جـــرائـــم النصـــب الإلكتـــــرونـــــي

مقدمة

- إن التطور الذي لحق البشرية بانتقالها الى عصر المعلوماتية و مجال التكنولوجيا الحديثة و الذي جعلها موردا أساسيا للمعلومات و مفتاحا للموارد المختلفة بالإضافة إلى كونه قوة اقتصادية و سياسية لمن يحن تنسيقها و استخدامها مما نجم عنه تحولات في جميع الميادين الاقتصادية و الاجتماعية و غيرها و كان يشهد ببروز فجر المعلومات و الذي ادى الى زيادة استخدام الحاسب الآلي وزيادة أهميته و هذا التقدم في المجال التقني و تزايد اعتماد الإعلام الآلي في تسير شؤون المجتمعات أصبح مصحوبا بفرض جديد لارتكاب صور جديدة و مستحدثة ماسة بالمعلوماتية الا ان هذا التطور تجلى في ابرز مظاهر التكنولوجيا الجديدة للمعلومات و الاتصالات و تطوير أجيال للحاسب الآلي أصبحت تقدم للدولة و مؤسساتها و أجهزتها الإدارية والأمنية من التسهيلات و الإمكانيات التي تساهم في رفع كفاءتها و قدرها على التصدي للجريمة إلا أن هذا التطور اظهر ما يعرف بالمجرم المعلوماتي الذي لم يكن شخصا ظاهرا أما الأعيان بل أصبح شخصا لا يرى .

إلا أن هذا التطور جاء بجرائم جديدة كتحويل الاموال بطرق غير شرعية أو جرائم ماسة بالأشخاص المتعلقة بمعطيات الحاسب الالي من خلال شبكة الانترنت إضافة الى تأثيرها في الدول المتقدمة كان لها بعض التأثير على الدول السائرة في طرق النمو فالجزائر مثلا بدأت تظهر فيها خاصة بعد الانفتاح و تحرير السوق العالمية ، فكان للجزائر دور في هذا المجال خاصة مع توقيعها اتفاقية الشراكة الأوروبية .

إن الجرائم الماسة بالمعلوماتية بدأت تظهر بالجزائر من خلال ماهية محصورة في بعض الهجمات الصغيرة التي أصبحت تهدد المجتمع و لو كانت

جـــرائـــم النصـــب الإلكتـــرونـــي

الجزائر لا تمثل بيئة كاملة لهذا النوع من الجرائم الا ان الخبراء يبرزون بعض الجرائم الواقعة في مجال المعلوماتية و الإعلام الآلي و التي تتفرق بين متجسسين اقتصاديين بنسبة 5 بالمائة و طلبة جامعيين بنسبة 4 بالمائة و موظفي للمؤسسات ب 55 بالمائة .

- بإصدار المشرع الجزائري للقانون 15/04 الذي حاول الحد من هذه الجرائم و محاربتها و إلقاء القبض على مرتكبيها و توقيع الجزاء عليهم و الذي يظهر أهميته من خلا المشرع الجزائري بتعديل قانون العقوبات و الذي قام على تجريم الأفعال المقترنة بمجال المعلوماتية و وضع تشريعات جزائري لهذه الجرائم

- و محاولة منا لدراسة هذا الموضوع المهم و تكوين نظرة حول الجرائم المعلوماتية لتعرف على هذا النوع من الجرائم و الوسائل المقررة لحمايتها بالإضافة إلى العقوبات التي و ضعها المشرع الجزائري .

وفي دراستنا لهذا الموضوع قمنا بدراسته من خلال تقسيمه الى فصلين الفصل الاول نتحدث فيه عن ماهية جريمة النصب أي بالتطرق الى مفهوم هذه الجريمة و نطاقها بالإضافة إلى أركانها و تصنيفاتها ، أما الفصل الثاني فتناولنا فيه الحماية الجنائية للتعاملات الالكترونية سواء قبل المحاكمة او بعدها بالإضافة إلى العقوبات المقررة دوليا أو على الجانب الوطني .

و نظرا لعدم وجود دراسات سابقة في مجال جرائم المعلوماتية ما عدا بعض البحوث و الدراسات الهامشية و نظرا الى نقص المراجع خاصة من الجانب الجزائري و هذه من جملة العوائق التي واجهتنا في دراستنا لهذا الموضوع

بالإضافة الى عائق اللغات لان معظم الكتب تأتي باللغات الأجنبية ، الا انه و مع ذلك قمنا بإعداد هذا البحث بكل مجهود قدرنا على تقديمه .

جـرائـــم النصـب الإلكتـــرونـــي

خطة البحث

- المقدمة

- المبحث التمهيدي : الجرائم الالكترونية و دور الحاسب الالي فيها .

المطلب الاول :تعريف الجريمة المعلوماتية.

المطلب الثاني :دور الحاسب الالي في الجريمة المعلوماتية .

- الفصل الأول : الجرائـم الالكترونية و طبيعتها القانونية .

المبحث الاول :ماهية جريمة النصب الالكترونية .

المطلب الأول : مفهوم جريمة النصب الالكترونية .

الفرع الأول : تعريف جريمة النصب الالكترونية .

الفرع الثاني : نطاق جريمة النصب الالكترونية .

المطلب الثاني :أركان وتصنيفات جريمة النصب الالكترونية .

الفرع الأول : أركان جريمة النصب الالكترونية .

الفرع الثاني : تصنيفات جريمة النصب الالكترونية .

المبحث الثاني : دوافع ارتكاب الجريمة الالكترونية و خصائص مرتكبيها .

المطلب الاول : الاسباب الدافعة لارتكاب جريمة النصب الالكترونية.

الفرع الاول : الدوافع الشخصية .

الفرع الثاني : الدوافع المادية .

المطلب الثاني : خصائص مرتكبي جريمة النصب الالكترونية .

- الفرع الأول : صفات المجرم المرتكب لجريمة النصب الالكترونية .

جـــرائـــم النصـــب الإلكتـــرونـــي

- الفرع الثاني : انواع المجرمين المرتكبين لجريمة النصب الالكترونية.

- الفصل الثاني :الحماية الجنائية للتعاملات الالكترونية .

- المبحث الاول : الحماية الجنائية الموضوعية و الاجرامية .

- المطلب الاول : الحماية الجنائية الموضوعية .

- الفرع الاول : الحماية الجنائية للتعاملات الالكترونية و فقا للقواعد العامة .

- الفرع الثاني : الحماية الجنائية للتعاملات الالكترونية بنصوص خاصة .

- المطلب الثاني : الحماية الجنائية الإجرائية

- الفرع الاول : الحماية السابقة عن المحاكمة .

- الفرع الثاني : الحماية في مرحلة المحاكمة .

- المبحث الثاني : الجوانب الاجرائية للتعاملات الالكترونية .

- المطلب الاول:العقوبة الجزائية على المستوى الوطني .

- الفرع الاول : عقوبة الشخص الطبيعي.

- الفرع الثاني :عقوبة الشخص المعنوي .

- المطلب الثاني : العقوبة الجزائية على المستوى الدولي .

- الفرع الاول : دور هيئة الامم المتحدة و المجلس الاوروبي.

- الفرع الثاني : الدور العربي .

- الخاتمة

جـــرائـــم النصـــب الإلكتـــــرونـــــي

المبحث التمهيدي

الجرائم الالكترونية و دور الحاسب الآلي فيها

المطلب الأول : تعريف الجريمة المعلوماتية .

- إن تعريف الجريمة عموما ، في نطاق القانون الجنائي الذي يطلق عليه أيضا تسميات قانون الجزائي و قانون العقوبات ، وينهض بكل تسمية حجج و أسانيد القانون يتأس على بيان عناصرها المناط بالقانون تحديدها ، إذا من دون نص على النموذج القانوني للجريمة لا يتحقق إمكانية المساءلة عنها ،سندا الى قاعدة الشريعة الجنائية التي توجب التي توجب عدم جواز العقاب عند انتفاء النص ،وسندا القياس محظور في ميدان النصوص التجريمية الموضوعية ، و هو ما يستوجب التميز بين الظاهرة الإجرامية و الجريمة .-21

و لذلك فان جرائم المعلوماتية تعرف وفق التحديد المقدم بأنها : الأفعال غير المشروعة المرتبطة بنظم الحواسب . و من خلال تعريف الجريمة المعلوماتية هذا بالشكل العام ،يظهر أنها أسلوب غير مشروع معاقب عليه قانونا ،صادرا عن إرادة إجرامية ، محله معطيات الحاسب الآلي و السلوك ، و يشتمل على الفعل الايجابي و الامتناع عن الفعل ، و هذا باعتبار المشروعية تنفي عن الفعل صفة الجريمة ، وهو الفعل المعاقب عليه قانونا لان إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ، و من خلال النص على ذلك حتى و لو كان السلوك مخالفا إلى للأخلاق ، و محل جريمة الحاسب الآلي هو دائما معطيات الكمبيوتر بدلالتها الواسعة. (بيانات مدخلة ، و معلومات معالجة، و مخزنة و البرامج بأنواعها إضافة للمعلومات المستخرجة و المتبادلة بين النظم) -22-

جـــرائـــم النصـــب الإلكتـــرونـــي

جانب من الفقه و المؤسسات ذات العلاقة بالموضوع ، وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل ،وهي تحديدا سمية الدراية و المعرفة التقنينية ،ومن بينها :

تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد لأبحاث و تبنتها الوزارة في دليلها لعام **1979** حيث عرفتها بأنها :

"DAVID THOMPSON"

تعريف الأستاذ- بأنها :

« أية جريمة يكون متطلبها لاقترافها لدى فاعلها المعرفة بتقنية الحاسب الآلي »

تعريف الأستاذ **"STEIN SCHJQLBERG"** بأنها :

«أي فعل غير مشروع تكون المعرفة بتقنية الحاسب الالي اساسية لارتكابه،و التحقيق فيه و ملاحقته قضائيا »-**23**

تعريف الأستاذ- **" SHEKLON J.HEEHT"** بأنها :

«واقعة تتضمن معرفة تقنية الحاسب الالي ، و شخص يتحمل الخسارة ، و مجرم يحصل عن عمد على مكسب من الجريمة يق فيه و ملاحقته قضائيا »-**24**

تعريف الفقيه : **" PARKER DONN . B** في مؤلفه **" FINTING.C.CRIME** بأنها : ((أي فعل معتمد مرتبط باي وجه بالحسابات يتسبب في إمكانية تكبد مجني عليه خسارة أو حصول مرتكبه على مكسب)) و يستخدم لدلالة على الجريمة تعبير إساءة استخدام الحاسب الآلي . **25**

و يعرفها خبراء متخصصون جرائم المعلوماتية ، و الحاسب الآلي من بلجيكا في معرض ردهم على استبيان التعاون الاقتصادي **O E C D**

((كل فعل ، أو امتناع من شانه الاعتداء على أموال المادية و المالية ، و المعنوية يكون ناتجا بطريقة مباشرة ، أو غير مباشرة ، عن طريق تدخل تقنية المعلوماتية)) ، وهذا التعريف تبناه الكثير من الفقهاه و الدارسين للقانون ، لأنه من أفضل التعريفات التي أعطت مفهوما واسعا ، و إحاطة شاملة بقدر الإمكان بظاهرة جرائم التقنية و المعلوماتية ،و هو يعبر عن ابرز صور الجريمة .

كما يعرفها خبراء في منظمة التعاون و التنمية بأنها : ((كل سلوك غير مشروع أو غير أخلاقي ، أو غير مصرح به ، يتعلق بمعالجة الآلية للبيانات او نقلها))**26**

هذا التعريف وضع في نقاش أثناء اجتماع باريس سنة **1983** ضمن حلقة (الإجرام المرتبط بتقنية المعلومات)، كما تبنى هذا التعريف الفقيه الألماني **ULRICH SIEHER** و يعتمد فيه على معايير ، منها "وصف و اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها "

و تعريف كذلك بانها " فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيرا احترازيا "**27**

GOA

كما عرفها مكتب المحاسبة العامة للولايات المتحدة الأمريكية بأنها:

الجريمة الناجمة عن إدخال بيانات مزورة في ، و إساءة استخدام المخرجات ، إضافة إلى افعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر "28

و من ضمن المفاهيم التي تعتمد على اكثر من معيار ، يعرف جانب من الفقه الجريمة المعلوماتية ، و الحاسب الآلي و فق معاير قانونية ، فأولها " تحديد محل الجريمة " و ثانيها "و سيله ارتكابها " ، و في كل المعايير "الحاسب الآلي " له دور أساسي في الجريمة لما يلعبه من دور الضحية ، و الوسيلة في نفس الوقت حسب الفعل المرتكب كما يرى هذا الجانب من الفقه ، ومن هؤلاء :

الأستاذ : **SNEDINGHOLF. THOMAS** في مؤلفه ((المرشد القانوني لتطور و حماية و تسويق البرمجيات)) حيث يعرفها بأنها((أي ضرب من النشاط الموجه ضد نظام الحاسوب او المنطوي على استخدامه)) ، وهذا التعريف ينصب على النشاط الموجه ضد الكيانات المادية إضافة للمنطقية (المعطيات و البرامج البيانات).

و يعرفها الأستاذين : **JACK BOLOGNA ET LINDQUIST RBERT .J**

بأنها : ((جريمة يستخدم فيها الحاسوب كوسيلة ، أو ادات لارتكابها أو يمثل ارغراء بذلك ، او جريمة يكون الحاسب الآلي نفسه ضحيته)) 29

جـــرائـــم النصـــب الإلكتـــــرونـــــي

الأستاذ: جون فوستر **FORESTER** بأنها : " كل أشكال السلوك غير المشروعة الذي يرتكب استخدام الحاسوب " 30

و من الفقه الفرنسي :

تعريف الفقيه **Masse** جريمة المعلوماتية التي يلعب الحاسب الالي دورا أساسيا فيه (استخدام اصطلاحات الغش المعلوماتي) بأنها ((الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح)) ، و يعتبرها من جرائم الأموال .

و يعرفها الفقيهين الفرنسيين : **Lestane/ vivant** بانها :

((مجموعة من الأفعال المرتبطة بالمعلوماتية ، و التي يمكن ان تكون جديرة بالعقاب))31

كما حدد البعض مفهوم الجرائم المعلوماتية من خلال منظارين :

أ) المنظار الاول : عندما يكون المعلوماتية موضوعا للاعتداء ، و تتفق هذه الحالة عندما تقع الجريمة على المكونات المادية للكمبيوتر ، من اجهزة ، و معدات ، و كابلات ، و شبكات ربط و آلات طباعة، و تصوير ، وغيرها او عندما تقع على المكونات المعلوماتية ، او غير المادية . مثل البرامج المستخدمة ، و البيانات ، و المعطيات المخزنة في ذاكرة الكمبيوتر .

ب) المنظار الثاني : عندما تكون المعلوماتية اداة ، ووسيلة اعتداء ، و تحقق هذه الحالة عندما يستخدم الجاني الكمبيوتر كوسيلة لتنفيذ جرائمه ، سواء على الأشخاص ، كانتهاك حرمة الحياة الخاصة أو القتل .33

وقد تقع على الأموال كالسرقة – الاحتيال – التزوير – غيرها ، و يسمى هذا النوع " بالأعمال الإجرامية التي يرتكبها بمساعدة الكمبيوتر " و يصعب كشفها و يصعب كشفها ، لإمكانية ارتكاب من مسافة بعيدة ، و قدرة الجاني على تدمير الأدلة في اقل زمن ممكن ، وهي لا تترك أي اثر مادي .

جـــرائـــم النصـــب الإلكتـــرونـــي

المطلب الأول : دور الحاسب الآلي في الجريمة المعلوماتية

المطلب الثاني :

- يلعب الحاسب الآلي ثلاث ادوار في ميدان ارتكاب الجرائم المعلوماتية ، ودورا رئيسيا في حقل اكتشافها و يكون ذلك وفق الأدوار الأساسية التالية :

- اولا : قد يكون الحاسب الالي هدف للجريمة :

و ذلك في حالة الدخول غير المصرح به إلى النظام ، أو زراعة الفيروسات ، لتدمير المعطيات و الملفات المخزنة أو تعديلها ، كما في حالة الاستلاء على البيانات المخزنة ، أو المنقولة عبر النظم ، ومن أوضح المظاهر لاعتبار الحاسب الآلي هدفا للجريمة هو القيام بتصرفات غير قانونية عندما تكون السرية و السلامة مع توفر قدرة الاعتداء عليها ، أي توجيه هجمات إلى معلومات به ، أو خدمات يقصد المساس بها ، أو محتواها ،أو تعطيل قدرة الاعتداء عليها ، أي توجيه هجمات الى معلومات به ، أو خدمات يقصد المساس بها ، أو محتواها ، أو تعطيل القدرة على كفاءة الأنظمة للقيام بأعمالها

وهدف هذا النمط الإجرامي هو نظام الحاسب الالي ، و بشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام ، دون تحويل ، و دون ان يدفع الشخص مقابل الاستخدام (سرقة خدمات الحاسب الآلي أو وقته)، و غالبية هذه الأفعال الإجرامية تتضمن ابتداء ا من دخول غير المصرح به إلى النظام الهدف ،و التي توصف بشكل شائع في هذه الفترة بأنشطة الهاكرز كناية عن فعل الاختراق .

و الأفعال التي تتضمن سرقة المعلومات تتخذ أشكالا عديدة ، معتمدة على الطبيعة التقنية للنظام محل الاعتداء ، و كذلك الوسيلة التقنية المتبعة لتحقيق الاعتداء ،

فالحاسب الآلي هو مخزن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية و المعلومات العسكرية و خطط التسويق و غيرها . 61

وهذه تمثلا هدفا للعدد من الجهات ، بما فيها أيضا جهات التحقيق الجنائي ، و المنظمات الإرهابية و المخابرات ، و الأجهزة الأمنية ، و غيرها ، و لا يتوقف نشاط الاختراق على ملفات ، الأنظمة الغير الحكومية ، بل يمتد إلى الأنظمة الخاصة التي تتضمن بيانات قيمة ، وبعض طوائف هذا النمط من استهداف الأنشطة للسرقة ، و الاعتداء على الملكية الفكرية ،كسرقة الأسرار التجارية ، و إعادة إنتاج ونسخ الملصقات ، و المصنفات المحمية،وتحديدا برامج الحاسوب،وفي حالات أخرى، فان افعال الاختراق التي تستهدف أنظمة المعلومات الخاصة لها منافع تجارية، أو إرضاء لا طماع شخصية ، كما أن الهدف في هذه الطائفة ، يتضمن أنظمة سجلات طبية ، و أنظمة الهاتف ، و نماذج تعبئة البيانات للمستهلين و غيرها .

-- ثانيا :الحاسب الالي اداة لارتكاب جرائم تقليدية :

تكون في حالة استغلال الحاسب الالي للاستلاء علة الاموال باجراء التحويلات الغير مشروعة او استخدام التقنية في عمليات التزييف و التزوير او استخدام التقنية في الاستلاء على ارقام بطاقات الائتمان و اعادة استخدامه التقني في الاستلاء على الأموال بواسطة ذلك حتى ان الكمبيوتر يستخدم كوسيلة لجرائم القتل من خلال الدخول الى قواعد البيانات الصحية و و العلاجية او تحرير الأجهزة الطبية المخبرية عبر التلاعب برمجياتها او كما في اتباع الوسائل لتاثير على عمل برامج التحكم بالطائرة او السفينة بشكل يؤدي الى تدميرها وقتل ركابها

ثالثا : الحاسب الالي بيئة الجريمة .

و ذلك في حالة تخزين البرامج المفترضة فيه او في حالة استخدام الحاسب الالي لنشر مواد غير قانونية او استعماله ادات اتصال و استخدامه لتخزين صفقات ترويج المخدرات و انشطة الشبكات الاباحية و نحوها .

و التقاط البرامج و المعطيات او أي عنص اخر من النظام المعلوماتي او استخدام او نقل او انتاج برنامج او معطيات او أي عنصر من عناصر النظام دون موافقة صاحب الحق بالإضافة الى تخريب تعييب كل او جزء من نظام المعالجة الالية للمعلومات او عرقلة ادائه لوظيفته او الادخال العمدي للفيروس او الاهمال في النظام المعلوماتي بدون موافقة مالك النظام

جـــرائـــم النصـــب الإلكتـــرونـــي

الفصل الأول : الجرائـم الالكترونية و طبيعتها القانونية

المبحث الأول :ماهية جريمة النصب الالكترونية .

- ان ظاهرة جرائم المعلوماتية ،أو الجرائم التقنية العالمية ،او الجريمة الالكترونية ، أو جرائم أصحاب الياقات البيضاء ،ظاهرة إجرامية مستجدة نسبيا تقع في جانبتاها أجراس الخطر لتنبيه مجتمعات العصر الراهن لحجم مخاطر، وخل الخسائر الناجمة عنها باعتبارها (بيانات،معلومات ،وبرامج بكافة أنواعها)،فهي جريمة تقنية تعتمد على الحاسب الآلي بشكل رئيسي،يقار فيها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية توجه إلى النيل من الحق في المعلومات ، وتطال معطيات الحاسب الآلي المخزنة و المعلومات المنقولة .-1

وتبرز مدى خطورة جرائم المعلوماتية ، من خلال أنها تطال الحق في المعلومات ، و تمس الحياة الخاصة للأفراد و تهدد الأمن القومي ،و السيادة الوطنية و تشيع فقدان الثقة التقنية ، و تهدد إبداع العقل البشري ،وهذا يقودنا إلى إدراك ماهية هذه الجرائم المعلوماتية و تحديد مفهومها القانوني كجريمة ، وتبيان الطبيعة الموضوعية لها ، وان إظهار موضوعها وخصائصها ، و أنواعها ،ودور الحاسب الآلي فيها .-2

---

01 – يونس عرب ،دليل امن المعلومات الخصوصية (جرائم الكمبيوتر و الانترنت)،الجزء الأول إصدار اتحاد المصارف العربية ،2001 .

02-يونس عرب،ورقة عمل مقدمة إلى مؤتمر الأمن العربية ،تنظيم المركز العربي للدراسات و البحوث الجنائية ،أبوظبي ،من 10 إلى 2002/02/12

المطلب الأول: مفهوم جريمة النصب الالكترونية

لقد مسك الفقهاء و الدارسون للجرائم المتعلقة بالمعلوماتية عددا كبيرا من التعريفات ، وهي تتباين ، وتتمايز تبعا لموضوع العلم المنتمية إليه ، وتبعا لمعيار التعريف ذاته ، فاختلف الباحثون في الظاهرة الإجرامية الناشئة من استخدام الحاسب الآلي من الجهة التقنية ، و القانونية ،وقد تعددت المفاهيم المختلفة للجرائم المعلوماتية نظرا لتعقيداتها ، ومحل قيامها ، وارتباطها بالجانب التقني . و اختلافها عن الجرائم التقليدية الموجودة في القانون الجنائي ، و الاجتهاد في ميدان تحديد المفهوم الأساسي و الرئيسي للجريمة المعلوماتية كان من خلال طائفتين رئيسيتين :

فأولها طائفة التعريفات التي تقوم على معيار واحد،وهو قانوني ، وتعريفات بدلالة الموضوع للجريمة ،او السلوك محل التجريم ،أو الوسيلة المستخدمة، وتشمل أيضا تعريفات قائمة على أساس شخصي .

وثانيا طائفة التعريفات القائمة و أنماطها،إلا أن هذه المفاهيم لا يجدر ذكرها دون المرور على التطور التاريخي الذي مرت به جرائم التقنية العالمية أو المعلوماتية ،منذ ظهور الحاسب ،كاختراع تقني احدث ثورة في مجال المعلوماتية ،و أنظمة الحاسب الآلي و الانترنت -03-

---

03 – يونس عرب ،المرجع السابق ، ص 06

جـــرائـــم النصـــب الإلكتـــرونـــي

الفرع الأول : تعريف جريمة النصب الالكترونية.

ان تعريف الجريمة عموما في نطاق القانون الجنائي الذي بطلق عليه أيضا تسميات قانون الجزاء و قانون العقوبات ، و ينهض بكل تسمية حجج و أسانيد قانونية 04 يتأسس علي بيان عناصرها بيان عناصرها المناط بالقانون تحديدها ،إذ من دون نص على النموذج القانوني للجريمة لا يتحقق إمكانية المسألة عنها، سندا إلى قاعدة الشريعة الجنائية التي توجب عدم جواز العقاب عند انتقاء النص ،وسندا إلى أن القياس محظور في ميدان " النصوص التجزيمية الموضوعية " و هو ما يستوجب التميز بين الظاهرة الإجرامية و الجريمة

ولذلك فان جرائم المعلوماتية تعرف وفقا للتحديد المقدم بأنها :" الأفعال الغير مشروعة المرتبطة بنظم الحاسوب ".

- يعرف النص بأنه (الاستلاء علي حيازة مال الغير كاملة بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال) ، كما عرفه بعض الفقه بأنه :

(الاستلاء بطريقة الاحتيال على شيء مملوك للغير بنية تملكه)، أو هو (الاستلاء على منقول مملوك للغير بخداع المجني عليه و حمله على تسليمه)-01-

و يتميز النصب عن السرقة – رغم تماثلهما في الموضوع و الغاية – في الاستلاء على الحيازة الملكية للمال يتم في السرقة بغير رضا حر من المجني عليه سواء كان مالكا أو حائزا لهذا المال ، بينما يحصل في النصب بتسليم المشتبه بالاحتيال -02- عن طريق استعمال الجاني لإحدى الطرق الاحتيالية التي ينص عليها نص التجريم – عادة – في جريمة النصب.

جـــرائـــم النصـــب الإلكتـــرونـــي

الفرع الثاني : نطاق جريمة النصب الالكترونية.

- إذا كانت جرائم الانترنت تتميز بطبيعة خاصة و هو صعوبة اكتشافها وضبط مقترفيها على النحو الذي رأيناه عند الحديث عن طبيعة هذه عند الحديث عن طبيعة هذه الجرائم فهي بالإضافة إلى تلك الطبيعة الخاصة تتميز أيضا بأساليب خاصة عند اقترافها . فهي أساليب يغلب عليها الطابع الفني و التقني بعكس الجرائم التقليدية التي يغلب عليها الطابع اليدوي .

فمرتكبي هذه الجرائم استوعبوا جيدا تكنولوجيا الحاسب الآلي و استغلوا خبراتهم المكتسبة منها في تطوير الوسائل التقليدية لارتكاب او ابتكار و سائل جديدة غير معروفة لكي تناسب هذا التطور التكنولوجي الهائل في مجال الحاسب لاستخدامها للاعتداء على الحاسب و مكوناته سواء كانت مادية أو غير مادية ، و التالي تختلف هذه الأساليب باختلاف عنصر الحاسب الذي يكون مكلا للاعتداء .

ويغلب على هذه الوسائل الطابع التقليدي على أساس أنها ترد على معدات الحاسب المادية من اسطوانات و شرائط ممغنطة و ما يحويهما من برامج و معلومات أو بيانات معالجة اليكترونيا.

و من الأساليب المتصورة ممارستها لارتكاب جرائم تكون معدات الحاسب المادية موضوعا لها ،جميع أساليب السرقة و النصب و الإتلاف و غيرها من الأساليب التي تضر أو تهدد بالضرر أموال الغير سواء كانت أموالا خاصة بالأفراد او خاصة بأموال الدولة .

مثل السرقة الدعامة المادية و محتويها من برامج و بيانات ، أو سرقة البطاقة الممغنطة التي تستخدم لسحب النقود من الحاسب او الحصول على سلع و خدمات

جـــرائـــم النصـــب الإلكتـــــرونـــــي

من الشركات و التجار أو إحدى الجهات التي تقدم خدمة مقابل مثل المواصلات و التليفونات . و من أمثلة الأساليب المستخدمة في ارتكاب جرائم الإتلاف مثل إتلاف البرامج و البيانات باستخدام عدة وسائل تقليدية منها :

تدمير الدعامات التي تحتويها سواء بإحراقها او ضغطها أدوات ثقيلة أو تفجيرها باستخدام القنابل المتفجرة أو سكب سوائل ساخنة على الأجزاء الحساسة من الحاسب او لصق ورقة (صنغرة) على أجزاء من البطاقات المثقبة لتخريب الأجهزة القارئة لها أو إلقاء رماد السجائر المشتعلة على الشرائط و الاسطوانات الممغنطة .هذه الأساليب تتدرج من المعرفة الفنية البسيطة إلى المعرفة الفنية المتقدمة جدا . و من الأساليب التي لا تطلب سوئ معرفة فنية متواضعة تصل إلى

حد مجرد سلوك مادي ذلك الذي يقتصر على مجرد الاطلاع البصري للمعلومات التي قد تظهر على شاشة الحاسب أو القيام بالتصنت عليها في حالة تجسدها في صورة سمعية أو عن طريق الاستعانة بوسيط يعمل على تكبير الصوت الصادر من هذا الحاسب.

و هنا يحصل الجاني على ما يريده بطريق مباشر -01-

أما الأساليب التي تتطلب معرفة فنية عالية المستوى فهي تلك الحالات التي يستطيع فيها الجاني من خلالها القيام بعملية ما يسمى (السطو المسلح الالكتروني) و الذي يكون الهدف منه هو التقاط أو تسجيل المعلومات و البيانات المعالجة الكترونيا و هي في مرحلة انتقالها و بثها من الحاسب إلى نهاية طرفها بواسطة أجهزة شبكة اتصالات بعيدة" **LEMATIQUE** " و المعالجة

جـــرائـــم النصـــب الإلكتـــرونـــي

عن بعد "TELERAITMENT " و يمكن عرض بعض هذه الوسائل فيما يلي :

- أ- التقاط المعلومات التي توجد مابين الحاسب و النهاية الطرفية :

و يحدث هذا الالتقاط بواسطة توصيل خط تحويل يعمل على تكبير الذبذبات الالكترونية و إرسالها إلى نهاية الطرفية التي تقوم بعملية التجسس و من الممكن أن يحدث ذلك أيضا باستخدام جهاز مرسل صغير يمكنه نقل البيانات عن بعد .

و يمكن التقاط كذلك عن طريق وضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية و بالتالي يحدث التقاط الإشاعات العابرة عن طريق النقل الجوي للمعلومات عند بثها بالقمر الاصطناعي و احتجاز مضمونها .

-ب- التوصيل المباشر بواسطة خط تليفوني :

و يتم ذلك بوضع مركز تنصت يجعل من تسجيل الاتصالات أمرا يسيرا ، كما يمكن الاستعانة أيضا بوضع ميكروفونات صغيرة لأدائها.

-ج- التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي :

و تكمن خطورة هذه الوسيلة في أنها يمكن أن تؤدي إلى إعادة تكوين خصائص المعلومات التي تبث و تنقل من خلال الأنظمة المعلوماتية و هذا لا يحتاج تسجيل الإشعاعات الصادرة من الحاسب كما لا يحتاج إلى حل شفراتها.

-د- التدخل الغير مشروع في نظام الحاسب بواسطة طرفية بعيدة :

جـــرائـــم النصـــب الإلكتـــرونـــي

وتعد هذه الوسيلة الفنية من اخطر الوسائل التي يلجا إليها المجرم المعلوماتي إذ يكون بإمكانه نسخ أو تدمير بعض البيانات و المعلومات بكل يسر و لا يحتاج إلا لمجرد الحصول على حاسب ألي - ميكروي- و مودم مع ضرورة التعرف على كلمة السر او مفتاح شفرة النظام للحاسب المجني عليه .

و هكذا فان المجرم المعلوماتي او مرتكبي جرائم الانترنت لم يكتفوا بالوقوف مذهولين امام تكنولوجيا الحاسب و إمكانيته الفائقة التي بلغت حد الخيال من قدرة على التخزين و الاسترجاع بسرعة فائقة بالإضافة إلى دقتها و مرونتها في التشغيل -01-بل نجد هؤلاء وقد استوعبوا هذه التكنولوجيا بطريقة متقدمة جدا و استغلوا خبراتهم المكتسبة منها في تطوير الوسائل التقليدية لارتكاب و ابتكار وسائل جديدة و غير معروفة للجريمة تتناسب مع هذا التطور التكنولوجي الهائل .انه صراع الأبدي بين الخير و الشر .

جـــرائـــم النصـــب الإلكتـــرونـــي

المطلب الثاني : أركان و تصنيفات جريمة النصب الالكترونية

الفرع الأول : أركانها :

الركن المادي : يتمثل في سلوك إرادي تترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سببية مادية ففيها بتثمل هذا الركن في جرائم الانترنت ؟

باستقرائنا للتعريف نستنتج انه من سلوك إرادي ، و نتيجة إجرامية و رابطة سببية .

ـ أ ـ **سلوك إجرامـي:** يعتبر السلوك الإجرامي المادي عبر الانترنت محلا لجملة من التساؤلات لا سيما فيها ما يتعلق ببدايته او الشروع في ارتكاب الجريمة ،و هو يختلف عما هو الحال في العالم المادي ، و ذلك لان ارتكاب الجريمة عبر الانترنت تحتاج بالضرورة إلى منطق تقني . أي أنها تتم عبر الانترنت أو باستخدام المعالجة الآلية للبيانات ، كما أنها تحتاج إلى ممارسة نشاط تقني محدد يتمثل في استخدام الحاسوب و الانترنت .

و من امثلة السلوك المادي في الجريمة عبر الانترنت :المصرفي الذي ينوي سرقة مبلغ من المصرف الذي يعمل فيه باستخدام الانترنت ،ثم الدخول على شبكة المصرف عبر مزودات مجهولة يمكن الاستعانة من خلالها ببرمجيات اختراق موضوعية على مواقع هكرة يتم تجديدها باستمرار .

ففي هذا المثل فان المصرفي المذكور يمارس النشاط المادي للاختلاس عن طرق الحاسوب و الانترنت .

- ب – **النتيجة الإجراميـة:** يعد هذا العنصر احد عناصر الركن المادي في الجريمة إلى جوار السلوك الإجرامي و علاقته السببية . و تثير مسالة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة من أهمها : تحديد هل جريمة مرتكبة سلوكا و نتيجة في العالم الافتراضي أم أن هناك امتدادا للنتيجة ليتحقق منتهاها في العالم المادي ؟.

- ج – **علاقة السببية :** هي العنصر الثاني من العناصر التي يتكون منها الركن المادي في الجريمة ،و يجب لقيام جريمة الانترنت ، ان تكون هناك رابطة مادية ما بين السلوك المادي و النتيجة الإجرامية المتحققة . فمثلا يجب لتحقيق جريمة انتهاك الحق في الخصوصية عبر الانترنت أن يكون هناك دخول على الانترنت باستخدام حاسوب عامل و القيام بالاختراق الخوادم المختلفة في مسارها ،ثم بعد ذلك التعدي على خصوصية موقع ما . و كذلك يمكن اعتبر علاقة السببية قائمة بمجرد ثبوت الضرر في مجرد البث . و هذا ما قررته محكمة استئناف مقاطعة "COLOMBIA BRITISH " الكندية في إحدى أحكامها.

أن كل جريمة تحدث باستخدام الانترنت انما تحدث كلها او بعضها حسب الأحوال في العالم الافتراضي . و إذا كان النشاط المادي يحدث كله في العالم الافتراضي و كذا العلاقة السببية ، فان النتيجة الإجرامية لها كيان منفصل لكونها تحدث بشكل انقسامي ما بين حدوثها في العالم المادي جزئيا او كليا ، و من أهم الآثار المترتبة عنها أنها تؤثر على قواعد الاختصاص في الدول . فمثل الولايات المتحدة الأمريكية ، جعلت النتيجة الإجرامية القضاء الأمريكي – و لاية " TENNESSEE

في قضية توماس يعترف باختصاص باختصاص القضاء لمجرد تحقق النتيجة في الولاية المذكورة و بغض النظر إذا ما كانت كاليفورنيا تجرم مثل هذا العمل 02

وهذا و تجدر الإشارة إلى أن جرائم الانترنت تنتشر فيها فكرة النتيجة المحتملة ،و ذلك راجع الى طبيعة النشاط التقني الذي قد يترتب عليه نتائج عدة فمثلا :من قد يقصد القرصنة و يتحقق معها انتشار الفيروسات ،فان ذلك يعتبر نتيجة محتملة لتشمل الجريمة التي ليس لها منحنة على الإطلاق أي الحالة التي لا يكون فيها للضحية على الإطلاق أي الحالة التي لا يكون للضحية و جود مادي و إنما رقمي فقط – و هو ما يقرره في القسم (ط).2422. sec 184 sl ،و جسدت هذه الحالة في قضية V.ROOTS U S A أمام القضاء الأمريكي ،

و التي حسم فيها موضوع التوسع في الاحتمال- 01-

الركن المعنوي : و يطلق عليه الركن الأدبي أو الشخصي ، و هو المسلك الذهني أو النفسي للجاني ، و الركن المعنوي في جرائم الانترنت له ثلاث صور :

- أ- **العمد** : لما كانت جرائم الانترنت من جرائم التقنية العالمية ،التي تتطلب المعرفة و التعليم التخصصي من قبل من يمارس هذا النوع من وسائل الاتصال فانه كان من التصور غالبا عدم وقوعها الا في صورة واحدة و هي صورة العمد – أي ان مرتكب تلك الجريمة قد خطط و دبر لارتكاب بها سواء من اجل الحصول على معلومة أو لاختراق شبكة حاسوب أخر . فمثلا : جريمة القذف و السرقة تتطلب من الفاعل إرادة ارتكاب السلوك وتحقيق نتيجة ، و قد يكون الجاني هنا عاما أو خاصا.01

و تجدر الإشارة إلى أن القضاء الأمريكي يقع في حيرة تقرير مدى إمكانية امتداد البحث في الركن المعنوي ،و تحديدا العمد إلى الجرائم الأخرى ذات الامتداد

جـــرائـــم النصـــب الإلكتـــرونـــي

بالجريمة الأولى في جرائم الانترنت ، و المتمثلة في جريمة الاختراق .إذ أن المخترق قد يرتكب الجريمة لمجرد الاختراق ،و في هذه الحالة نكون أمام جريمة عمديه في صورة قصد عام ، إلا انه في اغلب الأحيان ،يتعدى ذلك الى أكثر من مجرد الاختراق كما لو كان غرضه بعيدا عن ذلك كالتعدي أو الالفاء أو التعدي علة الحق في الخصوصية.

و في هذا نجد اتجاه في القضاء المقارن يعتبر أن الجريمة الثانية هي جريمة موضوعية لا تحتاج لركن معنوي ،ولقد برزت الفكرة اول مرة في قضية الولايات المتحدة الأمريكية ضد موريس -01- و الذي أسس دفاعه على انتقاء الركن المعنوي و بالتالي العمد لديه ،ولقد امتد هذا الخير إلى استئناف ، حيث وضعت المحكمة هذا الجدل في الصيغة الاستفهامية التالية : " هل يلزم ان يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول ، بحيث تثبت نية المتهم في الولوج إلى الحاسب فيديرالي ،ثم يلزم إثبات نية المتهم في تحدي خطر استخدام نظام المعلومات في الحاسوب .و بالتالي تحقيق خسائر ، و مثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح "

- ولقد ذهبت المحكمة في ردها على هذا إلى التأكيد على التفسير اللغوي لتشريع 1984 و تعديله في عام 1986 ، و هذا ما جعلها تؤكد على الركن المعنوي الواجب توفره في جريمة موريس إنما يتأسس على العمد و الذي يتحقق بالإرادة في جريمة الولوج

- اما القضاء الفرنسي ، فعلى غرار مثيله الأمريكي ، نجد ان منطق سؤ النية يكتساح النصوص التى تطبق بشان جرائم الانترنت مثلما مقرر في المادة 15 و

226 عقوبات فرنسي جديد ، حيث يشترط سوء النية حيث و جود عدوان على البريد الالكتروني 01

- **ب – القصد المتعدي** : يمكن ان يتوافر القصد المتعدي في جرائم الانترنت ،و مثال ذلك : الحالة التي يكون فيها الولوج بقصد اللهو في حركة أو مسار القطارات ، فيخرج الأمر عن السيطرة و يتم تدمير بيانات تحريك القطارات عبر الحاسوب و بالتالي تحث كارثة تكون نتيجتها خسائر مادية و بشرية كبيرة . او كمن يرسل فيروسا عبر البريد الالكتروني إلى احد الأفراد بقد الانتقام منه دون ان يكون على دراية بالوسيط الخادم و مدى إمكانية حدوث انتشار الفيروس في ذلك الاخير . فيتسبب في اجتياح الفيروس في كل حاسوب مرتبط بذلك الخادم . فهنا قصد الشخص قد تجاوز ما كان يهدف إلى تحقيقه 02

- **ج – الخطأ الغير العمدي :** للخطأ مكانة في تطورات الركن المعنوي في جرائم الانترنت ،إذ أن هناك الجرائم تتم نتيجة لخطا لم يكن مقصودا .كتدمير أجهزة المؤسسة نتيجة إفراط من قبل الموظف المسؤول الذي يستخدم جهاز الحاسب العائد لها بعمليات لحساب الخاص معتمدا على مهاراته في تجنب متاعب الفيروسات . او كاستخدام القرص المرن في اجهزة هذه المؤسسات و نقل فيروسات لها مما ينجم عنه تدمير بشك جزئي أو كلي . و تجدر الإشارة إلى أن المشرع الأمريكي يتجه إلى اطغاء الطابع الخطأ على الجريمة الثانية التي تتجاوز جريمة الدخول العمدي إلى نظام حاسوب عامل لدى فيدرالية أو مالية 01

الفرع الثاني : تصنيفات جريمة النصب الالكترونية .

- لعل أهم أنواع الطرق الاحتيالية المستخدمة في النصب المعلوماتي هو التلاعب المعلوماتي و الذي يقصد به(التلاعب بالبرامج و البيانات للتغير فيها بما يترتب عليه إيهام المجني عليه بصحتها بما يجعله يسلم بها)03

فجريمة النصب المعلوماتي تبدو من الوضوح بمكان في الحالات التي يتوصل فيها شخص عن طرق التلاعب في منظومات المعالجة الالكترونية للبيانات إلى الاستلاء على مال الغير ،كان يتلاعب البيانات المدخلة او المخزنة داخل الحاسب أو في برامجه لاستخراج شيكات تدفع له ،او لتحويل كل او بعض أرصدة الغير او الفوائد المستحقة لهم إلى حسابه ،أو التلاعب في الإشارات الالكترونية المرتدة من الحاسب المركزي إلى جهاز المصرف الآلي للنقود لاختلاس أموال من أرصدة العملاء أو من رصيد جهاز المصرف نفسه دون التأثير في بيانات الحاسب المركزي و في حسابات العملاء 04

كما يمكن أيضا استخدام الحاسب الآلي بهدف التزوير و التزييف ،و حالة الفواتير المزورة هي المثال الواضح على ذلك ،و في الواقع فانه يوجد في هذه الحالة مستندات من مستخرجات ناتجة عن الحاسب الآلي تكون ذات طبيعة من شانها إيهام بوجود أموال و وهمية ، و ذلك بسبب إعدادها بطريقة الكترونية و حسابية من شانها الإيحاء بوجود قوة و أموال ،ويرجع ذلك للثقة التي يعطيها الأشخاص للوثائق المستخرجة من الحاسبات الآلية . 01

جـــرائـــم النصـــب الإلكتـــرونـــي

- كما يمكن كذلك استخدام الحاسب الآلي في ارتكاب جرائم النصب المعلوماتي عن طريق إحدى الوسائل التدليسية (كاستخدام صفة غير صحيحة أو اسم كاذب) و الدليل الواضح على ذلك هو استعمال الكارت الائتماني أو البطاقة البنكية الممغنطة باسم كاذب أو لصفة كاذبة 02 ،و تعتبر الجرائم المتعلقة بإساءة استخدام البطاقات البنكية الممغنطة أو الكروت الائتمانية الممغنطة من الجرائم المقلقة ،خصوصا من المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور و الحداثة ،و تمنح فيها البطاقات الائتمانية ويستخدم كذلك بأقل قدرة ممكنة من الإجراءات.

ففي وقتنا الحاضر أصبح فتح الحساب البنكي او الائتماني في اغلب دول العالم من الحقوق التي اعترف بها القضاء للناس كافة ، بل ان فتح حساب بنكي أصبح من الأمور الواجبة (كما في حالة لو كان الموظف أو العامل يحصل على مرتبة أو اجر من خلال احد البنوك أو المصارف الآلية الائتمانية) وقد نتج عن ذلك ان أصبح الحصول على إحدى البطاقات البنكية من الأمور المرتبطة بأحقية الفرد في فتح حساب بنكي . و منح البطاقات الائتمانية يتم من قبل البنك او المؤسسة الائتمانية باسم الشخص و إن صغرت فيه و ودائعه ، و كما إن دفاتر الشيكات يتم الحصول عليها و استخدامها ، فكذلك الحال بالنسبة للبطاقات الائتمانية او البنكية ، فهي تستخدم كذلك بنفس السهولة في تسوية المدفوعات التي يقوم بها الفرد نظير الشراء و الحصول على الخدمات المختلفة من التجار و غيرهم ، و مهما كانت قيمة هذه المدفوعات سواء قلت أم كثرت .

و تتعدد صور إساءة استخدام البطاقات البنكية ، و لعل من أشهر تلك الصور

جـــرائـــم النصـــب الإلكتـــــرونـــــي

(جرائم استخدام البطاقات المسروقة او منتهية صلاحية ،و جرائم تزوير البطاقات الحقيقية ، و صورة قيام صاحب البطاقة ذاته بسحب مبالغ نقدية اكبر من المبلغ المسموح له بسحبها من آلة التوزيع الآلي للنقود مستغلا بذلك الثغرات التي مازلت هذه الآلات تعاني منها حتى ألان) ، و تتنوع كذلك طرق تنفيذ جريمة سحب مبالغ نقدية اكبر من المبالغ المسموح بسحبها من آلة الصرف الآلية للنقود ، فبعض حاملي البطاقات البنكية يكتفون باستخدام تلك البطاقة في سحب مبالغ أكثر مما ينبغي لهم سحبه . و البعض الأخر – و هم الأكثر خطورة – يقومون بإبلاغ البنك بضياع بطاقتهم الائتمانية – دون أن يكون ذلك صحيحا – ثم يقومون على الفور ، وقبل ان يقوم البنك بالتحفظ على أموالهم و حمايتها ،باستخدام البطاقة البطاقة المبلغ عنها ضياعها في سحب مبالغ معينة من حساباتهم البنكية ، بحيث يعطوا انطباعا بان السارق البطاقة او من و جدها هو الذي قام بسحب تلك المبالغ النقدية . 01

جـــرائـــم النصـــب الإلكتـــرونـــي

المبحث الثاني :دوافع ارتكاب جريمة الالكترونية .

المطلب الاول : الأسباب الدافعة لارتكاب جريمة النصب الالكترونية

الفرع الأول : تعريف جريمة النصب الالكترونية.

1- غالبا ما يرتكب المبرمج جرائم الكمبيويوتر نتيجة إحساسه بالقوة و الذات و بقدرته على اقتحام النظام فيندفع تحت تأثير الرغبة القوية في تحقيق الذات من اجل تأكيد قدرته الغنية على ارتكاب احد جرائم الكمبيوتر وقد يكون الهدف من ارتكاب الجريمة الحقد و الكراهية فقد دفع الانتقام بمحاسب شاب إلى أن يتلاعب في برامج الكمبيوتر الخاص بدعريم الشركة التي يعمل بها حيث برمجها على ان تخترق كل البيانات الخاصة بدعريم الشركة بعد مضي ستة أشهر من تاريخ تركه العمل وحدث ما أراد ، فبعد ان ترك العمل وبعد مرور ستة أشهر اختفت البيانات الخاصة بدعريم الشركة نهائيا على جهاز الكمبيوتر .

2- وقد يكون دافع الشخص لمرتكب جرائم الكمبيوتر دافع مذهبي أي يقوم به الشخص لعالم الجماعة التي ينتمي إليها و من أمثلة ذلك ما تقوم به جماعات الألوية الحمراء في ايطاليا حيث تعرضت عدة وزارات و جماعات و مؤسسات مالية في ايطاليا لهجوم من جماعة الالوية الحمراء عن طرق تدمير مراكز المعلومات الخاصة بها ولقد أصدرت هذه الجماعة منشور بتحديد أهداف هذه الجماعة في عام 1998 شرحت فيه إستراتيجيتها و أغراضها و أهدافها و يبدأ المنشور بتحديد أهداف هذه الجماعة و هي مهاجمة الهيئات متعدد الجنسيات التي ترمز للامبريالية و إعادة توزيع الحركة الثورية بتنظيمين الحزب الشيوعي المحارب و يحصر بالهيئات متعدد الجنسيات تلك الموجودة بالولايات المتحدة

الأمريكية و يعتبرون الكمبيوتر سلاح خطير ضد الإرهاب بفضل قدرته على حفظ المعلومات

3- بالإضافة إلى المؤشرات الشخصية فمن المعلوم أن البرامج و المعلومات المخزنة داخل جهاز الكمبيوتر لها قيمة مادية كبيرة بغض النظر عن قيمة المادة المخزونة داخل هذا الجهاز سواء كانت - سيدي – او ديسك – فهذه البرامج او المعلومات ذات قيمة مالية مرتفعة لذلك تسعى بعض الشركات التجارية و الصناعية الحصول على هذه البرامج و المعلومات عن طريق سرقتها بواسطة القائمين على أجهزة الكمبيوتر و غالبا ما يقوم بذلك مقابل رشوة الموظف أو إغرائه أو خداعه أو استغلال نقطة ضعفه .

4- الولع في جمع المعلومات و تعلمها فهناك من يقوم بارتكاب جرائم الكمبيوتر بغية الحصول على الجديد في المعلومات ، فالقرصان يكرس كل جهده من تعلم كيفية اختراق المواقع و غالبا ما تكون مجموعة تتعامل مع بعضها البعض .

5- حب المغامرة و الإثارة جاء على لسان احد القراصنة في كتاب قراصنة أنظمة الكمبيوتر للمترجمة أمنة يوسف علي –ص 11 ((كانت القرصنة هي النداء الأخير الذي يبعثه ماغي فقد كنت أعود إلى البيت بعد يوم عمل سهل المدرسة و أدير تشغيل جهاز الكمبيوتر و أصبح عضوا في نخبة قراصنة الأنظمة و كان الأمر مختلفا برمته حيث لا وجود لعطف الكبار و حيث الحكم هو لمعرهبتك فقط في البدء كنت أسجل أسماء في لوحة الشرات الخاصة حيث يقوم الأشخاص الآخرين الذين يفعلون مثلي بالتردد على هذه الموقع ثم أتصفح أخبار المجتمع و أتبادل المعلومات مع الآخرين في جميع أنحاء البلاد وبعد ذلك ابدا عملية القرصنة الفعلية و خلال ساعة واحدة بيداء عقلي بقطع مليون في الساعة و أتنقل

جـــرائـــم النصـــب الإلكتـــرونـــي

من جهاز كمبيوتر إلى أخر محاولا العثور على سبيل الحصول محاولا العثور على سبيل للوصول إلى هدفي و كان يرافق ذلك تزايد سرعة الأدرينالين و كل خطوة اخطوها كان يمكن ان تسقطني بيد السلطات كنت على حافة تكنولوجيا و اكتشاف ما ورائها و اكتشاف الكهوف الالكترونية التي لم يكن من المفترض وجودي بها .

الفرع الثاني :الدوافع المادية

- **تحقيق مكاسب مالية** : أحيانا يكون الهدف من ارتكاب جريمة الكمبيوتر الحصول على ربح مالي عن طريق المساومة على البرامج او المعلومات المتحصلة بطريقة الاختلاس من جهاز الكمبيوتر او عن طريق سحب الي مزورة او منتهية الصلاحية ولد أشارت مجلة Sécurité informatique على لسان الأستاذ Parker وهي مجلة مختصة في الأمن المعلومات أن 43% من الحالات الغش المعلن عنها بوشرت من اجل اختلاس أموال 63 % من اجل سرقة 19% من أفعال الإتلاف 15% سرقة وقعت الآلة أي الاستعمال غير المشروع للكمبيوتر لأجل تحقيق منافع شخصية .

المطلب الثاني : خصائص مرتكب جريمة النصب الالكترونية

جـــرائـــم النصـــب الإلكتـــــرونـــــي

الفرع الأول : صفات المجرم المرتكب جريمة النصب الالكترونية.

1- يتميز بالذكاء : ان الجريمة الالكترونية تتطلب من المجرم الذي يقوم بجريمة النصب الالكتروني نوع من الذكاء المرتفع الذي يساعده في هذه العملية من اختراقات و قرصنة و الذي يزيد تعلمه لاختراقات جديد مما يستعمل ذكائه في عمليات صعبة ممكن ان تسمح بالشراكات و المؤسسات و حتى امن الدولة و التجسس لعالم دولته أو لدولة أخرى.

2- لا يميل لاستعمال القوة و العنف : فالمجرم في جريمة النصب يكون لا يميل إلى القوه و العنف و المشاجرات مع الأشخاص بل يميل السير الحسن لأموره و تعامله مع مجتمعه .

3- يتميز بأنه اجتماعي: فهو لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به و مع توافقه مع أفراد و التعامل الحسن و السير الجيد لأمور مما يزيد من تكيفه مع المجتمع مع توافر الشخصية الإجرامية لهذا الشخص الذي لا يظهرها امام مجتمعه بل يريهم فقط الوجه الجيد و الحسن و الطيب

- فالذكاء في نظر الكثيرين ليس سوى قدرة على التكيف و لا يعني التقليل من شان المجرم الالكتروني و هذا ما يزيد من خطورته

الفرع الثاني : أنواع المجرمين مرتكبي جرائم الكمبيوتر .

جـــرائـــم النصـــب الإلكتـــــرونـــــي

1- المجرمين الهواة : و يطلق عليه صغار النوابغ المعلوماتية و غالبا ما يكونوا من طائفة الشباب الذين لديهم معلومات لا باس بها عن أنظمة تشغيل الكمبيوتر و غالبا ما يرتكبوا هذه الجرائم عن طرق الصدفة البحث أي ان الدافع الإجرامي لم يكن متوفر لديهم عند اتصالهم بجهاز الكمبيوتر .

2- المجرمين المحترفين:و هذه الطائفة من المجرمين هم أكثر خطورة من الطائفة الأولى و يحدثون أضرار كبيرة في البرامج و المعلومات .

- هناك دراسة أجراها معهد **STAND- FORD-RESEARCH**

تبين الجرائم المرتكبة من الأشخاص مستخدمين الكمبيوتر و هو على الترتيب 25 % من الجرائم التى يرتكبها المحلل ثم ياتي بعده المبرمج بحوالي 18 % ثم الصراف 16 % ثم الشهي الأجنبي على المنشاة 12 % و أخيرا 11 % يرتكبها المشغل.

جـــرائـــم النصـــب الإلكتـــرونـــي

الفصل الثاني :الحماية الجنائية للتعاملات الالكترونية

- سنتناول في هذا الفصل الحماية الجنائية 908 في التعاملات الالكترونية و الذي سنقسم فيه هذا الفصل إلى مبحثين المبحث الأول سنتطرق فيه إلى الحماية الجنائية الموضوعية و الإجرائية أم المبحث الثاني سنذكر الجوانب الإجرائية للتعاملات الالكترونية على المستوى الوطني و على المستوى الدولي مبرزين أهمية الدور العربي في هذا المجال من الجريمة .

فيعتبر الكمبيوتر الوسيلة الأساسية للقيام بهذه التعاملات الالكترونية ، فمن الطبيعي ان يحتاج هذا النظام

– الكمبيوتر- إلى حماية و قد أدركت كثير من التشريعات المقارنة هذه الحقيقة ،فأدخلت نصوص خاصة لحماية هذا النظام من صور المساس به و المعلومات المتواجدة بداخله ،فلم يعد التشريع الأمريكي على سبيل المثال محل للمناقشة حول اذا كان تدخل المتهم في كمبيوتر غيره و نسخه لملفاته او النصب عليه مشكلا لجريمة و لا كن الأمر أصبح مستقرا، أن ذلك يشكل جريمة من جرائم الكمبيوتر تتمثل بالتدخل بقصد الغش

المبحث الأول :الحماية الجنائية الموضوعية و الإجرائية لجريمة النصب الالكترونية

ان الحماية الجنائية للتعاملات الالكترونية سواء من الناحية الموضوعية أو الجزائية أو كانت هذه الحماية وفقا للقواعد العامة أو بنصوص خاصة فان الأثر الكبير يكون على الجانب الإجرائي أي في مرحلة المحاكمة و ما يتنج عن هذه الحماية من فرض عقوبات او غرامات مالية على المجرمين القائمين بهذه الجرائم و ما ذاك إلا حماية للتعاملات الالكترونية و فرض الرقابة و توقيع الجزاء على المخالفين

المطلب الأول: الحماية الجنائية الموضوعية للتعاملات الالكترونية .

تسري كثيرا من القواعد العامة في قانون العقوبات على التعاملات الكترونية لتمد مظلة الحماية لتلك التعاملات و نقصد بالقواعد العامة بقانون العقوبات تلك التي تتعلق بأنواع تجريم السرقة و النصب و تلك التي تتعلق بتزوير المحررات لذلك سوف نتناول أبعاد هذه الحماية التي تقررها القواعد العامة في قانون العقوبات بالنسبة لطرفي التعاملات الالكترونية و هما المستهلك و التاجر و كذلك الوسطاء بينهما كالبنوك و المصارف لبيان ما إذا كانت القواعد العامة كالسرقة و النصب تسري على التعاملات

الالكترونية ، اذا كانت القواعد العامة في قانون العقوبات تكفي لتوفير الحماية الجنائية فقد أدركت التشريعات عديدة هذه الحقيقة عندما أفردت نصوص خاصة لحماية التعاملات الالكترونية و حماية أطرافها قد تمثل ذلك في إيراد نصوص خاصة لحماية النظام كوسيلة للتعاملات الالكترونية بالإضافة إلى حماية البنك الذي يعتبر كوسيط في مجال التعاملات الالكترونية بالإضافة الى وضع نصوص خاصة لتنظيم مسؤولية مزودي الخدمات باعتبار ان عملهم ضروري من الناحية الفنية لإتمام الاتصالات الالكترونية

الفرع الأول :الحماية الجنائية في التعاملات الالكترونية في ظل قانون العقوبات وفقا للقواعد العامة

1- صعوبة القول بسريان جرائم الأموال على المعلومات الالكترونية :

من المقرر ان جرائم الأموال في التشريعات المختلفة تقع على مال منقول مملوك للغير فتنص المادة 311 م ق ع المصري على ان ((كل من اختلس منقول مملوك للغير فهو سارق)) و بالمثل فان المادة 341 من نفس القانون في خصوص خيانة الأمانة تعاقب كل من اختلس او استعمل او بدد مبالغ او امتعة او بضائع او نقود او تذاكر كما تعاقب المادة 363 في شان النصب كل من توصل الى الاستلاء على نقود او عروض او سندات دين او سندات مخالصة او أي متاع منقول فاذا كانت البيانات مسجلة على دعامة مادية ((ديسك او اسطوانة)) فلا تثار صعوبة قانونية ذلك لان الدعامة تعتبر مال منقول يحميه التجريم في جرائم الأموال فعلى خلاف المعلومة تكتسب الدعامة طابعا

جـــرائـــم النصـــب الإلكتـــــرونـــــي

ماديا محسوسا تطبيقا لذلك قضي بوقوع جريمة السرقة إذا كان محلها دعامة مسجلة عليها بيانات ام في الفرض الذي يكون فيه للمال طبيعة معنوية وليس مسجلا على دعامة مادية ان صعوبة قانونية تثارحول حمايتها بالتجريم الوارد في جرائم الاموال وذلك لشك حول توافر الشرط المسبق للجريمة الالكترونية قد كان ذلك سببا في ان بعض الاحكام استبعدت وقوع جرائم الاموال اذا كان محل الأفعال أموالا ذات طبيعة معنوية و بناءا عليه فان برامج التلفزيون لا تصلح لان تكون محل للسرقة و بذلك قضت محكمة استئناف باريس في احد أحكامها التي لم تقم التماثل بين سرقت التيار الكهربائي و فك شيفرات البرامج ذلك لان التيار الكهربائي يحتاج الى دعامة لينتقل من خلالها ، بينها يرد فك الشيفرا على موجات عبر الأثير و بالتالي ليس لها أي دعامة مادية و تقول المحكمة سرقت الكهرباء و سرقة البيانات المعلوماتية تفترض و جود دعامة مادية أي كانت الأمر الذي لا يتوافر في موضوع الدعوة من هنا فإنها انتهت إلى عدم انطباق جريمة السرقة على المتهم الذي قام بفك شيفرت البرامج المشفرة فجريمة التقليد بالنسبة للبرامج إذا توافرت لهذه الأخيرة الشروط الواجب توافرها مثل الأصالة (إذا قام المتهم بتخزين تلك البرامج او نسخها على دعامة جديدة) فالقضاء الفرنسي يقول في محكمة استئنافه على " انه لا يوجد في الأوراق ما يسمح بوقوع السرقة بالديسكات أو المعلومات .

و بعد صدور عدة أحكام من طرف القضاء انتهى القول لوقوع السرقة و النصب على المعلومات فقد اتجهت أحكام القضاء الفرنسي الى وقوع السرقة من مستخدمين لإحدى الشركات التي قامت بنسخ الديسكات الخاصة بالشركات دون موافقتها و في هذا الاتجاه أيضا اتجه القضاء البلجيكي إلى اعتبار المعلومات في الكمبيوتر من قبل الأموال التي تصلح أن تكون محلا لوقوع جريمة النصب و السرقة في المعلومات

2- الطبيعة المعنوية للبرامج و الصور الالكترونية :

ظهرت حماية قانونية و من ضمنها حماية الجنائية لسر الأعمال فقد وضعت الجمعية الاستشارية للمجلس الاربي تعريفا نوعيا منذ سنة 1984 في القانون النموذجي لسر الاعمال بان كل معلومة تتعلق بالصناعة و التجارة له قيمة للمشروع او للفرد الذي يحوزه بشكل خاص

اما في المانيا صدر قانون بشان الجرائم الاقتصادية لسنة 1976 وسع مجال القانون الخاص بالمنافسة الغير مشروعة فالمادة 18 فقرة 02 من قانون الالماني تعاقب أي شخص حصل بدون اذن على سر تجاري او صناعي و ذلك بالاستعانة بوسيلة فنية . و ذلك كله يبرز ضرورة التدخل بنصوص خاصة لتوفير الحماية الجنائية للأموال ذات الطابع المعنوي .

3- ظهور فكرة المنقول المعلوماتي في جرائم الاموال :

جـــرائـــم النصـــب الإلكتـــرونـــي

على الرغم من الطبيعة المعنوية للمعلومات الالكترونية اذا لم تكن مسجلة على دعامة مادية وتم الاستلاء عليها بدون الاستلاء على تلك الدعامة فان اتجاها من الفقه ذهب نحو الاعتداد بصفة المنقول لهذه المعلومات الالكترونية فيرى البعض ان المعلومات أموال تصلح ان تكون محلا لنصب و السرقة كما يتجه القضاء في عديد من الدول مثل القضاء البلجيكي الى اعتبار المعلومات في الكمبيوتر من قبيل الأموال التي تصلح لوقوع جريمة السرقة و النصب على المعلومات و في نفس هذا الاتجاه ذهبت المحاكم الهولندية و تبنى كذلك القضاء الفرنسي نفس الاتجاه عندما قضت بتوافر أركان النصب في حكمها على ان المعلومات لم اختلاسها مع الدعامة ((ديسك – اسطوانة – الجهاز نفسه)) بيد ان هناك تطور دائما في هذا المجال من الجرائم وقد أخد المشرع الفرنسي قانون العقوبات الذي دخل حيز التنفيذ ابتداء من سنة 1994 نحو الاعتدال بالأموال ذات الطبيعة المعنوية عندما لم يستعمل الصياغة التقليدية ((مال منقول مملوك للغير)) كمحل جرائم النصب فبعد التعديل الذي أصبح ساريا في سنة 1994 على قانون العقوبات الفرنسي في مجال جريمة النصب بحيث تسري على الخدمات و ليس على المال المنقول المملوك للغير فقط ، على خلاف ما تتجه إليه القواعد العامة و التي لا يزال يعتنقها على خلاف المشرع الفرنسي المشرع المصري فقد كانت المادة 405 من ق ع الفرنسي قبل التعديل تعبر عن محل النصب بأنه((أصول

منقولات، مستندات ... الغ)) وبعد صدور النص الجديد الذي يعبر عن محل النصب بأنه مال آيا كان أو خدمة .

4- مدى انطباق صفة المنقول على التحولات النقدية :

العديد من الجرائم التي تقع بواسطة الكمبيوتر يتمثل بعضها في إجراء تحويلات نقدية الخاصة بأحد البنوك غير ان بعض التشريعات لا تعتبر تلك التحويلات واردة على مال منقول او مملوك للغير بل تعتبرها منشئة حقا للبنك المحول اليه في ضمة البنك المحول منه و بناءا عليه لا تعتبر تلك التشريعات إجراء تلك التحويلات بطريق الغش مشكلا لجريمة النصب و من تلك التشريعات التشريع البلجيكي و الألماني و اليوناني و الياباني و القانون في لوكسمبورغ

ان معظم تشريعات المقارنة تعتبر ذلك مشكلا لتسليم رمزي تقع به جريمة النصب و فقا لوصف القانوني الصحيح و من تلك التشريعات القانون الكندي و الهولندي و السويسري و الانجليزي و معظم قوانين ولايات المتحدة الأمريكية

الفرع الثاني : الحماية الجنائية لتعاملات الالكترونية بنصوص خاصة .

1- ضرورة استحداث نصوص خاصة بحماية معلومات داخل الكمبيوتر :استشعر المشرع في العديد من الدول إلى إدخال تشريعات جديد تحمل معلومات دخل نظام الكمبيوتر نظرا لقصور القواعد التقليدية بقانون العقوبات عن حماية هذا النظام من هذه النصوص ما يجرم مجرد التدخل في نظام الكمبيوتر منها ما جرب إتلاف المعلومات المبرمجة و منها ما يجرب تغيير هذه المعلومات

2- المعلومات داخل الكمبيوتر جديرة بالحماية على المعلومات الورقية : تظهر جدارة المعلومات المبرمجة آليا بالحماية الجنائية عن المعلومات التي تحتويها الملفات الورقية من ضعف النوع الأول من المعلومات و من أهميته في آن واحد ، فالمعلومات المعالجة آليا ضعيفة داخل النظام عنها داخل الملفات الورقية هذه الأخيرة يمكن إخفاؤها بسهولة عن المعلومات داخل النظام كما ان المعلومات المعالجة اليا تتميز بالضخامة و التنوع و منها ما يتعلق

بالحياة الخاصة للأفراد كل هذه الاعتبارات دعت مشرعي كثير من البلدان الى استحداث صور من التجريد من حماية المعلومات داخل الكمبيوتر من الاطلاع عليها بينما لا يوجد مثيلا لتلك النصوص بالنسبة للمعلومات الورقية .

3- الاتجاه إلى تجريم مجرد الدخول او البقاء في التشريعات المختلفة : تعاقب غالبية التشريعات الحديثة على الدخول في نظام الكمبيوتر و قد اتجه مشروع قانون التجارة الالكترونية في مصر هذا الاتجاه عندما نص في المادة 26 منه على انه "مع عدم الإخلال بايت عقوبة اشد وردت قي قانون أخر يعاقب بالحبس و بغرامة لا تقل عن 30.000 ثلاثة ألاف جنيه او بإحدى هتين العقوبتين كل من دخل بطريق الغش او التدليس على نظام المعلومات او قاعدة البيانات التي تتعلق بالتوقيعات الالكترونية و يعاقب بنفس العقوبة من اتصل او أبقى الاتصال بنظام معلومات او قاعدة البيانات بصورة غير مشروعة

- يعتبر القانون السويدي لسنة 1983 أول قانون يعاقب على الدخول في نظام الكمبيوتر المملوك للغير.

موقف التشريعات الحديثة تتباين في تجريم الدخول الغير المصرح بها . من هذه التشريعات ما يقد تجريم الدخول بقيد يتعلق بالركن المعنوي فيستلزم توافر قصد خاص لدى المتهم و هو قصد التأثير في البيانات او التأثير في نظام الكمبيوتر نفسه على هذا للعقاب على هذا الدخول .من هذه التشريعات التشريع الالماني و الكندي

و النمساوي و الياباني . و من التشريعات ما لا يعاقب على الدخول الا اذا اتجهت نية المتهم الى الاستلاء على اموال الغير عن طرق الغش و من ذلك قانون ولاية فرجينية بالولايات المتحدة الأمريكية ما ان قانون جرائم الكمبيوتر في ولاية تينسي يعاقب الدخول اذا اتجهت نية المتهم إلى الاستلاء على مال الغير بطريق الغش أو إلى إتلاف البيانات او برامج النظام. و من التشريعات ما يقيد تجريم الدخول الغير المصرح به بتوافر عنصر في الركن المادي و تستلزم هذه التشريعات ان يحدث التداخل المعاقب عليه في خصوص انظمة معينة ك الاجهزة الحكومية او اجهزة المؤسسات المالية او الاجهزة التي تحتوي على معلومات تتعلق بالامن القومي و العلاقات مع الدول الأجنبية ((هذا النوع الأخير من الأجهزة عادت ما ينتمي إلى الأجهزة الحكومية و ان امكن تصور وقوعه على اجهزة تخص الأفراد)).من هذه القوانين القانون الفيدرالي الامريكي لسنة 1994 في شان الغش و إساءة استعمال الكمبيوتر و في نفس الاتجاه تعاقب تشريعات أخرى على مجرد الدخول بغض النظر عن نية المتهم في ارتكاب جريمة معينة مثل قانون الاسترالي و القانون الفلندي و القانون الهلندي و القانون السويدي و القانون الاسرائيلي .

و من التشريعات ما تورد هذا التجريم بشكل مطلق و بالتالي فانها تعاقب على مجرد الدخول دون استلزام قصد خاص و دون تطلب قيد معين تتعلق بالركن المادي و من هذه التشريعات قوانين لبعض لولايات الامريكية كولاية كليفورنيا فهذا الاخير يعاقب

جـــرائـــم النصـــب الإلكتـــرونـــي

بوصف الجنحة كل شخص دخل عمدا في نظام الكمبيوتر او شبكة الكمبيوتر او برنامج الكمبيوتر او في البيانات المبرمجة مع علمه بعدم رضا صاحب النظام عن ذلك .كما ان التشريع الفرنسي يتجه نفس الاتجاه فتنص المادة 323 فقرة اولى من قانون العقوبات الفرنسي على تجريم الدخول في نظام الكمبيوتر في قولها " يعاقب على الدخول او الاستمرار البقاء في نظام المعلومات المبرمجة او في جزء منه بقصد الغش بالحبس مدة لا تزيد عن سنة و غرامة مالية لاتزيد على مئة الف فرنك " وقد شددت المادة السابقة العقوبة المقررة عن هذه الجريمة اذا ترتب على هذا الدخول محو او تعديل في البيانات المبرمجة في الجهاز عند اذن تصبح العقوبة الحبس مدة لا تزيد عن سنتين و بغرامة لا تزيد عن 200 ألف فرنك .

المطلب الثاني :الحماية الجنائية الإجرائية للتعاملات الالكترونية.

لا تقتصر الحماية الجنائية في التعاملات الالكترونية على الجانب الموضوعي الذي يتعلق بقواعد التجريم و العقاب و لا كنها تمتد لتشمل جوانب اجرائية تتسم بطابع من الخصوصية يتماشى مع ما تتسم به تلك المعاملات من طابع خاص . هذا الطابع الخاص بنعكس مع ما يتخذ من إجراءات للتحقيق و إجراءات للمحاكمة . فيكفل قانون الإجراءات الجنائية حماية للبيانات المتواجدة في أجهزة الكمبيوتر من خلال ما هو مقرر قي القواعد العامة في الإجراءات الجنائية السابقة على المحاكمة بالإضافة الى ما تقرره تشريعات عديدة من أحكام خاصة بتلك الحماية بالنسبة إلى تلك البيانات لذا سوف نركز على ما تتميز به أحكام الحماية المقرر في الدعوى التي تتعلق بالمعاملات الالكترونية من خصائص تنفرد بها

أ- دراسة الطبيعة الخاصة بأعمال جمع الاستدلالات في دعوى المعاملات الالكترونية

ب – إجراءات التفتيش و ضبط الأدلة في مجال التعاملات الالكترونية التي تصادف الحماية للتعاملات الالكترونية في

جـــرائـــم النصـــب الإلكتـــرونـــي

مرحلة المحاكمة التي تؤثر عليها بعض الصعوبات مردها ان تشريعات المقارنة تختلف فيما بينها بالنسبة لكثير من الأفكار و المفاهيم . من ذلك اختلاف التشريعات في النظر الى جرائم النصب الالكترونية فعلى حين تمن و تجرم القوانين بعض الدول جرائم النصب الالكترونية أيا كانت فبعض الدول الأخرى تقتصر على بعض الأفعال فقط التي تتضمن نصبا الكترونيا و تختلف حتى في تحديد مفهومها بالنسبة الى الدول الإسلامية تتغاضى عن بعض الأفعال و لا تعتبرها جريمة ام الدول الغربية فهي تضيق نطاق الجريمة .

- فتتكفل الأحكام العامة بالإضافة الى النصوص الخاصة في الإجراءات الجنائية حماية قانونية للتعاملات الالكترونية في مرحلة المحاكمة هذا النوع ينعكس على تلك الأحكام العامة بل و أصبح مبررا لإدخال نصوص خاصة لتنظيم الدعة الجزائية في مرحلة المحاكمة سواء من ناحية تحديد المحكمة المختصة بنظر جرائم التعاملات الالكترونية او من ناحية سلطة المحكمة في تقدير الدليل في مجال التعاملات الالكترونية

الفرع الاول :الحماية الجنائية السابقة عن المحاكمة ((- أبعاد سلطة مأموري الضبط القضائي في جمع الاستدلالات في مجال التعاملات الالكترونية)).

1- صعوبة الكشف عن الجرائم المعلوماتية و معرفة مرتكبيها :

تواجه مامور الضبط القضائي صعوبة كبيرة عندما يقوم بضبط مقتحمي الكمبيوتر و هذه الصعوبة تكمل في الحصول على الدليل على هذا الفعل فيحيط مقتحمو الكمبيوتر أنفسهم بوسائل تقنية حتى لا يتمكن رجال الضبط القضائي من اقتفاء أثرهم و يقوم مقتحم الكمبيوتر " هاركر" أحيانا بالدخول الى جهاز الكمبيوتر عن طريق جهاز اخر .و ترجع أسباب دخول المقتحم في النظام الأخير الى الأسباب التالية :

أ- الحصول على الأدوات و البرامج من كمبيوتر الغير حتي يستعمله في أغراض غير مشروعة .

ب- حماية جهازه حتى لا يتبعه احد.

ج- استغلال الجهاز الثاني حتى يقوم الهاكر باستعمال كمبيوتر الغير مستغلا ما يتاح له من خدمات على نفقة صاحب هذا الجهاز .

و يزيد من صعوبة الكشف عن جرائم الكمبيوتر في حالات عديدة إن كثيرا من المجني عليهم لا يرغبون في التبليغ عن هذا النوع من الجرائم .

2- جواز التحريات التي لا تتعلق بحرمة الحياة الخاصة :

- لرجال الضبط القضائي ان يقوم بالتحريات التي ترد على البيانات تتعلق بالإفراد المشتبه فيهم ما دام ان تجميع تلك البيانات لا يتضمن اعتداء على حرمة الحياة الخاصة .

تطبيقا لذلك قضي بان مقام به رجال الضبط القضائي في كندا من الرجوع إلى أجهزة شركة الكهرباء لمعرفة مدى استهلاك احد المشتركين للكهرباء ، ذلك انه كان محلا للاشتباه فيه لأنه يقوم بزراعة نبتات مخدرة في المنزل التابع له لا يتعلق بحرمة الحياة الخاصة و بالتالي فانه ليس نوعا من التفتيش فهو إذا يدخل في أعمال التحريات التي يملك رجال الضبط القيام بها دون سبق الحصول على إذن بالتفتيش و الحقيقة ان ما ينتمي الى الحياة الخاصة التي لا يجوز التدخل فيها عن طريق جمع الاستدلالات و ما لا ينتمي الى الحياة الخاصة التي تقبل ان تكون محلا لجمع الاستدلالات ،يثار بالنسبة إلى الحق في الصورة فالإنسان له الحق في الصورة ،غير انه للمتهم حق في الصورة الاصل ان صورة الشخص من البيانات الخاصة فلا يجوز التقاطها حتى و لو كان في مكان عام و مؤدى ذلك ان الشخص يتمتع بالحق في الصورة فهذه من البيانات التي تنتمي إلى الحياة الخاصة . تطبيقا الى ذلك قضي

جـــرائـــم النصـــب الإلكتـــــرونـــــي

في كندا انه لا يجوز التقاط صورة امرأة دون رضا منها ولو كانت في مكان عام ، أما إذا كان التهم يتزعم مظاهرة و يهتف بالآخرين فانه لا يجوز لرجال الضبط تصويره في هذا الوضع لأنه لا يحرس على حرمة حقه في الصورة .

ان اسرار البنوك تنتمي بحسب الى الاسرار التجارية و ليس الى مجال الحياة الخاصة بذلك قضي في الولايات المتحدة الامريكية حكم ((**miller**))بان الشرطة من سلطتها ان تامر البنك بتقديم معلومات عن شيك خاص باحد عملائها هذا السر لا ينتمي الى حرمة الحياة الخاصة للافراد و انما يمكن ان يتعلق بسرية الحسابات المصرفية خذا النوع من البيانات قد تحميها نصوص في تشريعات معينة (كالقانون الفرنسي و المصري) و مع ذلك يسمح قانون العقوبات الفرنسي بالزام رجل البنك بتقديم ما لديه من معلومات بنكية تتعلق بالمتهم في جريمة بناء على امر من النيابة او قاضي التحقيق او المحكمة (المادة 132 فقر 22 من قانون العقوبات الفرنسي) و اتفق القانون المصري مع القانون الفرنسي في جواز كشف سرية الحسابات المصرفية بمقتضى امر من النيابة او المحكمة في الحالات التي حددها القانون (القرار بقانون رقم 205 لسنة 1990 في شان سرية الحسابات للبنوك) لقد ادخل المشرع الامريكي المادة ،3422 - 3401 && **usc** 12 ليحظر على السلطات العامة الحصول على ملفات العملاء لدى المصارف و المؤسسات المالية إلا بمقتضى أمر قضائي او إذن بالتفتيش.

جـــرائـــم النصـــب الإلكتـــرونـــي

لقد سمح القرار بقانون رقم 539 -2001 الصادر في 05 يوليو 2001 لوزير الداخلية الفرنسي ان يتبنى تطبيق نظام المعلومات المعالجة اليا الخاصة بالمشتبه فيهم و المجني عليهم بهدف البحث الجنائي ، و نستفيد من هذا ان المعالجة الالكترونية أصبحت مقبولة في مراحل مخالفة لإجراءات و منها مرحلة جمع الاستدلالات و من ثم لا تعتبر ماسة بحرمة الحياة الخاصة بالنسبة لاطلاع رجال الضبط القضائي عليها .

3- حق رجال الضبط القضائي في دخول أندية الانترنت و تفتيش الأجهزة : من المستقر عليه انه من حق جال الضبط القضائي دخول أماكن العامة دون الحصول على اذن مسبق و ذلك بهدف الإشراف على تنفيذ اللوائح و القوانين و هذا الحق لا يجيز لرجال الضبط القضائي ان يقوموا بفتح الأشياء المغلقة الموجودة في المحلات العامة فهذا ما قضت به محكمة النقد المصرية – لرجال الشرطة العامة في دوائر اختصاصه دخول المحال العامة المفتوحة للجميع لمراقبة تنفيذ القوانين و اللوائح و هذا إجراء اداري مقيد بالغرض السالف البيان و لا يجاوزه الى التعرض الى حرية الأشخاص او استكشاف الأشياء الفلقة الغير الظاهرة – و بتطيق ذلك في المجال الالكتروني فانه ليس من حق رجال الضبط اقضائي عند دخولهم الى اندية الانترنت – السيبر- ان يقوم بهذه الصفة بفتح الكمبيوتر المغلق او الجلوس الى كمبيوتر مفتوح و البحث في المحركات المختلفة فيه إنما يجوز لهم فقط ان يدخلوا الى تلك الأندية و إذا رأوا مفتوح و فيه مثلا صور جنسية هنا تقوم

حالة التلبس التي تجيز لهم ضبط و تنفتيش هذه الاجهزة (187 قانون العقوبات المصري)

وقد صدر بفرنسا القانون رقم 647 لسنة 1991 في 11 يوليو 1991 معدلا القانون رقم 1180 لسنة 1990 الصادر في 29 ديسمبر 1990 ليسمح في المادة 40 منه لموظفي ادرارة الاتصالات اللا سلكية المخولين بقرار من وزير الاتصالات سلطة الضبط القضائي بدخول الأماكن العامة في ساعات فتحها للجمهور لضبط الجرائم المتعلقة بالاتصالات اللاسلكية أما التفتيش و الضبط فانه يلزم له اذن من السلطات القضائية المختصة فلا يجوز لهم دخول أماكن السكن الا بمقتضى اذن قضائي

و تقدر القواعد العامة بوجود تميز بين رجال الضبط القضائي بدخول اماكن العامة و بين قيامهم بتفتيش الاجهزة المتواجدة في تلك الاماكن فحق الدخول هو حق يمارسه رجل الضبط القضائي مثله في ذلك مثل أي شخص من مرتدي تلك الأماكن و تاسيسا على انه من حق رجل الضبط في دخول الاماكن العامة مثله في ذلك مثل أي شخص عادي يدخل تلك الاماكن فانه من حقه ايضا ان يقوم بما يقوم به الشخص العادي أي استعمال الاجهزة المتواجدة فاذا اطلع على وقوع الجريمة فانه يتخذ الاجراءات الضبط متفقة مع صحيح القانون

4- مدى حق رجل الضبط القضائي في الاستعانة ببرامج الاختراق لكشف المتدخلين : يستطيع المحقق ان يقتفي اثر المقتحمين

للكمبيوتر باستعمال الوسائل الاتية منها الاستعانة بمرشد سري و تطوير المصادر التى تزوده بالمعلومات و استخدام برامج معدة سلفا لاقتفاء اثر مقتحمي الكمبيوتر غير ان ذلك مشروط بعدم التعدي على الحق في الخصوصية أي لعدم الدخول الاجزاء الخاصة من الكمبيوتر او شبكة الانترنت (البريد الالكتروني – المحركات الفورية) و بالتالي فان رجل الضبط القضائي عندما يقوم بعمل من عمل التحريات يتعين عليه ان يبقى في مواضع المتاحة للجمهور و الدخول فيها مثل مواقع الويب .

5- وسائل الملاحظة من اعمال جمع الاستدلالات في مجال الاتصالات الالكترونية : يجب التمييز بين نوعين من الإجراءات حيث تتمثل الملاحظة في وسيلتين الأولى تتمثل في معرفة رقم الهاتف الذي تم توصيله الى الجهاز و الثانية تقتصر على معرفة الجهاز نفسه هاتان الوسيلتين من الملاحظة تختلفان عن اعتراض الرسائل الالكترونية حيث لا تشكلان اعتداء على الحياة الخاصة كما ان معرفة رقم الهاتف الخاص لفرد معين لا يشكل اعتداء على الحياة الخاصة و بالتاي فان لا يستلزم صدور اذن بهذا النوع من الملاحظة من جهة قضائية و هذا على خلاف اعتراض المراسلات الالكترونية و تسجيلها .فمثلا قضي في كندا بان مجرد الاتصال بشخص معين يعتبر من قبيل الاتصال الهاتفي التليفوني الذي يقضي بتسجيله سبق الحصول على إذن لمراقبة المحادثات التليفونية دون اشتراط ان يكون هناك محادثة فعلية مما يؤيد الراي هذا ان الاتجاه السائد في التشريعات المقارنة بخصوص ارقام

التيليفونات التي يصدر من أصحابها اتصالات غير مرغوب فيها او معاكسات تيليفونية يمكن تسجيلها دون سبق الحصول على اذن كما في فرنسا وفقا للقانون الصادر سنة 1991 في هذا الخصوص و هذا ما تبعته فيه الولايات المتحدة الأمريكية و المملكة المتحدة و بلجيكا .

اما بالنسبة للوضع في القانون المصري فانه لا يتضمن نص صريحا يعالج مسالة الكشف ان أسماء الاطراف بالمحادثة غير ان المادة 90 مكرر من قانون الإجراءات المصري تعالج مسالة تسجيل محتوى المحادثة نفسها فتنص المادة السابقة على ان " لرئيس المحكمة الابتدائية المختصة في حالات قيام دلائل قوية على ان مرتكب الجرائم المنصوص عليها في المادتين 166 مكرر و 308 مكرر من قانون العقوبات المصري قد استعانة في ارتكابه بجهاز تيليفوني معين امر بناءا على تقرير مدير عام مصلحة التليغرافات و التليفونات و شكوى المجني عله في الجريمة المذكورة بوضع جهاز تليفون تحت الرقابة لمدة يحددها .و في غياب نص صريح من القانون المصري بخصوص الكشف عن الارقام نرى ان ذلك يدخل في عموم التحريات و لا يلزم الكشف عنه اجراءات خاصة من اذن او غيره .

6- جواز الكشف عن هوية المشترك و حركة اتصالاته من جانب مزودي الخدمة : اذا تعلق الامر ببيانات تخص هوية المشترك و بالارقام التي اتصل بها الكترونيا فإننا نرى ان هذا النوع لا يتعلق

جـــرائـــم النصـــب الإلكتـــرونـــي

بحرمة الحياة الخاصة و بناءا عليه فان مقدم خدمة الاتصالات الالكترونية من حقه ان يتعاون مع رجال الضبط القضائي بتزويدهم بتلك البيانات دون الحاجة الى اذن تفتيش و الضبط لدى مزود تلك الخدمات .

لقد وردى في الاتفاقيات الاروبية في شان جرائم السيبر لسنة 2001 انه يجوز لدول أطراف في تلك الاتفاقية ان تسمح لسلطاتها التحري عن هذه البيانات المتعلقة بالمشترك و لو تعلق الاتصال باكثر من مزود للخدمات المادة 18 .

لقد حددت الاتفاقية المقصود بتلك البيانات بقولها انها تتعلق بنوع خدمة الاتصال التي اشترط فيها الشخص و الوسائل الفنية لتحقيقها و مدة الخدمة و شخصية المشترك و رقم دخوله للحصول على تلك الخدمة و الفواتير التي ترسل اليه و أي معلومات تتعلق بطريقة الدفع او أي معلومات اخرى تتعلق بأداء الخدمة او بالاتفاق بين هذا المشترك و مزود الخدمة كما عنيت الاتفاقية ذاتها بالقول ان تلك البيانات تشمل أي معلومات تختزن في الكمبيوتر او في أي شكل اخر التي تتواجد لدى مزود الخدمات تتعلق بالمشترك في خدماته بخلاف المعلومات التي تتعلق بحركة تداول البيانات او محتوى تشمله تلك البيانات . و يتضح مما سبق ان الاتفاقية لا تستلزم سبق الحصول على اذن قضائي للكشف عن هذه البيانات و بناءا عليه يجوز لدول الاطراف ان تخول لرجال الضبط القضائي سلطة الاطلاع على تلك البيانات في إطار قيامهم بواجبه في جمع

الاستدلالات و يترتب على ذلك أيضا ان رجال الضبط القضائي له امر مزود الخدمات ان يقدم هذا النوع من البيانات و ذلك بموجب امر بالاطلاع على تلك البيانات فتنص المادة 17 من الاتفاقية في شان جرائم السيبر على انه "لدولة الطرف ان تسن التشريعات ما يتيح للسلطات المختصة الحق في تامر أي شخص يتواجد على اقليمها بحيازة او تحت سيطرته تلك المعلومات المخزنة في الكمبيوتر او في وسيلة تخزين تتعلق بالكمبيوتر او مزود الخدمات الذي يقدم خدمات لاقليم الدولة ان يقدم ما لديه من معلومات تتعلق بالمشترك في تلك الخدمات التى في حيازته او تحت سيطرته .

7- مراقبة المراسلات الالكترونية في حالة الضرورة الاجرائية من جانب رجال الضبط القضائي :تسمح بعض التشريعات كالقانون الامريكي بوضع اجهزة لتسجيل الاتصالات الالكترونية في حالة الضرورة بدون اذن اذا توفر خطر الحال على الحياة او خطر جسيم على السلامة الجسمية للأشخاص او في حالة التأمر اذا كن ذلك يقتضي وضع جهاز تسجيل او تتبع الأثر قبل الحصول على اذن الالزم لذلك مادامت الأسباب قد توافرت ما يدعو إلى الاعتقاد أن هذا الإذن سوف يصدر ثم صدر هذا الإذن في خلال 48 سا فاذا لم يصدر الامر بذلك في تلك المهلة كان من المتعين ان تنتهي تلك المراقبة و ترفع الاجهزة المعنية و ما يجري عليه القانون الامريكي بجواز تفتيش الكمبيوتر في حالة الضرورة الإجرائية هو اجراء استثنائي لا تسمح به القوانين ذات الاصل اللاتيني .

الفرع الثاني :الحماية الجنائية الإجرائية في مرحلة المحاكمة .

اولا : تحديد المحكمة المختصة

- من المهم تحديد المحكمة المختصة للفصل في النزاع لانه يترتب على ذلك تحديد القانون الواجب تطبيقه في حالة تنازع القوانين و بالتالي يمكن القول ان المحكمة المختصة هي التي تحدد القانون واجب التطبيق لذلك فان تحديد المحكمة المختصة نظر الدعوى له أهمية واضحة تتمثل في ان قاضي الدولة سوف يقوم بتحديد قاعدة الإسناد وفقا لقانون دولته أي أن الأمر لا يقتصر على الجانب الإجرائي بل يتعداه إلى القواعد الموضوعية التي سوف ينزلها القاضي عن موضوع الدعوى كما انه من مصلحة المدعي ان يرفع دعواه امام محكمة دولته حيث يعرف لغتها و يتابع اجراءاتها فعلى سبيل المثال اذا حدث نزاع بين فرنسي و انجليزي و كانت المحكمة الفرنسية هي المختصة فان القاضي هنا سوف يطبق القانون الفرنسي و لذلك اهمية تتمثل في ان المتقاضي الفرنسي سوف يجد سهولة في رفع الدعوى و ذلك لعلمه باللغة و الاجراءات اما اذا رفع الفرنسي الدعوى في مصر على سبيل المثال فانه سوف يجد صعوبة تتعلق باللغة حيث انه لا يعرف اللغة العربية و سوف يواجه ايضا صعوبة في الاجراءات لعدم علمه بها و يلاحظ ان القضاء في كثير من الدول يمد اختصاصه في الدعاوى المدنية و الجنائية الى وقائع حدثت في الخارج من ذلك ان

الدائرة المدنية لمحكمة النقذ الفرنسية قضت باختصاص القاضي الفرنسي في قضية كان احد اطرافها فرنسيا بينما كان الطرفان الاخران من جنسية انجليزية و لا توجد أي علاقة تربطهم بفرنسا حيث وقع النزاع في انجلترا و لا كن احد الخصوم كان متعاقدا مع شركة التامين الفرنسية و بررت المحكمة هذا الحكم بان الاختصاص الدولي للمحاكم الفرنسية لا يستند فقط على الحقوق المتولدة من وقائع متنازع عليها و لاكنه ياخذ ايضا جنسية الاطراف معنى ذلك ان الاختصاص الدولي للمحاكم الفرنسية لم ياخذ هنا بمعيار المدعى عليه و لا كن اخذ بمعيار الجنسية بغض النظر عما اذا كان الفرنسي هو المدعي او المدعى عليه هذا الاختصاص الموسع للمحاكم الوطنية لم يظهر فقط في المواد المدنية بل انه امتد الى المواد الجنائية .

ثانيا : تطبيق مبدأ العالمية في قضايا الكمبيوتر و الانترنت

- تأخذ بعد التشريعات المقارنة بمبدأ العالمية في تحديد الاختصاص القضاء الوطني الجنائي فمثلا بلجيكا انتهجت هذا النهج من الاختصاصات .

ويقصد بهذا المبدا ان المحاكم الوطنية تختص بمحاكمة مرتكبي بعض الجرائم على الرغم من وقوعها في خارج اقليم الدولة و ان المتهمين ليسوا من مواطنين تلك الدولة لا كن لان الجريمة ذات طبيعة دولية أي تخل بقيمة من قيم المجتمع العالمي مقل جرائم المخدرات و الإرهاب و القرصنة و جرائم الجنسية و الواقعة على

الأطفال و يلاحظ ان قانون العقوبات في دولة الامرات العربية المتحدة يأخذ مبدأ العالمية في بعض الجرائم فتنص المادة 21 "على تطبيق مبدا العالمية في الجرائم التالية جريمة تخريب او تعطيل و سائل الاتصال الدولية و يقصد بذلك عادة جرائم خطف الطائرات ، جرائم الاتجار بالمخدرات ، جرائم التجار بالرقيق الأبيض – النساء – و ذلك يتحقق في حالة الدعارة ، جرائم التجار بالصغار او الرقيق ، جرائم القرصنة ، جرائم الارهاب الدولي و يكون سريان القوانين الجزائية الإماراتية من اختصاص القضاء الإماراتي بتلك الطائفة من الجرائم ممتدا الى الفاعل فيها كذلك الى الشريك ايا كان مكان وقوع الجريمة "

أما القانون المصري فانه لا يأخذ بهذا المبدأ .

3 - امتداد قواعد الاختصاص في الجرائم الالكترونية :

تقدر القواعد العامة بان المحكمة الجنائية تختص بنظر الدعوى اذا وقعت الجريمة كلها او بعضها على اقليم الدولة وفقا لمبدا الاقليمية 05-113 قانون العقوبات المصري .

بل ان القضاءفي بعض الدول كفرنسا يختص بالجرائم الواقعة خارج اقليم الدولة اذا كانت مرتبطة به ارتباطا لا يقبل التجزئة مع جرائم وقعت على الاقليم الفرنسي و ذلك وفقا لما يتجه اليه القضاء الفرنسي . و في مجال الانترنت تقضي المحاكم الفرنسية باختصاصها بنظر الدعوى بالنسبة للمعلومات التي يمكن لشخص مقيم على الاقليم الفرنسي ان يرجع اليها أي كان مكان تواجد يزود

الخدمات غير انه اذا وجد جهاز البث في خارج الاقليم الفرنسي فانه يلزم توافر قاعدة التجريم المزدوج بين القانون الفرنسي و قانون الدولة التي يصدر مكنها البث و يشكل ذلك عقيتا في بعض الاحيان امام اختصاص القضاء الوطني وذلك بسبب ان بعض صور التجريم لا تتواجد في اقليم دولة البث كما يحدث بالنسبة للنشر رسائل تحض على الكراهية بسبب العنصر او الدين و هو التجريم الذي يعرفه القانون الفرنسي دو قانون الولايات المتحدة الامريكية مثلا . و يعتبر ذلك اجتهادا من طرف القضاء الفرنسي لكي يمد اختصاصه الى الجرائم التي تقع عن طريق الانترنت .

4- معايير الاختصاص بالمحكمة بقضايا جرائم المعلوماتية

اذا توافر في القضية الواحدة عنصر دولي فان القاعدة تقضي باختصاص اكثر من دولة بنظر الدعوى تطبيقا لذلك قضت محكمة العدل الأوربية في قضية زارعي العنب الهولنديين الذين أضيروا في مزارعهم بسبب تلوث مياه نهر الراين الذي سببه احد مشروعات المناجم في فرنسا باختصاص محكمة وقوع الضرر في هولندا و باختصاص المحكمة الفرنسية و هي محكمة فعل الدار .

و بالمثل قضت محكمة الاستئناف لباريس قي قضية التعويض عن تشهير بإحدى السيدات رفعتها المدعية في مواجهة صحيفة انجليزية يتم توزيعها في فرنسا فقضت باختصاص المحكمة

الفرنسية بنظر دعوى التعويض حتى على الرغم من ان المدعية سيدة انجليزية و ليس مشهورة في فرنسا

يختلف الأمر إذا وقعت الجريمة عن طريق شبكة الانترنت حيث ان الاختصاص يؤول للمعايير المقررة وفقا للقواعد العامة و التي تتلخص في مكان إرسال الرسالة و مكان تحقق الضرر- اذا تعلق الأمر بالتعويض عن الجريمة -.

و المعرف ان اختيار المحكمة المختصة يترتب عليه تحديد القانون واجب التطبيق في حالة جرائم التي تقع عن طريق الانترنت و ذلك بسبب اختصاص أكثر من دولة و بمحاكمة المتهم و وقد قضت بذلك محكمة العدل الأوربية في 1995 /03/08 في قضيت قذف وقع عن طرق النشر في إحدى الصحف التي يتم توزيع في عدة دول **AFF.C 68/93** بان من حق المتهم اللجوء الى دولة من الدولة التي تم فيها النشر فقد اقرت المحكمة حق المتهم في اللجوء الى دولة من الدول التي تم فيها النشر و يترتب على ذلك نتيجة هامة مؤداها ان من يقوم بنشر رئسائل عبر الانترنت يتعين عليه ان يراعي ان هذه الرسائل لا تخالف قوانين الدول المختلفة ما دام انه يتعرض للمساءلة في أي دولة يصل اليها هذا البث . تطبيقا لذلك قضت لمحكمة الابتدائية بباريس باختصاص المحاكم الفرنسية و بالتالي تطبيق القانون الفرنسي اذا كان مركز البث موجود في خارج الاقليم الفرنسي و بناءا عليه اذ كان الجهاز الخادم موجودا في امريكا بين تذهر الرسائل التي يقوم

ببثها هذا الجهاز في فرنسا فان المحاكم الفرنسية ينعقد لها الاختصاص و في ذلك تقوم المحكمة السابقة " تتعتبر الجريمة مرتكبة في كل مكان تظهر فيه الرسائل المؤثمة محل البث ".

وفقا لهذا الاتجاه الموسع فان الجريمة المعلوماتية تقع عدة افعال و تعطي الاختصاص لكل دولة يقع فيها الفعل . من ذلك ان يقوم شخص في فرنسا بالدخول على الشبكة لتعديل ببنات مسجلة في قاعدة البيانات في هلندا و من الواضح ان هذا الاتجاه يؤدي الى تعدد جهات الاختصاص .

فالقاعدة في مبدأ الإقليمية أن اختصاص يعود الى قضاء الدولة إذا وقع على إقليمها جزءا من الجريمة و يطبق القانون في بلجيكا و سويسرا و اليونان هذه النظرية . بالاضافة الى قانون العقوبات الفلندي الذي يعطي الاختصاص للقضاء الوطني في مكان وقوع الفعل او مكان حدوث نتائج الجريمة او المكان المقصود حدوثها فيه في حالة الشروع .

و من التشريعات المقارنة كالولايات المتحدة الامريكية ما يعطي الاختصاص الى محاكمها الجنائية اذا حدثت اثار الجريمة على اقليمها فهذا الاتجاه موسع ايضا فبالنسبة الى المحاكم الامريكية اختلف في تحديد معيار الاختصاص من ولاية الى اخرى

5- تحديد المحكمة المختصة لجرائم المعلوماتية بنصوص خاصة

وضعت كثيرا من الدولة قواعد خاصة للاختصاص في مجال جرائم المعلوماتية منها القانون الانجليزي الذي يسري على المسؤول عن تجميع تلك البيانات او المستخدمين الذين يديرون هذا العمل او من يمثلهم مادام انهم يقيمون في انجلترا و بالمثل فان القانون الهولندي يسري على تجميع البيانات الذي يقع خارج البلاد اذا كان المسؤول عنه يقيم في البلاد و اذا كانت تلك البيانات تتضمن معلومات عن افراد يقيمون بدورهم في هولندا و بالتالي لا يسري القانون الهولندي اذا كان المسؤول عنها لا يقيم في هولندا .

غير انه قضي في انجلترا بعدم اختصاص المحاكم الانجليزية في قضية تتلخص وقائعها في ان المتهم في لندن قام بتحويل مبالغ مالية بالفاكس من بنك في نيويورك الى حساب اخر في بنك في جوناف و قد استندت محكمة الاستئناف في قضائها السابق الى ان هذا الفعل الذي يشكل جريمة نصب وقع في الولايات المتحدة الامريكية بيد اننا نرى ان النشاط وقع في انجلترا و ان هذا الاخير يجب ان يكون مختصا استنادا إلى مبدأ الإقليمية .

6- مزايا تقرير الاختصاص لمحكمة مكان تواجد الجهاز الخادم في جرائم المعلوماتية :

تسري قواعد العامة في غياب نص خاص بخصوص المحكمة المختصة حيث للمدعي ان يلجا الى محكمة مكان الجهاز الخادم او محكمة تحقق النتيجة و لكن المشكلة ان هذه الاخيرة قد تتحقق في

اكثر من مكان بل في اكثر من دولة غير ان اختصاص محكمة جهاز الخادم يحقق المزايا التالية :

- سهولة معرفة مكان تواجد الجهاز بينما يصعب احيانا معرفة صاحب الرسالة التي تبث عبر موقع الانترنت و ربما اذا كان سجل هذا الموقع اسم وهمي او بدون اسم محدد او ربما يكون في الخارج و يستدعي الامر لرفع الدعوى في مكان اقامته، السفر الى الخارج و متابعة اجراءات الدعوى في الخارج.

- عادة ما يكون القائم بالسكين مليئ يمكن الرجوع عليه بالتعويض على خلاف صاحب الرسالة المؤثمة .

- رفع الدعوى امام محكمة الجهاز الخادم يجيز التعويض عن سائر الاضرار التي تحققت في اماكن مختلفة من العالم على خلاف الحال عند رفع تلك الدعوى امام احدى المحاكم التي تصل اليها شبكة الانترنت .

- رفع الدعوى امام محكمة جهاز الخادم يسمح للمحكمة بان تصدر امرا الى القائم بالتسكين بمنع الدخول الى الموقع الذي تضمن رسائل مؤثمة او ضارة بالاخرين .

- 7- الاختصاص في حالة الاشتراك في الجريمة : تاخذ كثير من الدول بنظرية استعارة الاجرام في تحديد اختصاص قضائها بمعنى ان قضاءها لا يختص بمحاكمة الشريك في الجريمة التي وقعت في الخارج و كان هذا القضاء غير مختص اصلا في محاكمة الفاعل

الاصلي ، مع ذلك فان دول اخرى تقرر اختصاص قضائها بمحاكمة الشريك في الحالة السابقة و ذلك مثل فرنسا حيث ينص قانون العقوبات الفرنسي على هذا النوع من الاختصاص في المادة 113 فقرة 05 منه وقد استلزم القانون الفرنسي توافر شرطين لقيام هذا الاختصاص :

الاول : ان يكون الفعل معاقب عليه في القانونين الفرنسي و الاجنبي و ان يكون قصد صدر حكم نهائي اجنبي يقرر وقوع الجريمة الأصلية في الخارج .

ثانيا : ان يكون دور المتهم المتواجد في الاقليم الفرنسي انه شريك فيها وليس فاعلا اصليا كما لو قانم بارسال المواد المعاقب عليها الى جهاز الخادم المتواجد في خارج البلاد .

8- تاثير الارتباط بين جرائم الكمبيوتر على اختصاص المحاكم :

اذا كان القضاء الوطني يختص بمحاكمة احداث جرائم فانه يختص ايضا بجرائم اخرى المرتبطة بالجريمة الأصلية حتى و لو كانت تلك الجرائم المرتبطة لا تدخل أصلا في اختصاصه . لذا قضت محكمة النقض الفرنسية بان القضاء الفرنسي يختص بمحاكمة المتهم الاجنبي اذا ارتكب جريمة وقعت في الخارج مادامت هذه الجريمة مرتبطة مع الاخرى و قعت في فرنسا من طرف نفس المتهم و يتحقق ذلك كثيرا في مجال جرائم المعلومات اذا وقعت عن طريق الانترنت بحيث يتم التداخل من اكثر من دول .

9- سلطة المحكمة في اصلاح الضرر الناشئ عن جرائم الكمبيوتر و الانترنت :

للمحكمة ان تامر بما تراه من تدابير ترمي الى اصلاح الضرر من ذلك ان تامر بوقف دعاية معينة على شبكة الانترنت و للمضرور الا ان ينتضر محكمة الموضوع ان تفصل في الدعوى و ان يطلب الى قاضي الامور المستعجلة ان يصدر امر وقف رسائل المعينة على الرغم من وجود منازعة متعلقة لموضوع الدعوة وقبل الفصل في هذا الموضوع.

ا

المبحث الثاني : الجوانب الإجرائية للتعاملات الالكترونية

لقد ألقت الثورة المعلوماتية بظلالها على قوانين العقوبات خاصة بتلك الدول التي استفادت من ثمار هذه الثروة و وجب عليها في الوقت ذاته ان تتفادى عيوبها و ما ظهر من جرائم فتاكة تصدت لها قوانين العقوبات و عاقبت عليها و الملاحظ في هذا المجال انه كلما كان الاعتناء الاكبر على تقنية المعلومات كلما كانت الحاجة اكثر إلحاحا لوضع نصوص لحماية هذه المعلوماتية الذي يؤدي بدوره الى فرض و معاقبة المجرمين الذين يقومون على مخالفة القوانين و النظم الدولية فالجوانب الاجرائية امر مهم لتطبيق العقوبة سواءا على لمستوى الوطني و سواءا كان هذا الشخص طبيعي او معنوي او كانت على المستوى الدولي .

جـــرائـــم النصـــب الإلكتـــرونـــي

المطلب الأول العقوبات الجزائية على المستوى الوطني :

يتناول المشرع الجزائري الجزاءات المقررة لهذا النوع من الجرائم الحديثة من خلال القانون 15/04 الذي تضمن في مواده عقوبات ردعية أصلية و تكميلية تطبق على الشخص الطبيعي و المعنوي تبنيا الى مبدا المسالة الجزائية فاعطت المادة 394 مكرر 1 الى مكرر 5 من نفس القانون حالات تسليط العقوبة على الاشخاص الذين يرتكبون جرائم ماسة بالانظمة المعلوماتية و و ضعت نظام عقابي بتناسب مع ذات الشخص الطبيعي و المعنوي و ذلك تماشيا مع المادة 13 من الاتفاقية الدولية من الاجرام المعلوماتي التي تجعل العقوبات المقررة رادعة و مشددة

جـــرائـــم النصـــب الإلكتـــرونـــي

الفرع الاول عقوبة الشخص الطبيعي

1 - العقوبة الاصلية : وضع المشرع الجزائري عقوبات حسب الخطورة الإجرامية للتصرفات المجرمين

1-1 الدخول و البقاء بالغش (الجريمة البسيطة)

اعتبر المشرع جنحة و أعطى لها عقوبة طبقا للمادة 394 مكرر من القانون 04-15 وهي من 03 اشهر الى سنة حبسا و غرامة مالية تصل من 10.000 د ج الى 50.000 د ج .

1-2 الدخول و البقاء بالغش (الجريمة المشددة)

هنا ضاعف المشرع العقوبة في حالة حذف او تغيير للمعطيات المنظومة المعلوماتية و ذلك بتقرير العقوبة من 06 اشهر الى سنتين غرامة مالية من 50.000 دج الى 150.000 دج اذا ترتب عن الدخول او البقاء الغير مشروع تخريب لنظام تشغيل المنظومة المعلوماتية و هذا طبقا للمادة 394 فقرة 02 من قانون العقوبات الجزائري .

1-3 الاعتداء العمدي على المعطيات

العقوبة المقررة في حالة الاعتداء العمدي على المعطيات داخل النظام طبقا للمادة 394 مكرر 02 من قانون العقوبات هي الحبس من 03 اشهر الى 03 سنوات و غرامة مالية من 200.000 ددج الى 500.000 د ج ، اما في حالة حيازة او افشاء او نشر او

جـــرائـــم النصـــب الإلكتـــرونـــي

استعمال المعطيات المتحصل عليها من احدى الجرائم الماسة بالأنظمة المعلوماتية و العقوبة المقررة هي الحبس من 02 شهرين الى 03 سنوات و غرامة مالية من 100.000 دج الى 5.000.000 دج طبقا الى الفقرة الثانية من المادة السابقة .

2- العقوبات التكميلية:

الى جانب العقوبات الأصلية التي تطبق على المجرم المرتكب للجريمة المعلوماتية فان المشرع الجزائري أضاف عقوبات تكميلية طبقا للمادة 394 مكرر 06 من القانون 15/04 هي كالاتي

2-1 المصادرة :

تشمل الاجهزة و البرامج و الوسائل المستخدمة في ارتكاب احدى الجرائم الماسة بالانظمة المعلوماتية مع مراعاة حقوق الغير حسن النية .

2-2 اغلاق المواقع :

و منا الامر يتعلق بالمواقع التي تكون محلا للجرائم الماسة بالنظام المعلوماتي .

2-3 اغلاق المحل او مكان الاستغلال :

هنا يجب ان يتوفر عنصر العلم بالجريمة لصاحبها في المحل مثل اغلاق المقهى الالكتروني الذي ترتكب فيه الجريمة

3- الظروف المشددة :

1 –1 نصت المادة 394 مكرر القرة 02 و 03 على الظرف الذي تشدد به العقوبة أي عقوبة جريمة الدخول البقاء الغير المشروع داخل النظام المعلوماتي و يتحقق الظرف عندما ينتج عن الدخول و البقاء حذف او تغيير للمعطيات التي يحتويها النظام او تخريب نظام اشتغال المعلومة ففي الحالة الاولى تتضاعف العقوبة طبقا للقفرة الاولى من المادة 394 مكرر و في الحالة الثانية تكون العقوبة من 06 اشهر الى سنتين و غرامة مالية تقدر 50.000 دج الى 150.000 دج و هذا الظرف المشدد هو ظرف مادي يكفي ان تقوم بينه و بين الجريمة الاساسية علاقة سببية حتى يمكن القول بتوافره .

2-3 تتضاعف العقوبة في حالة استهداف الدفاع الوطني او الهيئات او المؤسسات الخاضعة للقانون العام .

الفرع الثاني عقوبة الشخص المعنوي:

جاء في المادة 12 من الاتفاقية الدولية للاجرام المعلوماتي مبدا مسالة الشخص المعنوي فاقر المشرع الجزائري من خلال القانون 15/04 و ذلك بامكانية قيام المسؤولية الجزائية للشخص المعنوي عن الجرائم المحددة و ذلك حسب الشروط المنصوص عليها في القانون و العقوبات المقررة و المطبقة على الشخص المعنوي في مواد الجنايات و الجنح هي :

- حل الشخص المعنوي .

- غلق المؤسسة او فرع من فروعها لمدة لا تتجاوز الخمس سنوات .

- الإقصاء من الصفقات العمومية العمومية لمدة لا تتجاوز 05 سنوات .

- لمنع من مزاولة نشاط او عدة نشاطات مهنية او اجتماعية .

- مصادرة الشيئ الذي اتعمل في ارتكاب الجريمة او نتج عنها

- نشر او تعليق الحكم .

- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 05 سنوت و تنصيب الحراسة على ممارسة النشاط الذي ادلا الى الجريمة او الذي ارتكبت الجريمة بمناسبته .

- اما بالنسبة للغرامة المالية فهي تعادل 05 مرات الحد الاقصى بالنسبة للشخص الطبيعي و هذا وفقا للما جاءت به المادة 394 مكرر 04 من القانون 15/04 .

جـــرائـــم النصـــب الإلكتـــرونـــي

المطلب الثاني : العقوبات الجزائية على المستوى الدولي

ان الإجرام المعلوماتي في تزايد مستمر يوما بعد يوم وقد اتسع نطاقه كثيرا اثر الانتشار الواسع للحواسب الالية و شبكات الاتصال الخاص بها و كثرة الاعتماد عليه في مختلف جوانب الحياة اذ بات قطاع كبير من الناس على اتصال و ثيق بهذه المعلوماتية ولم يتردد المنحرفون منه في استغلاله لأغراضهم الدنيئة و توظيف معارفهم بها بالاعتداء على حقوق الآخرين دون ان يتجهم احد عناء التحرك من مكانه و انشار الواسع لشبكة الانترنت و سع كثيرا من مجال هذه الجرائم إضافة الى صعوبة إثباتها و ملاحقة مرتكبيها اذ انها جرائم عابر للحدود او ذات طابع دولي جعل كل دولة تقف بمفردها عاجزة عن التصدي لها هذا الوضع استدعى من الدول ان تلم شملها و توحد جهودها في مواجهة هذا الاجرام فتحركت من خلال العديد من المنظمات الدولية و الاقليمية لابرام الاتفاقيات في هذا الخصوص و سوف تنعرض فيما يلي لدور الذي لعبته كل من الدول المتحدة و الاتحاد الاروبي و بالاضافة الى اهمية الدور العربي

جـــرائـــم النصـــب الإلكتـــــرونـــــي

الفرع الاول :دور هيئة الامم المتحدة و المجلس الأوربي .

1- دور هيئة الامم المتحدة.

تبدل الامم المتحدة جهودا كبيرة في سبيل تعزيز العمل المشترك بين اعضاء المنظمة من اجل التعاون في مواجهة الاجرام المعلوماتي ذلك من خلال اشرافها على عقد المؤتمرات الدولية الخاصة بمنع الجريمة و معاملة المجرمين او من خلال الوكالات و المنظمات العاملة تحت لوائها كالمنظمة العالمية للملكية الفكرية " wipo" .

ففيما يخص مؤتمرات منع الجريمة فقد كلف المؤتمر السابع المنعقد ب ميلانو عام 1985 لجنة الخبراء 20 بدراسة موضوع حماية نظم المعلومات و الاعتداء على الحاسوب الالي و اعداد تقرير يعرضه على المؤتمر الثامن و لقد اكد هذا الاخير على ضرورة الاستفادة من التطورات العلمية و التكنولوجية لمواجهة هذه الحركة و اشار الى مسالة الخصوصية و اختراقها بالاطلاع على البيانات الشخصية المخزنة داخل نظام الحاسب الالي و ضرورة اعتماد ضمانات لصون سريتها كما اكد على ضرورة تشجيع التشريعات الحديثة التي تتناول هذه الجرائم بصفتها نمطا من انماط الجريمة المنظمة و يمكن إجمال توصيات مؤتمر هافانا لعام 1990 في المبادئ التالية :

1- تحديث القوانين الجنائية الوطنية بما في ذلك تدابير المؤسسية .

2- تحسين امن الحاسب الالي و التدابير المعنية .

3- اعتماد اجراءات تدريب كافية للموظفين و الوكالات المسؤولة عن منع الجريمة الاقتصادية و الجرائم المتعلقة بالحاسب الالي و التحري و الادعاء فيها .

4- تلقين اداب الحاسب الالي كجزء من مفردات مقررات الاتصالات و المعلومات .

5- اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم بتلك الجرائم .

6- زيادة التعامل الدولي من اجل مكافحة هذه الجرائم .

اما المؤتمر التاسع لمنع الجريمة و معاملة المجرمين المنعقد في القاهرة عام 1995 فقد اوصى بوجود بحماية الانسان في حياته الخاصة و في ملكيته الفكرية من تزايد مخاطر التكنولوجيا و وجوب التنسيق و التعاون بين افراد المجتمع الدولي لاتخاذ الاجراءات المناسبة.

و قد اوصى المؤتمر العاشر المنعقد في بودا بست – المجر- عام 2000 بوجوب العمل الجاد على الحد من جرائم المعلوماتية المتزايدة و لمعتبرة نمطا من انماط الجرائم المستحدثة و العمل على اتخاذ تدابير مناسبة للحد من اعمال القرصنة .

و اضافة الى هذه المؤتمرات لا يكفي ما تلعبه المنظمة العالمية للملكية الفكرية كاحدى الوكالات المتخصصة التابعة للولايات المتحدة من دور في مجال محاربة القرصنة المعلوماتية و حماية البرامج .

2- دور المجلس الاوربي .

لقد بدل و مازال المجلس الأوروبي جهودا كبيرة في مواجهة جرائم المعطيات و الحاسب الالي عموما ففي 1981/01/28 تم توقيع اتفاقية تحت إشرافه تعلقت بحماية الأشخاص في مواجهة المعالجة المعلوماتية للمعطيات الطبيعية و الشخصية ولقد اصدر المجلس العديد من القواعد التوجيهية في هذا المجال تضمنت و جوب تجريم العديد من جرائم المعلوماتية كما تضمنت العديد من الاجراءات الفنية لتجنب الوصول غير المرخص به الى المعلومات المخزنة كحماية كلمة السر المستخدمة في النهايات الطرفية و حماية الاوامر الخاصة بالتشغيل و ترميز المعلومات الشخصية .

اهم ما قام به المجلس الاوروبي في هذا المجال هو اشرافه على اتفاق بودابست الموقعة في 2001/11/23 و قد جاء في المذكرة التفسيرية لهذه الاتفاقية مايلي " هناك سيمات بارزة لتكنولوجيا المعلومات تتمثل في الاثر الذي احدثته و ما زالت تحدثه على تطور التكنولوجيا كذلك يكفي ان يتم ادخال البيانات الى شبكة معينة من خلال عنوان المرسل اليه حتى تصبح متوافرة لاي شخص يردي الدخول اليها و على ذلك يجب على القانون الجنائي

جـــرائـــم النصـــب الإلكتـــرونـــي

ان يحافظ على مواكبته لهذه التطورات التكنولوجية التي تقدم فرصا وا سعة لإساءة استخدام امكانيات الفضاء المعلوماتي و ان يعمل على ردع هذه الافعال الاجرامية مع تطبيق السلطات البشيرية المقررة في بيئة تكنولوجيا المعلومات "

و تتكون هذه الاتفاقية من ثمانية و اربعين مادة موزعة على اربعة ابواب ،يعالج الباب الاول منها استخدام المصطلحات و يتناول الباب الثاني الإجراءات الواجب اتخاذها على المستوى القومي و يظم ثلاثة أقسام أولها للقانون العقابي المادي او الموضوعي و ثانيها للقانون الإجرائي و ثالثها للاختصاص القضائي .

اما الباب الثالث قد تم تخصيصه للتعاون الدولي و هو يشتمل على قسمين أولهما المبادئ العامة و ثانيهما الاحكام الخاصة و اخيرا ياتي الباب الرابع الذي يتعرض لشروط الختامية قد تم التمهيد لهذه الابواب الاربعة بافتتاحية او المقدمة .

وقد شملت الاتفاقية في شقها الموضوعي النص على تسع جرائم موزعة على اربع فئات .

الفئة الاولى : الجرائم ضد سرية و سلامة و اتاحة البيانات و النظم المعلوماتية وقد تناولتها المواد من 02 الى 06 كما يلي

المادة 02 – الولوج غير القانوني.

المادة 03 – الاعتراض غير القانوني .

جـــرائـــم النصـــب الإلكتـــــرونـــــي

المادة 04- الاعتداء على سلامة البيانات .

المادة 05 – الاعتداء على سلامة النظام .

المادة 06 – إساءة استخدام جهاز الحاسب .

الفئة الثانية : الجرائم المعلوماتية المتصلة بالحاسب الالي تناولتها المادة 07 و 08 فالمادة 07 تحدثت عن التزوير المعلوماتي اما المادة 08 عن الغش المعلوماتي .

الفئة الثالثة : الجرائم المتصلة بالمحتوى و تناولتها المادة 09 و التي تنص على الجرائم المتصلة بالمواد الإباحية الطفولية .

الفئة الرابعة : الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية و الحقوق المجاورة نصت عليها المادة 10 و قد نتاولت المادة 11 الشروع و الاشتراك و تناولت المادة 12 مسؤولية الاشخاص المعنوية و تناولت المادة 13 الجزاءات و التدابير .

الفرع الثاني: الدور العربي .

يعتبر مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد كقانون نموذجي بموجب القرار رقم 229 لسنة 1996 يعتبر الخطوة الاهم عربيا في مجال مواجهة جرائم المعطيات و الحاسب الالي عموما و بالرجوع الى الباب السابع من القانون الخاص بالجرائم ضد الاشخاص نجده قد حوى فصلا خاصا بالاعتداء على حقوق الاشخاص الناتج عن المعالجة المعلوماتية و ذلك في المواد من 461 الى 446 حيث اشارة المواد الثلاث الولى فيها الى وجوب حماية الحياة الخاصة و اسرار الافراد من خطر المعالجة الالية و كيفية جمع المعلومات الاسمية و كيفية الاطلاع عليها اما المادة 446 فعاقبت على الدخول بطريق الغش الى كامل او جزء من نظام المعالجة الالية للمعلومات و عرقلت او افساد نظام التشغيل عند اداء و ظائفه المعتادة و تغيير المعلومات داخل النظام و تزوير و ثائق المعالجة الالية و سرقة المعلومات وسوف نتطرق الى اهمية الدور العربي في دولتين الأولى في الجزائر و الثانية في مصر .

الدور الجزائري :لقد شهد العالم في الآونة الاخيرة تطورا مذهلا و سريعا في مجال المعلوماتية و قد تسارعت وتيرة الاعتماد على هذه الاخيرة في شتى مجالات الحياة حتى ظلت ضروريتا لا يمكن الاستغناء عنها و اصبحت مقياسا لتطور الدول و الجزائر ليست بمنا عن هذا التحول المعلوماتي و هي و ان لم تبلغ مصاف الدول

المتقدمة فانها قد تارت بهذه الثورة المعلوماتية سلبا و إيجابا ، فلقد تاثرت بما جرته هذه الثورة من الوان جديدة من الاجرام لم تشهدها البشرية من قبل ارتبطت ارتباط و ثيقا بالحاسب الالي و ما حواه من معطيات .

هذه الجرائم طالت مصالح جديدة غير تلك لتي يحميها القانون فبدت الحاجة شديدة لوضع نصوص جديدة و لم يجد المشرع الجزائري بدا من تعديل قانون العقوبات و لقد جاء في عرض اسباب هذا التعديل "ان التقد التنكنولوجي و انتشار وسائل الاتصال الحديثة ادى الى بروز اشكال جديدة للاجرام مما دفع بالكثير من الدول الى النص على معاقبتها و ان الجزائر تسعى من خلال هذا المشروع الى توفير حماية جزائية لأنظم المعلوماتية و أساليب المعالجة الآلية للمعطيات و ان هذه التعديلات من شئنها سد الفراغ القانوني في بعض المجالات و سوف يمكن لا محالة من مواجهة بعض اشكال الاجرام الجديد ".

و كان التعديل بموجب القانون 15/04 المؤرخ في 2004/11/10 الموافق ل 27 رمضان 1452 ه المعدل و المتمم بالامر رقم 66 - 156 المتضمن قانون العقوبات و الذي افرد القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات و الذي تضمن ثمانية مواد مكن المادة 394 مكرر و حتى المادة 394 مكرر 07 و الذي نص على عدة جرائم هي :

جـــرائـــم النصـــب الإلكتـــرونـــي

1- الدخول او البقاء عن طرق الغش في كل او جزء من منظومات المعالجة الالية للمعطيات

2- الدخول او البقاء المؤدي الى حذف و اتغير المعطيات .

3- الدخول او البقاء المؤدي الى تخريب نظام اشتغال المنظومة .

4- ادخال او ازالة او تعديل المعطيات بطريق الغش في نظام المعالجة الالية .

5- تصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مرسلة عن طرق المنظومة المعلوماتية .

6- حيازة او افشاء او نشر او استعمال لاي غرض كان المعطيات المتحصل في احدى الجرائم المنصوص عليها في هذا القسم .

كما شددت العقوبة الى الضعف الى استهدفت الجريمة الدفاع الوطني او المؤسسات العمومية و شددت عقوبة الغرامة على الشخص المعنوي الى 05 مرات للحد الاقصى المقرر لشخص الطبيعي و ذلك بعد اقرار المواد 18 مكرر و 18 مككر 01 و 51 مكرر من التعديل نفسه لمسؤولية الشخص المعنوي بوجه عام .

كما عاقبت تلك المواد على الاشتراك في مجموعة او اتفاق يتألف بغرض الإعداد لجريمة او اكثر من الجرائم المنصوص عليها في هذا القسم .

ونص هذا التعديل ايضا على عقوبة مصادرة وسائل ارتكاب الجريمة و اغلاق المواقع التي تكون محلا لها و اغلاق المحل او المكان الذي ارتكبت فيه الجريمة ، كما عاقب التعديل ايضا على الشروع في جرائم هذا القسم .

و كانت مواجهت الجريمة المعلوماتية احدى بنود اتفاق يؤسسة اشراكه بين الجزائر و الاتحاد الاوروبي عقد بتاريخ 2002/04/22 و تضمنت ذلك المادة 86 .

2- الدور المصري :

لا يحوي قانون العقوبات المصري نصوصا تحمي معطيات الحاسب الالي او تحمي المال المعلوماتي عموما و المشرع المصري لا يحمي من البيانات الا انواع معينة دون ان يولي اعتبارا لطريقة معالجتها تقليدية كانت ام آلية هذه البيانات تحميها قوانين خاصة و تتعلق بما يلي :

1- بيانات الاحوال المدنية .

2- البيانات الضريبية و اقرارات الكسب غير المشروع (قانون الضرائب رقم 157 لسنة 1981) .

3- بيانات التعداد و الإحصاءات السكانية (القرار الجمهوري بالقانون رقم 35 لسنة 1960 المتعلق بالحصاء و التعديد و المعدل بقانون رقم 21 لسنة 1982).

4- بيانات حسابات البنوك و المعاملات المتعلقة بها (قرار رئيس الجمهورية بالقانون رقم 205 لسنة 1960).

وقد حاول البعض قياس البيانات او المعلومات الشخصية التي تتم معالجتها بواسطة اجهزة الحاسب الالي ثم تحفظ في بنوك المعلومات على بعض البيانات السابقة كتلك المتعلقة بالتعداد و الإحصاءات السكانية و عارضهم في ذلك البعض الأخر كما حاول اخرون تطبيق نص المادة 310 من قانون العقوبات المصري و بخاصة لحماية سر المهنة على حالة افشاء المعلومات الشخصية التي تتم معالجتها الكترونيا و تخزن في بنوك المعلومات و لقد لقوا معارضة أيضا .

و لأكن يجدر بالذكر ان ثمة مشروع لقانون التجارة الالكترونية تم إعداده بمصر بمعرفة مركز المعلومات و دعمه مجلس الوزراء و الذي تضمن تجريم للعديد من الافعال و التي تمس بمعطيات الحاسب الالي و فيما يلي الجرائم التي نص عليها هذا المشروع :

*كشف مفاتيح تشفير المودع بمكتب تشفير .

*استخدام توقيع الكتروني او موحوه او التعديل فيه او في مادة المحرر الالكتروني دون موافقة كتابية مسبقة من صاحب الحق .

* الدخول بطريق الغش او التدليس على نظام المعلومات او قاعدة البيانات او قاعدة تتعلق بالتوقيعات الالكترونية .

جـــرائـــم النصـــب الإلكتـــــرونـــــي

*الاتصال او الإبقاء على الاتصال بنظام المعلومات او قاعدة البيانات بصورة غير مشروعة .

*صنع او حيازة او الحصول على نظام معلومات ا برنامج لاعداد توقيع الكتروني دون موافقة صاحب الشأن.

* تزوير او تقليد محرر او توقيع الكتروني او شهادة اعتماد توقيع الكتروني .

*استعمال محرر او توقيع الكتروني مزور او شهادة مزورة باعتماد توقيع الكتروني .

*استخدام نظام او برنامج لحيلولة دون اتمام المعاملة التجارية بالوسائل الالكترونية .

*إذاعة او تسهيل إذاعة و لو في خير علانية المحرر او توقيع الكتروني او فض شيفرته دون مصوغ قانوني دون موافقة صاحب الشأن و تشدد عقوبة هذه الجريمة اذا كان فاعلها امينا على المحرر او توقيع الالكتروني بمقتضى صناعته او وظيفته اذا كان من العاملين لديه .

* الادخال العمدي او باهمال لفيروس الى نظام معلوماتي بدون موافقة مالك النظام او حائزه الشرعي .

وقد تراوحت عقوبات الجرائم السابقة الذكر بين الحبس او الحبس مع الشغل او الغرامة و مصادرة الاجهزة و الانظمة و البرامج

جـــرائـــم النصـب الإلكتـــرونـــي

المستخدمة في ارتكاب الجرائم مع غرامة بضعف ما عادى على المحكوم عليه من الربح او الفائدة من وراء الجريمة .

الخاتمة

- ان التطور في مجال المعلوماتية لم يبقى مقتصرا على الجانب الاقتصادي بل أصبح يمس جميع الجوانب سواءا من الجانب السياسي او الاجتماعي و الثقافي و العلمي حيث تنوعت استعمالاته ، الا ان هذا التطور لم يخالوا من مخاطر الاعتداء على المعطيات و البيانات المعلوماتية.

لذا قامت العديد من الدول باتخاذ التدابير و الإجراءات الرادعة لهذا النوع من الجرائم من خلال نص قوانين جديدة او تعديل القوانين القديمة للوقوف في وجه الإجرام المعلوماتي .

وهذا ما دعى المشرع الجزائري الى تعديل قانون العقوبات بما يتناسب مع التعديلات الدولية من خلال القانون 15/04 و الذي اعتبر خطوة هامة في مجال التشريع الجنائي و الذي كان تجسيدا لأحكام الاتفاقيات الدولية للإجرام المعلوماتي فوسع من نطاق العقوبة على الشروع بالاضافة الى العقوبات التكميلية ، بالاضافة الى محاولات الجزائر لحق الركب الدولي من خلال ما سنته الدول المتقدمة من قوانين على الرغم من الفراغ القانوني الموجود الذي لم يتطرق الى جميع الجرائم و ذلك لان الجزائر لم تحذوا حذو الدول المتقدمة و يستجد فيها من جرائم جديدة و في الأخير نطرح بعض الاقتراحات النظرية و التطبيقية لمواجهة جرائم المعلوماتية من خلال تخصيص قانون خاص بالاجرام المعلوماتي و جرائم الحاسب الالي و الانترنت و هذا ما قامت به بعض الدول الأجنبية و العربية.

جـــرائـــم النصـــب الإلكتـــــرونـــــي

* قائمة المراجع*

أولا : المراجع العامة :

- كامل سعيد ، شرح الأحكام العامة في قانون القوبات الأردني و القانون المقارن ، دار الفكر للنشر و التوزيع عمان . الطبعة الثانية 1983.

- محمد عبد الله أبو بكر موسوعة جرائم المعلوماتية (جرائم الكمبيوتر و الأنترنت) المكتب العربي الحديث الاسكندرية 2007.

ثانيا : المؤلفات الخاصة :

- آمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دارهومه للطباعة و النشر و التوزيع الجزائر 2006.

- هدى قشقوشي ، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة الطبعة الأولى 1992.

- يونس عرب ، دليل أمن المعلومات الخصوصية (جرائم الكمبيوتر و الانترنت) الجزء الأول ، إصدارات دار المعارف العربية 2001.

- الدكتور عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية مصر 2004.

-نبيلة هبه هروال ، الجوانب الإجرائية لجرائم الأنترنت ، دار الفكر الجامعي 2007.

هشام محمد فريد رستم ، العقوبات و مخاطر جرائم المعلوماتية ، دار النهضة العربية القاهرة 2000.

- اللواء الدكتور حسنين المحمدي بوادي ، إرهاب الانترنت الخطر القادم ، دار الفكر الجامعي ، الأسكندرية الطبعة الأولى 2006.

- الأستاذ محمد عبد الله أبو بكر ، موسوعة جرائم المعلوماتية و جرائم الأنترنت ، المكتب العربي الحديث الأسكندرية 2007.

- الأستاذ عبدالله عبد الكريم عبد الله ، جرائم المعلوماتية و الأنترنت ، منشورات الحلبي للمعرفة الطبعة الأولى 2007.

- الدكتورة شيماء عبدالغني محمد عطاء الله ، الحماية الجنائية للتعاملات الإكترونية ،دار الجامعة الجديدة ، الأسكندرية الطبعة 2007.

- محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي ، دار الجامعة الجديدة ، الأسكندرية 2007.

جـــرائـــم النصـــب الإلكتـــرونـــي

النصوص التشريعة :

القانون 15/04 المؤرخ في 2004/11/10 المعدل و المتمم للامر 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات ، (ج.ر رقم : 71 الصادرة بتاريخ : 2004/11/10).

النصوص الدولية :

الإتفاقية الدولية للجرائم المعلوماتية التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأروبي و تم وصفها بالتوقيع منذ تاريخ 2001/11/23.

مواقع الأنترنت :

www.arablaw.org

www.algerie.dz.com

www.entv.dz