتبوأ منصبا قياديا داخلها، و ذلك بموجب:

أ- سلطة تفويضية من الرجل أو المسئول القانوني؛

*ب-*تفويض قانوني باتخاذ القرارات نيابة عن الرجل أو المسئول القانوني؛

*ج-*سلطة قانونية في ممارسة السيطرة و التحكم من خلال هذا المسئول القانوني.

*2-*بالإضافة إلى الحالات التي سبق ورودها بالفقرة 1 من هذه المادة، تقوم كل دولة طرف بالاتفاقية باتخاذ الإجراءات الضرورية و اللازمة و ذلك لضمان إمكانية وقوع المسئول القانوني تحت طائلة القانون و ذلك في حالة عدم الكفاية أو الافتقار إلى عملية الإشراف أو السيطرة من قبل الشخص الطبيعي المشار إليه بالفقرة 1 مما يتسبب ذلك عن

إمكانية ارتكاب جريمة منصوص عليها وفقا لهذه الاتفاقية و ذلك لصالح رجل القانون عن طريق شخصا طبيعيا يعمل بموجب تفويض أو سلطة قانونية منه.

3-طبقا للمبادئ و الأسس القانونية الخاصة بالدولة الطرف بالاتفاقية، فإنه يجوز أن تكون المسائلة القانونية لرجل القانون أو للمسئول القانوني جنائية، أو مدنية أو إدارية.

4-تتم هذه المسائلة القانونية دون المساس بالمسائلة الجنائية للأشخاص الطبيعيين الذين يرتكبون الجريمة.

مادة 13- العقوبات و الإجراءات

1- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، و ذلك لضمان أن الجرائم المنصوص عليها وفقا للمواد من 2-11 يعاقب عليها القانون بموجب عقوبات فعالة، و متناسبة، و داعية للعدول، و التي تشمل الحرمان من الحرية.

2- تضمن كل دولة طرف بالاتفاقية أن رجال القانون الذين يقعون تحت طائلة القانون وفقا للمادة 12 يخضعون لعقوبات أو إجراءات فعالة، و متناسبة، و داعية للعدول، سواء كانت عقوبات أو إجراءات جنائية أو غير جنائية، بما في ذلك العقوبات المالية.

القسم الثاني : قانون الإجـــــراءات

الباب الأول: النصوص القانونية العمومية

مادة 14- مفهوم النصوص الإجرائية

1- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نصا تشريعيا أو قانونيا بحق التفويض أو الصلاحيات و الإجراءات الواردة بهذا الباب و ذلك للأغراض الخاصة بعمليات البحث الجنائي أو الإجراءات الجنائية تحديدا.

2- فيما عدا بالنسبة لما ورد بالأحرى على وجه التحديد بالمادة 21ن تقوم كل دولة طرف بالاتفاقية بتطبيق حق التفويض أو الصلاحيات و الإجراءات المشار إليها بالفقرة (1) من هذه المادة على:

أ-الجرائم المنصوص عليها وفقا للمواد من 2- 11 الواردة بهذه الاتفاقية؛

ب-الجرائم الأخرى التي يتم ارتكابها بواسطة منظومة الكومبيوتر؛

ج-تجميع الأدلة الخاصة بالجريمة في صورة إلكترونية.

3- *أ*-يجوز لكل دولة طرف بالاتفاقية الاحتفاظ بالحق في تطبيق الإجراءات المشار إليها بالمادة 20 على الجرائم أو قطاعات الجرائم أغلظ و أشد منه بالنسبة لمدى الجرائم التي تطبق عليها الإجراءات المشار إليها بالمادة 21.

و أن تنظر كل دولة طرف بالاتفاقية في أمر تفييد مثل هذا التحفظ حتى يمكن تطبيق الإجراء المشار إليه بالمادة 20 على أوسع نطاق.

ب-في حالة تعذر الدولة الطرف بالاتفاقية، و بسبب القيود الموجودة في التشريعات الخاصة بها، و التي كانت تسري وقت التصديق على الاتفاقية الحالية و إقرارها، تطبيق الإجراءات المشار إليها بالمادتين 20، 21 على إرسال المراسلات داخل منظومة الكومبيوتر الخاصة بجهاز توفير الخدمات المعلوماتية و تقديمها، و التي منظومتها:

1- يجري تشغيلها لصالح مجموعة من مستخدميها محصورة العدد و على أضيق نطاق.

2- لا تستعين بشبكات اتصال عمومية و غير متصلة بأية منظومة كومبيوتر أخرى، سواء عامة أو خاصة.

فإنه يجوز لهذه الدولة الطرف بالاتفاقية الاحتفاظ بالحق في عدم تطبيق هذه الإجراءات على مثل هذه الاتصالات. و أن تقوم كل دولة طرف بالاتفاقية بدراسة تقييد مثل هذا التحفظ حتى يتمكن تطبيق الإجراءات المشار إليها بالمادتين20، 21على أوسع نطاق.

مادة 15- الشروط و الإجراءات الوقائية:

1-تضمن كل دولة طرف بالاتفاقية أن عمليات تأسيس، و تنفيذ و تطبيق الصلاحيات و حق التفويض قانونا و الإجراءات الواردة بهذا القسم تتبع الشروط و الإجراءات الوقائية الواردة بموجب القانون الوطني المحلي الخاص بالدولة طرف الاتفاقية، و الذي يوفر الحماية الكافية لحقوق الإنسان و الحريات، بما في ذلك زيادة الالتزامات التي تعقب ذلك و التي قد تتعهد الدولة بها بموجب اتفاقية المجلس الأوروبي لعام 1950 الخاصة بحماية حقوق الإنسان و الحريات الأساسية، و الاتفاقية الدولية للأمم المتحدة لعام 1966 الخاصة بالحقوق المدنية و السياسية، و غيرها من الاتفاقيات الدولية الأخرى الخاصة بحقوق الإنسان التي يتم تطبيقها، و التي سوف تجسد المبدأ الأساسي للتناسبية.

2-تشمل هذه الشروط و الإجراءات الوقائية، كلما كان الأمر ملائما بالنسبة لطبيعة الإجراءات أو الصلاحيات أو التفويض بالسلطة المتعلقة بذلك، الإشراف القضائي المستقل و خلافه، أو الأسس التي تبرر تطبيق، و تحديد أو تقييد مجال و مدة تلك الصلاحية و حق التفويض بالسلطة أو الإجراء الخاص بذلك.

3-إلى حد التوافق و الصالح العام و خاصة الإدارة السليمة للعدالة، تقوم كل دولة طرف بالاتفاقية بدراسة تأثير النفوذ و السلطة و الإجراءات في هذا القسم على الحقوق، و المسئوليات، و المصالح المشروعة للأطراف الثالثة.

الباب الثاني: سرعة المحافظة على بيانات الكومبيوتر المخزونة

مادة 16- سرعة المحافظة على بيانات الكومبيوتر المخزونة

1-تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، حتى يمكن لسلطاتها المختصة طلب أو الحصول بالمثل على سرعة المحافظة على بيانات بعينها على الكومبيوتر، بما في ذلك خط سير البيانات التي يتم تخزينها بواسطة منظومة الكومبيوتر، و خاصة حالة وجود أسس للاعتقاد في إمكانية تعرض بيانات الكومبيوتر بصفة خاصة للضياع أو الفقدان أو التعديل.

2-في حالة قيام الدولة الطرف بالاتفاقية بتفعيل الفقرة 1 بعاليه بواسطة تقديم طلب إلى شخص للمحافظة على بيانات كومبيوتر بعينها تكون مخزونة بحوزة الشخص أو تحت سيطرته، فإن الدولة الطرف بالاتفاقية تقر هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا لإلزام ذلك الشخص بالمحافظة على وحدة و سلامة بيانات الكومبيوتر هذه لفترة زمنية طالما كان ذلك ضروريا، و لمدة لا يزيد عن تسعين يوما على الأكثر، حتى تتمكن السلطات المختصة من السعي لكشفها. و يجوز للدولة الطرف بالاتفاقية تقديم مثل هذا الطلب بالتالي لتجديدها.

3-تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإلزام الولي (المسئول) أو أي شخص آخر يحتفظ ببيانات الكومبيوتر بالمحافظة على سرية القيم بمثل هذه الإجراءات للفترة الزمنية المنصوص بها بموجب قانونها الوطني المحلي.

4-سوف تتبع السلطات أو الصلاحيات و الإجراءات المشار إليها بهذه المادة للمادتين 14، 15.

مادة 17- سرعة المحافظة على خط سير البيانات و الكشف الجزائي لها

1-تقوم كل دولة طرف بالاتفاقية، بالنسبة لخط سير البيانات المطلوب حفظها بموجب المادة 16 بإقرار تلك التشريعات و غيرها من الإجراءات الأخرى كلما كان ذلك ضروريا، و ذلك:

أ) لضمان توافر سرعة المحافظة على خط سير البيانات هذه بغض النظر عن مشاركة جهاز خدمة واحد أو أكثر في عملية إرسال هذا الاتصال أو المراسلات؛

ب) لضمان سرعة الكشف للسلطات المختصة بالدولة الطرف بالإتفاقية، أو للشخص الذي تعينه تلك السلطات، عن قدرا كافيا من خط سير البيانات حتى يمكن للدولة الطرف تحديد أجهزة الخدمة و الطريقة التي يتم إرسال الاتصال من خلالها.

2-تتبع السلطات أو الصلاحيات و الإجراءات المشار إليها بهذه المادة للمادتين 15، 15.

الباب الثالث: إصدار الأوامر

مادة 18- إصدار الأوامر

1- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، وذلك حتى تمنح سلطاتها المختصة السلطة و حق التفويض في توجيه الأوامر إلى:

أ-أحد الأشخاص على أراضيها لتقديم بيانات محددة على الكومبيوتر بحيازة ذلك الشخص أو تحت سيطرته، و مخزنة داخل منظومة كومبيوتر أو بداخل حجرة تخزين البيانات بالكومبيوتر.

ب-أحد أجهزة الخدمة لتقديم الخدمات الخاصة به بأراضي الدولة الطرف بالاتفاقية لتقديم معلومات أو بيانات خاصة بالمشترك صاحب الجهاز فيما يتعلق بتلك الخدمات الموجودة بحوزة أو تحت سيطرة جهاز تقديم الخدمة المعلوماتية هذا.

2-تتبع السلطات أو الصلاحيات و الإجراءات المشار إليها بهذه المادة للمادتين (14)، (15).

3-بالنسبة للغرض من هذه المادة، فإن اصطلاح "بيانات المشترك" يقصد به أية معلومات موجودة في صورة بيانات بالكومبيوتر أو أية صورة أخرى يتم حفظها بأحد أجهزة تقديم الخدمة المعلوماتية، و التي تتعلق بالمشتركين في الخدمات الخاصة به خلاف خط سير البيانات أو مضمونها و التي بموجبها يمكن التوصل إلى:

أ-نوعية خدمة الاتصال أو المراسلة المستخدمة، و الشروط الفنية التي يتم اتخاذها في ذلك، و الفترة الزمنية للخدمة،

ب- البيانات الشخصية للمشترك، و عنوانه البريدي أو الجغرافي، و رقم تليفونه و غير ذلك من أرقام الدخول الأخرى الخاصة به، و البيانات الخاصة بالفواتير و الدفع، و التي تكون متوافرة بموجب الاتفاق على الخدمة أو الترتيبات الخاصة بذلك.

ج- أية معلومات أخرى خاصة بموقع تركيب أجهزة و معدات الاتصالات، و التي تتوافر بموجب الاتفاق على الخدمة أو الترتيبات الخاصة بذلك.

الباب الرابع: البحث في، و مصادرة، بيانات الكومبيوتر المخزونة

مادة 19-البحث في، و مصادرة، بيانات الكومبيوتر المخزونة

1- تقوم كل دولة طرف بالاتفاقية بإقرار تلك الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كان ذلك ضروريا، و ذلك لمنح سلطاتها المختصة حق السلطة و الصلاحيات القانونية للبحث و الدخول علنا بالمثل على:

*أ)*منظومة الكومبيوتر أو جزء منها و بيانات الكومبيوتر المخزونة بها.

ب)غرفة تخزين بيانات الكومبيوتر و التي يجوز أن تكون بيانات الكومبيوتر مخزنة بها بأراضي

الدولة الطرف بالاتفاقية.

2- تقوم كل دولة طرف بالاتفاقية بإقرار تلك الإجراءا ر غيرها من الإجراءات الأخرى، كان ذلك ضروريا، و ذلك لضمان أنه في حالة قيام سلطاتها بعمليات ال ل بالمثل على منظومة كومبيوتر بعينها أو على جزء منها، وفقا للفقرة 1 -(أ) ، و لديها أسس للاعتقاد المطلوبة مخزنة بداخل منظومة كومبيوتر أخرى أو بداخل جزء منها على أراضيها، و أن هذه البيانا ول عليها قانونا من المنظومة الرئيسية أو متوافرة لها، فتصبح السلطات قادرة على توسيع عملية الب و نشاط أو الدخول بالمثل على المنظومة الأخرى.

3- تقوم كل دولة طرف بالاتفاقية بإقرار تلك الإجراء و غيرها من الإجراءات الأخرى، كان ذلك ضروريا، كي تمنح سلطاتها المختصة السلطة و حق التفويض أو حماية بيانات الكومبيوتر التي يتم الدخول عليها بالمثل و ذلك طبقا للفقرتين 1 و 2 و تشمل هذه الإجراء ض في:

*أ)*مصادرة أو حماية منظومة الكومبيوتر أو جزء منها أ ن بيانات الكومبيوتر و ذلك بطريقة مماثلة.

*ب)*إنشاء أو عمل نسخة بيانات الكومبيوتر هذه و يتم الا

*ج)*المحافظة على وحدة و سلامة بيانات الكومبيوتر المـ الصلة.

*د)*استخراج بيانات الكومبيوتر هذه التي لا يمكن الدخول هذه البيانات بداخل منظومة الكومبيوتر التي يتم الدخول عليها و معالجة هذه البيانا

*4-*تقوم كل دولة طرف بالاتفاقية بإقرار تلك الإجراءا و غيرها من الإجراءات الأخرى، كان ذلك ضروريا، و ذلك لمنح سلطاتها المختصة السلطة و حق التفو المر لي شخص لديه معلومات ودراية عن طبيعة عمل منظومة الكومبيوتر أو الإجراءات التي يتم تطبيق ت الكومبيوتر في هذا الخصوص، بتقديم، و بالقدر المعقول، المعلومات الضرورية حتى يمكن فهم الإجراء ها بالفقرتين 1، 2.

*5-*تتبع السلطات و الصلاحيات و الإجراءات المشار إلي للمادتين (14)، (15).

الباب الخامس: تجميع بيانات الكومبيوتر في الوقت الصحيح

مادة 20-تجميع بيانات الكومبيوتر في الوقت الصحيح

*1-*تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراء و غيرها من الإجراءات الأخرى كلما كان ذلك ضروريا، و ذلك لمنح سلطاتها المختصة السلطة و حق ا

*أ)*جمع أو تسجيل من خلال تطبيق الوسائل الفنية على رف بالاتفاقية؛

*ب)*التعاون مع و مساعدة السلطات المختصة في تجميع ط سير البيانات في الوقت الصحيح، بما يتفق و اتصالات بعينها على أراضيها رسالها بواسطة منظومة كومبيوتر.

*2-*في حالة تعذر قيام الدولة الطرف بالاتفاقية إقرا المشار إليها بالفقرة 1 (أ)، بسبب مبادئ المنظومة القانونية الوطنية الخاصة بها التي تم تشريها، فإ بدلا من ذلك إقرار الإجراءات التشريعية و غيرها من الإجراءات البيانات خلال خط الأخرى، كلما كان ، و ذلك لضمان جمع سيرها، و تسجيلها في الوقت الصحيح بما يتفق و اتصالات بعينها و التي يتم إرسال ها من خلال استخدام الوسائل الفنية الموجودة على أراضي تلك الدولة.

3- تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجرا و غيرها من الإجراءات الأخرى كلما كان ذلك ضروريا، و ذلك لإلزام أحد أجهزة تقديم الخدمة المـ افظة على سرية وقائع تنفيذ أية سلطات أو صلاحيات منصوص عليها في هذه المادة و عن أية معلوما

4-تتبع السلطة و الصلاحيات و الإجراءات المشار إليها بهذه المادة للمادتين 14، 15.

مادة 21- اعتراض مضمون البيانات

1-تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، فيما يتعلق بمعدل الجرائم الكبرى و الخطيرة المطلوب تحديدها من قبل القانون الوطني المحلي، و ذلك لمنح سلطاتها المختصة السلطة و حق التفويض لكي يتم:

أ)تجميع أو تسجيل من خلال تطبيق و استخدام الوسائل الفنية على أراضي تلك الدولة الطرف بالاتفاقية

*ب)*إلزام جهاز تقديم الخدمة المعلوماتية، من خلال السعة أو القدرة الفنية الخاصة به على:

1-تجميع أو تسجيل من خلال تطبيق و استخدام الوسائل الفنية على أراضي تلك الدولة الطرف بالاتفاقية .

2- التعاون مع و مساعدة السلطات المختصة في تجميع أو تسجيل، مضمون البيانات ، في الوقت الصحيح، التي تتعلق باتصالات بعينها على أراضيها و التي يتم إرسالها بواسطة منظومة كومبيوتر.

2-في حالة تعذر قيام الدولة الطرف بالاتفاقية بإقرار الإجراءات التشريعية المشار إليها بالفقرة 1-(أ) بسبب مبادئ المنظومة القانونية الوطنية الخاصة بها التي تم تشريعها، فإنه يجوز بدلا من ذلك إقرار الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا و ذلك لضمان تجميع مضمون البيانات و تسجيلها في الوقت الصحيح بالنسبة لاتصالات بعينها على أراضيها من خلال تطبيق و استخدام الوسائل الفنية على أراضي تلك الدولة.

3-تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، و ذلك لإلزام جهاز تقديم الخدمة المعلوماتية بالمحافظة على سرية وقائع تنفيذ أية سلطات أو صلاحيات منصوص عليها في هذه المادة و عن أية معلومات تتعلق بها.

4-تتبع السلطات و الصلاحيات و الإجراءات المشار إليها بهذه المادة للمادتين 14، 15.

الفصل الثالث: السلطة القضائيـــــــة

مادة 22- السلطة القضائيـــــة

تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار التشريع ليشمل أية جريمة منصوص عليها وفقا للمواد من 2-11 من هذه الاتفاقية عند ارتكاب جريمة:

أ- على أراضيـــــهـــــــــــــا أو،

ب- على متن إحدى السفن التي تحمل علم تلك الدولة الطرف بالاتفاقية، أو

ج- على متن إحدى الطائرات المسجلة بموجب قوانين تلك الدولة الطرف بالاتفاقية أو

د- بمعرفة أحد مواطنيها، إذا كانت الجريمة يعاقب عليها القانون بموجب القانون الجنائي في حالة ارتكابها، أو في حالة ارتكاب الجريمة خارج نطاق السلطة القضائية الإقليمية لأية دولة.

2- يجوز لكل دولة طرف بالاتفاقية الاحتفاظ بالحق في عدم التطبيق، أو التطبيق فقط في حالات أو ظروف معينة للوائح القضائية المعلنة بالفقرات من 1-(ب) و حتى 1-(د) من هذه المادة أو أي جزء منها.

3- تقوم الدولة الطرف في الاتفاقية بإقرار مثل هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا لإصدار التشريع ليشمل الجرائم المشار إليها بالمادة 24-فقرة 1، من هذه الاتفاقية، في حالات حيث يكون ذلك في وجود الشخص المزمع بأنه المتهم على أراضيها و لا تقوم بتسليمه لدولة أخرى طرفا بالاتفاقية، بناء على الجنسية فقط، بعد طلب التسليم.

4- لا يستثنى من هذه الاتفاقية أي تشريع جنائي تمارسه أحد الدول الأطراف بالاتفاقية وفقا لقانونها الوطني.

5- في حالة قيام أكثر من طرف من الدول ألأطراف بالاتفاقية بالمطالبة بتشريع قضائي فيما يعتقد بوجود جريمة منصوص عليها وفقا لهذه الاتفاقية، تقوم الدول الأطراف المعنية، متى كان ذلك مناسبا، بالتشاور بغرض تحديد التشريع القضائي الأكثر ملائمة للفصل فيها قضائيا.

الفصل الثالث:التعاون الدولي

القسم الأول: مبادئ العامة

الباب الأول: مبادئ عامة تتعلق بالتعاون الدولي

تتعاون الدول الأطراف بالاتفاقية مع بعضها البعض، وفقا لنصوص هذا الفصل، و من خلال تطبيق الاتفاقيات الدولية ذات الصفة و الخاصة بالتعاون الدون الدولي في الشؤون الجنائية، و الإجراءات المتفق عليها بمقتضى التشريع الخاص بالتماثل أو المتعلق بمبدأ المعاملة بالمثل، و القوانين الوطنية المحلية، لأقصى درجة ممكنة للأغراض الخاصة بعمليات التحقيق و البحث أو الإجراءات المتعلقة بالجرائم أو الخاصة بنظم و بيانات الكومبيوتر، أو لتجميع الأدلة الخاصة بالجريمة في صوره إلكترونية.

الباب الثاني: مبادئ تتعلق بعملية تسليم المجرمين

مادة 24- عملية تسليم المجرمين

1-/ -تطبق هذه المادة على عملية تسليم المجرمين فيما بين الدول الأطراف بالاتفاقية بالنسبة للجرائم المنصوص عليها وفقا للمواد من 2-11 بهذه الاتفاقية بشرط أن القانون بموجب القوانين، يعاقب عليها عن سنة واحدة الحرية لفترة لا تزيد بالدولتين المعنيتين طرفي الاتفاقية بالحرمان من على الأقل أو بعقوبة أشد.

ب-في حالة إذا ما تطلب الأمر تطبيق عقوبة مختلفة بدرجة أقل بموجب إجراء يتفق عليه وفقا للتشريع الخاص بالتماثل أو المتعلق بمبدأ المعاملة بالمثل أو بإحدى بتسليم المجرمين، بما في ذلك الاتفاقية الأوروبية الخاصة الاتفاقيات الخاصة التي تطبق فيما بين دولتين ETS 24 بتسليم المجرمين برقم المنصوص عليها بموجب هذه الاتفاقية الأقل طرفين أو أكثر، فتطبق العقوبة أو المعاهدة.

2- يرى إدراج الجرائم الموضحة بالفقرة1 م هذه المادة على أنها جرائم يتم فيها تسليم المجرمين بالنسبة لأية معاهدة لتسليم المجرمين توجد فيما بين الدول الأطراف. و تقوم الدول الأطراف بإدراج هذه الجرائم على أنها جرائم يتم فيه تسليم المجرمين بالنسبة لأية معاهدة لتسليم المجرمين يلزم إبرامها فيما بينها.

3- في حالة تلقي إحدى الدول الأطراف بالاتفاقية، و التي تجعل عملية تسليم المجرمين مشروطة بوجود معاهدة، طلبا للتسليم من دولة أخرى طرفا بالاتفاقية لا تربطها بها اتفاقية لتسليم المجرمين، فإنه يجوز لها دراسة هذه الاتفاقية باعتبارها السند القانوني لعملية التسليم فيما يتعلق بأية جريمة مشار إليها بالفقرة 1 من هذه المادة.

4- تعترف الدول الأطراف بالاتفاقية، التي تجعل عملية تسليم المجرمين مشروطة بوجود معاهدة، بالجرائم المشار إليها بالفقرة 1 من هذه المادة على أنها جرائم يمكن فيما تسليم المجرمين و تقر بذلك فيما بينها.

5- تخضع عملية تسليم المجرمين للشروط التي ينص عليها قانون الدولة المطلوب منها عملية التسليم أو بموجب المعاهدات الخاصة بتسليم المجرمين التي تطبق، بما في ذلك الأسس التي يجوز فيها للدولة الطرف بالاتفاقية و المطلوب منها عملية التسليم، أن ترفض القيام بعملية التسليم.

6- في حالة رفض عملية تسليم المجرمين في إحدى الجرائم المشار إليها بالفقرة 1 من هذه المادة و فقط بناء على جنسية الشخص المطلوب، أو نظرا لأن الدولة المطلوب منها عملية التسليم ترى أن لها تشريعا يشمل هذه الجريمة، تقوم الدولة المطلوب منها عملية التسليم ، بإحالة القضية، و بناء على طلب الدولة الطرف بالاتفاقية التي تطلب عملية التسليم، لسلطاتها المختصة بغرض الفصل فيه قضائيا ثم تقوم بعد ذلك بإبلاغ النتيجة النهائية للدولة الطرف بالاتفاقية الطالبة عملية التسليم في الوقت المناسب. و تتخذ هذه السلطات قرارها و إجراء عمليات التحقيق و اتخاذ الإجراءات الخاصة بها و بنفس الطريقة كما هو الحال بالنسبة لأية جريمة أخرى ذات طابع مشابه لها بموجب القانون الخاص بتلك الدولة الطرف بالاتفاقية.

7-أ- تقوم كل دولة طرف بالاتفاقية، في وقت التوقيع أو عند إيداع أصول التصديق، الخاصة بها أو قبولها، او موافقتها، أو انضمامها، بإخطار بالأمين العام للمجلس الأوروبي عن اسم، و عنوان كل جهة مسئولة عن إصدار أو تلقي طلبات التسليم أو أوامر الضبط التحفظي في حالة عدم وجود معاهدة.

ب-يقوم الأمين العام للمجلس الأوروبي بإنشاء و تحديث سجلا خاصا بالجهات المسئولة التي تخصصها الدول الأطراف بالاتفاقية. وتضمن كل دولة طرف بالاتفاقية أن التفصيلات التي يتم حفظها في هذا السجل صحيحة و موجودة طوال الوقت.

الباب الثالث: مبادئ عامة تتعلق بتبادل المساعدات

مادة 25- مبادئ عامة تتعلق بتبادل المساعدات

1- تقوم الدول الأطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض إلى أقصى حد ممكن و ذلك للأغراض الخاصة بعمليات التحقيق أو الإجراءات المتعلقة بالجرائم التي لها علاقة بنظم و بيانات الكومبيوتر، أو بالنسبة لتجميع الأدلة الخاصة بالجريمة في شكل إلكتروني.

2- تقوم أيضا كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية و غيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا و ذلك لتنفيذ الالتزامات المعلنة بالمواد من 27- 35.

3- يجوز لكل دولة طرف بالاتفاقية، في الظروف العاجلة، تقديم الطلبات الخاصة بتبادل المساعدات أو المراسلات و الاتصالات المتعلقة بذلك بوسائل الاتصال السريعة، بما في ذلك أجهزة الفاكس أو البريد الإلكتروني، إلى حد أن مثل هذه الوسائل توفر معايير و معدلات أمنية ملائمة و صحيحة تضفي نوعا من الموثوقية على البيانات (و قد يتضمن ذلك استخدام الشفرة عند الضرورة)، إلى جانب التأكيد الرسمي على المتابعة، عندما تطلب ذلك الدولة الطرف بالاتفاقية و المطلوب منها تقديم المساعدة. و تقبل الدولة الطرف بالاتفاقية و المطلوب منها تقديم المساعدة، و تستجيب للطلب بأية وسيلة وسائل الاتصال السريعة هذه.

4- ما عدا ما هو خلاف ذلك، و خاصة ما تنص عليه المواد في هذا الجزء، فسوف تخضع عملية تبادل المساعدات للشروط الواردة بالقانون الخاص بالدولة الطرف بالاتفاقية المطلوب منها تقديم المساعدة، أو بموجب المعاهدات الخاصة بتبادل المساعدات التي تطبق، بما في ذلك الأسس التي يجوز فيها لدولة الطرف بالاتفاقية و المطلوب منها تقديم المساعدة الحق في رفض تبادل المساعدات بالنسبة للجرائم المشار إليها بالمواد من 2-11 على أساس أن الطلب يتعلق فقط بجريمة تعتبرها جريمة مالية.

5- في حالة، ووفقا لنصوص هذا الفصل، السماح للدولة الطرف المطالب بتقديم مساعدة متبادلة مشروطة حال وجود جريمة مزدوجة، فإنه يرى استيفاء هذا الشرط، بغض النظر عما إذا كانت قوانينها تضع الجريمة داخل التصنيف ذاته للجريمة أم أنها تضع مسمى للجريمة بنفس الاصطلاح كما هو بالنسبة للطرف الطالب، إذا كان السلوك الذي يحدد الجريمة المطلوب تقديم المساعدة فيها يشكل جريمة بموجب قوانينها.

مادة 26- المعلومات التلقائية

1- يجوز للدولة الطرف بالاتفاقية، في حدود القانون الوطني الخاص بها، و دون طلب مسبق، إرسال معلومات لدولة أخرى طرف بالاتفاقية يتم الحصول عليها في إطار التحقيقات الخاصة بها في حالة إذا ما رأت أن الإفصاح عن هذه المعلومات قد يساعد الدولة الطرف بالاتفاقية التي تتلقى هذه المعلومات قد يساعد الدولة الطرف الطالب في بدء أو تنفيذ عمليات لتحقيق أو إجراءات تتعلق بجرائم منصوص عليه وفقا لهذه الاتفاقية، أو قد يؤدي إلى تقديم طلب للتعاون من قبل تلك الدولة الطرف بالاتفاقية بموجب هذا الفصل.

2- قبل تقديم هذه المعلومات، فإنه يجوز للدول الطرف بالاتفاقية و التي تقدم هذه المعلومات أن تطلب المحافظة على سرية هذه المعلومات استخدامها فقط وفقا لشروط. و في حالة عدم استجابة الدولة الطرف بالاتفاقية التي تقوم بتقديم المعلومات و التي ستحدد عندئذ ما إذا كان ينبغي مع ذلك تقديم هذه المعلومات. و في حالة قبول هذه المعلومات من قبل الدولة الطرف بالاتفاقية، التي تتلقى المعلومات لهذه المعلومات وفقا للشروط، فإنها تصبح ملزمة بها.

الباب الرابع: الإجراءات المتعلقة بالطلبات الخاصة بتبادل المساعدات في عدم وجود اتفاقية دولية قابلة ***للتطبيق***

مادة 27- الإجراءات المتعلقة بالطلبات الخاصة بتبادل المساعدات في عدم وجود اتفاقية دولية قابلة للتطبيق

1- في حالة عدم وجود أية معاهدة أو اتفاقية خاصة بتبادل المساعدات على أساس وجود تشريع مماثل أو يتعلق بمبدأ المعاملة بالمثل ساري المفعول ما بين دولتين طرفين بالاتفاقية الطالبة و المطالبة، فإنه يتم تطبيق نصوص الفقرات من 2-9 من هذه المادة. و لا تطبق نصوص هذه المادة في حالة وجود مثل هذه المعاهدة، أو الاتفاقية، أو التشريع، ما لم توافق الأطراف المعنية على تطبيق أي من أو كل البنود الباقية من هذه المادة بدلا منها.

2-أ- تقوم كل دولة طرف بالاتفاقية بتخصيص هيئة أو هيئات مركزية مسئولة عن الإرسال و الرد على الطلبات الخاصة بتبادل المساعدات أو تنفيذ هذه الطلبات أو إرسالها للجهات المختصة لتنفيذها؛

ب- تقوم الهيئات المركزية بالاتصال مباشرة ببعضها البعض؛

ج- تقوم كل دولة طرف بالاتفاقية، في وقت التوقيع، أو عند قيامها بإيداع أصول التصديق، الخاصة بها أو قبولها أو موافقتها، أو انضمامها، و دخولها إلى الاتفاقية، بإخطار الأمين العام للمجلس الأوروبي عن أسماء و عناوين الهيئات المخصصة لمتابعة هذه الفقرة؛

د- يتولى الأمين العام للمجلس الأوروبي إنشاء و تحديث سجلا خاصا بالهيئات المركزية التي تخصصها الدول الأطراف بالاتفاقية. و تضمن كل دولة طرف بالاتفاقية أن التفصيلات التي يتم حفظها في هذا السجل صحيحة و موجودة طوال الوقت.

3- يتم تنفيذ الطلبات الخاصة بتبادل المساعدات بموجب هذه المادة ووفقا للإجراءات التي تحددها الدولة الطالبة، ما عدا في حالة تعارض ذلك مع القانون الخاص بالدولة المطالبة.

4- يجوز للدولة المطالبة، إلى جانب الأسس الخاصة بالرفض الواردة بالمادة 25 (فقرة4)، أن ترفض تقديم المساعدة في حالة:

أ- إذا كان الطلب يتعلق بجريمة يعتبرها الطرف أو الدولة المطالبة جريمة سياسية أو جريمة لها علاقة بجريمة سياسية، أو

ب- إذا رأت أن تنفيذ الطلب من المرجح أن يمس سيادتها و استقلالها، أو أمنها، أو النظام العام بها، أو يضر بمصالحها الأساسية الأخرى.

5- يجوز للدولة الطرف بالاتفاقية و المطالبة تقديم المساعدة تأجيل الإجراءات الخاصة بالطلب إذا كانت مثل هذه الإجراءات قد تضر بالتحقيقات أو الإجراءات الجنائية التي تجريها سلطاتها.

6- تقوم الدولة المطلوب منها تقديم المساعدة، و قبل رفض أو تأجيل تقديم المساعدة ، و قبل رفض أو تأجيل تقديم المساعدة، إذا أن ذلك ملائما، و بعد التشاور مع الدولة الطالبة الطرف بالاتفاقية، بدراسة مدى إمكانية منح الطلب جزئيا أو طبقا لتلك الشروط التي تراها ضرورية.

7- تقوم الدولة المطالبة الطرف بالاتفاقية في وقت مبكر بإخطار نظيرتها الطالبة بنتيجة تنفيذ الطلب الخاص بالمساعدة. و أن يتم توضيح الأسباب بالنسبة لأي رفض أو تأجيل للطلب. كما تقوم الدولة المطالبة أيضا بإخطار نظيرتها الطالبة عن أية أسباب قد تؤدي إلى تعذر تنفيذ الطلب أو التي ترجح تأخيره إلى حد كبير.

8- يجوز للدولة الطالبة الطرف بالاتفاقية (التي تطلب المساعدة) أن تطلب من نظيرتها المطالبة (المطلوب منها تقديم المساعدة) المحافظة على سرية الوقائع الخاصة بأي طلب يتم تقديمه بموجب هذا الفصل و كذلك أيضا بالنسبة للموضوع الخاص به، فيما عدا بالنسبة للحد اللازم لتنفيذه. و في حالة – تعذر استجابة الدولة المطالبة الطرف بالاتفاقية (المطلوب منها تقديم المساعدة) للطلب الخاص بالسرية، فإنها تقوم في وقت مبكر بإخطار نظيرتها الطالبة (التي تطلب المساعدة)، و التي ستحدد بعد ذلك إذا ما كان بالرغم من ذلك يتم تنفيذ الطلب.

9-أ- في حالة حدوث طوارئ، فإنه يجوز للسلطات القضائية مباشرة بالدولة الطرف بالاتفاقية الطالبة (التي تطلب المساعدة)، إرسال الطلبات الخاصة بتبادل المساعدات أو المراسلات المتعلقة بذلك لنظيرتها بالدولة الطرف المطالبة بالاتفاقية (المطلوب منها تقديم تلك المساعدة). ففي أي من مثل هذه الحالات، يتم إرسال نسخة في نفس الوقت للهيئة المركزية بالدولة الطرف المطالبة (المطلوب منها تقديم تلك المساعدة) عن طريق نظيرتها الطالبة (التي تطلب المساعدة).

ب- يجوز تقديم أي طلب أو اتصال أو مراسلات بموجب هذه الفقرة عن طريق المنظمة الدولية للشرطة الجنائية – (انتربول).

ج- في حالة تقديم طلب وفقا للفقرة الفرعية (أ) من هذه المادة و عدم كفاءة الجهة في التعامل مع الطلب، فإنها تحيل الطلب للجهة الوطنية المختصة و إخطار الدولة الطالبة و الطرف بالاتفاقية مباشرة بأنها قامت بذلك.

د- يجوز للسلطات المختصة بالدولة الطالبة الطرف بالاتفاقية (التي تطلب المساعدة) القيام مبشرة بإرسال الطلبات أو المراسلات بموجب هذه الفقرة و التي لا تتضمن أية إجراء قسري إلى نظيرتها بالدولة المطالبة و الطرف بالاتفاقية (المطلوب منها تقديم المساعدة).

ه- يجوز لكل دولة طرف بالاتفاقية، وقت التوقيع أو عند إيداع أصول التصديق الخاصة بها ، أو بقبولها، أو موافقتها، أو انضمامها و دخولها في الاتفاقية، إخطار الأمين العام للمجلس الأوروبي بأن يتم، و لأسباب تتعلق بالفعالية، إرسال الطلبات بموجب هذه الفقرة إلى الهيئة المركزية التابعة لها .

مادة 28- السرية و القيود على عملية الاستخدام

1- في حالة عدم وجود معاهدة أو اتفاقية لتبادل المساعدات على أساس تشريع مماثل أو قائم على مبدأ المعاملة بالمثل و ساري المفعول فيما بين الدوليتين طرفي الاتفاقية، (الطالبة و المطالبة)، تطبق النصوص الخاصة بهذه المادة. و لا تطبق نصوص هذه المادة في حالة وجود مثل هذه المعاهدة أو الاتفاقية أو مثل هذا التشريع، ما لم توافق الدول الأطراف المعنية على تطبيق أي من أو كل الجزء الباقي من هذه المادة بدلا منها بشأن ذلك.

2- يجوز للدولة المطالبة (الطرف بالاتفاقية المطلوب منها تقديم المساعدة) أن تجعل عملية الدعم و المساعدة بالمعلومات أو الأدوات و اللوازم استجابة للطلب المقدم تتوقف على الشرطين التاليين:

أ- المحافظة على سريتها في حالة عدم الاستجابة للطلب الخاص بتبادل المساعدة في الأمور القانونية، في حالة عدم وجود مثل هذا الشرط.

ب- عدم استخدامها في تحقيقات أو الإجراءات بخلاف ما هو موضح بالطلب.

3- في حالة تعذر الدولة الطالبة(الطرف بالاتفاقية و التي تطلب المساعدة) على الاستجابة لأحد الشرطين المشار إليها بالفقرة الثانية، فإنها تقوم في وقت مبكر بإخطار الدولة الطرف الآخر، و التي ستحدد عندئذ إذا ما كان بالرغم من ذلك يتم تقديم المعلومات و في حالة قبول الدولة الطالبة (الطرف الذي يطلب المساعدة) لهذا الشرط، فإنها تصبح ملزمة به.

4- يجوز لأية دولة طرف بالاتفاقية تقديم مساعدة بمعلومات أو مستندات وفقا للشرط المشار إليه بالفقرة 2، إن تشترط على الطرف الآخر تقديم تفسير توضيحي، فيما يتعلق بهذا الشرط، و الاستخدام المعد بالنسبة لمثل هذه المعلومات أو المستندات

القسم الثاني: بنود محددة

الباب الأول: تبادل المساعدات بشأن الإجراءات التحفظية

مادة 29- سرعة المحافظة على بيانات الكومبيوتر المخزونة

1- يجوز لإحدى الدول الأطراف أن تطالب نظيرتها بطلب أو بالأحرى الحصول على سرعة المحافظة على البيانات التي يتم تخزينها بواسطة منظومة بكومبيوتر، و التي توجد داخل أراضي تلك الدولة الأخرى و التي تنوي الدولة الطالبة بصدد ذلك تقديم طلب خاص بتبادل المساعدات للبحث، أو الدخول بالمثل، أو المصادرة، أو الحماية بالمثل، أو الكشف عن البيانات.

2- يحدد طلب المحافظة الذي يتم تقديمه بموجب الفقرة 1 ما يلي:

أ- الجهة التي تطلب المحافظة ؛

ب- الجريمة موضوع التحقيق الجنائي أو الإجراءات الجنائية و ملخص موجز بالوقائع المتعلقة بها؛

ج- بيانات الكومبيوتر المخزونة و المطلوب المحافظة عليها و علاقتها بالجريمة؛

د- أية معلومات متوافرة تكشف عن شخصية صاحب (أو المسئول عن) بيانات الكومبيوتر التي يتم تخزينها، أو مكان وجود منظومة الكومبيوتر؛

ه- ضرورة المحافظة عليها؛

و- نية هذه الدولة الطرف بالاتفاقية في تقديم طلب تبادل المساعدة خاص بعمليات البحث، أو الدخول بالمثل، أو المصادرة، أو الحماية بالمثل، أو الكشف عن بيانات الكومبيوتر المخزونة،

3- عند ورود الطلب من دولة أخرى طرف بالاتفاقية، فتقوم الدولة المطالبة (المطلوب منها تقديم المساعدة) باتخاذ كافة الإجراءات الملائمة و ذلك لسرعة المحافظة على بيانات محددة بعينها وفقا للقانون الوطني المحلي الخاص بها. و بالنسبة للأغراض الخاصة بالاستجابة للطلب، فلا يلزم وجود ازدواجية في الجريمة كشرط لتوفير عنصر المحافظة هذا.

4- يجوز للدولة الطرف بالاتفاقية التي تشترط وجود جريمة مزدوجة كشرط للاستجابة للطلب الخاص بتبادل المساعدات الخاصة بالبحث أو الدخول بالمثل، أو المصادرة أو الحماية بالمثل الكشف عن البيانات المخزونة و الإفصاح عنها، بالنسبة للجرائم خلاف تلك المنصوص عليها وفقا للمواد 2-11 بهذه الاتفاقية، أن تحتفظ بالحق في رفض طلب الحفظ بموجب هذه المادة في الحالات التي تكون لها الحق فيها الاعتقاد بأنه في وقت عملية الكشف أو الإفصاح عن هذه المعلومات يتعذر استيفاء الشرط الخاص بوجود الجريمة المزدوجة.

5- بالإضافة إلى ذلك، فإنه يجوز فقط رفض طلب الحفظ إذا:

أ- كان الطلب يتعلق بجريمة ترى الدولة المطالبة (المطلوب منها تقديم المساعدة) أنها تشكل جريمة

سياسية أو جريمة لها علاقة بجريمة سياسية؛ أو.

ب- رأت الدولة المطالبة (المطلوب منها تقديم المساعدة) أن تنفيذ الطلب من المرجح أنه يمس سيادتها أو أمنها أو النظام العام فيها، أو الإضرار بمصالحها الأساسية الأخرى.

6- في حالة اعتقاد الدولة المطالبة الطرف بالاتفاقية (المطلوب منها تقديم المساعدة) بأن الحفظ لن يضمن توافر البيانات أو قد يهدد سرية، أو بالأحرى سلامة التحقيقات بالدولة الطالبة مستقبلا، إذن تقوم على الفور بإخطار الدولة الطالبة التي تحدد عندئذ إذا ما كان ينبغي على الرغم من ذلك تنفيذ الطلب.

7- إن أي حفظ يتم تفعيله ردا على الطلب المشار إليه بالفقرة 1 يجب أن يكون لفترة لا تقل عن ستين يوما حتى يمكن للدولة الطالبة الطرف بالاتفاقية تقديم طلب للبحث أو للدخول بالمثل، أو المصادرة، أو الحماية بالمثل، أو الكشف عن البيانات. و يعد تلقي هذا الطلب تضل البيانات مطلوب حفظها عليها تمهيدا لصدور قرار خاص بهذا الطلب.

مادة 30- سرعة الكشف عن خط سير البيانات المحفوظة

1- في حالة قيام الدولة المطالبة(الطرف بالاتفاقية المطلوب منها تقديم المساعدة) اكتشاف، من خلال تنفيذ الطلب المقدم وفقا للمادة 29 الخاصة بحفظ البيانات خلال خط سيرها بالنسبة لاتصال بعينه، إن جهاز تقديم الخدمة المعلوماتية للدولة الأخرى شارك في إرسال الاتصال، فتقوم الدولة المطالبة (المطلوب منها تقديم المساعدة) على وجه السرعة بالكشف عن القدر الكافي من البيانات خلال خط سيرها للدولة الطالبة، لتحديد ذلك الجهاز الخاص تقديم الخدمة المعلوماتية و الطريق التي تم إرسال هذا الاتصال من خلاله.

2- يجوز الامتناع فقط عن الكشف عن البيانات خلال خط سيرها بموجب الفقرة 1 إذا:

أ- كان الطلب يتعلق بجريمة ترى (الدولة المطالبة الطرف المطلوب منها تقديم المساعدة) أنها تشكل جريمة سياسية أو أنها جريمة ذات صلة بجريمة سياسية، أو

ب- رأت الدولة المطالبة (المطلوب منها تقديم المساعدة) أن تنفيذ الطلب من المرجح أن يمس سيادتها، أو أمنها و سلامتها، أو النظام العام فيها أو الأضرار بمصالحه الأساسية الأخرى.

الباب الثاني: تبادل المساعدات بشأن بالصلاحيات و التفويض في مجال التحقيقات

مادة 31- تبادل المساعدات المتعلقة بالدخول على بيانات الكومبيوتر المخزونة

1- يجوز للدولة الطرف بالاتفاقية أن تطلب من دولة أخرى طرف بالاتفاقية القيام بالبحث أو الدخول بالمثل، أو الصادرة أو الحماية بالمثل و الكشف عن البيانات المخزونة و ذلك بواسطة منظومة كومبيوتر توجد داخل أراضي الدولة المطالبة(المطلوب منها تقديم المساعدة)،بما في ذلك البيانات التي قد يتم حفظها وفقا للمادة .29

2- تستجيب الدولة المطالبة (المطلوب منها تقديم المساعدة)، للطلب من خلال تطبيق الأصول و الاتفاقيات و القوانين الدولية المشار إليها بالمادة 23، وفقا للنصوص القانونية الأخرى ذات الصلة و الخاصة بهذا الفصل.

3- يتم الاستجابة للطلب على وجه السرعة في حالة:

أ- وجود أسس للاعتقاد بأن البيانات ذات الصلة تصبح بصفة خاصة عرضه للضياع و الفقدان، أو عرضه للضياع و الفقدان، أو عرضة للتعديل أو التغيير.

ب- و بالأحرى تنص الاتفاقيات، و الأصول، و القوانين المشار إليها بالفقرة 2-الإسراع بالتعاون.

مادة 32- الدخول عبر الحدود على بيانات الكومبيوتر المخزونة بموافقة أو في حالة توافرها علنا يجوز للدولة الطرف بالاتفاقية، و بدون تفويض من دولة أخرى طرف بالاتفاقية:

أ)الدخول علنا و بشكل متاح-(مصدرا مشاع) على بيانات الكومبيوتر المخزونة، بغض النظر عن مكان تواجد البيانات جغرافيا، أو

ب)الدخول على، أو تلقي، عن طريق منظومة كومبيوتر بأراضيها، بيانات الكومبيوتر المخزونة الموجودة بدولة أخرى طرفا بالاتفاقية، و ذلك في حالة حصول الدولة الطرف على الموافقة القانونية و الطواعية من الشخص الذي له حق التفويض قانونا في الكشف عن البيانات للدولة الطرف بالاتفاقية من خلال منظومة الكومبيوتر هذه.

مادة 33- تبادل المساعدات في تجميع خط سير البيانات في الوقت الصحيح

1-تقوم الدول الأطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض فيما يتعلق بعملية تجميع البيانات خلال خط سيرها في الوقت الصحيح و التي تكون لها علاقة باتصالات بعينيها على أراضيها و التي يتم إرسالها بواسطة منظومة كومبيوتر.و طبقا لنصوص الفقرة 2 فإن هذه المساعدات تحكمها الشروط و الإجراءات المنصوص عليها بموجب القانون الوطني للدولة.

2-تقوم كل دولة بتقديم مثل هذه المساعدة على الأقل تقديرا فيما يتعلق بالجرائم التي قد تتوافر فيها عملية تجميع البيانات من خلال خط سيرها في الوقت الصحيح في قضية محلية أو وطنية مماثلة.

مادة 34- تبادل المساعدات المتعلقة باعتراض مضمون البيانات

1- تقوم الدول أطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض فيما يتعلق بعملية تجميع أو تسجيل مضمون البيانات في الوقت الصحيح و الخاصة باتصالات معينة يتم إرسالها بواسطة منظومة كومبيوتر و إلى الحد الذي تجيزه القوانين بموجب المعاهدات و القوانين الوطنية التي تطبق.

الباب الثالث: شبكة المنظومة

مادة 35- شبكة المنظومة

1- تقوم كل دولة طرف بالاتفاقية بتخصيص نقطة اتصال متاحة طوال الأربع و العشرين ساعة يوميا وسبعة أيام أسبوعيا و ذلك لضمان توافر تقديم المساعدات المباشرة لغرض التحقيقات أو الإجراءات الخاصة بالجرائم المتعلقة بنظم وبيانات الكومبيوتر، أو لتجميع الأدلة الخاصة بالجريمة في شكل إلكتروني. و يشمل هذا النوع من المساعدة تسهيل، أو إذا ما كان القانون الوطني الخاص بها و التطبيق يجيز مباشرة تنفيذ الإجراءات التالية:

أ- توفير الأدوات و الأجهزة الفنية.

ب- المحافظ على البيانات طبعا للمادتين 29، 30.

ج- تجميع الأدلة، و توفير المعلومات القانونية و الاستدلال على المشتبه فيهم و تحديد مكانهم.

2- *أ*- سيكون لنقطة الاتصال الخاصة بالدولة الطرف بالاتفاقية القدرة على إجراء الاتصالات بمثيلها بدولة أخرى نظيرتها على وجه السرعة.

ب-إذا كانت نقطة الاتصال التي تخصصها الدولة الطرف بالاتفاقية ليست جزء من الجهة أو الجهات المسئولة عن تبادل المساعدات الدولية أو عمليات تسليم المجرمين في تلك الدولة، فإن نقطة الاتصال تضمن قدرتها على التنسيق مع تلك الجهة أو الجهات على وجه السرعة. العاملين المدربين و المزودين بالأجهزة و المعدات.

3- تضمن كل دولة طرف بالاتفاقية توافر و ذلك لتسهيل عملية تشغيل الشبكة.

الفصل الرابع: البنود النهائية

مادة 36- التوقيع و الدخول في حيز التنفيذ

1-تصبح هذه الاتفاقية علنية بالنسبة للتوقيع من قبل الدول الأعضاء بالمجلس الأوروبي و الدول غير الأعضاء التي شاركت في دراسة التفاصيل الخاصة بها.

2-تخضع هذه الاتفاقية لعمليات التصديق، أو القبول، أو الموافقة. و سيتم إيداع الأصول الخاصة بعمليات التصديق أو القبول، أو الموافقة لدى الأمين العام للمجلس الأوروبي.

3-تدخل هذه الاتفاقية حيز التنفيذ في اليوم الأول من الشهر التالي لعملية إنهاء فترة الثلاثة شهور من تاريخ قيام خمس دول، من بينها ثلاث دول أعضاء على الأقل بالمجلس الأوروبي، بالتعبير عن موافقتها على الالتزام من جانبها بالاتفاقية وفقا للنصوص بالفقرتين1-2.

1-بالنسبة لأية دولة موقعة و بالتالي تعبر عن موافقتها على الالتزام بها من جانبها، فإن هذه الاتفاقية تدخل حيز التنفيذ في اليوم ألأول من الشهر التالي لعملية انتهاء فترة الثلاثة شهور من تاريخ الإعراب عن الموافقة بالالتزام بالاتفاقية وفقا لنصوص الفقرتين 1، 2 .

مادة 37- الانضمام للاتفاقية

1-بعد دخول هذه الاتفاقية في حيز التنفيذ، فإنه يجوز لجنة الوزراء بالمجلس الأوروبي، و بعد التشاور مع الدول المبرمة للاتفاقية و الحصول على موافقتها بالإجماع، توجيه الدعوة لأية دولة ليست عضو بالمجلس و لم تشارك في دراسة التفاصيل الخاصة بها للانضمام لهذه الاتفاقية. و يتم اتخاذ القرار بالأغلبية المنصوص عليها بالمادة 20- د من التشريع الخاص بالمجلس الأوروبي و عن طريق الاقتراع الإجمالي لممثلي الدول المبرمة للاتفاقية و التي يحق لها قانونا المشاركة في عضوية لجنة الوزراء.

2- بالنسبة لأية دولة تنضم للاتفاقية بموجب الفقرة (1) بعاليه، فسوف تدخل الاتفاقية في حيز التنفيذ في اليوم الأول من الشهر التالي لعملية انتهاء فترة الثلاثة شهور من تاريخ إيداع أصول الانضمام لدى الأمين العام للمجلس الأوروبي.

مادة 38 - التطبيق الإقليمي

1- يجوز لأية دولة، في وقت التوقيع على الاتفاقية أو عند إيداع أصول التصديق الخاصة بها، أو قبولها أو الموافقة عليها ، أو الانضمام إليها و الدخول فيها، تحديد الإقليم أو الأقاليم التي يتم تطبيق هذه الاتفاقية عليها.

2- يجوز لأية دولة، في أي موعد لاحق، و بموجب إقرار موجه للأمين العام للمجلس الأوروبي، التوسع في تطبيق هذه الاتفاقية على أي إقليم أو دولة أخرى يتم تحديدها بالإقرار. و بالنسبة لهذا الإقليم أو الدولة فسوف تدخل الاتفاقية حيز التنفيذ في اليوم الأول من الشهر الذي يلي انتهاء فترة الثلاث شهور من تاريخ ورود الإقرار للأمين العام (للمجلس الأوروبي).

3-يجوز سحب أي إقرار يتم تقديمه بموجب الفقرتين السابقتين، بالنسبة لأي إقليم أو دولة يتم تحديدها بهذا الإقرار و التراجع فيه بموجب إخطار موجه للأمين العام للمجلس الأوروبي و تصبح سحب الإقرار ساري المفعول في اليوم الأول من الشهر الذي يلي انتهاء فترة الثلاثة شهور من تاريخ ورود هذا الإخطار للأمين العام (للمجلس الأوروبي) .

مادة 39- نتائج الاتفاقية

1-إن الغرض من الاتفاقية الحالية هو استكمال المعاهدات أو الاتفاقيات المتعددة الأطراف أو الثنائية فيما بين الدول الأطراف بالاتفاقية، بما في ذلك النصوص الخاصة:

- بالاتفاقية الأوروبية الخاصة بتسليم المجرمين، و التي أصبحت جاهزة على التوقيع في 13 ديسمبر 1957 (رقم 24 ETS).
- الاتفاقية الأوروبية الخاصة بتبادل المساعدات في الأمور الجنائية، و التي أصبحت جاهزة على التوقيع باستراسبورج في 20 أبريل 1959 (رقم 30 ETS)
- الملحق الإضافي للاتفاقية الأوروبية الخاصة بتبادل المساعدات في الأمور الجنائية، و الذي أصبح جاهزا على التوقيع باستراسبورج في 17 مارس 1978 (اتفاقية رقم 99 ETS)

2-و في حالة سابقة قيام دولتين أو أكثر من الدول ألأطراف بالاتفاقية بإبرام اتفاقية أو معاهدة تتعلق بالأمور التي يتم التعامل فيها بهذه الاتفاقية أو بالأحرى قيامها بإقامة علاقاتها بناء على مثل هذه الأمور، أو في حالة قيامها بعمل ذلك مستقبلا و بالتالي فإنه سيحق أيضا لها قانونا تطبيق تلك الاتفاقية أو المعاهدة أو تنظيم تلك العلاقات. إلا أنه، في حالة قيام الدول الأطراف بالاتفاقية بتأسيس علاقاتها فيما يتعلق بالأمور التي يتم التعامل فيها بهذه الاتفاقية الحالية، فضلا عما تحكم اللوائح الخاصة بها، فقد تفعل تلك الدول ذلك بطريقة قد لا تتفق و الأهداف و المبادئ الخاصة بالاتفاقية.

3-لن يؤثر أي شيء بهذه الاتفاقية على الحقوق، و القيود، و الالتزامات، و المسؤوليات غير ذلك من تلك الأمور الخاصة بأية دولة من الدول الأطراف بالاتفاقية.

مادة 40- الإقرارات

يجوز لأية دولة، بموجب إشعار تحريري موجه للأمين العام للمجلس ألأوروبي، في وقت التوقيع على الاتفاقية أو عند إيداع أصول التصديق الخاصة بها، أو قبولها، أو الموافقة عليها، أو الانضمام إليها، إن نقر بأنها تستفيد من إمكانية طلب عناصر إضافية كما هو منصوص عليه بموجب المواد 2، 3، 6- فقرة 1 (ب)؛ 7 ؛9- فقرة 3؛ 27- فقرة 9 (ه).

مادة 41- البند الفيدرالي (الخاص بالدولة الفيدرالية)

1-يجوز للدولة الفيدرالية الاحتفاظ بالحق في القيام بالالتزامات بموجب الفص الثاني من هذه الاتفاقية الذي يتفق و مبادئها الأساسية التي تحكم العلاقة ما بين حكومتها المركزية و الدول التأسيسية أو غيرها من الكيانات الإقليمية الأخرى المماثلة بشرط أن تظل قادرة على التعاون بموجب الفصل الثالث.

2-في حالة التحفظ بموجب الفقرة 1 (أ) فإنه لا يجوز للدولة الفيدرالية تطبيق الشروط الخاصة بمثل هذا التحفظ لاستبعاد أو بالتالي تقليص التزاماتها فعليا للتكفل بالإجراءات المعلنة بالفصل الثاني، وعلاه على ذلك فهي تتمته بإمكانية فعالة و أساسية في تنفيذ القانون فيما يتعلق بتلك الإجراءات.

3-بالنسبة لنصوص هذه الاتفاقية، و التي يصبح تطبيقها بموجب السلطة القضائية بالدول التأسيسية أو غيرها من الكيانات الإقليمية ألأخرى المماثلة، و التي لا تلتزم بالمنظومة الدستورية للنظام الفيدرالي لاتخاذ الإجراءات التشريعية، تقوم الحكومة الفيدرالية بإخطار السلطات المختصة بتلك الدول بالشروط الموضحة إلى جانب رأيها المفضل، لمساعدتها على اتخاذ الإجراءات الملائمة لتفعيلها.

مادة 42- التحفظات

يجوز لأية دولة، بموجب إشعار تحريري موجه للأمين العام للمجلس الأوروبي، و في وقت التوقيع على الاتفاقية أو عند إيداع أصول التصديق الخاص بها، أو قبولها، أو الموافقة عليها، أو الدخول فيها و الانضمام إليها، أن تقر بأنها تستفيد من التحفظ (أو التحفظات) المنصوص عليها بالمادة 4-فقرة2 و المادة 6- فقرة3، و المادة 9- فقرة 4، و المادة 10- فقرة 3، و المادة 11-فقرة3، و المادة 14-فقرة 3، و المادة 22-فقرة 2، و المادة 29-فقرة4، و المادة 41 فقرة 1 و لا يجوز تقديم أية تحفظات أخرى.

مادة 43- الوضع القانوني للتحفظات و التراجع عنها

1-يجوز للدولة الطرف بالاتفاقية التي تتقدم بأحد التحفظات وفقا للمادة 42 أن تتراجع عنه كليا أو جزئيا بواسطة إشعار تحريري موجه للأمين العام للمجلس الأوروبي و يسري هذا التراجع في يوم ورود مثل هذا الإشعار أو الإخطار إلى الأمين العام للمجلس الأوروبي. و إذا أفاد الإخطار بأن يتم تفعيل عملية التراجع عن هذا التحفظ في التاريخ الذي يتم

تحديده في تلك المسألة، و أن يكون هذا التاريخ في وقت لاحق من تاريخ ورود الإخطار للأمين العام، فيسري مفعول هذا التراجع في ذلك التاريخ اللاحق.

2-تقوم الدولة الطرف بالاتفاقية التي تتقدم بأحد التحفظات كما هو مشار إليه بالمادة 42 بالتراجع عن مثل هذا التحفظ، كليا أو جزئيا، بمجرد أن تسمح الظروف بذلك.

3-يجوز للأمين العام للمجلس الأوروبي الاستعلام بصفة دورية لدى الدول الأطراف بالاتفاقية التي تتقدم بتحفظا واحدا أو أكثر كما هو مشار إليه بالمادة 42 بالنسبة للاحتمالات المتوقعة للتراجع عن مثل هذا التحفظ (هذه التحفظات).

مادة 44- التعديلات

1-يجوز لأية دولة طرف بالاتفاقية اقتراح التعديلات على هذه الاتفاقية فيقوم الأمين العام للمجلس الأوروبي بإخطار بها الدول الأعضاء بالمجلس الأوروبي و الدول الغير الأعضاء التي شاركت في الدراسة التفصيلية الخاصة بهذه الاتفاقية، و كذلك أيضا أية دولة تنضم إلى، أو يتم توجيه الدعوة إليها للانضمام إلى، هذه الاتفاقية وفقا لنصوص المادة 37.

2-يتم الإخطار بأي تعديل تقترحه إحدى الدول الأطراف بالاتفاقية إلى اللجنة الأوروبية لمشكلات الجريمة التي تحيل الرأي الخاص بها فيما يتعلق بالتعديل المطروح إلى لجنة الوزراء.

3-تقوم لجنة الوزراء بدراسة التعديل المطروح و الرأي الذي تحيله اللجنة الأوروبية لمشكلات الجريمة و، بعد التشاور مع الدول الأطراف الغير أعضاء بهذه الاتفاقية، فإنه يجوز إقرار التعديل.

4-يتم إرسال النص الخاص بأي تعديل تقره لجنة الوزراء وفقا للفقرة 3 من هذه المادة إلى الدول الأطراف بالاتفاقية لقبوله و الموافقة عليه.

5-يصبح أي تعديل يتم إقراره وفقا للفقرة 3 من هذه المادة في حيز التنفيذ في اليوم الثلاثين من قيام جميع الدول الأطراف بالاتفاقية بإخطار الأمين العام للمجلس الأوروبي بقبولهم ذلك و الموافقة عليه.

مادة 45- تسوية المنازعات

1-يتم إخطار اللجنة الأوروبية بمشكلات الجريمة فيما يتعلق بتفسير و تطبيق هذه الاتفاقية.

2-في حالة حدوث نزاع ما بين دول أطراف بالاتفاقية فيما يتعلق بتفسير و تطبيق هذه الاتفاقية، فإنها تسعى للوصول إلى تسوية النزاع من خلال التفاوض أو أية وسيلة سلمية أخرى من الخيارات الخاصة بها بما في ذلك إحالة النزاع إلى اللجنة الأوروبية لمشكلات الجريمة، أو أمام إحدى محاكم فض المنازعات التي تصبح قراراتها ملزمة على الأطراف، أو أمام محكمة العدل الدولية، حسبما يتفق عليه من قبل الأطراف المعنية.

مادة 46- مشاورات الدول الأطراف

1-تقوم الدول الأطراف بالاتفاقية ، كلما كان ذلك ملائما بالتشاور فيما بينها بصفة دولية و ذلك بغرض تسهيل:

أ-فعالية الاستفادة و التنفيذ لهذه الاتفاقية بما في ذلك تحديد أية مشكلات خاصة بذلك و كذلك أيضا النتائج الخاصة بأي إقرار أو تحفظ يتم تقديمها بموجب هذه الاتفاقية؛

ب-تبادل المعلومات الخاصة بالسياسة القانونية الهامة أو التطورات التكنولوجية المتقدمة الخاصة بالإجرام السيبيري و تجميع الأدلة في صورة إلكترونية ؛

ج-دراسة الإضافات أو التعديلات الممكنة للاتفاقية.

2-يتم إخطار اللجنة الأوروبية لمشكلات الجريمة بصفة دورية فيما يتعلق بنتائج المشاورات المشار إليها بالفقرة.1

3-تقوم اللجنة الأوروبية لمشكلات الجريمة، كلما كان ذلك ملائما بتسهيل المشاورات المشار إليها بالفقرة 1 و اتخاذ اللازم لمساعدة الدول الأطراف بالاتفاقية خلال بذل مساعيها و جهودها لاستكمال أو تعديل الاتفاقية في السنوات الثلاث

الأخيرة من دون دخول الاتفاقية حيز التنفيذ، فتقوم اللجنة الأوروبية لمشكلات الجريمة، بالتعاون مع الدول الأطراف بالاتفاقية، بإجراء مراجعة لكافة البنود الخاصة بالاتفاقية و التوصية عند الضرورة بأية تعديلات ملائمة.

4-فيما عدا ما يقوم به المجلس الأوروبي، فإن ما يتم تكبده من نفقات تنفيذا للبنود الخاصة بالفقرة 1 قد تتحملها الدول الأطراف بالاتفاقية بالطريقة التي تقررها.

5-تقوم الأمانة العامة للمجلس الأوروبي بمساعدة الدول الأطراف بالاتفاقية في تنفيذ مهام عملها وفقا لهذه المادة.

مادة 47- الفسخ

1-يجوز لأي دولة طرف بالاتفاقية، وفي أي وقت فسخ هذه الاتفاقية بواسطة إخطار موجه إلى الأمين العام للمجلس الأوروبي.

2-تصبح عملية الفسخ هذه سارية المفعول في اليوم الأول من الشهر الذي يلي انتهاء فترة الثلاثة شهور من تاريخ ورود الإخطار للأمين العام (للمجلس الأوروبي).

مادة 48- الإخطار

يقوم الأمين العام للمجلس الأوروبي بإخطار الدول الأعضاء بالمجلس الأوروبي و الدول غير الأعضاء التي شاركت في الدراسة التفصيلية الخاصة بهذه الاتفاقية، و كذلك أيضا أية دولة تنضم إلى، أو يتم توجيه الدعوة إليها للانضمام إلى، هذه الاتفاقية بما يلي:

أ- أية توقيعات على الاتفاقية.

ب- إيداع أية أصول للتصديق، أو القبول، أو الموافقة، أو الانضمام للاتفاقية.

ج- أي تاريخ خاص بدخول هذه الاتفاقية حيز التنفيذ وفقا للمادتين 36، 37.

د- أي قرار يتم تقديمه بموجب المادة 40 أو أي تحفظ يتم تقديمه وفقا للمادة 42.

ه- أي إجراء، أو إخطار، أو اتصال آخر يتعلق بهذه الاتفاقية.

و شهادة على ما ورد بهذه الوثيقة، فقد قام الموقع أدناه، بحكم كونه مفوضا قانونا على النحو الملائم لذلك، بالتوقيع على هذه الاتفاقية.

وقد تم ذلك في مدينة بودابست، في هذا اليوم الموافق الثالث و العشرين من شهر نوفمبر 2001 و باللغة الإنجليزية، وباللغة الفرنسية، و أن النصين كليهما صحيحا على حد سواء، و في داخل نسخة واحدة يتم إيداعها بالسجلات الخاصة بالمجلس الأوروبي. و يتولى الأمين العام للمجلس الأوروبي إرسال نسخ معتمدة و موثقة إلى كل دولة من الدول الأعضاء بالمجلس الأوروبي، و إلى الدول غير الأعضاء التي شاركت في الدراسة التفصيلية الخاصة بهذه الاتفاقية، و إلى أية دولة يتم توجيه الدعوة إليها للانضمام إلى هذه الاتفاقية و الدخول فيها.

الملحق الثاني

القانون العربي الإسترشـــــادي
لمكافحة جرائم تقنية أنظمة المعلومات
و ما في حكمهـــــا

المادة (1)

في تطبيق أحكام هذا القانون يقصد بالكلمات و العبارات الآتية، المعاني الموضحة قرين كـــــــل منها:

***البيانات:**

كل ما يمكن تخزينه و معالجته و توليده ونقله بواسطة الحاسب الآلي، كالأرقام و الحـــــــروف و الرموز و ما إليها..

***البرنامج المعلوماتي:**

مجموعة من التعليمات و الأوامر ، قابلة للتنفيذ باستخدام الحاسب الآلي و معدة لإنجاز مهمة ما.

***النظام المعلوماتي:**

مجموعة برامج و أدوات معدة لمعالجة و إدارة البيانات و المعلومات.

***الشبكة المعلوماتية:**

ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات و تبادلها.

***الموقع:**

مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

***الالتقاط:**

مشاهدة البيانات أو المعلومات أو الحصول عليها.

المادة (2):

مع عدم الإخلال بأية عقوبة أشد في قانون العقوبات (الجزاء) أو في أي قانون آخر، يعاقب على الأفعال المنصوص عليها في المواد التالية، بالعقوبات المقررة فيها.

المادة (3):

كل من دخل عمدا و بغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس...و الغرامة...أو بإحدى هاتين العقوبتين.

فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو بإعادة نشر بيانات أو معلومات شخصية يكون الحد الأدنى لعقوبة الحبس... و لعقوبة الغرامة....

المادة (4):

كل من ارتكب تزويرا في أحد المستندات المعالجة في نظام معلوماتي يعاقب بالحبس مدة لا تقل عن... و يعاقب بذات العقوبة كل من استعمل المستند المزور مع علمه بالتزوير.

المادة (5): إذا ارتكب الجاني أيا من الجرائم المنصوص عليها في المادة (3) أثناء أو بسبب تأديته وظيفته، أو سهل ذلك للغير، يكون الحد الأدنى لعقوبة الحبس... و لعقوبة الغرامة...

فإذا توفر أي ظرف من الظروف المشددة المنصوص عليها في الفقرة الثانية من المادة المذكورة يكون الحد الأدنى لعقوبة الحبس...و لعقوبة الغرامة...

المادة (6):

كل من أدخل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات يغرض ذلك و لم يتحقق غرضه يعاقب بالحبس... و الغرامة... أو بإحدى هاتين العقوبتين.

فإذا تحقق الغرض كان الحد الأدنى لعقوبة الحبس... و لعقوبة الغرامة ...

المادة (7):

كل من أعاق أو شوش أو عطل عمدا و بأية وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات يعاقب بالحبس... و الغرامة ... أو بإحدى هاتين العقوبتين.

المادة (8):

كل من تنصت أو التقط أو اعترض بدون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها، يعاقب بالحبس... و الغرامة ... أو بإحدى هاتين العقوبتين.

المادة (9):

كل من استعمل الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه، و لو كان هذا الفعل أو الإمتناع مشروعا، يعاقب بالحبس... و الغرامة ... أو بإحدى هاتين العقوبتين.

المادة (10):

كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها إلى الإستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند و ذلك بالإستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس... و الغرامة ... أو بإحدى هاتين العقوبتين.

المادة (11):

كل من استخدم الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها في الوصول، بدون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية و ما في حكمها بقصد استخدامها في الحصول على بيانات الغير أو أمواله أو ما تتيحه من خدمات، يعاقب بالحبس... و الغرامة ... أو بإحدى هاتين العقوبتين.

المادة (12):

كل من انتفع، بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها بخدمات الإتصالات يعاقب بالحبس... و الغرامة...

المادة (13):

كل من أنتج أو أعد أو هيأ أو أرسل أو خزن عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها ما من شأنه المساس بالنظام العام أو الآداب العامة، يعاقب بالحبس... و الغرامة...

فإذا كان الفعل موجها إلى حدث يكون الحد الأدنى لعقوبة الحبس... و لعقوبة الغرامة...

المادة (14) : مع عدم الإخلال بالأحكام المقررة لحماية حقوق الملكية الفكرية، يعاقب كل من نشر أو نسخ عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها مصنفات فكرية أو أدبية أو أبحاث علمية أو ما في حكمها بدون وجه حق، يعاقب بالحبس... و الغرامة ... أو بإحدى هاتين العقوبتين.

فإذا كان النشر أو النسخ بقصد التسويق أو الربح، تكون العقوبة الحبس...

المادة (15):

كل من دخل بدون وجه حق، في موقع خاص لشركة أو مؤسسة أو غيرها لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه يعاقب بالحبس و الغرامة أو بإحدى هاتين العقوبتين.

المادة (16):

كل من اعتدى على أي من المبادئ أو القيم الدينية أو الأسرية أو حرمة الحياة الخاصة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها، يعاقب بالحبس مدة لا تقل عن...

المادة (17):

كل من أنشأ أو نشر موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها بقصد الاتجار في الجنس البشري أو تسهيل التعامل فيه يعاقب بالحبس... و الغرامة...

المادة (18):

كل من أنشأ أو نشر موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها، بقصد الإتجار أو الترويج أو التعاطي بالمخدرات أو المؤثرات العقلية و ما في حكمها أو تسهيل التعامل فيها يعاقب بالحبس... و الغرامة...

المادة (19):

كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه، أو قام باستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع، أو بتحويل الموارد أو الممتلكات، مع العلم بمصدرها غير المشروع، و ذلك عن طريق استخدام الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر موقعا لارتكاب أي من هذه الأفعال، يعاقب بالسجن...

المادة (20):

كل من أنشأ أو نشر موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها لأي مجموعة تدعو لتسهيل و ترويج برامج و أفكار مخالفة للنظام العام يعاقب بالحبس ... و بالغرامة...

المادة (21):

كل من أنشأ أو نشر موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في العمال الإرهابية يعاقب بالسجن...

المادة (22):

كل من دخل عمدا و بغير وجه حق موقعا أو نظاما مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني يعاقب بالسجن...

فإذا كان الدخول بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو بث أفكار تمس ذلك، يكون الحد الأدنى لعقوبة السجن...

المادة (23):

كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ووقعت الجريمة بناء على التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة المقررة لها.

و يعاقب بنصف العقوبة المقررة للجرائم المنصوص عليها في المواد (16-22) و لو لم تقع الجريمة الأصلية.

المادة (24):

يعاقب على الشروع في الجرائم المنصوص عليها في المواد (3-15) بنصف العقوبة المقررة لها و يعاقب على الشروع في الجرائم المنصوص عليها في المواد (16-22) بذات العقوبة المقررة لها.

المادة (25):

مع عدم الإخلال بحقوق الغير حسني النية، يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو المشروع الذي يكون محلا لارتكاب أي من هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالكها، و ذلك إغلاقا كليا أو للمدة التي تقدرها المحكمة.

المادة (26):

تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه حتى و لو ارتكبت كليا أو جزئيا خارج إقليم الدولة، متى أضرت بأحد مصالحها و يختص القضاء الوطني بنظر الدعاوى المترتبة عليها.

المادة (27):

فضلا عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه وفقا لمواد (16-22).

رقم الإيداع

ج11/(2004)01-ن(0143)

الملحق الثالث

مشروع قانون اتحادي رقم ( ) لسنة 2004في شأن مكافحة جرائم تقنية أنظمة المعلومات

نحن زايد بن سلطان آل نهيان رئيس دولة الإمارات العربية المتحدة

بعد الاطلاع على الدستور،

وعلى القانون الاتحادي رقم (1) لسنة 1972 بشأن اختصاصات الوزارات وصلاحيات الوزراء المعدلة له،

وعلى القانون الاتحادي رقم (9) لسنة 1976 في شأن الأحداث الجانحين والمشردين،

وعلى القانون الاتحادي رقم (4) لسنة 1979 في شأن قمع الغش والتدليس في المعاملات التجارية،

وعلى القانون الاتحادي رقم (10) لسنة 1980 في شأن المصرف المركزي والنظام النقدي وتنظيم المهنة المصرفية والقوانين المعدل له،

وعلى القانون الاتحادي رقم (15) لسنة 1980 في شأن المطبوعات والنشر،

وعلى القانون الاتحادي رقم (3) لسنة 1982 بإنشاء المركز الوطني للحاسب الآلي والقوانين المعدلة له،

وعلى قانون العقوبات الصادر بالقانون الاتحادي رقم (3) لسنة 1987،

وعلى القانون الاتحادي رقم (1) لسنة 1991 في شأن مؤسسة الإمارات للاتصالات.

وعلى قانون الإثبات في المعاملات المدنية والتجارية الصادر بالقانون الاتحادي رقم (10) لسنة 1992،

وعلى قانون الإجراءات المدنية الصادر بالقانون الاتحادي رقم (11) لسنة 1992،

وعلى قانون الإجراءات الجزائية الصادر بالقانون الاتحادي رقم (35) لسنة 1992،

وعلى القانون الاتحادي رقم (37) لسنة 1992 في شأن العلامات التجارية والقوانين المعدلة له،

وعلى القانون الاتحادي رقم (44) لسنة 1992 في شأن تنظيم وحماية الملكية الصناعية لبراءات الاختراع والرسوم والنماذج الصناعية،

وعلى القانون الاتحادي رقم (14) لسنة 1995 في شأن مكافحة المواد المخدرة والمؤثرات العقلية،

وعلى القانون الاتحادي رقم (4) لسنة 2002 في شأن تجريم غسيل الأموال،

وعلى القانون الاتحادي رقم (7) لسنة 2002 في شأن حقوق المؤلف والحقوق المجاورة،

وبناء على ما عرضه وزير.....، وموافقة مجلس الوزراء والمجلس الوطني الاتحادي، وتصديق المجلس الأعلى للاتحاد،

أصدرنا القانون الآتي:

تعريفات

المادة (1)

الدولة:	دولة الإمارات العربية المتحدة
الوزير:	.....
الجهة المختصة:	.....
اتصالات:	مؤسسة الإمارات للاتصالات
البيانات:	كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي وبوجه خاص الكتابة والصور والصوت والأقلام والحروف والرموز والإشارات وغيرها.
البرنامج المعلوماتي:	مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام الحاسب الآلي ومعدة لإنجاز مهمة ما.
النظام المعلوماتي:	مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.
الشبكة المعلوماتية:	ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.
الموقع:	مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.
الالتقاط:	مشاهدة البيانات أو المعلومات أو الحصول عليها.

المادة (2)

مع عدم الإخلال بأية عقوبة أشد ينص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب على الجرائم المنصوص عليها في هذا القانون بالعقوبات المقررة فيها.

المادة (3)

كل من دخل وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس.....والغرامة.....أو بإحدى هاين العقوبتين فإذا ترتب على الدخول إلغاء أو الحذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن.....والغرامة.....

المادة (4)

كل من زور أحد المستندات المعالجة في نظام معلوماتي يعاقب بالحبس مدة لا تقل عن..... وبالغرامة.....ويعاقب بذات العقوبة كل من استعمل المستند المزور مع علمه بالتزوير.

المادة (5)

كل من ارتكب أيا من الجرائم المنصوص عليها في المادة (3) من هذا القانون أثناء أو بسبب تأدية عمله أو سهل ذلك للغير فتكون العقوبة الحبس مدة لا تقل عن.....والغرامة التي لا تقل عن.....

كل من أدخل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمهما، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات يعاقب بالحبس مدة.....والغرامة.....أو بإحدى هاتين العقوبتين

المادة(7)

كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأية وسيلة كانت عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمهما يعاقب بالحبس مدة .....والغرامة.....أو بإحدى هاتين العقوبتين.

المادة (8)

كل من تنصت أو التقط أو اعترض، بدون وجه حق ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، يعاقب بالحسب مدة.....والغرامة.....أو بإحدى هاتين العقوبتين

المادة (10)

كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه يعاقب بالحبس مدة.....والغرامة.....أو بإحدى هاتين العقوبتين.

المادة (11)

كل من استخدم الشبكة المعلوماتية أو أحد الأجهزة الحاسب الآلي وما في حكمها، في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية وما في حكمها بقصد استخدامها في الحصوص على بيانات الغير أو أمواله أو ما تتيحه من خدمات، يعاقب بالحبس مدة.....والغرامة.....أو بإحدى هاتين العقوبات.

المادة (12)

كل من انتفع بدون وجه حق بخدمات الاتصالات عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها يعاقب بالحبس مدة.....والغرامة.....

المادة (13)

كل من أنتج أو أعد أو هيأ أو أرسل أو خزن عن طريق شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها ما من شأنه المساس بالنظام العام أو الآداب العامة، يعاقب بالحبس ...أو الغرامة.....

فإذا كان الفعل موجها إلى حدث يعاقب بالحبس مدة لا تقل عن .....والغرامة.....

المادة (14)

معى عدم الإخلال بالأحكام المقررة لحماية حقوق الملكية الفكرية يعاقب كل من نشر أو نسخ عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها مصنفات فكرية أو أدبية أو أبحاث علمية أو ما في حكمها، بدون وجه حق بالحبس مدة.....والغرامة..... أو بإحدى هاتين العقوبتين، فإذا كان النشر أو النسخ بقصد التسويق أو الربح تكون العقوبة الحبس مدة .....

المادة (15)

كل من دخل بدون وجه حق موقعا في الشبكة المعلوماتية لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه يعاقب بالحبس مدة.....والغرامة..... أو بإحدى هاتين العقوبتين.

المادة (16)

كل من اعتدى على أي من المبادئ أو القيم الدينية أو الأسرية أو حرمة الحياة الخاصة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها يعاقب بالحبس مدة لا تقل عن.....

المادة (17)

كل من أنشأ أو نشر موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الاتجار في الجنس البشري أو تسهيل التعامل فيها يعاقب بالحبس مدة.....والغرامة.....

المادة (18)

كل من أنشأ أو نشر موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، بقد الاتجار أو الترويج أو التعاطي بالمخدرات أو المؤثرات العقلية وما في حكمها أو تسهيل التعامل فيها يعاقب بالحبس مدة.....والغرامة.....

المادة (19)

مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال المشار إليه، يعاقب بالسجن مدة.....كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه أو قام باستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر موقعا لارتكاب أي من هذه الأفعال.

المادة (20)

كل من أنشأ موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار مخالفة للنظام العام يعاقب بالحبس مدة...والغرامة.....

المادة (21)

كل من أنشأ موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها أو ألأعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال.

المادة (22)

كل من دخل وبغير وجه حق موقعا أو نظاما مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني، يعاقب بالسجن مدة.

المادة (23)

كل من حرض أو ساعد أو اتفق مع الغير على ارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، ووقعت الجريمة بناء على التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة المقررة لها.

المادة (24)

مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أيا من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو المشروع الذي يكون محلا لارتكاب أيا من هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالكها، وذلك إغلاقا كليا أو للمدة التي تقدرها المحكمة.

المادة (26)

فصلا عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي لاالذي يحكم عليه وفقا للمواد من (16 إلى 22) من هذا القانون.

المادة (27)

يكون لموظفي الجهة المختصة الذين يصدر بتحديدهم قرار من وزير العدل والشئون الإسلامية والأوقاف بالاتفاق مع الوزير صفة مأموري الضبط القضائي في ضبط الجرائم والمخالفات التي تقع بالمخالفة لأحكام هذا القانون، والقرارات الصادرة تنفيذا له كل في نطاق اختصاصه وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم.

المادة (28)

يلغى كل نص يخالف أحكام هذا القانون.

المادة (29)

ينشر هذا القانون في الجريدة الرسمية يوعمل به اعتبارا من تاريخ نشره.

زايد بن سلطان آل نهيان

رئيس دولة الإمارات العربية المتحدة

صدر في قصر الرئاسة بأبو ظبي:

بتاريخ: / / 1424 هـ

الموافق: / / 2000م

الملحق الرابع

مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 4-9 تشرين اول 1994 – البرازيل / ريو دي جانيرو بشان جرائم الكمبيوتر .

في الشق الموضوعي – الجرائم

لقد اوصى المؤتمر بان تتضمن قائمة الحد الادنى للافعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر ما يلي :

1- **الاحتيال او الغش المرتبط بالكمبيوتر** :- ويشمل الادخال والاتلاف والمحو لمعطيات الكمبيوتر او برامجه ، او القيام باية افعال تؤثر بمجرى المعالجة الالية للبيانات وتؤدي الى الحاق الخسارة او فقدان الحيازة او ضياع ملكية شخص وذلك بقصد جني الفاعل منافع اقتصادية له او للغير.

2- **تزوير الكمبيوتر او التزوير المعلوماتي** :- ويشمل ادخال او اتلاف او محو او تحوير المعطيات او البرامج او اية افعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد – فيما لو ارتكبت بغير هذه الطرق – من قبيل افعال التزوير المنصوص عليها في القانون الوطني .

3- **الاضرار بالبيانات والبرامج (الاتلاف)** :- وتشمل المحو والاتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه.

4- **تخريب واتلاف الكمبيوتر** :- وتشمل الادخال او المحو او الاتلاف او التخريب او اي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر او نظام الاتصالات (الشبكات).

5- **الدخول غير المصرح به** ، وهو التوصل او الولوج دون تصريح الى نظام او مجموعة نظم عن طريق اناتهاك اجراءات الامن .
الاعتراض غير المصرح به ، وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر او عدة نظم او شبكة اتصالات

في الشق الاجرائي

قرار صادر عن المؤتمرالدولي الخامس العشر للجمعية الدولية لقانون العقوبات حول القواعد الاجرائية في بيئة جرائم الكمبيوتر

1. يتطلب التنقيب (L'enquête) بالنسبة لجرائم الحاسب الالي ، والجرائم الاكثر تقليدية في بيئة تكنولوجيا المعلومات – لمصلحة الدفاع الاجتماعي الفعال – ان نضع تحت تصرف سلطات التحقيق (L'instruction) والتحري (La poursuite) مكنات قسرية كافية تتعادل مع الحماية الكافية لحقوق الانسان وحرمة الحياة الخاصة.

2. لتجنب تعسف السلطات الرسمية ، فان القيود التي ترد على حقوق الانسان عن طريق رجال السلطة العامة ، لا يمكن ان تكون مقبولة الا في الحالة التي تكون فيها مرتكزة على قواعد قانونية واضحة ودقيقة ومتمشية مع المعايير الدولية لحقوق الانسان.

ان الانتهاكات غير المشروعة لحقوق الانسان التي يرتكبها رجال السلطة العامة ، يمكن ان تبطل الدليل المتحصل عليه ، بالاضافة الى تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون.

3. على ضوء هذه المبادئ العامة يجب ان يحدد بوضوح ما يلي :

أ- السلطات التي تقوم باجراء التفتيش (La perquisition) والضبط (La saisie) في بيئة تكنولوجيا المعلومات ، وخاصة ضبط الاشياء غير الحسوسة (Biens non corporels) وتفتيش شبكات الحاسب.

ب- واجبات التعاون الفعال من جانب المجني عليهم (Victimes) ، والشهود (Temoins= ، وغيرهم من مستخدمي utilisaterurs تكنولوجيا المعلومات ، فيما خلا المشتبه (suspect) (خاصة لكي تكون المعلومات متاحة في صورة بمكن استخدامها للاغراض القضائية fins)) judiciaries).

ت- لسماح للسلطات العامة باعتراض (interception) الاتصالات داخل نظام الحاسب ذاته ، او بينة وبين نظم الحاسبات الاخرى . مع استخدام الادلة التي يتم الحصول عليها في الاجراءات امام المحاكم .

4. نظرا لتعدد وتنوع البيانات المدرجة في نظم معالجة البيانات (des systèmes de traitement informatique) ، فان تنفيذ المكنات القسرية (المنوطة برجال السلطة العامة) يجب ان يكون متناسبا مع الطابع الخطير للانتهاك ، ولا يسبب سوى الحد الادنى من اعاقة (génante) الانشطة القانونية للفرد . كما يجب عند بدء التحريات (investigations) ان يوضع في الاعتبار – بالاضافة الى القيم المالية التقليدية – كل القيم المرتبطة ببيئة تكنولوجيا المعلومات ، مثل ضياع فرصة اقتصادية ، التجسس ، انتهاك حرمة الحياة الخاصة ، مخاطر الخسارة الاقتصادية ، كلفة lecout اعادة بناء تكامل البيانات كما كانت من قبل .

5. القواعد القائمة في مجال قبول ومصداقية الادلة ، يمكن ان تثير مشاكل عند تطبيقها ، نظرا لتقييم تسجيلات الحاسبات (L'évaluation des enregistrements informatiques) في الاجراءات القضائية لذا ينبغي ادخال بعض التغييرات التشريعية في حالة الضرورة .

الملحق الخامس

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول
أحكام عامة

الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

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

ج – معطيات معلوماتية : 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،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني

مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أوالتخريب أوالجرائم الماسة بأمن الدولة،

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث

القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادة 8 : يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنه المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

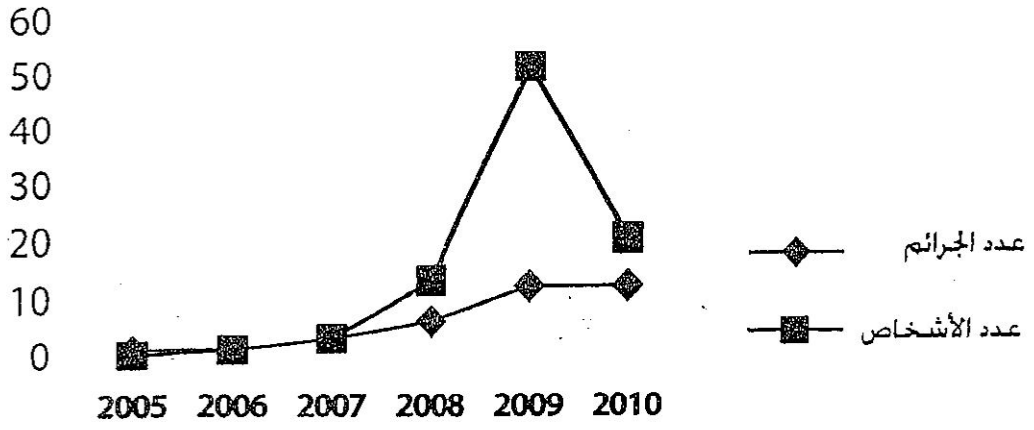
الملحق السادس

1) قضايا المساس بأنظمة المعالجة الآلية للمعطيات التي طرحت على المحاكم وعدد الأشخاص المتابعين (إلى غاية 30 افريل 2010)

السنة	2005	2006	2007	2008	2009	2010	المجموع
عدد الجرائم	01	01	03	06	12	12	35
عدد الأشخاص المتابعين	00	01	03	13	51	20	88

ملاحظة :

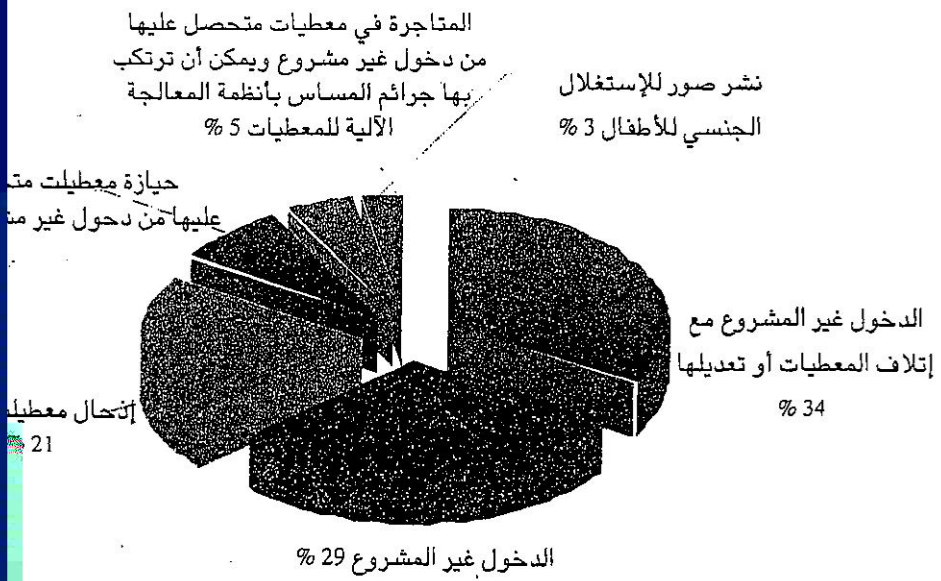
ارتفاع عدد الأشخاص المتابعين خلال سنتي 2009 و2010 يرجع إلى ارتفاع عدد المتابعات من اجل جرائم المساس بأنظمة المعالجة الآلية للمعطيات مقترنة بجرائم اختلاس الأموال العمومية والتزوير



2) قضايا المساس بأنظمة المعالجة الآلية للمعطيات مفصلة حسب

(2005 – افريل 2010)

نوع الجريمة	العدد	النسبة ال
الدخول غير المشروع مع إتلاف المعطيات أو تعديلها	13	%34
الدخول غير المشروع	11	%29
إدخال معطيات خلسة	08	%21
حيازة معطيات متحصل عليها من دخول غير مشروع	03	%08
المتاجرة في المعطيات متحصل عليها من دخول غير مشروع ويمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات	02	%05
نشر صور للاستغلال الجنسي للأطفال	01	%03
المجمـــــــــــــوع	38	%100



مرتكبي جرائم المساس بأنظمة المعالجة الآلية للمعطيات

ـــــن : مابين 25 و30 سنة ..... %68

علوماتية : تقني أو طالب ..... %99

حية : غالبا مهنية ..... %84

ـــــع :

ب ..... %65

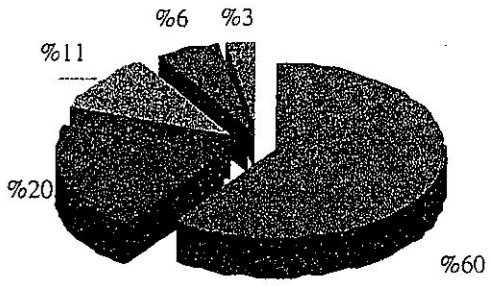
..... %15

..... %15

..... %5

حايا جرائم المساس بأنظمة المعالجة الآلية للمعطيات

	العدد	النسبة المئوية
مؤسسات ذات تجاري	21	%60
	07	%20
أجنبية	04	%11
ين	02	%06
نبية	01	%03
	35	%100



إدارات عمومية ومؤسسات ذات طابع صناعي وتجاري

شركات خاصة

شركات خاصة أجنبية

أشخاص طبيعيين

هيئة عمومية أجنبية

الملخص

موضوع الدراسة المعنون جرائم المساس بأنظمة المعالجة الآلية للمعطيات على قدر من الأهمية كباقي الجرائم المعلوماتية ، التي دفعت بالمشرع الجزائري على غرار باقي التشريعات للنص عليها و إضافة القسم السابع مكرر من قانون العقوبات بموجب القانون 15/04 المعدل و المتمم بالقانون 23/06 ، الذي تضمن ثماني مواد جرمت أربع فئات من الإعتداءات من دخول و بقاء غير شرعي في النظام بصورتيه البسيطة و المشددة المؤدية لإتلاف المعطيات ، المساس العمدي بالمعطيات و التعامل بمعطيات غير مشروعة و التي تستدعي بالضرورة دراسة المفاهيم المتعلقة بالمعطيات و أنظمة المعالجة ، و أهم سيمات المجرم المعلوماتي و خصائص الجريمة المعلوماتية عامة .

إضافة للنص على الجانب الإجرائي و الخصوصيات التي شمل بها المشرع الجزائري هذا النوع من الجرائم من حيث القانون الواجب التحقيق و الاختصاص القضائي من جهة ، و أساليب التحري الخاصة بهذه الفئة من الجرائم دون غيرها المنصوص عليها بقانون الإجراءات الجزائية و كذا بعض الأحكام الخاصة المنصوص عليها بالقانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال للحصول على ما يسمى بالدليل الإلكتروني، إلى جانب الأحكام المتعلقة بالجزاءات المقررة للشخص المعنوي و الطبيعي ، و كذا عقوبة الشروع و الاتفاق الجنائي، إضافة للدور الذي يلعبه التعاون الدولي في مكافحة هذه الجرائم المتسمة بطابع دولي عابر للحدود.

الكلمات المفتاحية:

الجريمة المعلوماتية؛ المعالجة الآلية؛ الدليل الإلكتروني؛ الدخول و البقاء؛ الإتلاف؛ المساس بالأنظمة؛ التعامل بالمعطيات؛ الاعتداءات المنطقية؛ الحماية الفنية؛ الحماية الجزائية.

نوقشت يوم 19 مارس 2014