الجمهوريـة الجزائريـة الديمقراطيـة الشعبيـة

وزارة التعليم العالي و البحث العلـمي

جامعة الدكتور مولاي الطاهر – سعيـدة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في العلوم القانونية و الإدارية

تخصص : علم الإجرام

بعنوان

# الجريمة الواقعة على المواقع الإلكترونية


إعداد الطالب :

رحالي جيلالي

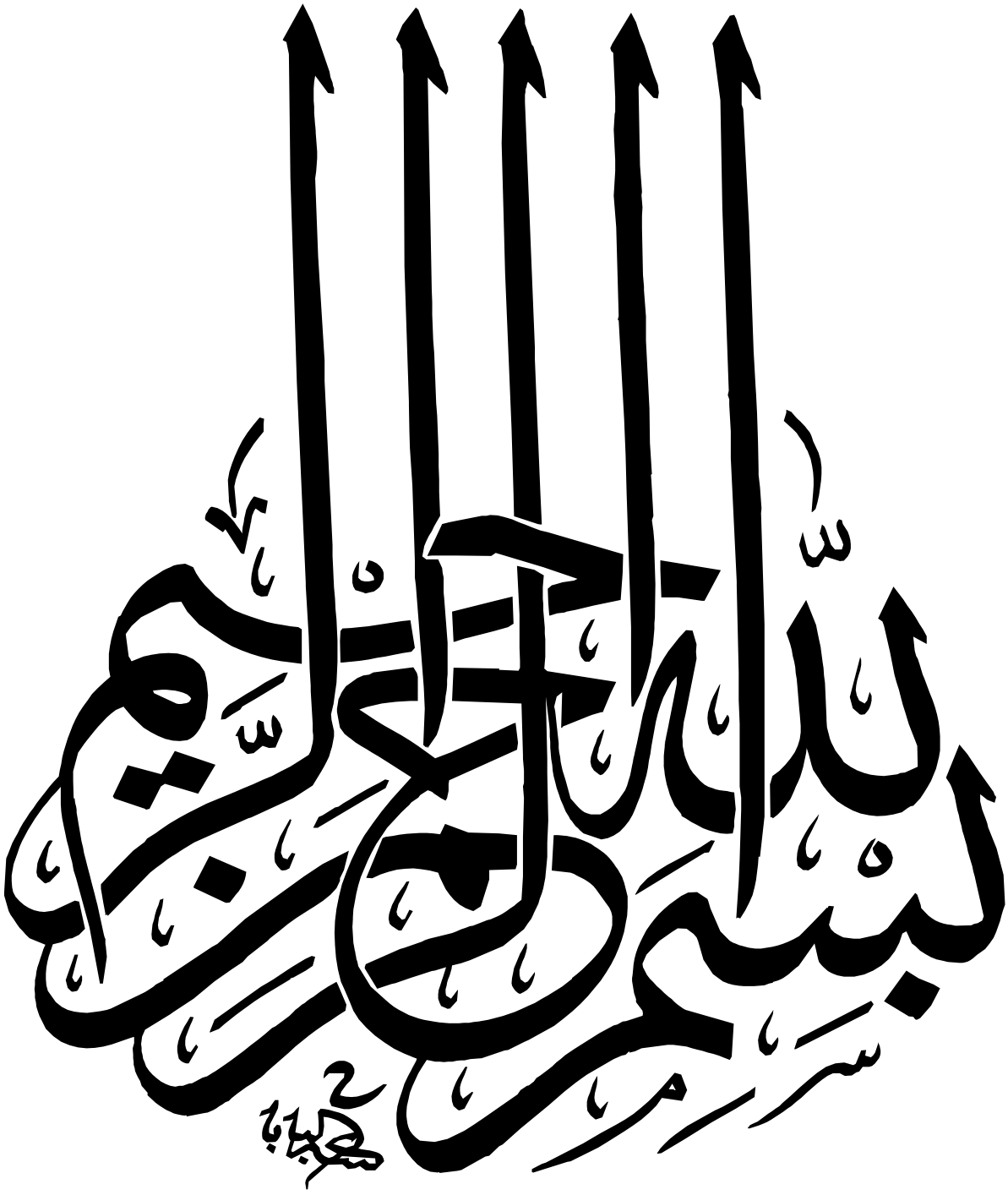
الأستاذ المشرف :

د. بن صغير عبد المؤمن.


لجنة المناقشة :

| | | | |
|---|---|---|---|
| عثماني عبد الرحمان | أستاذ | جامعة سعيدة | رئيسا |
| بن صغير المؤمن | أستاذ | جامعة سعيدة | مشرفا و مقررا |
| فليح كمال عبد المجيد | أستاذ | جامعة سعيدة | عضوا مناقشا |
| بوادي مصطفى | أستاذ | جامعة سعيدة | عضوا مناقشا |
| بن عيسى أحمد | أستاذ | جامعة سعيدة | عضوا مناقشا |

السنة الجامعية 2016-2017


بسم الله الرحمن الرحيم

# إهداء

أهدي هذا العمل المتواضع إلى روح والدي رحمات الله عليه

و إلى والدتي أطال الله في عمرها

وإلى روح الحاجة قاسمي عافية و التي فقدناها خلال هذا الأسبوع

إلى زوجتي وأولادي

إلى كل من ساعدني من قريب أو من بعيد على إتمام هذا العمل

جيلالي

# كلمة شكر و عرفان

" رب أوزعني أن أشكر نعمتك التي أنعمت علي و على والدي و أن أعمل صالحا ترضاه و أصلح لي في ذريتي إني تبت إليك و إني من المسلمين " .

سورة الأحقاف الآية 15 .

بعد الحمد لله و الشكر له عز و جل با لقدرة و حسن العطاء أتقدم بأسمى و أخلص معاني التقدير و الاحترام و بجزيل الشكر و العرفان إلى اللجنة الموقرة و التي قبلت مناقشة هذا العمل المتواضع ، و إلى كل من علمني حرفا .

إلى كل عمال إدارة معهد الحقوق دون استثناء.

و أتقدم و أخص بالذكر إلى أستاذي الفاضل الأستاذ بن صغير المشرف على عملي على سعة صدره و رحابة قلبه .

و كل شكري إلى من ساعدني في إنجاز هذا العمل من قريب أو بعيد .

# مقدمة

**مقدمة :**

المعلومات مورد لا يقل ولا ينضب، تتزايد دوما ولا تتناقص بالاستخدام أو تستهلك،ترتبط بالزمان والمكان، وتتفاعل مع التطور، وعلى متلقيها ومدى علاقتها بحاجته تتوقف إلى حد كبير قيمتها وهي في الحقبة المعاصرة مفتاح للموارد الأخرى، وسلعة أو خدمة تباع وتشترى ومصدر قوة اقتصادية وسياسية لمن يحسن جمعها وتنسيقها واستخدامها، إذ توصف الطفرة المعاصرة في نمو وتكاثر المعلومات بانفجار المعلومات، فكما نتج عن تحكم البشرية في القدرة الميكانيكية وإحلالها بدرجة كبيرة مكان القوة العضلية للإنسان ما يسمى بالثورة الصناعية، كذلك يقف التحكم في المعلومات من خلال التطوير المتواصل للمعلوماتية كمساعد للقدرات التنظيمية للعقل البشري وراء ثورة كلية شاملة تجتاح العالم الآن هي الثورة المعلوماتية الموسومة أيضا بالثورة الصناعية الثالثة التي تعزز الإمكانيات الفكرية والقدرة المنطقية للإنسان، وتنقل الحضارة الإنسانية من عصر الصناعة إلى عصر أو مجتمع المعلومات.

ومع هذه الثورة، وما نجم عنها من تحولات اقتصادية و اجتماعية تشهد ببزوغ فجر المعلومات تزايد استخدام الحاسب الآلي حيث لم يعد ثمة مجال اقتصادي أو اجتماعي أو صناعي أو إداري إلا وتباشر الحاسبات وتقنية المعلومات دورا أساسيا في أدائه و تطويره، وهكذا جاء تقدم تقنيات الحاسبات و المعلومات وتزايد الاعتماد عليها في تسيير شؤون المجتمعات، مصحوبا بفرص جديدة لارتكاب أشكال وصور مستحدثة تحمل طابع هذه التقنيات وتساير على الدوام تيار تقدمها ( Techno – Crimes ) من الجرائم الفنية باعتمادها على الحاسب كأداة لارتكابها[1] فالعالم يشهد في الوقت الراهن ثورة تكنولوجية هائلة تتجلى أبرز مظاهرها في ثورة المعلومات و الاتصالات و الهندسة الوراثية والأجيال الجديدة للحاسبات الآلية.

ولا شك في أن هذه التكنولوجيا الحديثة تقدم للدول وأجهزتها الأمنية الكثير من التسهيلات والإمكانات التي تسهم في رفع كفاءتها وتطوير قدرتها على التصدي للجريمة، إلا أن هذا التطور

1. محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة غريب، القاهرة 1984 ، ص 5 .

التكنولوجي أدى و يؤدي في الوقت نفسه إلى تطوير وتحديث الجريمة من حيث الأساليب والمضامين وبخاصة في ظل اتجاه التنظيمات أو العناصر الإجرامية إلى توظيف بعض مخرجات التكنولوجيا الحديثة كالمعلوماتية في أنشطتها وممارستها الإجرامية، و في هذا الصدد تقول " روى جودسون " خبيرة بمركز المعلومات الوطني الأمريكي " لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة[1] فالإعلام الآلي الذي ارتقى بمستوى الإنسان وانتقل به إلى عصر المعلوماتية و التقدم هو ذاته الذي يستخدمه بارونات الجريمة وعصابات المافيا، فإذا كانت الأسلحة المتطورة والمعدات الحديثة من الأمور الشائعة الاستخدام في ممارسة الجريمة.فإن الجديد في هذا المجال هو تكثيف استخدام نظم المعلومات و الاتصالات الحديثة في الأنشطة الإجرامية لتمكينها من التخطيط لأنشطتها وتنفيذها .

فالمعلوماتية مثل كل تطور جديد تحمل في طياتها جانبًا مظلما يتجسد في مجال القانون الجنائي بظهور المجرم المعلوماتي أو ظاهرة الإجرام المعلوماتي بصفة عامة، إذ لم يعد مجرم القرن الأخير إنسانا مقنعا يشهر سلاحه في وجه ضحيته بل أصبح رجلا ذا ياقة بيضاء فالصراع قائم بين العلم والجريمة صراع مستمر بين استخدام العلم من أجل الإنسان وأمنه واستقراره، وبين استخدامه ضد الإنسان وزعزعة أمنه واستقراره.

لذلك فوسائل الإعلام لا تخلو أسبوعيا من الأخبار المتعلقة بأمن الشبكات الحاسوبية، فالحرب مستمرة بين مدمني الكومبيوترات الطفيليين و المختصين بأمن الشبكات الكمبيوترية، فالأنباء متنوعة فهناك خبر عن تمكن مجموعة من مدمني الحواسب من اختراق شبكة أنظمة المعلومات الدفاعية الأمريكية و المسؤولة عن الأقمار الصناعية و الاتصالات العسكرية، و هناك خبر عن تسلل لأنظمة وزارة الخارجية الأمريكية وآخر عن فيروس I LOVE YOU و CODE-RED إلخ وما أحدثته من خسائر مادية عبر الشبكات العالمية، مما أدى إلى تسليط الأضواء على جريمة الحاسوب[1]

---

1. محمد ناجي، أمن المعلومات، من ينتصر في النهاية، مجلة الشرطة، العدد 1999 ، 342، ص 34.

ولذلك فمع إدراك خطورة و سهولة ارتكاب أشكال الإجرام الجديدة التي أفرزتها بيئة المعالجة الآلية للمعطيات و التنبه لآثارها السلبية بدأت مكافحتها تحظى باهتمام متزايد من الحكومات و حتى العديد من المنظمات الدولية، فأخذ الفنيون و خبراء أمن الحاسبات، فضلا عن رجال الصناعة يركزون جهودهم البحثية و تجاربهم العلمية على سد ثغرات الأنظمة الأمنية و تحسين وتطوير أساليب الحماية الفنية النظم و البرامج و المعلومات لتصل إلى أقصى درجة ممكنة من الفعالية، دونما إنكار من جانبهم للحاجة إلى القانون لإسباغ صفة عدم المشروعية على انتهاك أمن المعلومات و تحديد إطار رد الفعل الاجتماعي تجاهه، وبالتالي تعزيز هده الحماية الفنية مما أدى إلى تجنيد رجال القانون، حيث تكفل الفقه الجنائي في بلدان عدة كفرنسا و إيطاليا و ألمانيا بإبراز الصعوبات التي تعترض تطبيق النصوص التجريمية للتشريعات التقليدية القائمة على أشكال الإجرام الجديدة التي أفرزتها المعلوماتية، وسعى إلى بلورة مجموعة من الضمانات القانونية التي تكفل تحقيق التوازن بين الضرورة الملحة في عصرنا لاستفادة من إمكانات الحاسبات و تقنيات المعلومات و بين الحاجة الفردية و الاجتماعية إلى حماية حرمة البيانات الشخصية، و بادر إلى توجيه الأنظار إلى طائفة من الأفعال في بيئة المعالجة الآلية للبيانات تقتضي مصلحة المجتمع الملحة إدخالها في دائرة التجريم والعقاب[1].

ومع أن الإجرام المعلوماتي لم يتخذ في الواقع الجزائري بعد، والواقع العربي كذلك الأبعاد التي اتخذها في الدول المتقدمة، إلا أن ذلك لا ينف ضرورة التصدي لبوادره كي لا يستفحل مع وتيرة النمو المتسارع الذي تشهده دول عربية عدة – ومن بينها الجزائر – في استخدام النظم المعلوماتية فضلا عن ظروف العولمة والتبعية التكنولوجية من مناخ موات لانتهاك حرمة البيانات الشخصية والمساس بالأمن القومي لهذه الدول و سيادتها الوطنية.

ومن هنا تتجلى أهمية موضوع " الجريمة الإلكترونية " وسبب اختيارنا له رغم ما يكتنف هذا الموضوع من صعوبات جمة ترجع إلى حداثة استخدام الحاسب الآلي و ما يتسم به من صبغة علمية بحتة غريبة في تصورنا على رجال القانون.

---

1.سهير لطفي ، تقرير حول ندوة الجرائم الاقتصادية المستحدثة المنعقدة 2004/01/20، مجلة حق المؤلف بين الواقع والقانون، مركز الدراسات القانونية، جامعة القاهرة، دار النشر هايتي، 1990 ، ص 129.

أطلق المفكر الأمريكي " ألفين توفلر"[1]، وهو أحد رواد علم المستقبل في العصر الحديث مصطلح العصر المعلوماتي أو عصر ثورة المعلومات على المرحلة الحالية من عمر الإنسانية، التي شهدت ظهور وتطور تقنية المعلومات بظهور واختراع الحاسبات الآلية التي قدمت للمجتمع والإنسان حياة أفضل، حيث أنه لا يمكن تصور سريان نظام أي قطاع اقتصاديا كان أم تربويا أم صحيا....الخ دون استخدام هذه التقنية الجديدة التي أتاحت القيام بالكثير من الأعمال الصعبة الانجاز بسهولة و يسر، و التي حققت إمكانية التواصل الإنساني حيث بفضلها أصبح العالم اليوم عبارة عن قرية صغيرة يتصل فيها الأشخاص و الجماعات بعضهم ببعض رغم ألاف الكيلومترات التي تفصل بينهم . إلا انه لكل عملة وجهان فهذا الوجه المشرق المفيد للتكنولوجيا الجديدة وتطورها قابله وجه مظلم لا يخلو من المخاطر تمثل في ظهور نمط جديد للسلوك الإجرامي هو الجريمة الإلكترونية، التي ظهرت بأنماط وسلوكات مختلفة كثيرة المخاطر حيث مست هذه السلوكات وهددت حياة الأفراد المالية والشخصية وحتى النفسية لذا سارع المهتمون بدراسة الجريمة الإلكترونية إلى تحديد مفهومها و تبيان معالمها كخطوة أولى نحو المكافحة.

حيث عرفها الفقيه (Merwe) على أنها الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية أو هي ختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات.[2]

1. تعريف عن الدكتور طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، طبعة 2009، ص 154.

2. تعريف عن الدكتورة نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية ،ط 1، 2005، ص 28.

وعرفها الفقيه Trédman على أنها " أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات." [1]

و عرفها الفقيه باركر Parker على أنها كل فعل غير مشروع يكون العلم بتكنولوجيا الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته و تحقيقه من ناحية أخرى.

وقد عيب على هذه التعاريف أنها كانت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام الإلكتروني و أنها ضيقت من مجال الجريمة الإلكترونية بحيث حصرتها بالمعرفة الجيدة للإعلام الآلي رغم انه هناك حالات ترتكب فيها هذه الجريمة بمعرفة سطحية فقط.

لذلك ظهر اتجاه موسع لمفهوم هذه الجريمة كتعريف الفقيه" كلاوس تايدومان "الذي عرفها على أنها كافة أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي ".

و تعريف كل من الفقيهين " Michel et Credo " ألّلذين اعتمدا في تعريفها على تعداد الجرائم التي تعد جرائم إلكترونية و التي بيّناها على أنها كل استخدام للحاسب كأداة في ارتكابها و الحالات المتعلقة بالدخول غير المصرح به لحاسب المجنى عليه أو بياناته[2].

- و الاعتداءات المادية على جهاز الحاسب نفسه.
- و للاستخدام غير المشروع لبطاقات الائتمان.
- و تزييف المكونات المادية و المعنوية للحاسب.

كما عرفها الأستاذان Bernadatte H. Shell و Clemens Martin على أنها الجريمة المتعلقة بتكنولوجيا الحاسب و الأنترنيت و عددا أيضا الأفعال التي تعد جرائم معلوماتية على أنها كل عمليات الدخول و النسخ غير المشروع وسرقة وسائل الاتصالات الهاتفية و إزعاج و ترهيب فئة معينة من الناس أو من المؤسسات بالإضافة إلى نشر و توزيع

---

1 . تعريف عن الدكتور طارق ابراهيم الدسوقي عطية، الامن المعلوماتي، دار الجامعة الجديدة، طبعة 2009، ص 154.

2 . التعريفان عن الدكتور طارق ابراهيم الدسوقي، المرجع السابق، ص 154 و 157.

و الدعوة لمواد إباحية طفولية والإرهاب المعلوماتي[1]. و بين الاتجاهين السابقين ظهر اتجاه موفق يرى ضرورة الإشارة إلى الدور المهم الذي يلعبه الحاسب الآلي في ارتكابها بغض النظر عن المعرفة الجيدة بالإعلام الآلي حتى تعرّف على أنها جريمة معلوماتية أي أنه يكفي أن يكون هناك سلوك إجرامي للحاسب الآلي دور مهم في ارتكابه سواء كان هو الأداة لارتكاب هذا الفعل أو كان محلا له.

من هذه التعاريف يتبين لنا أن الجريمة الإلكترونية هي جريمة مستحدثة مرتبطة بالتقدم التكنولوجي و هي سلوك غير مشروع يجرمه القانون الجنائي يكون الحاسب الآلي أداة لهذا السلوك أو محلا له[2].

و تمتاز الجريمة الإلكترونية بمفاهيمها المختلفة بمجموعة من الخصائص ميزتها عن غيرها من الجرائم وهي أن هدفها يتحدد غالبا حول ثلاث دوافع متمثلة في الطمع و الكسب السريع للمال كما في حالات السرقة المعلوماتية و النصب والاحتيال المعلوماتي والانتقام من رب العمل أو أحد الزملاء.

و محاولة الفاعل فيها إظهار التحدي و القدرات التقنية و السيطرة على النظام المعلوماتي بتخطي حواجز الحماية المقررة للأنظمة المعلوماتية كما أن أضرارها تقع غالبا في نطاق التقنيات المتقدمة و في إدارات المعاملات الاقتصادية المالية الدولية و الوطنية لذلك فخسائرها غالبا ما تكون كبيرة وفادحة.

حيث يمكن الإشارة هنا إلى الدراسة الإحصائية التي قام بها مجموعة من الخبراء في جمعية BSA

---

1.Bernadette H. Shell et Clemens Martin. Livre cyber crime Edition 2004, contemporary world issues, P 02.

2. تعريف عن الدكتورة نائلة عادل محمد فريد قورة، المرجع السابق، ص 31.

(جمعية تحالف منتجي البرامج المعلوماتية) التي توصلت إلى أن جريمة القرصنة الإلكترونية سببت خسارة اقتصادية قدرها 51 مليار دولار في العالم سنة 2009.[1]

من الميزات الخاصة للجريمة الإلكترونية أن المجرم أو الفاعل فيها هو نمط مختلف من المجرمين، فهو على قدر لا بأس به من العلم و ينتمي إلى مستوى اجتماعي مرتفع و نادرا ما يكون محترفا للإجرام بل استغلال المركز الوظيفي والمهارة الفنية في استخدام الحاسبات الآلية لأغراض شخصية و التمادي في هذه العمليات هو الذي يؤدي به إلى ارتكاب جرائمه[2] كما تتميز الجريمة الإلكترونية أنها ترتكب دون استعمال أي أسلوب من أساليب العنف كما لا يوجد شعور بعدم الأمان في مواجهتها كما هو الحال في الجرائم التقليدية ولا يوجد شعور عام بلا أخلاقية الفعل أو بمساسه بمصالح أو قيم يحرص على حمايتها كجرائم نسخ البرامج دون ترخيص من صاحبها بدلا من شرائها .فعامل البعد عن مكان الجريمة و عامل الخفية و إمكانية تقمص الجاني أي شخصية و أي عمر حين ارتكابه جرائمه يؤدون إلى تميز هذه الجريمة بالميزات السابقة[3].

إضافة إلى ما سبق تتميز الجريمة المعلوماتية بصعوبة اكتشافها و إثباتها بسبب ارتكابها بطريقة تقنية كثيرة التعقيد وسهولة تدمير ومحو المعلومات الخاصة بارتكابها و أنها أيضا ذات طبيعة دولية متعدية الحدود حيث تتجاوز الفواصل الجغرافية لعدة دول و تنتج أثارها فيها في آن واحد نظرا للقدرة التي تتمتع بها الحاسبات الآلية في نقل المعلومات و تبادل الكم الهائل منها بين أنظمة معلوماتية تفصل بينهما ألاف الكيلومترات.

---

1. دراسة منشورة على موقع الانترنيت www.BSA.ORG ، زيارة الموقع يوم 2016/03/01.
2. علي عبد القادر القهوجي الحماية الجنائية لبرامج الحاسب الالي، المكتبة القانونية القاهرة، ، 1999، ص 37.
3. الدكتورة نائلة عادل محمد فريد قورة، المرجع السابق، ص51 .

من الخصائص السابقة تظهر أهمية اختياري لموضوع الجريمة الإلكترونية، ناهيك عن قلة المراجع فيه و صعوبته لكون هذه الجريمة مستحدثة و قابلة لتغير أوجهها وأنواعها، فهي مرتبطة بالتطور

التكنولوجي الذي يفاجئنا كل حين باختراعات مذهلة في العالم الرقمي مما ينبئ عن إمكانية ظهور إشكال جديدة للإجرام مستقبلا .

كل هذه الأسباب دفعتني لاختيار موضوع مكافحة الجريمة الإلكترونية، هذه المكافحة التي أصبحت ضرورة ملحة، على الدول إيجاد طرق و أساليب ناجعة للمواجهة، خاصة وأن آثار هذه الجريمة بخصائصها السابقة أصبحت تمس كل المجتمعات دون استثناء المتقدمة منها و المتخلفة و على المستوى الفردي و الجماعي، فعلى المستوى الاقتصادي أوضحت الدراسات المختلفة أن الخسائر الناجمة عن الجرائم المعلوماتية في ازدياد مستمر خاصة في البلدان التي تعتمد على نظم التقنية المعلوماتية رغم أن هناك صعوبة في وضع إحصائيات دقيقة ومحددة لحجم هذه الخسائر و هو ما يعبر عنه بالرقم الأسود الذي يشير إلى أن مسألة عدم التبليغ عن هذه الجرائم سينفي الرقم الحقيقي لهذه الجريمة و أن الأرقام المذكورة لتحديد حجم هذه الجرائم ما هو إلا عدد الجرائم المبلغ عنها و التي قد تكون أقل بكثير من حجمها الحقيقي" .كالدراسة التي قامت و هي شركة مختصة في حماية الأنظمة و البرامج Symantec بها شركة المعلوماتية سنة 2010 بينت فيها أن الاعتداءات على الأنظمة المعلوماتية و إصلاحها سنويا يسبب خسارة مالية قدرها 114 مليار دولار في العالم و أن هذه الاعتداءات مست 431 مليون شخص[1]

وقد أجريت دراسة حديثة سنة 2009 قام بها مجموعة من الخبراء في جمعية Business Soft Word Alliance وهي جمعية تحالف منتجي البرامج المعلوماتية BSA توصلت هذه الدراسة إلى أن جريمة القرصنة المعلوماتية تسبب خسارة اقتصادية تقدر ب 51 مليار دولار في العالم كما توصلت إلى انه إذا قلصت هذه الجريمة 10 % فقط لمدة 4 سنوات.

---

1.دراسة منشورة على موقع الانترنيت لجريدة ECOFIN ، تاريخ الولوج إلى الموقع 2016/01/19.

ستحقق أرباحا تقدر ب 142 مليار دولار و سيتم إنشاء حوالي 500 ألف منصب شغل في تكنولوجيا المعلومات[1].

أما على المستوى السياسي فقد اتجهت كثير من الدول إلى سلوك سياسة الحكومات الالكترونية الذي أول من نادى به و طبقه ، الولايات المتحدة الأمريكية الذي يتلخص محتواه في تحول الإجراءات الحكومية الداخلية أو الخارجية و المتمركزة حول توفير أو إيصال الخدمات للمتعاملين معها بفاعلية و كفاءة بصورة أفضل من خلال تقنيات المعلومات و الاتصالات الحديثة[3] و تطبيق مشروع الحكومة الالكترونية يعد وسيلة ناجعة اتخذتها الدول للتخلص من البيروقراطية والإجراءات الروتينية و تسهيل التعامل بين الحكومة و مؤسساتها و كذلك تسهيل التعامل بين الحكومة وقطاع الأعمال و المواطنين وذلك بتسهيل و تسيير انجاز المعاملات وتقديم الخدمات الكترونيا وتطبيق هذه الفكرة يؤدي لا محالة إلى المساس بحقوق الأشخاص في إطار الإجرام المعلوماتي لما توفره هذه الفكرة ( الحكومة الالكترونية ) من معلومات عن الأشخاص و المؤسسات ...أما على المستوى الشخصي للأفراد فالاعتداءات الجديدة على حرمة الحياة الخاصة حيث أن المعلوماتية بأدواتها المختلفة والمتمثلة في أجهزة الحاسبات و الشبكات المعلوماتية و ما لهذه الأخيرة من قدرة فائقة في جمع المعلومات و البيانات الاسمية و استرجاعها و تصنيفها و تحليلها وتبادلها دون أي عوائق كل ذلك يشكل تهديدا حقيقيا لحقوق الأفراد في احترام حياتهم الخاصة حيث أصبحت حياتهم بسبب التطور المعلوماتي و ظهور ما يسمى ببنوك المعلومات أصبحت عرضة للمساس بها بمختلف أنواع و أشكال الاعتداءات بعدما كانت شيئا مقدسا لا يمكن الوصول إليه[2]

إذن للأسباب السابقة وجدت الدول في مختلف أنحاء العالم نفسها بصدد مواجهة حقيقية للجريمة المعلوماتية و من هنا تثار إشكالية موضوع الدراسة ( مكافحة الجريمة المعلوماتية ) في كيفية هذه المواجهة وذلك بالتساءل عن ما هي أساليب مكافحة الجريمة المعلوماتية؟ و ما مدى فعالية هذه الأساليب في ردعها و محاولة القضاء عليها ؟ و ما موقف المشرع الجزائري من مكافحة هذه الجريمة.

للإجابة على هذه الإشكالية اخترت خطة دراسة اعتمدت فيها على تقسيم موضوع البحث إلى مبحث تمهيدي و فصلين:

1. دراسة منشورة على موقع الانترنيت www.BSA.ORG ، تاريخ زيارة الموقع يوم 2016/03/01.
2. نهلا عبد القادر المومني الجرائم المعلوماتية مذكرة ماجستير دار التفافة للنشر و التوزيع ط . 2 2010 ص47

# المبحث التمهيدي

**المبحث التمهيدي :**

تحدثنا فيه عن ماهية الجرائم الواقعة على المواقع الالكترونية و تطرقنا إلى التعريف بمن هم مجرمو الانترنت و ما دوافعهم .

**فصل أول :** تناولت فيه المكافحة القانونية الموضوعية و التحديات الإجرائية للجريمة الواقعة على المواقع الالكترونية على مستوى دول سباقة في المكافحة، بدراسة جهود كل واحدة منها مع دراسة أهم صور الجريمة المعلوماتية و أهم الأعمال غير المشروعة المتصلة بمحتوى المعلوماتية و البريد الالكتروني و أنشطة التصرف المعلوماتي غير القانونية ، و القيام بإطلالة سريعة على مستوى الجرائم المستحدثة في مجال المعلوماتية باستخدام وسائل فنية تقنية و مدى تكييفها القانوني و تنظيمها التشريعي . و عن موضوع التحديات الإجرائية للجريمة على المواقع الالكترونية تطرقنا إلى مطلبين : الأول أهم صور الجريمة الواقعة على المواقع الإلكترونية و تحدي الأحكام العامة للجريمة ، و المطلب الثاني جريمة غسل الأموال عبر الوسائل الإلكترونية.

**و فصل ثاني :**تناولنا فيه مجهود المشرع الجزائري للحد من الجريمة الواقعة على المواقع الإلكترونية و ذلك بالتحدث عن النصوص التقليدية في مجال الجريمة المعلوماتية ، و كذا النصوص القانونية المستحدثة .

و تطرقنا في ختام الموضوع إلى وضع خاتمة و هي تقييم لما تحدثنا عنه ومدى ملائمة المشاريع و النصوص للمعطيات الراهنة.

## مبحث تمهيدي :

## ماهية الجرائم الواقعة على المواقع الإلكترونية ، من هم مجرموا الأنترنت و دوافعهم.

### نبذة تاريخية عن الجرائم الواقعة على المواقع الإلكترونية :

الإنترنت هو عبارة عن شبكة تتألف من مئات الحاسبات الآلية المرتبطة بعضها ببعض إما عن طرق الهاتف أو عن طريق الأقمار الصناعية ،وتمتد عبر العالم لتؤلف في النهاية شبكة هائلة ، بحيث يمكن للمستخدم لها الدخول إلى أي منها في أي وقت، ولو في أي مكان يتواجد فيه على الكرة الأرضية، ولو حتى في الفضاء وهو جزء من ثورة الاتصالات، ويعرّف البعض الإنترنت بشبكة الشبكات، في حين يعرّفها البعض الآخر بأنها شبكة طرق المواصلات السريعة" [1]. بدأ الإنترنت في 1969/1/2 عندما شكّلتْ وزارة الدفاع الأمريكية، فريقاً من العلماء، للقيام بمشروع بحثي عن تشبيك الحاسبات، وركّزت التجارب على تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة، ومن ثم نقل هذه الأجزاء بأشكال وطرق مستقلة، حتى تصل مجّمعة إلى هدفها، وكان هذا الأمر يمثل أهمية قصوى لأمريكا وقت الحرب، ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة، فإن الأجزاء الصغيرة يمكن أن تواصل سيرها من تلقاء نفسها، عن أي طريق آخر بديل، إلى خط النهاية، ومن ثم تطّور المشروع وتحوّل إلى الاستعمال السلمي حيث انقسم عام ( 1983م) إلى شبكتين، احتفظت الشبكة الأولى باسمها الأساسي ( ARPANE) وبغرضها الأساسي، وهو خدمة الاستخدامات العسكرية، في حين سُمِّيتْ الشبكة الثانية باسم (MILNET) وخصصت للاستخدامات المدنية ،أي تبادل المعلومات، وتوصيل البريد الإلكتروني، ومن ثم ظهر مصطلح ((الإنترنت)) حيث أمكن تبادل المعلومات بين هاتين الشبكتين. وفي عام ( 1986م) أمكن ربط شبكات خمس مراكز للكمبيوترات العملاقة وأطلق عليها اسم (NSFNET) والتي أصبحت فيما بعد العمود الفقري، وحجر الأساس، لنمو وازدهار الإنترنت في أمريكا، ومن ثم دول العالم الأخرى

---

1. جميل عبدالباقي الصغير .الانترنت والقانون الجنائي ، (القاهرة:دار النهضة العربية، 2001) ،32.

لا أحد في الوقت الراهن يملك الإنترنت، وإن كان يمكن القول في البداية بأنّ الحكومة الأمريكية ،ممثلة في وزارة الدفاع، ثم المؤسسة القومية للعلوم، هي المالك الوحيد للشبكة، ولكن بعد تطّور الشبكة، ونمّوها، لم يعد يملكها أحد، واختفى مفهوم التملك، ليحل محله ما أصبح يسمي بمجتمع الإنترنت .

وقد ادى هذا النجاح في مجال شبكة الانترنت الى تقدم البحث العلمي كما استخدمت الشركات الانترنت للقيام بأعمالها التجارية والتسويقيه كما يستخدمها الافراد بحثاً عن المعلومات والتراسل فيما بينهم وتستخدمها المؤسسات العلمية والجامعات لتبادل المعلومات والتعليم عن بعد[1].

## المطلب الأول : تعريف جرائم الكمبيوتر والإنترنت، أنواعها و تصنيفها و أسباب صعوبة إثباتها.

### الفرع الأول : تعريف الجرائم الواقعة على المواقع الإلكترونية:

يمكن تعريف جرائم الكمبيوتر والانترنت أو الجرائم الواقعة على المواقع الإلكترونية بأنها تلك التي تطال المعرفة ،الاستخدام ، الثقة ، الأمن ، الربح والمال ، السمعة ، الاعتبار. أما جريمة الكمبيوتر ، فقد صك الفقهاء والدارسون لها عددا ليس بالقليل من التعريفات، تتمايز وتتباين تبعا لموضع العلم المنتمية إليه وتبعا لمعيار التعريف ذاته ، فاختلفت بين أولئك الباحثين في الظاهرة الإجرامية الناشئة عن استخدام الكمبيوتر من الوجهة التقنية وأولئك الباحثين في ذات الظاهرة من الوجهة القانونية ، . أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة ، فان أصحابها ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة

، من هذه التعريفات ، يعرفها جون فورستر [2] وكذلك Eslie D. Ball أنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ويعرفها تاديمان Tiedemaun بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك يعرفها مكتب

---

1) أسامة أبو الحجاج،. دليلك الشخصي إلى عالم الإنترنت ( القاهرة : نهضة مصر، 1998)،

2) حسن طاهر داود. جرائم نظم المعلومات. (الرياض : أكاديمية نايف العربية للعلوم الأمنية. 1420هـ ).

تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا) " [1] وجدير بالذكر، أن الدكتور سامي الشوا ، ينسب إلى الفقيه Tiedemaunتعريفه لجريمة الحاسوب بأنها " كل جريمة ضد المال مرتبطة بالمعالجة الآلية للبيانات [2] .جانب من الفقه

والمؤسسات ذات العلاقة بهذا الموضوع ، وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل ، وهي تحديدا سمة الدراية والمعرفة التقنية من هذه التعريفات ، تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها 18 لعام 199 ، حيث عرفت بانها " أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها ومن هذه التعريفات أيضا تعريف David Thompson بأنها " أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب " . وتعريف Stein Schjqlberg بانها " أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر اساسية لارتكابه والتحقيق فيه وملاحقته قضائيا " إن التطور الذي شهدته وسائل التقنية نفسها اظهر الاتجاه نحو تبسيط وسائل المعالجة وتبادل المعطيات ، وتحويل الأجهزة المعقدة فيما سبق إلى أجهزة تكاملية سهلة الاستخدام حتى ممن لا يعرف شيئا في علوم الكمبيوتر ، ولم يعد مطلوبا العلم والمعرفة العميقين ليتمكن شخص من إرسال آلاف رسائل البريد الإلكتروني دفعة واحدة إلى أحد المواقع لتعطيل عملها ، كما لم يعد صعبا ان يضمن أي شخص رسالة بريدية فيروسا التقطه كبرنامج عبر الإنترنت أو من خلال صديق فيبثه للغير دون أن يكون عالما أصلا بشيء مما يتطلبه بناء مثل هذه البرامج الشريرة ، كما أن ما يرتكب الآن باستخدام الهاتف الخلوي من أنشطة اختراق واعتداء أو ما يرتكب عليها من قبل أجهزة مماثلة يعكس عدم وجود ذات الأهمية

---

1) حسن طاهر داود. الحاسب وامن المعلومات. (الرياض : معهد الادارة العامة. 1421).

2) ، أحمد سليمان الزغاليل .الاتجار بالنساء والأطفال، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية ، تونس، 1420هـ تونس ( 43-90).

للمعرفة التقنية أو الدراية بالوسائل الفنية . أضف إلى ذلك أن جانبا معتبرا من جرائم الكمبيوتر والإنترنت – يعتبر أخطرها في الحقيقة – تنسب المسؤولية فيه للشخص المعنوي، سيما وأن واحدة من المسائل الرئيسة فيما تثيره جرائم الكمبيوتر هي مسألة مسؤولية الشخص المعنوي ، شأنه شأن الشخص الطبيعي عن الأفعال المعتبرة جرائم كمبيوتر.

أمام قصور التعريفات المؤسسة على معيار واحد ، سواء القائمة على معيار قانوني موضوعي أو شخصي ، برز عدد من التعريفات ترتكز على أكثر من معيار لبيان ماهية جريمة الكمبيوتر ، من هذه التعريفات ، ما يقرره الأستاذ John Carrol ويتبناه الأستاذ Gion Green من أن جريمة الكمبيوتر هي "أي عمل ليس له في القانون أو أعراف قطاع الأعمال جزاء ، يضر بالأشخاص أو الأموال ، ويوجه ضد أو يستخدم التقنية المتقدمة (العالية) لنظم المعلومات ."ويعتمد في التعريف كما نرى معايير عدة ، أولها، عدم وجود جزاء لمثل هذه الأفعال، ، وثانيها، تحقيق الضرر للأشخاص أو الأموال . وثالثها، توجه الفعل ضد أو استخدام التقنية المتقدمة لنظم المعلومات ، وهو معيار يعتمد موضوع الجريمة (تقنية نظم المعلومات) ووسيلة ارتكابها (أيضا تقنية نظم المعلومات) أساسا للتعريف. كما يعرفها الأستاذ Sheldon. J. Hecht بأنها: "واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب" وقريب منه تعريف الفقيه B. Parker Donnفي مؤلفه Crime Fighting Computer والذي يرى بأنها "أي فعل متعمد مرتبط بأي وجه، بالحاسبات، يتسبب في تكبد أو إمكانية تكبد مجني عليه لخسارة أو حصول أو إمكانية حصول مرتكبه على مكسب" ويستخدم للدلالة على الجريمة تعبير "إساءة استخدام الحاسوب ."، بأنها " كل فعل أو امتناع من شانه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية ، و يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، ويتيح إمكانية التعامل مع التطورات المستقبلية التقنية.وبالرجوع للتعريف المتقدم نجد انه يشير إلى إمكان حصول جريمة الكمبيوتر بالامتناع ، .ويعرف خبراء منظمة التعاون الاقتصادي والتنمية، جريمة الكمبيوتر بأنها:

"كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/ أو نقلها " ويتبنى هذا التعريف الفقيه الألماني Ulrich Sieher ، ويعتمد هذا التعريف على معيارين : أولهما، (وصف السلوك). وثانيهما، اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.ومن ضمن التعريفات التي تعتمد أكثر من معيار، يعرف جانب من الفقه جريمة الكمبيوتر وفق معايير قانونية صرفه ، أولها تحديد محل الجريمة، وثانيها وسيلة ارتكابها وهو في كلا المعيارين (الكمبيوتر) لما يلعبه من دور الضحية ودور الوسيلة حسب الفعل المرتكب. من هؤلاء الأستاذ Thomas. J. Smedinghoffفي مؤلفه (المرشد القانوني لتطوير وحماية وتسويق البرمجيات). حيث يعرفها بأنها "أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب". وكذلك تعريف الأستاذين Robert J. Lindquist و " Jack Bologna جريمة يستخدم الحاسوب كوسيلة mensأو أداة Instrument لارتكابها أو يمثل اغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها . "ومن الفقه الفرنسي، يعرف الفقيه Masse جريمة الكمبيوتر (يستخدم اصطلاح الغش المعلوماتي) بأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح .ويعرفها الفقهيين الفرنسيين Le stanc, Vivant بأنها : "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب."

.ولا بد من التمييز في التعريف بين ظاهرة إجرام الحوسبة، أو كما يسميها قطاع واسع من الفقه المصري ظاهرة الجناح أو الانحراف المعلوماتي وبين جرائم الكمبيوتر والإنترنت . ، وه ي الجرائم التقليدية ، باعتبار هذه الماديات مجسدة لمال منقول مادي تنهض به قواعد ومبادئ ونصوص القانون أما عن دور الكمبيوتر في الجريمة ، فانه متعدد في الحقيقة ، فهو إما أن يكون الهدف المباشر للاعتداء ، أو هو وسيلة الاعتداء لتحقيق نتيجة جرمية لا تتصل مباشرة بالمعطيات

وإنما بما تمثله او تجسده ، أو هو بيئة ومخزن للجريمة ، ويجب أن لا يوقعنا أي من هذه الأدوار في أي خلط بشان محل الجريمة أو وسيلة ارتكابها، فان محل جريمة دائما هو المعطيات (أما بذاتها أو بما تمثله) ووسيلة ارتكاب جريمة الكمبيوتر والإنترنت الكمبيوتر أو أي من الأجهزة التكاملية .وإذا كانت تعريفات الجريمة عموما تقوم على أساسين : عناصر الجريمة و السلوك ووصفه، والنص القانوني على تجريم السلوك وإيقاع العقوبة، فان الجديد في مجال جرائم الكمبيوتر هو إضافة عنصر ثالث يبرز محل

الاعتداء في هذه الظاهرة الإجرامية المستحدثة ، متمثلا بمعطيات الحاسوب .فقانون العقوبات ينطوي على نصوص تحرم الاعتداء على الأشخاص ، الأموال ، الثقة العامة ... الخ ، لكن المستجد ، هو الكيانات المعنوية ذات القيمة المالية أو القيمة المعنوية البحتة، أو كلاهما، ولولا هذه الطبيعة المستجدة في الأساس لما كنا أمام ظاهرة مستجدة برمتها، ولكان المستجد هو دخول الكمبيوتر عالم الإجرام ، تماما كما هو الشأن في الجرائم المنظمة، فهي في الحقيقة جرائم تقليدية المستجد فيها عنصر التنظيم الذي ينتج مخاطر هائلة واتساع نطاق المساهمة الجنائية وانصهار الإرادات الجرمية في إرادة واحدة هي إرادة المنظمة الإجرامية المعنية. وعلينا التأكيد هنا على أن جرائم الكمبيوتر ليست مجرد جرائم تقليدية بثوب جديد او بوسيلة جدية فهذا قد ينطبق على بعض صور الجرائم التي يكون الكمبيوتر فيها وسيلة لارتكاب الجريمة ، وليس صحيحا ما قاله الكثير من الإعلاميين الغربيين في المراحل الأولى لظاهرة الكمبيوتر انها ليست اكثر من ( نبيذ قديم في زجاجة جديدة ) . انها بحق ، جرائم جديدة في محتواها ونطاقها ومخاطرها ، ووسائلها ، ومشكلاتها ، وفي الغالب في طبائع وسمات مرتكبيها .

## الفرع الثاني: أنواع الجرائم المعلوماتية:

وتشمل هذه الطائفة فئتين، أولهما، الجرائم الواقعة على ذات المعطيات، كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات) التقنية. وثانيهما، الجرائم الواقعة على ما تمثله المعطيات آليا، من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات ، وجرائم التحوير والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها (تزوير المستندات المعالجة آليا واستخدامها).

### أ) الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة :

وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة.

**ب) الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات)** : تشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص والاعتداء على العلامة التجارية وبراءة الاختراع .أن الحماية الجنائية للمعلومات في نطاق القانون المقارن وفي إطار

الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على نحو غالب، التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج ، وحماية البيانات الشخصية المتصلة بالحياة الخاصة وحماية المعطيات بالنظر لقيمتها أو ما تمثله والذي عرف بحماية ) الأموال)، كل في ميدان وموقع مستقل. ولا بد لنا من الإشارة، أن حماية أمن المعطيات (الطائفة الثانية) انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرائم الطائفة الأولى الماسة بقيمة المعطيات بالنظر الى أن الباعث الرئيسي للاعتداء والغرض من معرفة أو إفشاء هذه المعلومات غالبا ما كان الحصول على المال مما يعد من الاعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم .

**ج) تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة :**

قد يكون هدف الاعتداء المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر والشبكات ، وهذا ما يعبر عنه بالمفهوم الضيق) لجرائم الكمبيوتر) وقد يكون الكمبيوتر وسيلة ارتكاب جريمة أخرى في إطار مفهوم (الجرائم المرتبطة بالكمبيوتر) ، وقد يكون الكمبيوتر أخيرا بيئة الجريمة أو وسطها أو مخزنا للمادة الجرمية ، وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن هذا الدور الأول جرائم التخزين ، ويقصد بها تخزين المواد الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها ، والثاني ، جرائم المحتوى أو ما يعبر عنه بالمحتوى غير المشروع او غير القانوني والاصطلاح الأخير استخدم في ضوء تطور إشكال الجريمة مع استخدام الانترنت ، وأصبح المحتوى غير القانوني يرمز إلى جرائم المقامرة ونشر المواد الإباحية والغسيل الالكتروني للأموال وغيرها ، والحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفي نفس الوقت

كوسيلة لارتكابها . وهذا التقسيم شائع بجزء منه ( وهو تقسيم الجرائم إلى جرائم هدف ووسيلة ) لدى الفقه المصري والفرنسي ، وتبعا له تنقسم جرائم الكمبيوتر إلى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات وإتلافها ، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر . إما تقسيمها كجرائم هدف ووسيلة ومحتوى فانه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في أوروبا تحديدا ، وأفضل ما يعكس هذا التقسيم الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت لعام 2001،الذي أوجد مشروع الاتفاقية الأوروبية تقسيما جديدا نسبيا ، فقد تضمن عدة طوائف رئيسة لجرائم الكمبيوتر والانترنت ومنها :

**د) الجرائم التي تستهدف عناصر (السرية والسلامة وموفورية) المعطيات والنظم :**

- الدخول غير قانوني ( غير المصرح به ) .
- الاعتراض غير القانوني .
- تدمير المعطيات .
- اعتراض النظم .
- إساءة استخدام الأجهزة .

**هـ) الجرائم المرتبطة بالكمبيوتر :**

- التزوير المرتبط بالكمبيوتر .
- الاحتيال المرتبط بالكمبيوتر .

**و ) الجرائم المرتبطة بالمحتوى:**

- طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية .

**الفرع الثالث: أسباب صعوبة إثبات جرائم الحاسب الآلي :**

هناك خمسة أسباب رئيسية وراء صعوبة إثبات جرائم الحاسب الآلي وهي :

أولا: أنها كجريمة لا تترك اثر لها بعد ارتكابها.

ثانيا: صعوبة الاحتفاظ الفني بآثارها إن وجدت.

ثالثا: أنها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.

رابعا: أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.

خامسا: أنها تعتمد على قمة الذكاء في ارتكابها .

**الفرع الرابع : المجرم في جرائم المعلومات.**

الحقيقة أنه، وحتى الآن، لم تتضح الصورة جلية في شأن تحديد صفات مرتكبي جرائم الحاسوب واستظهار سماتهم وضبط دوافعهم، نظرا لقلة الدراسات الخاصة بالظاهرة برمتها من جهة ونظرا لصعوبة الإلمام بمداها الحقيقي، بفعل الحجم الكبير من جرائمها غير المكتشفة، أو غير المبلغ عن وقوعها، أو التي لم تتم بشأنها ملاحقة قضائية رغم اكتشافها، لصعوبتها أو للنقص التشريعي الذي يحد من توفير الحماية الجنائية في مواجهتها[4].

ومحاولة منا للتعريف بخصوصية المجرم المعلوماتي واستجلاء ه سنجيب في هاته الفقرة عن من هو مرتكب الجرائم المعلوماتية؟

فمن هو مرتكب الجرائم المعلوماتية؟

يتجه الباحثون إلى الإقرار بأن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء ويعد من أفضل التصنيفات لمجرمي التقنية الذي أورده David icove, Paul serger et william Vonstouch في مؤلفهم جرائم الكمبيوتر الصادر عام 1995 حيث تم تصنيف مجرمي المعلوماتية إلى ثلاثة طوائف: المخترقون، المحترفون والحاقدون.

**أولا : المخترقون:**

يتحد في إطار هذه الطائفة نوعين من المخترقين أو المتطفلين:

- ✓ **الهاكرز**: les hackers
- ✓ **الهاكر** (hacker) أو المتسلل هو شخص بارع في استخدام الحاسب الآلي وبرامجه ولديه فضول في استكشاف حسابات الآخرين وبطرق غير مشروعة[1].

4- للمزيد من المعلومات حول الحماية الجنائية بالمغرب لبرامج الحاسوب أنظر: بشرى النية، " حماية الحاسوب عن طريق قواعد القانون الجنائي حماية للمصالح الخاصة والنظام العام، مقال منشور بالمجلة المغربية لقانون الأعمال والمقاولات، العدد 7، 2005، ومحمد بوطيبة حماية برامج الحاسوب طبقا لقانون 00- 2 المنظم لحقوق المؤلف والحقوق المجاورة، مقال منشور بمجلة القضاء والقانون، العدد 150، 2004.

فالهاكرز، وكما يدل على ذلك اسمهم، هم متطفلون يتحدون إجراءات أمن نظم الشبكات، لكن لا تتوفر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات الذات[2].

وتتألف هذه الطائفة أساسا من مراهقين وشباب ( طلبة وتلاميذ ثانويات) وشباب عاطل عن العمل[3].

✓ **طائفة الكراكرز: les crackers**

الكراكرز أو المقتحم هو شخص يقوم بالتسلل إلى نظم الحاسوب للإطلاع على المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها، ولقد تم استعمال هذا المفهوم الجديد سنة 1985 من طرف الطائفة الأولى، طائفة الهاكرز للرد على الاستعمال السيئ للصحفيين لمصطلح الهاكرز[4]

لقد استفادت هذه الطائفة كثيرا من التقنيات التي طورتها فئة الهاكرز وبد ؤوا يستخدمونها استخداما سيئا في اعتداءات تنم عن ميولات إجرامية.

---

**1.** ورد هذا التعريف في رسالة للماجستير وبالضبط في ملحق لهذه الدراسة خصص للمفاهيم الأساسية المتداولة في جرائم الحاسوب والانترنيت، هذه الدراسة قام بها الطالب: محمد بن عبد الله بن علي المنشاوي تحت عنوان: جرائم الانترنيت في المجتمع السعودي، تاريخ المناقشة 29- 04- 2003.

.**2** la criminalité informatique sur l'Internet, journal of Law ñ 1- val 26, mars 2002, p : 45 . Mohammed ----

**3–** فحسب دراسة قام بها المكتب الفدرالي الأمريكي ( federal bureau of investigation FBI ) غالبية الهاكرز الأكثر خطورة هم الشباب المتراوحة أعمارهم بين 18- 35 سنة.

**4.** -Bouchaib RMAIL, la criminalité informatique, criminalité a double dimension :internationale, thèse pour l'obtention du grade de ducteur en droit privé-option : droit des affaires, faculté des sciences juridiques, économiques et sociales-fés, 2005, p : 82.

والسمة المميزة الأخرى للمقتحمين تبادلهم للمعلومات فيما بينهم. وفي تطور حديث، تنظم هذه الطائفة نفسها بعقد مؤتمرات لمخترقي الكمبيوتر يدعى له الخبراء منهم للتشاور حول وسائل الاختراق ووسائل تنظيم عملهم.

هذا فيما يخص المخترقين فماذا عن طائفة المحترفين؟

**ثانيا : مجرموا الحاسوب المحترفون.**

التقنية كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكبها، ولذلك فإن هذه الطائفة تعد الأخطر من بين مجرمي الكمبيوتر والإنترنيت حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم الحاسوب كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي.

وإلى تحقيق جانب المعرفة التقنية المميزة والتنظيم العالي والتخطيط للأنشطة المنو ى ارتكابها، فإن أفراد هذه الطائفة يتسمون بالتكتم خلافا للطائفة الأولى فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ويحاولون ما أمكن عدم كشف طرقهم التقنية لارتكاب جرائمهم.

وحول الأعمار الغالبة على هذه الطائفة فإن الدراسات تشير إلى أنهم من الشباب الأكبر سنا من الطائفة الأولى وأن معظمهم تتراوح أعمارهم ما بين 25 و 40 سنة.

إذن بعد التعرف ولو بعج الة، عن الطائفتين الأوليتين ضمن هذا التصنيف بقي أن ندرس آخر طائفة والمتمثل في فئة الحاقدين.

**ثالثا : الحاقدون:**

هذه الطائفة يغلب عليها عدم توافر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارية وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم.

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يشقى الواحد منهم في الوصول إلى كافة عناصر المعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم أو إتلاف كل أو بعض معطياته، أو نشاط إنكار الخدمة تعطيل النظام أو الموقع المستهدف إن كان من مواقع الإنترنيت.

وليس هناك ضوابط محددة بشأن أعمارهم، كما لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة، ولا يفاخرون بأنشطتهم بل يعمدون على إخفائها، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد على ذلك.

هذه إذن الأصناف الثلاثة لمجرمي الحاسوب والإنترنيت، فماذا عن دوافعهم للتخصص في هذا النوع من الجرائم دون سواها؟ هذا ما سنحاول الإجابة عنه في الفقرة الثانية من هذا المطلب.

## المطلب الثاني : دور الحاسوب في الجريمة المعلوماتية ومحل الجريمة فيها و ما هي دوافع إرتكاب الجريمة المعلوماتية.

يجب عدم الخلط بين دور الحاسوب في الجريمة الذي يكون إما الهدف المباشر للاعتداء، أو وسيلة الاعتداء أو بيئة ومخزن للجريمة وبين محل الجريمة الذي يكون دائما المعطيات إما بذاتها أو بما تمثله.

لذلك سنقسم هذا المطلب ثلاث فروع نتناول في الأول دور الحاسوب في الجريمة وفي الثاني محل الجريمة فيه و في الثالث دوافع إرتكاب الجريمة المعلوماتية.

### الفرع الأول : دور الحاسوب في الجريمة المعلوماتية.

الحاسوب مجموعة من الأجهزة متكاملة مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة[1]، وباعتباره كذلك فإنه يلعب دور البطولة على مسرح الجريمة المعلوماتية، فهو إما أن يكون الهدف المباشر للاعتداء أو وسيلة الاعتداء لتحقيق نتيجة جرمية، لذلك فالحاسوب يلعب دورا هاما في ميدان ارتكاب الجرائم وآخر في حقل اكتشافها[2].

---

**1** . جرائم الكمبيوتر والإنترنيت لمحمد أمين الرومي، الطبعة 2003، ص: 13.

[2] . محمد الولادي" جرائم الحاسوب وحقوق المؤلف" يوم دراسي منظم بتعاون بين وزارتي العدل والاتصال. 28 أبريل 99 ص: 125.

وعليه سيتم تقسيم هذا المطلب إلى فقرتين نبسط في الأولى دور الحاسوب في ارتكاب الجريمة المعلوماتية، على أن نخصص الثانية لدوره في اكتشافها.

**أولا : دور الحاسوب في ارتكاب الجريمة المعلوماتية.**

قد يكون الحاسوب هدفا للجريمة، وذلك كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم، ومن أوضح المظاهر لاعتبار الحاسوب هدفا للجريمة في حقل التصرفات غير القانونية، عندما تكون السرية والتكاملية هي التي يتم الاعتداء عليه، بمعنى أن توجه هجمات الحاسوب إلى معلومات الحاسوب أو خدماته، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، وهدف هذا النمط الإجرامي هو نظام الحاسوب وبشكل خاص المعلومات المخزنة داخله، وغالبية هذه الأفعال الجرمية تتضمن ابتداء الدخول غير المصرح به إلى النظام الهدف والتي توصف بأنشطة الهاكرز كناية عن فعل الاختراق haching، أو إدخال فيروسات للجهاز، بحيث تعمل هذه الفيروسات على تدمير الجهاز أو البرامج أو إعاقة عمل البرنامج أو نسخه هو والمعلومات الموجودة على الجهاز.

ويمكن تعريف الفيروس بأنه " برنامج حاسب مثل أي برنامج تطبيقي آخر، ولكن يتم تصميمه بواسطة أحد المجربين بهدف محدد وهو إحداث أكبر ضرر ممكن بنظام الحاسب، ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ويتوالد ذاتيا وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة، وكذلك بين مواقع مختلفة في الذاكرة، حتى يحقق أهدافه التدميرية ومن أشهر أنواع الفيروسات، فيروس القردة [1]، ومايكل أنجلو[2] وحصان طروادة le cheval de Troie[3] إلى غير ذلك من

---

**1** – هذا الفيروس يقوم بعرض شاشة بها مجموعة من القرود التي تقوم بأعمال بهلوانية، وأثناء قفز القرود على الشاشة، فإن البرنامج يعمل نسخ من نفسه في أماكن متعددة كما يقوم بتدمير الفهرس الرئيسي للقرص الصلب.

**2**– يتلف قطاع بدء التشغيل على القرص، كما يتلف جدول تجزئة القرص الصلب، وسمي كذلك لأنه ينشط في يوم عيد ميلاد الفنان" مايكل أنجلو" 6 مارس.

**3**– لديه القدرة على الاختفاء في البرنامج الأصلي للمستخدم، وعندما يتم تشغيل هذا الأخير، ينشط هذا الفيروس ويبدأ نشاطه التدميري، ومن آثاره السيئة تعديل البرامج، وتزوير المعلومات، ومحو بعضها.

الفيروسات الكثيرة والمتنوعة التي لا تزال في تطور مستمر، نتيجة التطور المعلوماتي في نظم الحاسب الآلي، لذلك ينصح بتفادي عملية تبادل الأقراص ما بين جهاز وآخر، أو نسخ هذه الأقراص.

بعد أن بينا كون الحاسوب هدفا للجريمة، نبين فيما يلي كونه أداة لارتكاب جرائم تقليدية، كما في حالة استغلال الحاسوب للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير، أو استخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها والحصول على الأموال بواسطتها.

حتى أن الحاسوب قد يستخدم في جرائم القتل، كما في الدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها، أو تحوير عمل الأجهزة الطبية والمجهرية عبر التلاعب ببرمجياتها أو كما في إتباع الوسائل الإلكترونية لتأثير عمل برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي إلى تدميرها وقتل ركابها.

وكما يمكن للحاسوب أن يكون هدف أو أداة الجريمة فإنه يكون أيضا بيئتها، وذلك كما في تخزين البرامج المقرصنة فيه أو في حالة استخدامه لنشر المواد غير القانونية أو استخدامه أداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية.

**ثانيا : دور الحاسوب في اكتشاف الجريمة.**

يستخدم الحاسوب على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، عوضا عن أن جهات تنفيذ القانون تعتمد على النظم التقنية في إدارة المهام من خلال بناء قواعد البيانات ضمن جهاز إدارة العدالة والتطبيق القانوني، ومع تزايد نطاق جرائم الحاسوب، واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة، فإنه أصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها، إذ أنه للقضاء على ظاهرة إجرامية معينة ينبغي محاربتها بوسائل تفوقها من حيث التطور والتقدم، حتى إذا استعصى الأمر فبالوسائل التي ارتكبت بها.

من هنا يلعب الحاسوب ذاته دورا رئيسيا في كشف الجرائم المرتكبة من خلاله وتتبع فاعليها رغم الصفات الاستثنائية التي يمتاز بها أولئك والتي تختلف عن صفات المجرمين العاديين لما يمتازون به من ذكاء، وعلم بليغ بوسائل التكنولوجيا، بل وإبطال أثر الهجمات التدميرية لمخرقي النظم وتحديدا هجمات الفيروسات وإنكار الخدمة وقرصنة البرمجيات.

## الفرع الثاني: الاعتداء على كيانات الأجهزة التقنية المادية.

عند الحديث عن محل الجريمة المعلوماتية يجب عدم الخلط بين المكونات المادية للحاسوب التي يعتبر الاعتداء عليها داخلا في دائرة الجرائم التقليدية وبين المكونات المعنوية أو ما يصطلح على تسميتها بالمعطيات وهي المقصودة بالدرس والتحليل، لذلك سنعمد إلى تقسيم هذا المطلب إلى فقرتين نتناول في الأولى الاعتداء على المكونات المادية للحاسوب وفي الثانية نبسط الجرائم الموجهة للنظم والمعلومات.

### أولا : الاعتداء على كيانات الأجهزة التقنية المادية.

إن طبيعة وأبعاد ظاهرة جرائم الكمبيوتر، سيما في ظل تطور أنماطها يوما بعد يوم، مع تطور استخدام الشبكات وما أتاحته الإنترنيت من فرص جديدة لارتكابها، وخلقت أنماطا مستجدة تتميز بأحكام لا توفرها النظريات القائمة [1]، أدى إلى ضرورة حسم الجدل الواسع حول مدى انطباق النصوص القائمة على هذه الجرائم، أو وضع تشريعات ونصوص جديدة تكون قادرة على الإحاطة بمتطلبات وخصوصية جرائم الحاسوب.

وبما أن الحاسوب كم ذكرنا سابقا، يتكون من جزأين رئيسيين [2]. المكونات المادية وهي المكونات الصلبة، والمكونات اللامادية وهي البرامج أو المعطيات، فإنه عند الحديث عن محل الجريمة المعلوماتية يتم إقصاء جرائم الاعتداء على كيانات الحاسوب المادية من نطاق جرائم الحاسوب لترتد إلى موقعها الطبيعي وهو الجرائم التقليدية، باعتبار هذه الماديات مجسدة لمال منقول مادي تنهض به قواعد ومبادئ ونصوص القانون الجنائي. سواء استهدفت هذه الجرائم المكونات المادية

---

**1** – نظريات العلنية في جرائم الاعتبار ( الفعل الفاضح، السبب)، الضرر في جرائم التزوير، الحيازة في السرقة والتدليس والنصب... وهذه نظريات للقسم الخاص.

**2**– حماية برامج الحاسوب طبقا لقانون 00– 2 مجلة القضاء والقانون ع 150، ص: 84.

للحاسوب أو استهدفت نظامه باعتباره المعبر عن عصر التقنية، وغالبا ما يتم ارتكاب هذه الجرائم تعبيرا عن موقف سياسي من التقنية ذاتها أو بفرض استهداف أمن ونظام الدولة باعتبار وسائل التقنية من الوسائل الفاعلة في الإدارة والتخطيط ورافضة لقوة الدولة وفعالية نظامها، وتتجسد هذه الجرائم في الاعتداءات المادية كالإتلاف وسرقة الأدوات المعلوماتية والأشرطة المسجلة والأسطوانات لذلك نجد المشرع أناط تجريمها للقوانين التقليدية.

**ثانيا : الجرائم الموجهة للبرامج والمعطيات.**

لقد كان ولازال محل الجريمة المعلوماتية الشغل الشاغل للفقه المهتم بالمعلوميات منذ ظهور هذه التكنولوجيا المتطورة لما يطرحه من إشكالات على المستوى القانوني، خصوصا عندما نعلم أن محل الجريمة المعلوماتية هو المعلومات، هذه الأخيرة التي تعد مالا شائعا، ومن تم يجب أن تكون من حيث المبدأ حرة ولا يجب أن تحمى بالحقوق الاستئثارية والتي تقتصر على الأموال المادية، ويعد هذا المبدأ ( حرية الوصول للمعلومات) شرطا جوهريا لأي نظام اقتصادي وسياسي حر، وهو أيضا في غاية الأهمية من أجل تقدم الدول التي في طريقها للتنمية.

فإذا كانت المعلومات مالا شائعا فكيف يتصور أن يشكل الوصول إليها جريمة في نظر القانون؟

تعرف برامج الحاسوب بأنها مجموعة من الأوامر والتعليمات المحددة مكتوبة بلغة ما لتنفيذ عمليات محددة للوصول إلى نتائج تتماثل مع إجراء نفس العمليات بالطرق اليدوية، وقد جرم المشرع فعل الاعتداء على هذه البرامج الذي يتخذ صورا متعددة ومتنوعة تختلف باختلاف الحالة التي تكون عليها الوثيقة المعلوماتية، باعتبارها محلا للجريمة التي يتداخل فيها ما هو مادي كالشرائط الممغنطة والديسكان، وكل ما يلزم لاستقبال أو تسجيل المعلومات، بما هو معنوي، المحتوى الفكري contenu intellectuel والذي نميز بصدده بين الوثيقة المعلوماتية المعالجة معلوماتيا والوثيقة غير المعالجة معلوماتيا، وفيما يتعلق بالأولى نميز في داخلها أيضا بين نوعين، الوثائق المعالجة معلوماتيا وتلك المعالجة أتوماتيكيا أو آليا، لذلك نجد المشرع المغربي جرم من

ناحية الاعتداء على الوثائق المعالجة معلوماتيا ومن ناحية أخرى الاعتداء على نظام المعالجة الآلية للمعطيات، وبعبارة أخرى جرم أنماط السلوك الإجرامي التي تطال المعلومات المخزنة أو المعالجة في نظام الحاسوب أو المتبادلة عبر الشبكات، وهي إما تجسد أو تمثل أموالا أو أصولا أو أسرارا، أو بيانات شخصية، أولها قيمة بذاتها كالبرامج ونتيجة لذلك اختلف الفقهاء في محل الجريمة المعلوماتية، فاختراق أحدهم لنظام الحاسوب لأحد البنوك والتلاعب في البيانات المجسدة لأصول أو أموال بغرض الاستيلاء على المال، فعل قد يكفيه البعض بأنه سرقة للمال وقد يوصف بأنه تلاعب بالبيانات أو احتيال للحصول على المال أو غش للحاسوب، كما أن استخدام حاسوب شخصي للتواصل مع نظام الحاسوب لأحد مراكز أو بنوك المعلومات والاستيلاء على بيانات مخزنة فيه يكفيه البعض بأنه سرقة للمعلومات بالمعنى التقليدي للسرقة بعناصرها القائمة على فعل الأخذ أو الاختلاس ونقل الحيازة للمال المنقول المملوك للغير، طبعا سندا إلى اعتبارهم أن المعلومات مال منقول إن لم يكن ماديا لدى بعضهم فله حكم المنقول المادي، وقد يراه البعض متجردا من الصفة المادية، ومعنوي بطبيعته. لكن بعض الفقه يرد بأن ما يراه الآخرون هو الجريمة بذاته فإنه في الحقيقة نتيجة للفعل وأثر للاعتداء المباشر على المعطيات، ولو كانت في الحقيقة هدف الفاعل الرئيسي، فإنه يمكن وصفها مجازا بمحل الاعتداء غير المباشر أو الثانوي لكن في كل الأحوال ليست محل الاعتداء المباشر الذي انصب عليه سلوك الفاعل، من تغيير أو تلاعب أو نقل أو إتلاف أو استيلاء فمحل الاعتداء المباشر هو المعطيات بذاتها وبما تمثله.

ويرجع هذا التباين في الآراء في الحقيقة إلى التباين في تحديد الطبيعة القانونية للمعلومات، فمنهم من اعتبرها أموالا ذات طبيعة خاصة يجوز أن تكون محلا لحق ملكية أدبية أو فنية أو صناعية، والبعض الآخر بسط وصف المال على المعلومات في ذاتها مجردة عن دعامتها المادية نظرا لقابليتها للحيازة والتملك.

**الفرع الثالث: دوافع ارتكاب الجرائم المعلوماتية:**

يقول الدكتور Adam GRAYCAR مدير المعهد الأسترالي لعلم الإجرام، بأن الجريمة تحتاج إلى أربعة عناصر رئيسية لتشجيع المجرم على ارتكابها وهي:

أولا: دافع معين لارتكاب العمل.

ثانيا: هدف ضحية محاسبة.

ثالثا: الفرصة المواتية.

رابعا: غياب عيون الأمن[1].

إذن فالدافع والقصد يشكل أحد الركائز في جميع الجرائم. وبالنسبة لجرائم الحاسب الآلي والإنترنيت فهي لا تختلف في وضعها العام عن أسباب أي جريمة أخرى تقليدية.[2]

فثمة دوافع عديدة تحرك العينات لارتكاب أفعال الاعتداء المختلفة المنضوية تحت هذا المفهوم، ويمكن تلخيص هذه الدوافع فيما يلي:

**الفقرة الأولى: الدوافع الذاتية.**

**أولا: الرغبة الأكيدة في الانتقام:**

الانتقام موجود داخل النفس البشرية، فكثير من الأفراد يفصلون تعسفيا أو بغير وجه حق من شركة أو منظمة حكومية، أو حتى مصرف، وهم يملكون المعلومات والتدريب اللازمة والمعرفة الكافية بخفايا هذه الجهة، لذلك يرتكب الجاني الجريمة رغبة منه في الانتقام ليجعل الشركة أو المؤسسة تتكبد الخسائر المالية الكبيرة من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت لا بأس به[3].

**ثانيا: الطمع وحب الثراء السريع:**

فحب الفرد للمال هو عصب الحياة يدفعه للقرصنة أو السرقة أو الاختلاس عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع الغير المكلف.

ومنذ بدايات الظاهرة، فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطته.

---

**1** – فايز بن عبد الله الشهري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنيت، الدليل الإلكتروني للقانون العربي arablawinfe ص: 9.

**2** – تركي محمد الوطيان، جرائم الحاسب الآلي: دراسة نفسية تحليلية، هذا المقال موجود على الموقع / WWW.Minshawi.COM. PDR other/ oteyom.

**3.** – في هذا الإطار فقد قام أحد المسؤولين الإعلاميين بإحدى الشركات بعد فصله عن العمل بزرع قنبلة منطقية زمنية في برنامج الشركة أدى إلى انهيار النظام كاملا لمدة شهر كامل مما كبد الشركة خسائر كبيرة. أنظر بهذا العدد: Mohammed Bozobar أنظر المقال السابق ص: 523.

**الفقرة الثانية: الدوافع النفسية:**

**أولا: الرغبة في إثبات الذات والتفوق على تعقيد وسائل التقنية:**

الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنيت غالبا هي صورة البطل والذكي، الذي يستحق الإعجاب لا صورة الجرم الذي يستوجب محاكمته، فمرتكبوا هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة، فيحاولون إيجاد الوسيلة إلى تحطيمها، أو التفوق عليها.

**ثانيا: دوافع سياسية وإيديولوجية:**[1]

كثيرة هي المنظمات في عصرنا الحالي، والتي تتبنى بعض الآراء والأفكار السياسية، أو الدينية أو الإيديولوجية، ومن أجل الدفاع عن هذه الآراء تقوم بأفعال إجرامية ضد معارضيها.

وعلى سبيل المثال لا الحصر يكفي أن نادي Chaces Computer أو club Chaces computer الذي نادى في أواخر الثمانينات بضرورة الاعتراف بحق جديد من حقوق الإنسان يتمثل في الحق في التواصل مختلف أطياف الإنسانية عبر العالم دون قيود.

---

**1** - Philippe JOUGLEDX, droit des médias, faculté de droit d'aix- Marseille, dans le thème : « la criminalité dans le cuber- espace », 1999, p : 25 et suivants.

# الفصل الأول:
# المكافحة الموضوعية و التحديات الإجرائية للجريمة

# الفصل الأول :

## المكافحة الموضوعية و التحديات الإجرائية للجريمة الواقعة على المواقع الإلكترونية

فرض الإجرام المعلوماتي نفسه كظاهرة سلبية على المجتمعات بعد التطور المعلوماتي الذي وصلت إليه هذه الأخيرة، فبدا التأثير السلبي لهذا الإجرام واضحا و مهددا للأفراد و الجماعات والأموال و الحكومات على حد سواء، و لتدارك هذا الخطر بدت عملية المكافحة للجريمة المعلوماتية ضرورة حتمية يجب التصدي لها خاصة و قد وجدت الدول نفسها عاجزة عن أداء واجبها الدستوري والقانوني لحماية الأفراد وتحقيق الأمن و الاستقرار الاجتماعي المنوط بها إزاء الفراغ القانوني لمكافحة هذه الظاهرة فما كان منها سوى الإسراع إلى احتواء هذا النوع الجديد و الخطير من الإجرام بسد الفراغ القانوني لمكافحته و ذلك بتعديل قوانين عقوباتها القائمة و إصدار قوانين عقابية جديدة تتصدى لمكافحة مختلف أنواع الإجرام المعلوماتي الجديد، خاصة تلك الرائدة في مجال التطور المعلوماتي كفرنسا وأمريكا و كندا والمملكة المتحدة..... إلخ و قد اختلفت الأساليب التي لجأت إليها التشريعات في مختلف الدول في صياغة النصوص القانونية الخاصة بالجرائم المعلوماتية بحيث ظهرت عدة أنواع في هذه الأساليب كأسلوب الإضافة الذي مفاده إضافة الحالات التي يرتكب الجاني فيها النشاط الإجرامي بواسطة الحاسب الآلي إلى النصوص القائمة التقليدية.

أو أسلوب وضع نصوص جديدة قياسا على نصوص تقليدية قائمة بالفعل أو أسلوب One for All وضع نص رئيسي واحد يستطيع التعامل مع الأوجه المختلفة للجريمة المعلوماتية اتبعت هذا الأسلوب الولايات المتحدة الأمريكية[5].

أو أسلوب تجميع كل ما يتعلق بالجريمة المعلوماتية في قسم ملحق بالتشريع الجنائي مثلما هو معمول به في قانون العقوبات الكندي حيت اضيفت المواد الخاصة بالمكافحة الموضوعية للجريمة المعلوماتية في قسم ملحق بقانون العقوبات[6] أو تشريع مستقل مثلما فعل المشرع الفرنسي[7] في القانون رقم

1. نائلة عادل محمد فريد قورة، المرجع السابق، ص311 .

6. قانون العقوبات الكندي المعدل سنة1997 اضيفت المواد 342.01 و 342.02 و 326 و 327 و 430.1.1 في قسم ملحق.

78/17 الصادر في 1978/01/06 المسمى بقانون الاعلام الآلي و الحريات[1]. و هناك من التشريعات من جمعت بين أسلوبين أو أكثر في صياغة نصوصها، كالمشرع الجزائري الذي جمع بين اسلوب وضع تشريع مستقل عن طريق استخدام منظومة قانونية مستقلة كالقانون رقم 04/09 المؤرخ في05 اوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها و اسلوب تجميع كل ما يتعلق بالجريمة المعلوماتية بإضافة احكام جديدة و الحاقها بقانون العقوبات، او الحاق النصوص الجديدة الخاصة بالجريمة المعلوماتية بقوانين مستقلة خاصة كالقانون المتعلق بحقوق المؤلف والحقوق المجاورة.

و مكافحة الجريمة المعلوماتية موضوعيا تعني في بحثنا هذا دراسة هذه القوانين التي صيغت لسد الفراغ القانوني في مجال الإجرام المعلوماتي حتى لا تخرج الدول عن أهم مبدأ في قوانين العقوبات الذي هو مبدأ الشرعية الذي مفاده ألا جريمة و لا عقوبة إلا بنص و قد اخترت دراسة هذه القوانين في دول رائدة في هذا المجال على سبيل المثال في كل من فرنسا و كندا و أمريكا مع التعرض لموقف الجزائر أو المشرع الجزائري في مكافحة الجريمة المعلوماتية .

اما المصالح المستحدثة ، فتتمثل في استحداث مراكز قانوينة افرزتها الحياة الرقمية الجديدة مثل حقوق الملكية الفكرية على تصميم البرامج المعلوماتية، بالاضافة الى حقوق الملكية الصناعية ، والاسم التجاري للمواقع الاليكترونية المختلفة ،والحقوق الناتجة عن تشغيلها والخدمات التي تقدمها للعملاء. فإذا ما تأخرت القوانين والتشريعات اللازمة لمواجهة هذه الظاهرة الاجرامية ، الجديدة فسوف نواجة عشوائية سيبيرية كتلك العشوائية العمرانية التي نتجت عن تأخر قوانين التطوير العمراني.
لان الفضاء السيبري المتعولم وضع اكثر من 200 دولة في حالة اتصال دائم واصبحت شبكة الانترنت اليوم تشهد تعايشاً مستمرا في جميع المجالات العلمية والبحثية والاقتصادية ، بل والسياسية والاجتماعية على السواء ،وهو ما يقودنا الى ضرورة التعرض الى تحديات الجريمة المعلوماتية في ظل

1. Journal Officiel de la République Française du 7 janvier 1978 et rectificatif au J.O. du 25 janvier 1978).

الفراغ التشريعي في مواجهة هذه الجرائم من جهة ، وتحديات الجريمة المعلوماتية العابرة للحدود الاقليمية من جهة اخرى.

وعليه فإن اعطاء صورة عامة عن الجريمة المعلوماتية ، وما تثيره من اشكاليات في القانون الجنائي يقتضي ضرورة التعرض للمشكلات الموضوعية و الإجرائية التي يثيرها هذا النوع المستحدث من الجرائم ، وعليه فسنتعرض إلى المكافحة الموضوعية للجريمة الواقعة على المواقع الإلكترونية في مبحث أول ، قبل أن نصل إلى التحديات الإجرائية التي يثيرها هذا النوع المستحدث من الجرائم في مبحث ثان.

## المبحث الاول:

## المكافحة الموضوعية للجريمة الواقعة على المواقع الإلكترونية

بدأت الثورة المعلوماتية نتيجة اقتران تقنيتي الاتصالات من جهة، والمعلومات وما وصلت إليه من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها اليوم، حتى بات يطلق على هذا العصر عصر المعلومات. وتعد المعلومة أهم ممتلكات الإنسان، اهتم بها، على مر العصور، فجمعها ودونها وسجلها على وسائط متدرجة التطور، بدأت بجدران المعابد والمقابر، ثم انتقلت إلى ورق البردي، وانتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الأقراص الإلكترونية الممغنطة[1].

وباتحاد هاتين الطفرتين في عالم التكنولوجيا، ولد علم جديد هو علم تقنية المعلوماتية Telematique، وهو مصطلح يعبر عن اقتران التقنيتين، ويتكون من الجزء الأول من كلمتي Telecommunication، وهو الاتصال عن بعد، والجزء الثاني من كلمة Information، وتعني المعلومات، وهو علم اتصال المعلومات عن بعد.

هكذا جاء التقدم الفني مصحوباً بصور مستحدثة لارتكاب الجرائم، التي تستعير من هذه التقنية أساليبها المتطورة، فأصبحنا أمام ظاهرة جديدة هي ظاهرة الجريمة الواقعة على المواقع الإلكترونية .

لقد تباينت الصور الإجرامية لظاهرة الجريمة المعلوماتية وتشعبت أنواعها فلم تعد تهدد العديد من الصالح التقليدية التي تحميها القوانين والتشريعات منذ عصور قديمة، بل أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بثورتي الاتصالات و المعلومات .

فالمصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن بعيد بدأت تتعرض الى اشكال مستحدثة من الاعتداء بواسطة هذه التقنية الحديثة فبعد أن كان الاعتداء على الاموال يتم بواسطة السرقة التقليدية أو النصب،و كانت الثقة في المحررات الورقية يعتدى عليها بواسطة التزوير، أصبحت هذه الأموال يعتدي عليها عن طريق اختراق الشبكات المعلوماتية واجراء التحويلات الالكترونية من اقصى مشارق الأرض الى مغاربها في لحظات معدودة، كما اصبحت

---

**1** .د.هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة،أسيوط، 1992،ص5.

تلك الحقوق الثابتة في الاوعية الورقية يتم الاعتداء عليها في اوعيتها الالكترونية المستحدثة عن طريق اختراق الشبكات والانظمة المعلوماتية دون الحاجة الى المساس باي وثائق او محررات ورقية.
وبعد ان كانت الحياة الخاصة للإنسان تواجه الاعتداء باستراق السمع او الصورة الفوتوغرافية، اصبحت هذه الخصوصية تنتهك بواسطة اختراق، البريد الالكتروني والحواسب الشخصية ، و قواعد البيانات الخاصة بالتأمين الصحي والمستشفيات ومؤسسات الائتمان والتأمين الاجتماعي. تعد الجريمة المعلوماتية ، من أكبر التحديات التي نواجهها في عالمنا المعصر ، إن لم تكن أكبرها على الإطلاق ،والحديث عن هذه التحديات يتطلب أولاً إعطاء صورة عامة عن تحديد ماهيتها ، قبل التعرض إلى بحث مشكلة المسؤولية الجنائية الناتجة عنها، وهو ما يدعونا إلى التعرض إلى بحث عن اهم صور الجريمة المعلوماتية و تحدي الأحكام العامةللجريمة، مطلب أول قبل التعرض إلى جريمة غسل الاموال عبر الوسائل الإلكترونية في مطلب ثان.

## المطلب الأول : أهم صور الجريمة الواقعة على المواقع الإلكترونية و تحدي الأحكام العامة للجريمة.

تعد الجرائم المعلوماتية صنفاً مستحدثاً من الجرائم التي تتحدى القواعد التقليدية للتجريم و العقاب التي تقتضي ضرورة تحقق اركان الجريمة طبقاً لمبدأ شرعية الجرائم و العقوبات ، وهو ما سنعرض له في تناول صور هذه الجرائم في فرع أول قبل أن نعرض أنشطة الأنترنت غيرالمشروعة المتصلة بالمحتوى المعلوماتي و البريد الإلكتروني وأنشطة التصرف المعلوماتي الغير قانوني في فرع ثان.

### الفرع الأول: صور الجريمة المعلوماتية

إذا كانت الجرائم المعلوماتية لها صور متعددة بتعدد دور التقنية المعلوماتية من جهة ، وتعدد صور الجرائم التقليدية منجهة أخرى ،فإن ذلك لا يعني تناول هذاالموضوع بالطريقة المدرسية التقليدية التي تتمثل في سرد كل الجرائم التي يتناولها قانون العقوبات، بل يجب التعرض للحالات التي تثير مشكلة في تطبيق النصوص القانونية إما لتعذر المطابقة بينها و بين النصوص التقليدية أو بسبب الفراغ التشريعي لمواجهة هذه الجرائم ، ولما كان المجال لايتسع للحديث عن كل أنواع الجريمة المعلوماتية فقد تخيرنا أكثرها اثارة للمشكلات القانونية وهي جرائم الاعتداء على الحياة الخاصة و جرائم الأموال وجريمة التزوير.

## أولاً : جرائم الاعتداء على الحياة الخاصة للأفراد

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقلدية ،فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة.

يصعب بداية حصر عناصر الحق في الحياة الخاصة فهي تتكون من عناصر ليست محل اتفاق بين الفقهاء فيمكن القول بأنها تشمل حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنية[1].

اما علاقة الحياة الخاصة بالتقنية المعلوماتية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الاونه الاخيرة لخدمة اغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية[2] .

هكذا اصبحت الشبكات المعلوماتية مستودعا خطيرا للكثير من اسرار الانسان التي يمكن الوصول اليها بسهولة وسرعة لم تكن متاحة في ظل سائر وسائل الحفظ التقليدية فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان في العصر الحديث.

وقد كان ذلك في البداية بالنسبة للمعلومات التي يدلي بها بعض الأشخاص بإرادتهم الخاصة أثناء تعاملاتهم مع المؤسسات العامة والخاصة في البنوك و المؤسسات المالية كمؤسسات الائتمان وشركات التأمين والضمان الاجتماعي وغيرها ،فالبيانات الخاصة بشخصية المستخدم يمكن الوصول اليها عن طريق زيارة بعض المواقع على شبكة المعلومات ، لان شبكات الاتصال تعمل من خلال بروتوكولات موحدة تساهم في نقل المعلومات بين الاجهزة وتسمى هذه البروتوكولات الخاصة مثل بروتوكولات HITP الذي يمكن

عن طريقها الوصول الى رقم جهاز الحاسب الشخصي ومكانه وبريده الالكتروني ، كما ان هناك بعض المواقع التي يؤدي الاشتراك في خدماتها الى وضع برنامج على القرص الصلب للحاسب الشخصي وهو ما يسمى cookies

---

**1**. ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية القاهرة 1983 ص 207

**2**. أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة 1994 ص 48

وهدفه جمع معلومات عن المستخدمين . بل ان اخطر ما في استخدام هذه الشبكة يتمثل في ان كل ما يكتبه الشخص من رسائل يحفظ في ارشيف خاص يسمح بالرجوع اليه ولو بعد عشرون عاما[1]. ويظن الكثيرون ان الدخول باسم مستعار او بعنوان بريدي زائف لساحات الحوار ومجموعات المناقشة قد يحميهم ويخفي هويتهم، وفي الحقيقة فإن مزود الخدمة أو internet service provider (ISP) يمكنه الوصول إلى كل هذه المعلومات بل ويمكنه أيضا معرفه المواقع التي يزورها العميل.

وعلية فإن القوانين المقارنة اهتمت بهذه المسألة واتجهت إلى تبني العديد من الضمانات التي يمكن تلخيصها في:

1 -**مبدأ الأخطار العام** : وهو أن يعلم الجمهور الهيئات التي تقوم بجمع هذه البيانات وتنوع المعلومات التي تقوم بتسجيلها [2] فيجب أن تكون هناك قيود على انشاء الانظمة المعلوماتية المختلفة لمعالجة البيانات.

2 -**شرعية الحصول على المعلومة** : يجب أن يتم الحصول على المعلومة بطريقة تخلو من الغش والاحتيال حيث تمنع المادة 25 من القانون الفرنسي للمعلوماتية تسجيل أي معلومة الا اذا كانت برضاء صاحب الشأن.

3 -**التناسب بين المعلومات الشخصية المسجلة والهدف** من ذلك التسجيل، فعلى الجهة الراغبة في اقامة أي نظام معلوماتي ان تحدد الهدف من إقامته[3].

ولقد تضمنت بعض القوانين العربية العديد من النصوص والقواعد التي تحمي البيانات الشخصية وتفرد عقوبات على افشاء هذا النوع من البيانات مثال ذلك الفصل العاشر من قانون التجارة الإليكترونية المصري الصادر سنة 2004 الذي نص على حماية سرية البيانات المشفرة واحترام الحق في الخصوصية ،وكذلك قانون التجارة الالكترونية وقانون التجارة والمعاملات الالكترونية في امارة دبي الصادر سنة 2002 و قانون التجارة الإليكترونية التونسي الصادر سنة 2000 ، خاصة بعد ان صدر القانون العربي النموذجي لجرائم الكومبيوتر ، و الذي تم اعداده من قبل

---

1. عبد الفتاح بيومي حجازي – صراع الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – القاهرة 2007 ص 609
2. بدر سليمان لويس – أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية رسالة الدكتوراة – حقوق القاهرة 1982
3. عبد الفتاح بيومي حجازي – المرجع السابق ص 620 .

اللجنة المشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لمؤتمر وزراء الداخلية العرب تحت رعاية جامعة الدول العربية و جرى اقراراه بوصفه منهجا استرشاديا يستعين به المشرع الوطني عند اعداد تشريع في جرائم المعلوماتية ، فماهي حدود الحماية الجنائية للحياة الخاص في القانون الجنائي...

تتمثل النصوص االجنائية التي صيغت لحماية الحياة الخاصة في تجريم الأفعال التالية:

أول هذه الجرائم هي جريمة انتهاك حرمة المسكن وذلك لما للمسكن من أهمية كبرى ، لا لأن للمسكن حرمة كبرى فقط لكن لأن المسكن في ثقافة المشرع الذي وضع هذا النص يمثل قلعة حصينة لا يمكن اخاراقها الا بالدخول المادي غير المشروع وأو دون رغبة صاحبه .

أما جريمة الاطلاع على الرسائل التي أن كل موظف عمومي تابع لمصلحة البريد أو التلفون أخفى او اوقف رسالة او أطلع عليها وافشى للغير ما حوته ويراد من الرسالة المكاتبات والمحادثات التليفونية و البرقيات وما الى ذلك من وسائل الارسال، اما اذا ارتكب الافعال المذكورة اشخاص أخرون فلا تكون إلا بناء على شكوى الطرف المتضرر. فإذا كان المشرع قد توسع في مفهوم الرسالة حيث يمكننا سحب مفهومها في هذا النص على رسائل البريد الالكتروني الا ان هذه الحماية لا يمكن ان تمتد الى البيانات المخزنة في أي نظام من نظم المعلومات لأي جه اخرى سواء كانت عامة او خاصة ،فالحاسب الالي اليوم لم يعد جهازا للاتصال ومعالجة المعلومات، فقط بل اصبح مستودعا ضخما للمعلومات والبيانات في آن واحد.

نص المشرع كذلك على جريمة اذاعة معلومات تتعلق بإجراء جنائي ، وهنا الحماية مقتصرة على الإجراءات الجنائية .

أما جريمة إفشاء أسرار الوظيفة فتتمثل في انه يتضمن شرطا مفترضا يتمثل في ان الجاني في هذه الجريمة موظفا عموميا بالإضافة إلى أن هذه الحماية تقتصر على المعلومات الرسمية ومن ثم تكون هذه الحماية قاصرة على حماية البيانات الاسمية أو الشخصية غير الرسمية و المخزنة في نظم المعلوماتية معينة وهو ما نصل معه إلى عدم وجود أي نص يتعلق بحماية المعلومة أو البيان الخاصة بصفة عامة بغض النظر عن مصدرها و عن النظام المعلوماتي المخزنة فيه ، سواء تم جمعها من قبل الموظف العام أم غيره .

وقد قام المشرع بتجريم سوء استعمال ،او حيازة هذه البيانات ،او التقصير في التزام تسجيلها ،او الإخلال بواجب الحفاظ على سريتها ،او اساءة استخدامها ،او الحصول على البيانات بطريقة غير مشروعة أو حجبها آو إتلافها او تغييرها.

إلا أن هذه الحماية تقتصر على المعلومات المخزنة في هذا النظام الوطني المنصوص عليه في هذا القانون ولا تنطبق على غيره من البيانات، سواء تلك المخزنة في المؤسسات العامة أو الخاصة، كشركات التأمين والمستشفيات والمصارف.

هكذا نجد أنه على المشرع التدخل بالحماية الجنائية اللازمةلأن عناصر الحياة الخاصة لم تعد تقتصر على المسكن و الصورة و المحادثات الهاتفية أو الرسائل البريدية ، فتقنية المعلومات في عصر العولمة قد أفرزت عناصر مستحدثة للخصوصية يجب أن تشكل مراكز قانونية جديدة ، في حاجة ماسة للحماية.

هكذا نجد أن الحق في الحياة الخاصة بعناصره المستحدثة غير مشمول بالحماية الجنائية اللازمة ، فهل تحظى الأموال بهذا القدر من الحماية الجنائية ؟

## ثانياً: جرائم الاعتداء على الأموال

إذا كان قانون العقوبات الليبي شأنه شأن كل قوانين العقوبات الأخرى قد جرم الاعتداء على الأموال في صوره التقليدية كالسرقة والنصب وخيانة الأمانة واختلاس الأموال العامة ، فقد كان ذلك في ظل عصر لا يعرف سوى النقود الورقية أو المعدنية وما يحل محلها من صكوك أو أوراق مالية كالكمبيالات والسند الأدنى في عصر المصارف التقليدية ذات المقر المحدد مكانيا وقد كان أقصى ما وصلت إليه من تقدم متمثلا في إجراء التحويلات المصرفية بإجراءات ورقية معقدة و مقابل رسوم مالية معينة. فإذا كان الركن المادي للسرقة المتمثل في الاختلاس يمكن أن يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر لم يحدد المشرع شكل السلوك الإجرامي لها ، يمكن أن يتم بأي فعل يؤدي إلى حرمان المجني عليه من المال المنقول وإدخاله في حيازة الجاني ، كذلك الحال بالنسب لجريمة النصب حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الآخر بالطرق الاحتيالية ، فهل ينطبق ذلك على جرائم السرقة و الاحتيال التي ترتكب عن طريق التقنية المعلوماتية ؟

لذا سوف نعرض إلى الوسائل الفنية التي يتم عن طريقها الاختلاس قبل أن نعرض تكييفها القانوني في ظل الفراغ التشريعي في معظم الدول العربية.

الوسائل الفنية للتحويل الإلكتروني للأموال يتم التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال لكن يمكن الاشارة إلى أكثرها انتشاراً.

1 - **استخدام برامج معده خصيصا لتنفيذ الاختلاس** : أشهر هذه الوسائل هو تصميم برامج معينة تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى أخر سواء كان ذلك من المصرف نفسة او من حساب أخر في مصرف اخر على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، وأشهر هذه الوقائع قيام احد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري لتطوير أنظمة المعلومات بِالاستيلا ء على مبالغ طائلة من المصرف بعد أن تمكن من اختيار خمسة حسابات راكدة في خمس فروع محليه للمصرف واعد لها برنامجا تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات التي حسابات أخرى فتحت باسمه في الفروع نفسها على أن تتم عملية التحويل أثناء وجوده بالطائرة في طريقة إلى المملكة المتحدة عائدا إلى بلاده بعد انتهاء عقد عمله ، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا[1]. كما توجد برامج أخرى تقوم بخصم مبالغ ضئيلة من حسابات الفوائد على الودائع المصرفية بإغفال الكسور العشرية بحيث يتحول الفارق مباشرة إلى حساب الجاني لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة ومما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ هو أن هذه الاستقطاعات تتم على مستوى ألاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل حساب على حده بحيث يصعب أن ينتبه إليه العميل[2].

2 **التحويل المباشر للأرصدة** : يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور ،أشهرها قيام احد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف وقيامه بتحويل 12 مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط وعادة ما يتم

---

**1**.هشام فريد رستم – قانون العقوبات مخاطر المعلومات مكنة الآلات الحديثة أسيوط 1992ص 81

**2** David Bainbridge- Introduction to computer law-third edition-Pit Man publishing1996 p237

ذلك أيضا عن طريق إدخال معلومات مزيفة وخلق حسابات و مرتبات وهمية وتحويلها إلى حساب الجاني ،ويمكن أن يتم التحويل المباشر أيضا عن طريق التقاط الإشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الأقمار الصناعية فهناك بعض الأنظمة إلى تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات اليكترومغناطيسية ثبت أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز وإعادة بثها مرة أخرى بعد تحويرها[1]. وهو ما نصت عليه اتفاقية بودابست في المادة 5

3- **التلاعب بالبطاقات المالية** : لقد ظهرت اولى هذا النوع من الاحتيال بالتقاط الارقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الالي للنقود الى أن ظهرت الصرافة الالية Electronic Banking والنقود المالية digital Cash .

أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الارقام السرية الخاصة بها وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن ان تسجل عليها أرقام هذه البطاقات. و في هذا النوع من الاعتداءات لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها سواء تم ذلك عن طريق سرقة البطاقة نفسها ، أو عن طريق سرقة الرقم السري واستخدامه استخدام غير مشروع للتحايل على المؤسسات المالية وصرف هذه المبالغ خاصة أن النموذج التجريمي لجريمة النصب لم يشترط في الوسائل الاحتيالية ان تكون مرتكبة ضد الانسان فيكفي ان ترتكب هذه الوسائل الاحتيالية ضد الآلة ما دامت تؤدي الى الحصول على نفع غير مشروع اضرارا بالاخر من وهو ما نصت عليه المادة 461 ع .

4 - **جرائم الاعتداء على أجهزة الصرف الآلي للنقود** : تثور هذه المشكلة في حالة استخدام الجهاز لصرف ما يتجاوز الرصيد الفعلي اذا تم ذلك بواسطة العميل صاحب البطاقة فالمسألة هنا لا تعدوأن تكون مسألة مديونية بين المؤسسة المالية والعميل ولا يمكن تكييفها بأنها سرقة طبقا للمادة 444 ع لان الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية طالما ان هذه الاخيرة تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه.

---

**1**..محمد سامي الشوا ثورة المعلومات وبعكسها على قانون العقوبات دار النهضة العربية القاهرة 1994ص 70-72 وما بعدها

**5 -جرائم الاستيلاء على النقود الالكترونية :** يمكن تعريف النقود الالكترونية Electronic Cash بأنها "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً، وغير مرتبطة بحساب مصرفي، تحظى بقبول غير من قام بإصدارها، وتستعمل كأداة دفع". وتتمثل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أو على القرص الصلب للحاسب الشخصي للمستهلك، فهي تختلف عن البطاقات الإئتمانية، لأن النقود الإلكترونية يتم دفعها مسبقاً، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين هما: العميل والتاجر، دون الحاجة إلى تدخل طرف ثالث، كمصدر هذه النقود مثلاً [1] فهي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الالكترونية أن تحل فعليا محل تبادل العملات النقدية [2]، ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع[3]

## 6. جريمة التوصل او الدخول غير المصرح به

تعد أنشطة الدخول او التوصل غير المصرح به او غير المخول به Unauthorized Access ، الانشطة الجرمية الاكثر انتشارا most windespread بين جرائم الكمبيوتر والانترنت ، ويقوم التوصل غير المصرح به بالاساس على الدخول الى نظام الحاسوب او شبكة المعلومات ، عادة من خلال استخدام وسيلة اتصال عن بعد ( كالموديم modem ) او من خلال التوصل عبر نقاط الاتصال والموجهات الموجودة على الشبكة للدخول الى نظام كمبيوتر معين بغرض التوصل مع البيانات او البرامج المخزنة في النظام ، ويتطلب هذا النشاط غالبا تجاوز او كسر اجراءات الحماية التقنية للنظام system security ، كتجاوز كلمة السر pssword

---

**1**. محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004، ص142–148.

**2**. منير الجنبيهي – ممدوح الجنبيهي – البنوك الالكترونية ط 2 – 2006 دار الفكر الجامعي – الإسكندرية ص47

**3**. عبد الفتاح بيومي حجازي – صراع الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – دار للنشر والبرمجيات القاهرة 2007 ص 609

واجراءات التعريف والجدران النارية وغيرها او التوصل لنقطة ضعف في نظام حماية البرامج والنفاذ منها. ومعظم الذين يرتكبون هذه الانشطة بآلياتها التقنية المتعددة تكون انشطتهم مجردة عن اغراض لاحقة ، ولا يكون هدفهم – في الغالب – الاضرار بالبيانات والملفات او تدميرها destroying data or files ، وفي الغالب يسعى مقترفو هذه الانشطة الى الاطلاع على المعلومات المحمية . غير ان حماية المعلومات من اخطار هذه الانشطة ، واحتمال تطور هذه الانشطة من مجرد هدف الاطلاع الى اهداف اكثر خطورة ك التلاعب بالمعطيات او اتلافها او ارتكاب غير ذلك من جرائم الحاسوب او استخدام الدخول لارتكاب جرائم اخرى بواسطة الكمبيوتر ، دفعت غالبية دول العالم الى تجريم هذه الانشطة كما هو الشأن في قوانين كل الدول الاوروبية وامريكا واليابان.

ومن الوجهة التقنية ، يمثل فعل التوصل غير المصرح به مع نظام الحاسوب الفعل الاول من بين انشطة جرائم الكمبيوتر والانترنت ، قد ينتهي النشاط به وقد يمتد النشاط الى ابعد من مجرد التوصل ، وهذه الحقيقة التقنية تثير الجدل حول ما اذا كان التوصل غير المصرح به بذاته فعلا جرميا ، فيجرم لذلك مجرد الدخول الى النظام حتى لو لم يكن ثمة فعل آخر لاحق لها السلوك، ام انه مجرد فعل تحضيري لجرم لاحق – ان ارتكب – غير مجرم بذاته . ثم اذا اعقب التوصل اتيان فعل آخر؟! فهل نكون امام تعدد في الجرائم ، ام ان التوصل يمثل حالة الشروع في الجريمة التي هدف الى ارتكابها بفعل التوصل ؟! ثم ما هي الأفعال المكونة للركن المادي لهذه الجريمة عند النص عليها استقلالا عن اي فعل لاحق ؟! وما هي الوسائل التقنية لاتيان هذه الأفعال ؟!

وقد جاء موقف القوانين المقارنة بشأن جريمة التوصل غير المصرح به مع نظام الكمبيوتر بما يلي :

ان القوانين المقارنة التي وضعت لمواجهة جرائم الحاسوب ، جرمت في غالبيتها ، جريمة التوصل غير المصرح به مع نظام الحاسوب . لكنها تتفاوت في تحديد المراد بهذه الجريمة ، ففي القانون الفرنسي ( 1988 المعدل لعام 1994) يجرم المشرع مجرد التوصل مع نظام الحاسوب او البقاء فيه ، وكذلك ينهج ذات القانون البريطاني ( 1990 ) مع تباين في نطاق الأفعال المكونة للجريمة بين القانونيين ،

في حين نجد القانون الامريكي ( 1984 والتشريعات اللاحقة عليه ) يقرن فعل الاتصال بدون تصريح مع تحقيق نتائج محددة ، كالحصول على المعلومات او استخدام النظام او اتلاف المعطيات . وتتردد بقية القوانين محل الدراسة بين هذه الاتجاهات ، فنجد قوانين معظم الولايات الامريكية سلكت مسلك القانون البريطاني في تجريم مجرد التوصل مع نظام الحاسوب ، فنص قانون كاليفورنيا لعام 1985 على انه يعتبر مرتكبا لجنحة كل من دخل عمدا الى منظومة أو شبكة حواسيب او الى برنامج او بيانات عالما بحظر ذلك من قبل مالكها او مستأجرها ، ولعل مسلك القوانين الخاصة بالولايات الامريكية يستند الى منهج مشروع القانون الفدرالي لحماية نظم الحاسوب لسنة 1984 ، الذي جرم في المادة الثانية الاتصال عمدا بغير تصريح لحاسوب او بنظام حاسوب او بشبكة تتضمن حاسوبا . ، ونجد مثلا ، القانون السويسري ينهج منهج القانون الامريكي (قانون غش واساءة استخدام الحاسوب لسنة 1984) وعلى هدي مسلك القانونين الفرنسي والانجليزي سلكت معظم القوانين الاوروبية .

## 7. جريمة الاستيلاء على المعطيات .

يعرف الاستاذ محمود نجيب حسني السرقة ، بانها " اعتداء على ملكية منقول وحيازته بنية تملكه " وعرفها قانون العقوبات الأردني في المادة (1/399) بانها " اخذ مال الغير المنقول دون رضاه " وجريمة السرقة ، اعتداء على حق الملكية ، ولهذا فان الملكية هي المحل الرئيسي للاعتداء ، وهي كذلك اعتداء على الحيازة من اجل استطاعة الاعتداء على الملكية . واما موضوع جريمة السرقة ، فهو (المال المنقول) وفق القانون الأردني واللبناني (م 635) والكويتي (م 217) والقطري (م21) والسوري (م 621) والمغربي (م 505) وقانون ابو ظبي (م 78) . وهو (المنقول) وفق القانون المصري ، (والشئ) وفق العديد من قوانين العقوبات المقارنة كالفرنسي (م 379) والبلجيكي والهولندي (م 310) والتونسي (م 258) والبحريني (م 231) (والشئ المنقول) وفق القانون الالماني (م 242) والايطالي (م 624) والسويسري (م 137) . و (الشئ المادي) وفق القانون النمساوي (م 127) . وجامع هذه الاوصاف لتحديد محل السرقة ان تتوفر الصفة المادية في المحل وان يكون مالا ( كل شئ يصلح محلا لحق عيني) لان الحيازة التي تنالها السرقة بالاعتداء ، يراد بها الحيازة المادية ، المتمثلة بسيطرة

الحائز على الشئ ومباشرة سلطاته المادية عليه ، وان يكون محل السرقة مملوك للغير ، اذ لا تقوم السرقة اذا كان المال مملوك ا للمتهم أو كان لغير المالك . وان يكون منقولا ، وهو ما يتم نقله من مكان إلى مكان دون تلف ، وقد الحق بالمنقول العقارات بالتخصيص والعقارات بالاتصال ، وعلة تطلب ان يكون محل السرقة منقولا ، هو ان فعل الاخذ أو الاختلاس (كما يسمى في القانون المصري) يتطلب تغيير موضع الشئ كوسيلة لاخراجه من حيازة المجني عليه .

وقد توسعت النظم القانونية في دلالالة تعبير المال أو الشئ المادي ، اما عبر الاجتهاد القضائي أو بنصوص صريحة في قوانين العقوبات ، فادخلت في نطاقه القوى المحرزة ، كالطاقة الكهربائية ، اما استنادا إلى اعتبار الكهرباء ذات كيان مادي ملموس وتصلح محلا للملكية والحيازة ، أو بالاستناد إلى قيمة الكهرباء وان كانت مجرد حالة للمادة . وليس المقام تحليل الاتجاهات في مسألة صلاحية القوى المحرزة لتكون محلا لجريمة السرقة، ونكتفي بالقول ان الموقف من تجريم سرقة الكهرباء في بداياته يشابه إلى حد بعيد الجدل الحاد الذي دار حول صلاحية معطيات الحاسوب وكذلك صلاحية المعلومات عموما للسرقة ، هذا الجدل الذي لم يحسم الا باقرار نصوص خاصة تجرم الاعتداء على القوى المحرزة [1].

وتتطلب جريمة السرقة – عموما – توافر الركن المادي المتمثل بفعل الاخذ دون رضى المالك (القانون الأردني) أو الاختلاس وفقا للقانون المصري ، والنتيجة الجرمية المتمثلة لخروج الشئ محل السرقة من حيازة المجني عليه إلى حيازة الجاني ، وعلاقة السببية التي تربط الفعل بالنتيجة . وحيث ان الاعتداء في السلوك الاجرامي ينصب على حيازة الغير ، فان عنصر الاخذ أو الاختلاس يتعين تحديده بالاستناد إلى نظرية الحيازة [2]، ويعرف تبعا لذلك بانه " اخراج الشئ من حيازة المجني عليه دون رضاه وادخاله في حيازة اخرى " [3].

---

1. انظر المراجع المشار اليها في الهامش السابق .
2. الدكتور نور الدين هنداوي، الحماية الجنائية للحيازة، الطبعة الأولى، دار النهضة العربية، القاهرة، 1993.
3. انظر د. حسني ، و د. السعيد ، المرجعين السابقين المشار اليهما في الهامش 182.

واما الركن المعنوي في جريمة السرقة ، فيتخذ صورة القصد الجنائي ، ولا يكفي الجريمة توفر القصد العام متمثلا بعنصري العلم والارادة ، وانما يتطلب ركن السرقة المعنوي قصدا خاصا ، يتمثل بنية

تملك المال موضوع السرقة ، وتقوم هذه النية على عنصرين : سلبي ، يتمثل بارادة حرمان المالك من سلطاته على الشئ ، ومظهره العزم على عدم رد الشئ . وعنصر ايجابي ، قوامه ، ارداة المتهم ان يحل محل المالك في سلطاته على الشئ ، وبالتالي فان نية التملك كما يقول د. محمود نجيب حسني " لا تتجه إلى الملكية كحق ، ولكن تتجه إليها كمركز واقعي وفحوى اقتصادي ، أي مجموعة من السلطات والمزايا الفعلية " [1].

هذه هي المعالم الرئيسة لجريمة السرقة في القانون الجنائي التقليدي ، وليس المقام التوسع في تناول احكامها ، غير أننا في معرض بيان الاتجاهات حول امكان انطباق نصوص جريمة السرقة على جريمة الاستيلاء على المعطيات سنتعرض حسبما تقتضي الدراسة إلى جوانب اخرى من احكام هذه الجريمة.

في ضوء هذا التحديد هل ينطبق نص الرقة التقليدي على الاستيلاء على المعطيات ؟؟

يرصد الفقه [2] ثلاث صور يتحقق فيها الاستيلاء على معطيات الحاسوب:-

اولها :- الالتقاط الذهني للبيانات بالنظر أو الاستماع ، و يتم هذا الالتقاط " بالاختزان أو الحفظ الواعي أو العرضي للمعلومات اثر مطالعتها بالبصر ان كانت قد ظهرت على شاشة الحاسوب في شكل مرئي ، أو بعد وصولها إلى الاذن ان تمثلت في صورة صوتية صادرة على الاجهزة . وثانيها :- النسخ غير المشروع للبيانات المخزنة الكترونيا ، اما عن طريق التعامل المباشر مع نظام الحاسوب ، المخزنة فيه البيانات على هيئة نبضات كهربائية في الدارات المدمجة ، أو على وسائط التخزين الرئيسة أو الثانوية ( hard & flopy disk ) ، واما عن طريق التوصل غير المرخص به مع نظام الحاسوب ، عبر الاتصال عن بعد كما عرضنا فيما تقدم .

---

1. د. حسني ، المرجع السابق ، ص 866 .
2. انظر في هذا الصدد د. رستم ، المرجع السابق .

وثالثها :- اعتراض معطيات الحاسوب خلال نقلها والتقاطها بواسطة احدى الطرق التي عرضنا لها سابقا . اما صورة الاستيلاء على الدعامات المادية المتضمنة للبيانات ، فقد اكدنا في غير مقام ، انها لا تثير مشاكل في تطبيق النصوص الجنائية التقليدية المشيدة على حماية الاموال المادية .

والسؤال الذي يثور في هذا المقام ، هل يعتبر الاستيلاء المتحقق في هذه الاساليب أو ما تماثلها أو ينشأ من اساليب تقنية للاستيلاء على معطيات الحاسوب – في ظل تطور الوسائل التقنية واساليب وتكتيك الجناة – مما يدخل في نطاق السلوك الاجرامي المكون لجريمة السرقة التقليدية ؟

لما كانت نصوص جريمة السرقة التقليدية – كما اسلفنا – تتطلب ان ينصب سلوك الجاني على شئ ذي طبيعة مادية ، فان اولى مشكلات تطبيق نصوص السرقة على الاستيلاء على المعطيات ، عدم توافر الطبيعة المادية لها.

اما المشكلة الثانية ، فهي مدى اعتبار المعطيات مالا بذاتها ، وهو من قوام عناصر موضوع أو محل جريمة السرقة .

والمشكلة الثالثة مدى قابلية المعطيات للحيازة باعتبار ان السلوك الاجرامي (الفعل) في اطار الركن المادي للجريمة يقوم بالاستيلاء على الحيازة .

تعد مسألة تحديد طبيعة المعطيات ، حجر الاساس في تقدير الموقف من قابلية انطباق النصوص التقليدية . لا على جريمة السرقة فحسب ، بل وعلى طائفة معتبرة من جرائم الحاسوب . وما اثير بشانها من خلاف حاد ومتعارض ، اشبه ما يكون بالخلاف الذي اثير حول مدى شمول نصوص السرقة لانشطة الاستيلاء على القوى المحرزة كالكهرباء وخطوط الهاتف . وكذلك يقع هذا الخلاف في نطاق الجدل الدائر حول امكان وقوع السرقة على المعلومات عموما ، مجردة من دعاماتها المادية كالورق أو المستندات أو غير ذلك .

ويكاد يكون متفقا عليه ، في الفقه واتجاهات القضاء ، ان الاستيلاء على المعطيات من خلال التقاطها الذهني ، بالنظر واستراق السمع ، لا يقوم به فعل الاخذ أو الاختلاس في جريمة السرقة التقليدية

ان الاتجاهات الفقهية ، واحكام القضاء بعد اخذ ورد اتفقت على عدم امكان انطباق نصوص السرقة على الاستيلاء على معطيات الحاسوب أو المعلومات عموما لغياب الصفة المادية ولعدم اعتبارها من قبيل الاموال التي يقع عليها السلوك الاجرامي في جريمة السرقة . وانعكس هذا الموقف على اتجاه التشريعات المقارنة التي ذهبت الى النص صراحة على جرم الاستيلاء على المعلومات (سرقتها) بالرغم من سعة بعض نصوص السرقة التقليدية في النظم المقارنة ، يقدم الدليل المعزز على

صحة حجج هذا الاتجاه القائل بعدم امكان تطبيق نصوص السرقة التقليدية على جريمة الاستيلاء على المعلومات .

إن نصوص السرقة في قوانين العقوبات العربية القائمة لا يمكن ان تطبق على جرائم الاستيلاء على معطيات الكمبيوتر ، باية مرحلة كانت عليها هذه المعطيات من نظام المعالجة او النقل ونستند في هذا الراي الى ما يلي :-

تخلف الطبيعة المادية لمعطيات الحاسوب ، وكذا المع لومات الذي لا ينفيه العديد من مؤيدي بسط النصوص التقليدية على صور الاعتداء عليها .

واستنادا الى ان المعلومات ليست مالا في ذاتها ، مع ادراكنا الكلي لان المعلومات اصبحت المحدد الاستراتيجي لراس المال بل واهم عناصر الذمة المالية – براينا – في العصر الرقمي الذي نعيش .

ان المعلومات غير قابلة للحيازة المادية وفقا للفهم القانوني المستقر في اطار نظرية الحماية الجنائية للحيازة التي تاسست عليها نصوص السرقة التقليدية .

وبالاستناد إلى ان اقوى ركائز الاتجاه الفقهي والقضائي المؤيد لبسط نصوص السرقة التقليدية يتمثل بالوصف الذي يحدده النموذج القانوني لمحل الجريمة بـ (الشئ) غير منعوتا بصفة دالة على تحديده ، خلافا للوصف السائد في تشريعات الدول العربية (مال منقول ، او منقول او منقول مادي او نحوها ) ) وبالاستناد إلى ان العديد من هذ هالاراء ،قد خلط بين مرتكزات الحماية الجنائية للملكية ، ومرتكزات حماية الملكية الفكرية وحقوق ا لمؤلف .

ان المستقر في فقه القانون الجنائي ، ان محل جريمة السرقة هو المال المنقول ذو الطبيعة المادية المملوك للغير ، ولذلك فان ابعد مدى قد وصله التوسع في مد ، بل ومط النصوص الجنائية في هذا المجال ، طال في القليل من قضاء الدول ، تجريم سرقة القوى المحرزة ولم تسوغه الغالبية الا عبر النص التشريعي صراحة .

ان الجهد المبذول في تطويع النصوص التقليدية ، لا يتفق مع تسارع وتيرة التطور في ميدان السلوك الاجرامي خاصة في عصر التقنية .

ان من اهم المبادئ المستقرة في القانون الجنائي ، مبدا الشرعية الذي يحظر العقاب على اي سلوك دون ان يكون مجرما صراحة بموجب النص القانوني . ومبدأ وحظر القياس في النصوص الجنائية الموضوعية الذي يمنع القياس من اصله فلا يقبل معه قياس سرقة الماديات على الاستيلاء على

المعنويات ، لا لانغلاق العقل عن مقتضيات التطور – كما يرى البعض – ولكن لاتصال هذه المبادئ باعلى قيم الانفتاح ، وهما كفالة العدالة وحماية حقوق الإنسان والشرعية الدستورية .

وانطلاقا من تميز ركائز الحماية الجنائية للمعلومات عموما ومعطيات الحاسوب عن حماية الاموال المادية ، التي تستدعي اقامة التوازن بين الحق في تدفق وانسياب المعلومات ومنع احتكارها ، وبين اليات حماية الاعتداء عليها ، والقيود القانونية المنظمة لهذا الحق ا لآخذ في النماء كحق متميز من حقوق الإنسان المؤسسة على التضامن الاجتماعي .

واستنادا إلى ان التمييز بين صور الاستيلاء التقنية على المعلومات ، لا يأخذ بعين الاعتبار ما يحمله المستقبل من تطورها وتبدلها ، كما انه يجافي المنطق الذي يرفض تغيير الاحكام بشان ذات الموضوع ( محل الجريمة ) بتغير الوسيلة التقنية .

واخيرا ، وبالاستناد إلى ان النموذج القانوني لجريمة السرقة في قوانيني العقوبات العربية عموما ، يقوم على عناصر واضحة في دلالتها ، لا تقبل بسط دلالاتها على سرقة المعلومات والمعطيات ، متمثلة بالسلوك الاجرامي المادي – ( فعل ا لأخذ / الاختلاس ) ، ومحل الجريمة المادي ( مال منقول مملوك للغير ) ، وباقتصار مفهوم الحيازة على ما يحتاز ماديا لا معنويا ، خلافا لمفهوم الحيازة في الق وانين المدنية

## 8 . جرائم احتيال الكمبيوتر وأغراضها.

الغش او الاحتيال او النصب تعبيرات يجري استخدامها بمعان مترادفة وان كانت تتمايز في الحقيقة ان من الوجهة اللغوية او الدلالات الاصطلاحية ، ويستخدم قانون العقوبات الاردني تعبير الاحتيال اما القانون المصري ، فيستخدم تعبير النصب ، وكلا القانونين لم يوردا تعريفا للاحتيال او النصب، وانما اوردا الافعال المكونة للجريمة في كل منها .

ويعرف الغش عموما ، بأنه " الخداع الذي يعمد اليه شخص للحصول من الغير بدون حق على فائدة او مزية ، ويعرفه ( Jack Bologna) بأنه " خديعة معتمدة Intentional deception لاخر ترتكب عادة للحصول على منفعه اقتصادية او سياسية او اجتماعية غير مستحقة من الوجهة القانونية "[1]

أما غش الكمبيوتر / الحاسوب ، او كما يسميه البعض ، الاحتيال المعلوماتي او الاحتيال باستخدام الحاسوب ، فقد تباينت بشأنه التعريفات وتعددت ، واساس تباينها تحديد الافعال المنطوية تحت هذا الوصف ، فيعرفه الاستاذ الامريكي ( T.Squires) بأنه " اساءة استخدام نظام الحاسوب ينطوي على حيله او خدعه مضلله " كما عرفته احدى الدراسات المسحية التي اجريت في امريكيا ، بأنه " فعل او مجموعة من الافعال غير المشروعة والمتعمدة التي ترتكب بهدف الخداع او التحريف للحصول على شئ ذي قيمة ، ويكون نظام الحاسوب لازما لارتكابها او اخفائها "[2]

أما التعريف الذي يقره المجلس الاوروبي لغش الحاسوب ، فه و " تغيير او محو او كبت معطيات او بيانات او برامج الكمبيوتر او أي تدخل اخر في مجال انجاز او معالجة البيانات (من شأنه) التسبب في ضرر اقتصادي او فقد حيازة ملكية شخص اخر ، او بقصد الحصول على كسب اقتصادي غير مشروع له او لشخص اخر " [3] وفي معرض تحليله لهذا التعريف ، يشيراستاذنا كامل السعيد الى ان التعريف واسع النطاق " الى الحد الذي يستحل نطاقا واسعا من الانشطة بعضها لا يرتبط بالكمبيوتر " لكنه بنفس الوقت يحقق فائدة تتمثل " بتوجيه الانتباه الى الجانب الحاسم في الموضوع وهو التلاعب في البيانات بقصد الحصول على شكل من اشكال المصلحة المالية على حساب طرف اخرى " .

ولعل التعريف الذي وصفته لجنة تدقيق الحسابات بالمملكة المتحدة ، والذي ارتكزت عليه لجنة (اوديت) Audit commision البريطانية في دراساتها الاربعة بشأن غش الحاسوب يعطي دلالة دقيقة ومحددة لمفهوم غش الحاسوب ، فجاء في هذا التعريف أنه " كل سلوك احتيالي وخداعي مرتبط بالكمترة computerisation يهدف الشخص بواسطته الى كسب فائدة او

---

[1]. المرجع السابق ، ص 45 .

[2].المرجع السابق ، ص 46 .

[3] .د. السعيد ، ورقة العمل ، المرجع السابق ، ص 4 .

مصلحة مادية " [1]. ، وعليه ، فان " جرائم احتيال الحاسوب ، تنصب على معطيات الحاسوب المخزنة في النظام الممثلة لاموال او اصول او خدمات ، يهدف الجاني فيها الى تحقيق مكسب او مزيه ، وتتم بالتلاعب – وفق الدلالة التقنية الواسعة – بمعطيات الحاسوب المخزنة او نظام المعالجة الالية .

وصور احتيال الكمبيوتر عديدة بل وعصية في احيان كثيرة عن الحصر لتباينها من حيث وسائل الاعتداء التقني نفسه او تباينها من حيث البيانات محل الاعتداء ، ويمكن القول بايجاز انها كافة الوسائل التقنية للتوصل الى البيانات المالية او التي تتصل بحقوق مالية .

لقد كانت اكثر الوسائل التقنية رعبا فيما سبق من انشطة في بداية ظاهرة جرائم الكمبيوتر الوصول الى نظام احد المصارف عن بعد عبر الاتصال المباشر بشبكة البنك او عبر خطوط الهاتف التي تتيح مدخلا لشبكة نظام البنك (وما يتضمنه ذلك من استخدام كلمات الغير السرية ان كانت معلومة وتجاوز اجراءات الامن ، او تخمينها ان لم تكن كذلك ) ، فيقوم الجاني بالعبث بالبيانات المالية اما باجراء التحويلات او بتغيير البيانات لكسب حقوق او الخلاص من التزامات ، او بزرع البرامج التي تحول آليا بعض المبالغ الى حسابات خاصة به او بشركائه ، او لاخفاء عملية اختلاس حصلت او غير ذلك من انشطة واغراض الدخول هذه ، وجامع هذه الانشطة ان الجاني يقوم باعمال احتيالية موجهة لنظام الكمبيوتر فيجني المنافع المادية عن طريق العبث بالبيانات او البرامج او حتى عمليات النظام ذاته. اما في الوقت الحاضر ، فان احتيال الانترنت المتمثل باستغلال مواقع الانترنت لجني مبالغ الاخرين عبر مشاريع وهمية لمنتجات او خدمات او من خلال الوصول الى ارقام بطاقات ائتمان الزبائن سواء بجمعها عند تلقي الموقع الوهمي لها او التوسل للوصول اليها من مواقع اخرى ومن ثم استغلالها في عمليات شراء غير مشروعة او الوفاء بمبالغ مقابل خدمات للجاني ، وانشطة التلاعب بالاسهم المالية وادارة المحافظ الالكترونية ومزادات البضائع على الانترنت ، تمثل الانشطة الاكثر رعبا لانتشارها الواسع ولما تلحقه بمواقع الانترنت والشركات القائمة عليها من مخاطر كبيرة وخسائر فادحة.

[1] .المرجع السابق ، ص 4 . ومصطلح الكمترة ، يستخدمه استاذنا كامل السعيد ولم نجده لدى غيره من الفقه العربي لتعريب كلمة computerisation وقد اشرنا سابقا انه استخدم لدى تعريب مؤلف غاري بيتر المشار اليه فيما تقدم ، ويستخدم الدكتور هشام رستم بديلا عنه تعبير " التحسيب الالكتروني " ومع ان الشائع في الدراسات التقنية استخدام تعبير الحوسبة الا ان استخدام تعبير الكمترة يفضل هذه الاستخدامات لدلالته التقنية الواضحة.

ولو رجعنا الى الدراسات المبكرة حول هذه الظاهرة لوجدنا مثلا ان الدكتور كامل السعيد يورد صورتين او شكلين للتلاعب بالمعطيات ، أولهما محاولة تأمين منفعة نقدية مباشرة ، كتحويل مبلغ من حساب شخص الى حساب الفاعل في البنك وثانيهما تخلص الفاعل من الوفاء بدفعات مستحقة عليه ، ويمثل أستاذنا على الصورة الثانية بحالة استعمال الفاعل دون ترخيص كلمة السر العائدة لطرف ثالث للتوصل الى استعمال حر لقاعدة البيانات بواسطة أي فواتير Bills يتم ارسالها للطرف الثالث " [1] وكلتا الصورتان كما نلاحظ ، تتحقق فيهما المنفعة الاقتصادية للفاعل ، ومحلهما المعطيات المخزنة في الحاسوب المجسدة الأموال أو الأصول . فالهدف الرئيسي من التلاعب الذي تقوم به جريمة غش الحاسوب كما يقول د . هشام رستم " هو البيانات data (المعطيات) التي تمثل في نظم الحاسبات اموالا او اصولا او موجودات Assets " ورغم ان مختلف انواع المعطيات عرضة لجرائم غش الحاسوب ، الا ان هذه الجرائم تستهدف بشكل شائع ورئيسي حس ب تحديد الفقيه Ulrich Seiber ما يلي :- :

1 – البيانات الممثلة للمستحقات المالية والايداعات المصرفية وتقديرات الائتمان وحسابات ونتائج الميزانيات .

2 – حسابات المرتبات وأوامر الدفع وحساب التكلفة والنفقات وقوائم المبيعات وكشوف الاعانات الاجتماعية والضمان والتقاعد .

3 – انظمة التحويل الالكتروني للاموال والودائع المصرفية والبطاقات المالية بانواعها .

والجرائم التي تستهدف انظمة التحويل الالكتروني للاموال والودائع المصرفية ، تمثل باجماع الفقه اخطر جرائم غش الحاسوب ، ذلك ان الخسائر الكبيرة والهائلة الناتجة عن غش الحاسوب التي اشرنا لها سابقا ، تعد متواضعة مقا بل احتمالات الخسارة الناتجة عن التلاعب بانظمة التحويل الالكتروني للاموال والودائع المصرفية ، وهذا يرجع الى المبالغ الهائلة المتجسده في هذه البيانات التي يجري نقلها بوقت قياسي والى شيوع استخدام تقنيات النقل الالكتروني للاموال التي تهيء نشوء مجتمع التعامل دون نقود ، لا في النطاق الوطني بل وعلى المستوى الاقليمي والدولي ايضا ، وكذلك لاتساع النشاط الاجرامي في هذا الميدان لما يجنيه الجناة من كسب وفير وبسبب تحققه

1. المرجع السابق ، ص 4 .

ايضا في وقت قصير وتجاوزه الحدود الوطنية للدولة مما يشعر الجناة بالامان . وللتدليل الواقعي على مخاطر هذه الانشطة فانه في امريكا وحدها ، وعبر انظمة EFT كان يتم في مطلع التسعينات تداول معاملات مالية تقدر بنحو 900 بليون دولار يوميا ، وعلى مستوى البنوك فان بنكا واحدا مثل City Bank تعالج نظم حواسيبه معاملات ماليه تقدر بنحو 30 بليون دولار في اليوم الواحد لعملائه في مائة دولة .

اما عن الاساليب التقنية للتلاعب في معطيات الحاسوب الممثلة بذاتها للافعال المكونة للسلوك الاجرامي في جريمة غش الحاسوب فهي متعددة تبعا لتعدد الوسائل التقنية وتبعا لطبيعة المعطيات محل الاعتداء واكثر الفقه يعرض لها من واقع الحالات العملية ونتعرض لها تاليا بالذكر فقط :-

اولا : التلاعب في البيانات المدخلة Input Data

ثانيا : التلاعب في البرامج :

ثالثا : التلاعب في معطيات نظم الحواسيب عن بعد [1]

واما عن خصائص الاحتيال التقليدي من الوجهة القانونية فانها:- اولا :جريمة اموال . وثانيا ، تقوم على تغيير الحقيقة او تشويهها في ذهن المجني عليه . ولهذا يقترب الاحتيال من التزوير ، لكنه يتميز عن التزوير بانه وسيله للاعتداء على الملكية ، كما يتميز التزوير بطلب عناصر اخرى غير تغير الحقائق ، كوقوع التغير في سند او صك كتابي. ويقوم الركن المادي لجريمة الاحتيال – عموما – على فعل الخداع ( السلوك الاجرامي ) عبر واحد او اكثر من الصور التي يحددها القانون حصرا وعلى النتيجة الجرمية المترتبة عليه ، والمتمثلة بتسليم المجني عليه مالا الى المحتال . و علاقة السببية التي تربط السلوك بالنتيجة. ومن المسائل الهامة في مجال دراستنا هذه التاكيد على ان تحديد القانون للوسائل التي يقوم بها السلوك الاجرامي انما هو تحديد حصري .

ويشترط لقيام جريمة الاحتيال ان يكون موضوع الاحتيال مالا مملوكا للغير وان يتوفر لموضوع الاحتيال طبيعة مادية ، وعلة ذلك – كما يقول الدكتور محمود نجيب حسني – " ان النتيجة الجرمية في الاحتيال هي التسليم الذي يفترض مناولة من المجني عليه او من يمثله او يعمل لمصلحته الى المحتال او من يعينه " وتتحقق كذلك الجريمة اذا انصبت على الاسناد التي تتضمن تعهدا او ابراء

1 انظر بشان الحالات العملية المعروضة ، د. رستم ، المرجع السابق .

(وهذه الاسناد تحقق لها الصفة المادية صكوك ) اذا كانت بحيازة المجني عليه ، والتي تتصرف دلالتها في غير هذه الحالة الى الواقعة القانونية التي تنشا التعهد او تنهيه .

اما الركن المعنوي للاحتيال فيتخذ صورة القصد الجنائي ، ولا تقوم جريمة الاحتيال على نحو غير مقصود (بالخطا) ، وتتطلب جريمة الاحتيال - الى جانب القصد الناشيء عن علم الجاني بتوافر اركان الاحتيال واتجاه ارادته الى فعل الخداع وتسلم المال – قصدا خاصا يتمثل بنية الفاعل الاستيلاء على المال الذي تسلمه ، أي اتجاه نية الفاعل الى تملك المال الذي تسلمه .

في ضوء هذه المعالم الرئيسة بشان جريمة الاحتيال او النص ب او الغش في القانون الجنائي ، هل تعتمد القواعد والاحكام التي تحكم هذه الجريمة في قوانين العقوبات الى المدى الذي يتيح انطباقها على جرائم غش الحاسوب ؟

تتحدد قابلية انطباق نصوص القانون الجنائي التقليدية المنظمة لجريمة الاحتيال او النص ب على جريمة غش الحاسوب او الاحتيال باستخدام الكمبيوتر من خلال الاجابة على التساؤلات الرئيسة التالية :

1 -هل يعتد بالاحتيال الواقع على غير الشخص الطبيعي وتحديدا على الحاسوب بوصفة آلة ؟

2 -هل يعتبر تسليم الاموال عن طريق التحويل الاكتروني تسليما ماديا محققا للنتيجة الجرمية في جريمة الاحتيال ؟

3 –هل تعتبر الوسائل التقنية المكونة للسلوك في جريمة غش الحاسوب مما يدخل في مفهوم او دلالة الوسائل المعتبرة في القوانين الجنائية المكونة للسلوك الاجرامي في جريمة الاحتيال التقليدية؟

اما بالنسبة للتساؤل الاول ، فان سبب اثارته ان غالبية قوانين العقوبات تتطلب ان يقع الاحتيال على شخص طبيعي ، من قبيلها القانون الايطالي ( وتستخدم تعبير فرد) والقانون السويسري والالماني والدنماركي واليوناني والياباني والفرنسي - مشروع عام 1958- والمغربي والكويتي والقطري (وتستخدم تعبير الشخص) والاردني والفرنسي والمصري ( وتستخدم تعبير الغير ) ، فهل يمكن مد نطاق نصوص هذه القوانين وهي تستخدم هذه التعبيرات للانطباق على خداع الحاسوب او احتيال الكمبيوتر ؟

لا تسعفنا قوانين العقوبات العربية عموما للقول بامكان الانطباق ، اضافة الى عدم وجود احكام قضائية عربية – في حدود ما نعلم - تساهم في تبين اجابةعلى هذا التساؤل ، اما في الفقه والقضاء

المقارنين فان خلافا ظهر بشان المسالة بين مؤيد ومعارض للتسوية في الحكم بين خداع الانسان والالة .

يرى Ulrich Seiber ان قابلية نصوص الاحتيال للتطبيق على الغش الذي يباشر على انظمة الحواسيب ، تتوقف على شرط مؤداه ، ان يكون الجاني قد خدع ايضا الشخص الذي يقوم بفحص البيانات ، فاذا لم يقم بذلك فان النصوص لا تنطق . ويعارض القاضي Mjaeger – في معرض ايضاحه لاسباب الحكم الذي اصدره والقاضي بعدم انطباق المادة 496 من قانون عقوبات لوكسمبرغ الخاصة بالاحتيال او غش الحاسوب ، الحجة التي تقو ل بان الآلة انما يستحدثها انسان ، وان هذا الاخير هو الذي يكون قد خدع لان آلته لا تكون قد استعملت طبقا للتصور الاصلي الذي وضع لها .

اما في المملكة المتحدة فان القضاء الانجليزي في قضية R.V,Gld عام 1981 – التي يعرض لها ويحللها على نحو تفصيلي الدكتور كامل السعيد [1] قد اقام تسوية بين الالة والشخص في مسالة قبول السند المزور ، وسنتناول هذه القضية لدى بحثنا للتزوير . وخلافا لذلك حكم القضاء الانجليزي في قضية Moritzعام 1982 الخاصة بعائدات قيمة الضرائب الاضافية لاحدى الشركات ان الخداع يتطلب عقلا بشريا يمكن خداعه والتحايل عليه ، هذا على الرغم من ان الماده 15 من قانون السرقة الانجليزي لعام 1968 التي تجرم الحصول بالخديعة على مال بحوزة الغير بنية حرمانه منه بصفة مؤبده ، والماده الاولى من قانون السرقة لسنة 1978 التي تجرم الحصول بالخديعة على خدمة ، يمكن تفسيرها على نحو متسع يسمح بتطبيقها على خداع نظام معلوماتي او آله .

والواضح انه في ضوء تحديد النصوص لصفة من يقع عليه الاحتيال بانه شخص او فرد طبيعي فان محاولات مد نصوص القانون لتشمل غش الحاسوب او خداع الاله تقف امامه عوائق قانونية حاده في مقدمتها مبدا حظر القياس في القانون الجنائي الموضوعي ، ومبدا الشرعية الراسخ .

وبراينا ، فان المبادئ الراسخة في القانون الجنائي ، ومقتضيات تعزيز النظام القانوني لمجابهة هذه الجرائم الخطرة ، وحقيقة ان النصوص التقليدية – حتى في الاحوال التي امكن تفسيرها على نحو واسع – لم تنه الجدل ولا التباين في حل مسألة التسوية بين خداع الانسان وخداع الالة ، كل

**1**. د. السعيد ، ورقة العمل ، المرجع السابق ، ص 11 .

ذلك يعزز القول بعجز النصوص الجنائية عن الانطباق على هذه الجريمة المستحدثة .

اما عن التساؤل الثاني والخاص بمدى اعتبار التحويل الالكتروني للاموال من قبيل التسليم المحقق لنتيجة السلوك في جريمة الاحتيال ، فان التعارض بشأنه اتخذ مدى واسع . ونجد لدى الفقيه او الاستاذ الواحد اكثر من موقف تتباين فيما بينها .

فالدكتور هشام رستم ، بالاستناد الى تحليل اتجاهات الفقه المقارن ، يرى وجوب التمييز بين حالتين : اولهما : اذا كان محل الاستيلاء نقودا او اصولا كالتوصل الجاني الى معرفة الرقم السري لصاح ب بطاقة ائتمان مسروقة او معثور عليها ويستخدمها في سحب امواله من اجهزة الصرف الالي للنقود ، او كتلاعب الجاني في البيانات المدخلة او المخزنة في الحاسوب او برامجه كي يستخرج الحاسوب باسمه او باسم شركاه شيكات او فواتير بمبالغ غير مستحقة ليستولي عليها او يتقاسمها مع شركائه ، ففي هذه الحالات لا تثور مشكلة ، ويتحقق الاستيلاء او التسليم بالمعنى المقرر قانونا بجريمة الاحتيال التقليدية . اما الحالة الثانية ، فاذا كان محل جريمة الاحتيال النقود الكتابية او البنكية ( بيانات الارصدة في البنوك ) ، كأن يتم الاستيلاء عليها عن طريق القيد الكتابي ومثالها تلاعب الجاني في البيانات المخزنة في الحاسوب او في برامجه كي يحول كل او بعض ارصدة الغير او فوائدها الى حسابه ، ففي هذه الحالة يجد الدكتور هشام رستم ان الحكم بشأن تحقق نتيجة الجريمة باستلام المال والاستيلاء عليه مرهون بنطاق النص القانوني ، ففي قوانين كل من المانيا واليابان لا تصلح النقود البنكية (بيانات النقود ) محلا للاعتداء بالمعنى المقرر لمحل جرائم الاحتيال والسرقة . في حين انها – كما يذكر الدكتور هشام – تصلح في دول اخرى مثل كندا وهولندا وسويسرا وانكلترا ومعظم الولايات الامريكية ، وكذلك النمسا ، حيث قضت المحكمة العليا في الاخيرة بأن تعبير المال الوارد بالمادتين 133 عقوبات ( الخاص بخيانة الامانة ) و 134 عقوبات ( الخاصة بالاحتيال ) يشمل النقود الكتابية .

ويلخص الدكتور هشام رستم ، الا انه وبالاستناد الى اعتبار التسليم غير متطلب له المناولة المادية حسب ما هو مستقر في الفقه المصري والفقه الفرنسي ، ولان محكمة النقض قد توصلت في العديد من احكامها الى ان " الدفع التي يتم عن طريق القيد الكتابي يعادل تسليم النقود ، وسندالوجود اتجاه فقهي فرنسي يرى امكان تطبيق نص المادة 405 عقوبات من قانون العقوبات الفرنسي الخاصة بالاحتيال و( المطابقة للنص المصري تقريبا ) على بعض صور جرائم غش الحاسوب واعتبار نتيجة الجريمة متحققة (والاستيلاء عن طريق تحويلات الكترونية تجري بين الحسابات ، فان اعتبار التسليم

في جريمة غش الحاسوب متحققا لا يتعارض مع القانون المصري (الموافق لجميع القوانين العربية تقريبا) لان التسليم في جريمة النصب " يحققه وضع الشيء تحت تصرف الجاني بحيث يتمكن من حيازته بغير عائق ولو لم يستول عليه استيلاء ماديا " [1]

اما الدكتور جميل عبد الباقي [2] ، فانه يرى ان التسليم المادي يتحقق بالنسبة للجرائم الناشئة عن استخدام الحاسب الآلي كاداة ايجابية (وتشمل عنده التدخل في المعطيات بإدخال معطيات وهمية ،او مزورة باستبدالها او محوها او التدخل في البرامج بتحويلها او التلاعب بها او تغيير برامج النظام بكافة صورة) وكذلك الجرائم الناشئة عن الاستخدام التعسفي لبطاقات الائتمان بجميع انواعها ، ففي هذه الجرائم يرى ان التسليم المادي يتحقق .ويدعم رايه بان محكمة النقض الفرنسية لم تشترط ان يكون هناك تسليم مادي لقيام النصب ، واكتفت بما يعادل التسليم ، وبان محكمة النقض الفرنسية اعتبرت ان الدفع الذي يتم عن طريق القيد الكتابي يعادل تسليم الاموال ماديا . وفي معرض عرضه للاتجاهات الفقه بشان مدى انطباق ما قررته محكمة النقض على جرائم الحاسوب . يذكر الدكتور جميل عبد الباقي ان البعض يرى امكان ذلك في حالات التدخل في البرمجة او المعطيات المقدمة للحاسوب التي تؤدي الى الغاء رصيد مدين واستنادا الى ان تحويل الاموال ايا كانت وسيلة التقنية قد تم بالقيد الكتابي بدون تسليم الاموال نقدا للجاني ، ويذهب الى تاييد هذا الراي واعتبار تحويل الاموال بالقيد الكتابي ملم يدخل في مفهوم الجريمة الواردة في المادة 405 من قانون العقوبات الفرنسي ،

اما بشان الابراء ، فان القضاء الفرنسي قد حكم بتطبيق عقوبة النصب(الاحتيال)على احد الاشخاص لقيامه بادخال سيارته الى ساحة انتظار السيارات ولكنه بدلا من وضع النقود الأصلية المطلوبة في عداد الموقف وضع نقودا عديمة القيمة ، وحكم بذلك بتطبيق عقوبة النصب على الشخص الذي وضع قطعة معدنية عديمة القيمة داخل جهاز التلفون [3]، وتأسس الحكم في هاتين الجريمتين على ان الجاني في كل منهما ، وان كان لم يتسلم شيئا ماديا ، الا انه استطاع بتحايله ان

---

1 . د. رستم ، المرجع السابق ، ص84.

2 .د. الصغير ، المرجع السابق ، ص 119 وما بعدها

3 . المرجع السابق ، ص 119 .

يتخلص من المبلغ الذي كان يجب عليه دفعه ، وقد اتجه جانب من الفقه الى مد نطاق هذه الاحكام الى بعض صور السلوك في جريمة غش الحاسوب . الا ان الدكتور جميل عبد الباقي لا يتفق مع هذا الاتجاه ولايرى انطباق حكم محكمة النق ض على صورتي الاستخدام التعسفي لجهاز الحاسوب او الاستيلاء على البيانات اثناء نقلها لان الشخص لم يتسلم أي شيء مادي ، كما انه لم يحصل على اعفاء من الدفع او ابراء من الوفاء .

ونجد البعض ، دون بذل محاولة تحليل جريمة غش الحاسوب المستحدثة ، يتخذ حكما مطلقا بامكان تطبيق نصوص جريمة الاحتيال التقليدية بكافة اركانها وشروطها على جريمة غش الحاسوب ، لان الطبيعة التقنية لجرائم الحاسوب حسب هذا الرأي – لا تضيف جديدا في مجال الاحتيال التقليدي الا المجرد الوسيلة المستخدمة[1].

اما التساؤل الثالث ، بشأن مدى شمول دلالات الوسائل الاحتيالية التي يقوم بها السلوك في جريمة الاحتيال التقليدية ، لاساليب التلاعب في المعطيات المكونة للسلوك الاجرامي لغش الحاسوب ، فقد كان محل نقاش وتعارض في الفقه الفرنسي واتيح للقضاء الفرنسي اصدار قرارات بشأنه .

يذكر الدكتور هشام رستم في هذا الصدد ان ما يظهر من اتجاهات الفقه الفرنسي بشأن هذه المسألة ان غش وخداع انظمة الحاسبات لسلب المال ، تتحقق به الطرق الاحتيالية بمفهومها المستقر (التقليدي ) ككذب تدعمه اعمال مادية ووقائع خارجية ، حيث يتوافر فيه ، بجانب الكذب ، واقعة خارجية تؤيده هي ابراز او تقديم المستندات او المعلومات المدخلة الى الحاس وب ، ويؤيد الدكتور هاشم هذا الاتجاه بالاستناد الى ان جانبا من الفقه المصري قد وصف غش العداءات والاجهزة الحاسبة ، بأنه نوع من تجسيد الكذب الذي تتحقق به الطرق الاحتيالية . ويدلل على ذلك برأي الاستاذين الفاضلين ، احمد فتحي سرور ومحمود نجيب حسني .

والحقيقة ان الاستشهاد براي هذا الفقه – براينا – ليس صائبا ، فان كان الاستاذ الفاضل محمود نجيب حسني ، قد قرر ان من يستعين بعداد او ساعة لاظهار ان الاستهلا ك يزيد على الحقيقة ويطالب بناء على ذلك بمبالغ لا حق له فيها ، فان ذلك يقع في نطاق الخداع الذي يستعين الفاعل لتحقيقه بظروف خارجية من ضمنها الاستعانة بشئ ذي كيان مادي. هذا من جهة ، ومن جهة اخرى ، فان الفقيه المذكور في معرض بيانه شرط توافر الصفة المادية لموضوع الاحتيال ، يعتبر

1. د. قشقوش ، السابق ، ص 152 .

الكهرباء مثلا ، ذات كيان مادي ، اضافة الى ان القضاء المصري استقر على انزال القوة المحرزة منزلة الاشياء المنقولة ، عوضا عن ان هذا التفسير مؤسس على ان فعل الاحتيال قد وقع على من قدمت له المستندات ، في حين ان الفعل قد وقع حقيقة على نظام الحاسوب .

ويرى كذلك الدكتور هشام رستم ، ويشاطره الرأي جانب من الفقه [1]، بالاستناد الى ما تقرر لدى جانب من الفقه الفرنسي وبعض احكام القضاء ، ان الطرق الاحتيالية ( بالمفوم التقليدي متحققة باستخدام الجاني المستندات غير الصحيحة التي يخرجها الحاسوب بناء على ما وقع في برامجه او البيانات المخزنة داخله من تلاعب كي يستولى على اموال لا حق له فيها [2].

ومع الاقرار بأن المستندات المخرجة من الحاسوب ، اذا ما استعان بها الجاني في ارتكاب فعل الخداع ، تقوم بها جريمة الاحتيال ، فان هذا الاقرار يؤسس على ان الجاني استخدم مستندات ذات طبيعة مادية شأنها شأن كافة المحررات والصكوك التي يمكن استخدامها في فعل الاحتيال ، لكن ، اغفال عملية التلاعب بالبيانات التي يظهرها المستند المستخرج داخل نظام الحاسوب ، انما هو انكار لجريمة تامة حدثت وتحققت ، وما الاستعانة بالمستند الا من قبل استخدام مستند مزور ، اذا ما اكتملت عناصر اخرى ، تنشأ به جريمة استخدام مزور.

ويعترض جانب من الفقه على ادخال وسائل غش الحاسوب في نطاق الطرق الاحتيالية التقليدية ، استنادا الى ان الادعاءات الكاذبة وفق ما بينته الاحكام الفرنسية ، تنطوي بالضرورة على علاقة مباشرة بين شخصين (المحتال والمخدوع) وهو ما ينتفي في حالة مباشرة الطرق الاحتيالية في مواجهة آلة ، مثل الحاسوب ، ويرى بعض الفقه المعارض بالمقابل بأن خداع الالة ممكن تقبله على اساس انه يوجد خلف الالة انسان . وقد تضاربت احكام القضاء المقارن بشأن هذه المسألة ، خاصة في فرنسا ، ولا يتسع المقام لتناولها ، غير ان المشرع الفرنسي حسم هذا التعارض – من بعض النواحي – لاصداره قانونا خاسا ببعض جرائم الحاسوب (قانون 1988 المعدل 1994).

وما اصدار غالبية الدول – خاصة تلك التي تزداد فيها جرائم الحاسوب على نحو ملحوظ – لقوانين خاصة او تعديل قوانينها لتجريم احتيال الكمبيوتر ، الا تأكيد على ادراك الطبيعة الخاصة لهذه الجرائم ، وتحديدا محل الاعتداء ، وخصائصها المميزة ، وهذا بدوره يمثل دلالة قوية ، وان

1. د. قشقوش ، السابق ، ص 28.
2. د. رستم ، السابق ، ص 270.

كانت غير مطلقة ، على عدم صواب الاتجاهات المتحمسة لمد نطاق النصوص الجنائية التقليدية على جرائم الحاسوب ، خاصة اذا كان البعض من اصحاب هذه الاتجاهات لا يرى ان هذه الجرائم تضيف جديدا على كثير من النصوص التقليدية الا من حيث وسيلة الجريمة .

## 9. جرائم التزوير المعلوماتي [1]

التزوير forgery بشكل عام ، " هو تغيير الحقيقة ايا كانت وسيلته وايا كان موضوعه " [2] وهو يتسع للعديد من الجرائم التي نصت عليها قوانين العقوبات . اما التزوير في المحررات ، فهو حسب تعريفه المستقر في الفقه ين الفرنسي والمصري " تغيير الحقيقة في محرر باحدى الطرق التي نص عليها القانون ، تغييرا من شأنه احداث ضرر مقترن بنية استعمال المحرر المزور فيما اعد له" [3]. وقد عرف قانون العقوبات الاردني التزوير بأنه " تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد اثباتها بصك او مخطوط يحتج بهما نجم او يمكن ان ينجم عنه ضرر مادي او اجتماعي" (مادة 260) وبالرجوع الى قوانين العقوبات العربية ، نجدها في معرض تجريم التزوير عموما ، وتزوير المحررات على وجه الخصوص قد نصت على تجرم العديد من الصور ، فقد نص قانون العقوبات الاردني – على سبيل المثال – على هذه الجرائم في الفصل الثاني من الباب الخامس تحت عنوان الجرائم المخلة بالثقة العامة ( المواد 260 – 272 ) ، وساوى في العقوبة بين مرتكب التزوير ومستعمل المحرر المزور . وكذلك فان قانون العقوبات المصري نظم جرائم التزوير في الباب السادس عشر من الكتاب الثاني تحت عنوان التزوير (المواد 206 – 227 ) . ويهمنا في هذا المقام الاشارة الى ان المشرع المصري قد جرم استعمال المحررات المزورة ، لكنه نهج نهجا مختلفا عن المشرع الاردني بشأن العقوبات ، اذ تتعدد العقوبات فيما بين جرائم تزوير المحررات تبعا لنوع المحرر محل التزوير ، وتتباين عن عقوبات جرائم استعمال المحررات كما انها تتباين في الطائفة الاخيرة.

وتتشابه جرائم التزوير مع جرائم الاحتيال من حيث قيامهما على تغيير الحقيقة ، غير انهما تختلفان

---

1 . انظر في تفصيل ذلك ، د. حسني ، القسم الخاص ، المرجع السابق ،وكذلك المستشار مصطفى مجدي هرجه، التعليق على قانون العقوبات في ضوء الفقه والقضاء، الطبعة الثانية، مطابع روز اليوسف، جمهورية مصر العربية، 1992.

2 . د. حسني ، القسم الخاص ، المرجع السابق ، ص 192

3 . السابق ، ص 215 .

من زوايا متعددة ، اهمها ان جريمة تزوير المحررات لا بد ان تقع على محرر، ولا يشترط ذلك في جريمة الاحتيال . وغالبا ما تجتمع جريمتا التزوير والاحتيال ، ونكون بذلك امام حالة التعدد المادي للجرائم.

وتقوم جريمة التزوير على ركنين ، مادي ومعنوي ، وان كان جانب من الفقه [1] يجعل من بعض عناصر الركن المادي ، كالضرر ، ركنا مستقلا بذاته . اما الركن المادي فيقوم على ثلاثة عناصر :- تغيير الحقيقة ، وان يكون التغيير قد تم باحدى الطرق المحددة حصرا في القانون ، واخيرا ، ان يترتب على تغيير الحقيقة ضرر . وهذا العنصر الاخير هو ما ثار بشأه الخلاف حول موقعه ، الا ان السائد في الفقه اعتباره عنصرا من عناصر الركن المادي ، وتغيير الحقيقة يمثل السلوك الاجرامي الذي يقوم به التزوير فاذا انتفى انتفت الجريمة . ولا يشترط ان يكون التغير كليا ، أي ابدال كل البيانات بما يخالف الحقيقة ، ويكفي ان يكون تغيير الحقيقة جزئيا او نسبيا ، والمستقر في الفقه ان المقصود في التزوير ، ليس تغيير الحقيقة الواقعية المطلقة ، وانما تغيير الحقيقة النسبية .

وتغيير الحقيقة وح دهـ ، غير كاف في القانون ، وانما يلزم ان يتم باحدى الطرق المحددة حصرا في القانون ، والتي تقسم عموما الى طرق مادية تنال مادة المحرر وشكله ، وطرق معنوية ، تنال مضمون المحرر او ظروفه او ملابساته دون المساس بمادته او شكله ، ويكتمل الركن المادي بتحقق الضرر الناتج عن تغيير الحقيقة ، والضرر كما يعرفه الفقيه محمود نجيب حسني ، " اهدار حق واخلال لمصلحة مشروعة يعترف بها القانون ويكفل لها حمايته"[2] وبانتفاء الضرر ينتفي التزوير ، وللضرر انواع متعددة ، قد يكون ماديا او معنويا او ضررا احتماليا او ضررا اجتماعيا.

وموضوع جريمة التزوير ومحلها ، المحرر ، ولا وجود للتزوير اذا لم ينصب على تغيير الحقيقة في محرر ، ويعرف المحرر بانه " مجموعة من العلامات والرموز تعبر اصطلاحا عن مجموعة مترابطة من الافكار والمعاني الصادرة عن شخص او اشخاص معينين " [3] وهو في جوهر هـ كتابة مركبة من حروف وعلامات تعبر عن معنى او فكرة معينة ، وحسب الاتجاه التشريعي والفقهي الراجح ،

---

[1]. انظر في تفصيل هذه الاتجاهات د. حسني ، السابق ، ص 193 وما بعدها .

[2]. السابق ، ص 251 .

[3]. المرجع السابق ، ص 247 .

يفترض امكان ادراك مادة المحرر بالقراءة البصرية[1] وان ينتقل معنى الرموز والعلامات عن طريق المطالعة والنظر ، ومن المسائل الهامة المفترض الاشارة اليها ، والمتصل بموضوع وهدف دراستنا ، ان الفقه متفق على ان فكرة المحرر ، تفترض امكان استشفاف دلالة رموز المحرر بالنظر اليها ، ولذلك – وكما يقول الاستاذ محمود نجيب حسنى – لا يعتبر من قبيل المحررات ، الاسطوانة او شريط التسجيل الذي سجلت عليه عبارات ايا كانت اهميتها القانونية ، وكذلك ما يدخل على الصوت الذي يحمله من تشويه [2] .

والعنصر الاخر الهام من عناصر المحرر محل التزوير ، اضافة الى اتصاف علاماته ورموزه بثبات نسبي ، هو ان فكرة المحرر ، توجب ان يكشف عن شخصية محرر ه، وهذا العنصر مما يتصل بالوظيفة الاجتماعية للمحرر ، والمستقر فقها ان يكون المحرر معبرا عن فكرة بشرية . ولعل العناصر التكوينية لمحل جريمة التزوير التقليدية – المحرر – هي العامل الحاسم في منع انطباق نصوص جريمة التزوير على تزوير معطيات الحاسوب كما سنرى .

أما الركن المعنوي لجريمة التزوير ، فيتخذ صورة القصد الجنائي . ولا يكفي فيه القصد العام الذي يقوم على علم المتهم بأركان الجريمة ، واتجاه ارادته الى الفعل المكون لها وتحقيق نتيجته ، بل تتطلب هذه الجريمة توافر قصد جنائي خاص ، يتمثل بنية استعمال المحرر المزور فيما زور من اجله وعلى هذا فان القصد الجنائي في جريمة التزوير يعرف على نحو غالب لدى الفقه والقضاء بانه " تعمد تغيير الحقيقة في محرر تغييرا من شانه ان يسبب ضررا وبنية استعمال المحرر فيما غيرت من اجله الحقيقة " [3].

هذا عرض موجز ومكثف لماهية واركان جريمة التزوير ، ويثور السؤال ،

هل يمكن تطبيق نصوص القانون الجنائي على انشطة تزوير معطيات الكمبيوتر ؟.

بالرغم من ان غالبية الدول حسمت موقفها لجهة عدم انطباق نصوص التزوير على تزوير المعطيات واتخذت تدابير تشريعية لتجريم تزوير المعطيات وتوفير اداة قانونية لمكافحتها الا ان ثمة دول لم تنح هذا المنحى ولا يزال النقاش القديم الجديد بشان مسألة انطباق نصوص تجريم التزوير في المحررات

---

1. د. رستم ، السابق ، ص 326 .
2. د. حسني ، السابق ، ص 247 .
3. السابق ، ص 271

على تزوير البيانات المخزنة في نظام الحاسوب قائما ، وهذا الجدل يتجاذبه رايان ، احدهما – وهو الرأي الراجح بفعل تبنيه من قطاع واسع من الفقه ، والمعزز ايضا ببعض بـاحكام قضائية ، و بفعل تبنيه في التشريعات الجنائية الحديثة في القانون المقارن – يقوم على ان التزوير في معطيات الحاسوب ، لا يدخل تحت نطاق النصوص التقليدية . اما الرأي الثاني ، فيرى امكان تطبيق النصوص الجنائية المنظمة لجريمة التزوير التقليدية على جرائم تزوير الكمبيوتر . وليس المقام عرض وتقدير هذين الاتجاهين – وهو ما قمنا به تفصيلا في مؤلفاتنا المشار اليها في هذه الورقة – ونكتفي في هذا المقام ببيان خلاصة تقدير هذه الاتجاهات وفق ما سبق لنا التوصل اليه في دراستنا .

اننا وبالاستناد الى :-

انعدام وجود العناصر الرئيسة لمحل جريمة التزوير التقليدية (المحرر) في معطيات الحاسوب وتحديدا ،عنصر الكتابة المادية ، وعنصر ادراك مضمون المحرر بالنظر ، وعنصر التعبير عن الفكرة البشرية وعلاقة الشخص بالمحرر .

وسندا الى تاييد غالبية الفقه القانوني من مختلف النظم عدم انطباق نصوص تجريم التزوير التقليدية على تزوير معطيات الحاسوب. وتعزز وتايد هذا الاتجاه بـاحكام قضائية في فرنسا وامريكا وبريطانيا وغيرها من النظم المقارنة .

وسندا لتدخل مشرعي العديد من الدول للنص على هذه الجرائم المستحدثة من جرائم التزوير اما بنصوص خاصة او بتعديل النصوص التقليدية للتزوير ،كما هو الشان في كندا حيث عدل تعريف الوثيقة document في قانون العقوبات عام 1985 ليشمل بالاضافة الى الورق أي مادة material يتم عليها تسجيل او حفظ أي شيء يمكن قراءته او فهمه من قبل الانسان او نظام الحاسوب او أي جهاز اخر ، وكذلك في استراليا حيث اضيفت المادة 276عام 1983 لقانون العقوبات ونصت صراحة على معاقبة "كل من حرف او زور أو محا أو اتلف بطريقة غير مشروعة وبقصد الغش ، اية مادة لمعالجة البيانات ، وكذلك جرمت استخراج او انتاج معلومات غير صحيحة عن طريق المعالجة الالية واستخدامها او التصرف فيها على انها صحيحة اضرارا بالغير او بقصد حمل او اقناع الشخص للقيام بفعل على اساس انها صحيحة" وكذلك في المانيا ، حيث تضمن القانون الثاني لمكافحة الجريمة الاقتصادية لعام 1986 نصا في المادة (269) يقضي بتوقيع عقوبة الحبس لمدة لا تزيد على خمس سنوات او الغرامة على كل من يقوم بقصد الخداع في تعامل قانوني ، بـتخزين

او تغيير بيانات اذا ما استنسخت بهذا الشكل انتجت مستندا غير اصلي او مزور وكذا كل من يستخدم هذه البيانات المخزنة او المحرفة " وكذلك في فرنسا ،حيث جرم المشرع الفرنسي في الفقرتين (6،5) من من المادة 462 من قانون 1988 المشار اليه سابقا ، تزوير المستندات المعالجة اليا او استخدام هذه المستندات.

فان نصوص التجريم التقليدية المنظمة لجرائم التزوير ،غير قابلة للانطباق على جرائم تزوير معطيات الحاسوب بدلالتها الواسعة ، مما يستدعي تدخلا تشريعيا في البيئة العربية لمواجهة هذه الجرائم ، صيانة لاسس ومباديء النظام القانوني وكفالة للحقوق التي تهددها – على نحو جدي وخطر– هذه الانشطة الجرمية المستجدة .

## 10– جرائم تدمير المعطيات باستعمال الفيروسات والديدان والقنابل المنطقية و الموقوتة.

تناول المؤتمر العلمي الأول، الذي تعقده أكاديمية شرطة دبي، حول موضوع "الجوانب القانونية والأمنية للعمليات الإلكترونية –خلال الفترة من 26-28 إبريل 2003، ثلاثة محاور تدور جميعها – في كلياتها وجزئياتها حول الجوانب القانونية والأمنية والإدارية للعمليات الإلكترونية.

وقد أثار الباحث تناول موضوع إدارة الأزمات في مجال العمليات الإلكترونية دراسة تطبيقية على كارثة فيروسات الكمبيوتر والجرائم المتعلقة بالإنترنت باعتبارها، وبحق تشكل ظاهرة إذ بدأت كثير من الدول تعاني منها، ولقد تنوعت سبل المواجهة سواء تشريعية أو أمنية، بالنظر إلى آثارها وتداعياتها الخطيرة على الاقتصاد القومي.

ننطلق بداءة من الاشارة الى ان الاتلاف في نطاق جرائم الحاسوب وفقا لمحددات هذه الجرائم التي درسناها فيما تقدم هو الاتلاف الذي ينصب على معطيات الحاسوب من بيانات ومعلومات وبرامج ، ونعيد التاكيد هنا ان الاتلاف المنصب على الكيانات المادية للحاسوب– شانه شان سائر الجرائم الواقعة على هذه الكيانات كالسرقة وخيانة الامانة ، لا يعيق انطباق نصوص القوانين التقليدية عليه عائق .

فمن هنا يمكن القول أن فيروس الكمبيوتر هو مرض يصيب الجهاز. وهو عبارة عن برنامج صغير يمكن تسجيله أو زرعه على الاسطوانات المرنة أو الأقراص الصلبة الخاصة بالحاسب. ويظل هذا

الفيروس خاملاً خلال فترة محدودة ثم ينشط فجأة في توقيت معين ليدمر البرامج والمعلومات المسجلة في الحاسب، الأمر الذي يؤدي إلى إتلاف المعلومات أو حذفها أو تدوينه . ومن المعروف أن فيروسات الكمبيوتر هي برمجيات من صنع وتصميم البرمجيين .

وليست فيروسات بيولوجية. ومن المعروف أيضاً أن العديد من فيروسات الكمبيوتر (مثل الفيروسات البيولوجية) منها الخبيث الذي يسبب أضراراً ومنها الحميد الذي لا يسبب مشكلات بالنسبة لمستخدمي الإنترنت.

وتعد فيروسات الكمبيوتر أخطر العناصر التي تهدد أمن البرامج والبيانات، لأنها تؤدي إلى فقد النظام أو فقد تكامله أو تؤثر على كفاءة أدائه، كما تؤدي إلى إتلاف البرامج وضياع المعلومات. وتزداد الخطورة نتيجة أن هذا الفيروس ينتشر بسرعة بسبب اتساع نطاق تبادل المعلومات ووسائل الاتصال بين الحاسبات ولو كانت في أماكن مختلفة ومتباعدة. كما يلعب التوافق بين النظم والأجهزة وبالتالي لقرصنة البرامج دوراً في نقل هذه الفيروسات[1]

وسائل انتقال العدوى: ينتقل فيروس الكمبيوتر من خلال استخدام برامج غير أصلية ذلك أن احتمال وضع أحد المستخدمين للفيروس في أحد البرامج المنسوخة هو أمر قائم وينتقل الفيروس كذلك عن طريق البريد الإلكتروني وشبكات الاتصال.

كما أن بعض العاملين على الأجهزة قد يقومون بإدخال الفيروس إلى النظام حتى يتسبب في إنهياره، وذلك من أجل الانتقام من الإدارة صاحبة المشروع. والإرهاب أيضاً يستخدم التكنولوجيا في تنفيذ العمليات الإرهابية، عن طريق إدخال الفيروس إلى نظم معلومات الدول المعادية، كما أن الشركات الكبيرة أصبحت تستخدم الفيروس كوسيلة للتغلب على الشركات المنافسة. وقد ينتقل من خلال نقل الأجهزة.

**1**.راجع د. حسام الدين الأهواني – الدكتور جميل عبد الباقي الصغير، مرجع سابق، ص 197.

أعراض الإصابة بالفيروس :

تتمثل هذه الأعراض فيما يلي[1]:

بطء تشغيل الجهاز.

- ✓ توقف النظام عن العمل.
- ✓ نقص شديد في سعة الذاكرة المؤقتة.
- ✓ ظهور حروف غريبة عند الضغط على مفاتيح معينة.
- ✓ تغيير في حجم الملفات وعددها.
- ✓ عرض رسالة خطأ فجائية وغير عادية.
- ✓ تشغيل القرص أكثر من المعتاد.
- ✓ سماع صوت صفارة: مع ظهرو رسومات على الشاشة مصحوبة بتوقف الجهاز.

الأضرار التي يسببها الفيروس:

تسبب بعض الفيروسات الخبيثة[2]

تدمير شبكات الاتصالات والحاسبات.

- إتلاف بعض أجزاء من الدوائر المتكاملة وتدميرها تماماً.
- تقليل سرعة وكفاءة عمل وحدة التشغيل المرئية المعروفة بإسم الميكروبروسيسور.
- تقليل سرعة عمل وحدات الطباعة والأقراص المرنة والصلبة .
- إتلاف البيانات المسجلة على قواعد البيانات (بتغيير في بعض البيانات – حذف بعض البيانات – تبديل بعض السجلات)
- إدخال بيانات مضللة أو بيانات رسمية وغير موجودة أصلاً في السجلات الأساسية.

---

1. المرجع الاسبق، ص 203

2. تفصيل ذلك ، د. حسني ، القسم الخاص ، المرجع السابق ،وكذلك المستشار مصطفى مجدي هرجه، التعليق على قانون العقوبات في ضوء الفقه والقضاء، الطبعة الثانية، مطابع روز اليوسف، جمهورية مصر العربية، 1992.

- أما بالنسبة للأنواع الحميدة والتي لا تسبب أضراراً فهي برمجيات تعطي نوعاً من الدعابة والفكاهة
- للمستخدم مثل ظهور عبارات مسلية على الشاشة من وقت لآخر – عزف قطعة موسيقية هادئة – ظهور بعض الرسومات مثل الأزهار وشجرة الكريسماس – ظهور صور لبعض المعالم الأثرية الشهيرة ومشاهير الفنانين ولاعبي كرة القدم.[1]

وتنصب اساليب الاتلاف التقنية في ميدان نظم الحواسيب على المعطيات بدلالتها الواسعة ،البيانات والمعلومات المخزنة في نظم الحواسيب المختلفة والبرامج وكذلك المعطيات المتبادلة بين شبكات الحوائيب وعبر شبكات المعلومات ، وينتج عن هذه الاساليب اما محو كلي للمعطيات او تشويه من شانه اتلاف اجزاء منها ، يمنع امكان استخدام النظام على نحو طبيعي بفعل غياب تكامل عناصر ومعطيات النظام المتطلبة اصلا لسلامة عمله.

- وتتخذ اساليب اتلاف المعطيات عموما احد صورتين يندرج في نطاقهما العديد من الوسائل التقنية، اولهما،محو او تشويه البيانات المخزنه في نظم الحواسيب من خلال التوصل غير المرخص به مع النظام ، وقد تناولنا الوسائل التقنية وانشطة التوصل غير المرخص به مع نظام الحاسوب وخاصة الاعتماد على وسائل الاتصال والتشويه ، ولا نكرر ما ذكرناه في هذا المقام ، ونكتفي بالقول ان انشطة التوصل ومن ثم العمل مباشرة على اتلاف المعطيات ، اقل خطورة من وسيلة التدمير بواسطة الفيروسات التي تنصب بشكل رئيس على البرامج التطبيقية والبيانات المخزنة في الملفات .
- اما الوسيلة الثانية والذي ارتبط بها مفهوم ودلالة اتلاف معطيات الحاسوب ، فهي وسيلة

---

**1.** راجع د. عبد البديع محمد سالم، مرجع سابق، ص 686.

نشر البرامج الخبيثة والضارة ، واشهرها الفيروسات ، ولعل هذه الوسيلة هي من اكثر ما يتردد الحديث بشانها متصلا بجرائم الحاسوب ، ومن اكثر الظواهر معالجة على مستوى الدراسات التقنية القانونية ، كما انها المادة الغنية للاخبار المعلوماتية وتقارير امن المعلومات التي تنشر في مختلف وسائل الاعلام وفي مقدمتها الانترنت .

- وبرامج الفيروسات خضعت ولما تزل لتفسيرات متباينة في اطار الدراسات التقنية وتعددت الاتجاهات – العصية عن التقصي – بشان اثر برامج الفيروسات من حيث نطاق الاتلاف الذي تلحقه والمناطق التي تصيبها هذه البرامج في نظم الحواسيب وانواعها ، والكثير الكثير من المسائل المتصلة بها ، وهذا كله يرجع في الحقيقة الى التطور الهائل والسريع في تقنيات برمجة الفيروسات ، ولا ادل على مدى

–

هذا التغير من اتجاه عشرات الدراسات الى الحديث عن فيروسات تقليدية وفيروسات مستحدثة ، رغم ان هذه الظاهرة لم تبرز للعيان الا في الثمانيات بشكل ملحوظ .

وتقوم جريمة اتلاف الاموال المنقولة وغير المنقولة في القانون الجنائي ، شانها شان سائر الجرائم، على ركنين:- الركن المادي المتمثل بفعل الاتلاف والذي يتخذ صورا عديده حسب النص القانوني ، ففي القانون المصري (م ادة 361 ع‌قوبات) يقوم الفعل بتخريب المال او اتلافه او جعله غير صالح للاستعمال او تعطيله ، وينصب السلوك الاجرامي على الاموال المنقولة وكذلك الاموال غير المنقولة المملوكة للغير . والركن الثاني للجريمة هو الركن المعنوي ، ويتخذ صورة القصد الجنائي العام بعنصرية العلم والادارة وقد قضت محكمة النقض المصرية [1] "بان القصد الجنائي يتحقق في جريمة الاتلاف متى تعمد الجاني ارتكاب الفعل المنهي عنه بالصورة التي حددها القانون واتجهت ارادته الى احداث الاتلاف او التخريب وعلمه بانه يحدثه بغير حق" .

وجريمة الاتلاف من الجرائم المادية التي تتطلب تحقق نتيجة تتمثل باتلاف المال باحدى الصور مما يحلق اضرارا بالغير ، وهي جريمة وقتية ، وما يعنينا في مقام الدراسة التاكيد على ان النصوص التقليدية لجريمة الاتلاف تنظم افعال الاتلاف المنصبة على الاموال ذات الطبيعة المادية منقولة كانت

1. مشار الى هذا القرار في مؤلف د. رستم ، السابق ، ص 321.

ام غير منقولة ، فقانون الضرر الجنائي الانجليزي على سبيل المثال الصادر عام 1971 يعرف كلمة الاموال المعتبرة محلا لجريمة تخريب والحاق الضرر التي نص عليها في المادة ( 1/1) بانها "الاموال ذات الطبيعة الملموسة – المادية nature tangible سواء كانت اموالا عقارية ام شخصية " وبالتالي فان الاتلاف يكون ذا طبيعة مادية لان المشرع لا يحمي بتجريمه افعال التخريب والتعييب والاتلاف حق الملكية بوصفه حقا عينيا مجردا بل يحميه بوصفه تسلطا ماديا من المالك على ما يملك مما يفترض معه تجسد محل هذا الحق في كيان مادي ، وعليه لا تدخل الامورالمعنوية ( ويسميها البعض المال المعنوي ) في نطاق الاموال القابلة لان تكون محلا لجريمة الاتلاف [1]

امام هذه المعالم الرئيسة لقوام جريمة الاتلاف التقليدية ، يظهر لنا بشكل اولي ان النصوص الناظمة لهذه الجريمة في القوانين التقليدية ، لا يمكن ان تنطبق على اتلاف معطيات الحاسوب ولإبراز هذه النتيجة نتعرض تاليا لاتجاهات الفقه وموقف القانون المقارن والمسائل التي اثيرت بشانها :-

اولا : فيما يتصل باتلاف الكيانات المادية للحاسوب ، لا شبهة في امكان تطبيق النصوص التقليدية لأننا أمام محل للجريمة يتصف بالطبيعة المادية ، فاذا ما اكتملت عناصر جريمة الاتلاف وتحققت أركانها أمكن تطبيق النص عليها .

ثانيا : أما فيما يتصل باتلاف المعطيات المخزنه داخل الحواسيب أو المنقولة عبر شبكات المعلومات ، سواء أكانت بيانات أم معلومات أم برامج ، فان الفقه السائد [2] يقرر عدم امكان تطبيق نصوص جريمة الاتلاف على الأنشطة التي تنطوي عليها هذه الجرائم ، بالاستناد الى انتفاء الصفة المادية عن النبضات الكهربائية التي تختزن البيانات والبرامج على هيئتها ، والاستناد الى ان البيانات والمعلومات لا تعتبر مالا بحد ذاتها وان كانت تجسد أو تمثل أموالا أو أصولا .

ويمكن التوصل ايضا لهذه النتيجة عبر تحليل احكام القضاء الانجليزي ، تحديدا حكمه في قضية Cox. V. Rily وقضية Her Majesty. V. Wilson ، حيث يظهر التحليل التفصيلي لهذه الاحكام ، ان القضاء الانجليزي وان ك ان قد حكم بالادانة على افعال الاضرار بالبرامج والبيانات تأسيسا على الاضرار الجنائي الناجم عن الفعل او على الضرر الكيدي ، الا ان هذه

1. السابق ، ص 312 .
2. انظر الاراء الفقهية لدى د. رستم ، المرجع السابق ، ص 314 وما بعدها .

القرارات لم تلق القبول ، واوصت لجنة القانون بوجوب تعديل قانون الضرر الجنائي (1971) بانشاء جريمة جديدة مستقلة وخاصة بالحاسوب . وقد تحقق ذلك بصدور قانون اساءة استخدام الحاسوب لسنة 1990 ، وفي اول تطبيق لاحكامه ، قضت محكمة الاستئناف في حكم لها عام 1991 على نحو صريح وواضح ، وبدون ادنى موارية ، ان جريمة الضرر الجنائي يمكن تطبيقها حيثما يقع الضرر على بيانات الحاسوب [1].

ثالثا : اما فيما يتصل باتلاف الدعامات المادية التي تحتوي البيانات والبرامج، مثل الاشرطة والاسطوانات الممغنطة ، من حيث شمول الاتلاف في هذه الحالة للمادة الموجودة عليها (المعطيات غير المادية) فانها قد اثارت خلافا فقهيا بشان تحديد الوقف منها . فقد ذهب جانب من الفقه ، وبالاستناد الى نصوص التجريم التقليدية المنظمة لجريمة الاتلاف في قوانين بعض الدول ، كالنمسا والدنمارك والمانيا الاتحادية واليونان وايطاليا وهولندا واسكتلندا [2]، الى ان نصوص تجريم الاتلاف ينطوي في نطاقها اتلاف او تعييب البرامج والبيانات في حد ذاتها ، طالما كانت هذه البرامج والبيانات مسجلة على دعامة مادية ، لان مرتكب الفعل اما ان يتلف في هذه الحالة الدعامة المادية نفسها او يتسبب في الحاق ضرر وظيفي بها وهو ما يمكن ان تقع به جريمة الاتلاف .

وهذا الجانب من الفقه يتبنى موقف الاتجاه السائد بشان اتلاف المعطيات المخزنة او المنقولة المشار اليه في البند الثاني اعلاه . الا ان جانبا اخر من الفقه ، كبعض الفقه في بلجيكا وفنلدا واستراليا وامريكا ، لا يوافق على هذا الاتجاه بالاستناد الا ان التدخل في وظائف واستخدامات الدعامات المادية المسجل عليها بيانات او برامج لا يعتبر اتلافا لها .

وعلى الرغم من عدم حدة الخلاف بين الرأيين ، باعتبار ان الاتفاق بينهما قائم على عدم تطبيق نصوص التجريم التقليدية على اتلاف المعطيات لغياب الطبيعة المادية في للمعطيات ، وانحصار الخلاف حول مدلول اتلاف الدعامة المادية ، أينظر اليه مجردا عن محتواها ام يؤخذ محتواها بعين الاعتبار ؟ فان هذه المسألة براينا من المسائل المتصلة بتقدير البيانات ، فاعتبار البيانات مالا ، يحقق تطبيق النص طالما تحقق بالاساس وقوع الفعل على كيان مادي، اما عدم اعتبار البيانات مالا بذاتها –

---

**1**. د. السعيد ، ورقة العمل ، المرجع السابق ، ص 15 .

**2**. انظر Ulrich Sieber السابق ، ص 211 وما بعدها ، وكذلك ، رستم ، السابق ، ص 312 وما بعدها .

كما هو الصحيح براينا عند تخلف النص على ذلك – فانه يقصر تطبيق النص على اتلاف الكيان المادي ، وسندا له تتحدد قيمة الضرر الناتج ، ولا اعتبار للبيانات المخزنة .

ولما كان السائد فقها ، عجز النصوص التقليدية عن الاحاطة بجرائم اتلاف المعطيات ، فقد تدخل المشرع في العديد من الدول للنص على هذه الجرائم المستحدثة ، اما بتجريم اتلاف المعطيات كافعال مستقلة عن الاتلاف المعروف في القانون التقليدي ، او تعديل نصوص الاتلاف بالنص صراحة على التسوية في الحكم بين اتلاف الاموال المادية واتلاف المعطيات ، ومن الامثلة على القوانين المقارنة التي جرمت تزوير الكمبيوتر ، القانون الفدرالي الامريكي بشان غش واساءة استخدام الحاسوب لسنة 1984 في المادة 1030 / أ / 3 ، وقوانين معظم ولايات امريكا كما اشرنا فيما تقدم . وكذلك القانون المعدل لقانون العقوبات الكندي لعام 1985 ، حيث نص في المادة 387 على معاقبة كل من يقوم عن عمد Wilfuly ودون مبرر قانوني Without legal justiication او عذر excuse باتلاف او تشويه البيانات او محوها او جعل البيانات بلا معنى او بدون فائدة او غير مؤثرة او فعالة او باعاقة او مقاطعة الاستخدام المشروع للبيانات او منع من له الحق في الوصول الى البيانات من الوصول اليها . وكذلك عاقب المشرع الالماني في المادة 303 من قانون العقوبات المعدلة بموجب القانون الثاني لمكافحة الجريمة الاقتصادية عام 1986 ، كل من محا او ابطل او جعل غير نافع او احدث تغييرا في البيانات بصور غير مشروعة ، بالحبس لمدة لا تزيد عل عامين او الغرامة ، وشدد العقوبة لتصل الى خمس سنوات او الغرامة اذا ارتكبت هذه الافعال على بيانات ذات اهمية اساسية لقطاع الاعمال او السلطات الادارية ، او في الحالات التي تؤدي هذه الافعال الى تدمير او اتلاف او ازالة او تعديل نظام حاسوب او دعامة بيانات او جعلها غير مفيدة. وكما اشرنا سابقا ، جرم المشرع الفرنسي في قانون 1988 محو وتعديل البيانات المعالجة اليا او التدخل في طرق معالجتها ( م 4/462) وعاقب عليه بالحبس مدة تتراوح بين ثلاثة اشهر وثلاث سنوات او بالغرامة . وجرم كذلك تعطيل او افساد ( عن عمد ) تشغيل نظام المعالجة الالية للبيانات وعاقب عليه بذات العقوبة المشار اليها ( م 3/462) .

## الفرع الثاني: انشطة الانترنت غير المشروعة المتصلة بالمحتوى المعلوماتي والبريد الالكتروني وأنشطة التصرف المعلوماتي غير القانوني .

اشرنا فيما سبق الى هجمات انكار الخدمة التي تستهدف تعطيل مواقع الانترنت والنظم الخادمة لها عبر ضخ كميات هائلة من الطلبات والرسائل في وقت واحد لا لشيء الا لاسقاط النظام وتحويله الى عاجز عن العمل او للمساس بتكاملية وصحة المعطيات والمعلومات . كما اشرنا لانشطة اثارة الاحقاد والاساءة للافراد والتحرش بهم ومضايقتهم وابتزازهم عبر الرسائل الالكترونية ، وكذلك نسبة الاساءات الى اشخاص آخرين لا علم لهم بها باستغلال اسمهم او عناوينهم الالكترونية، وانشطة مواقع الحوار غير القانونية ، وارسال رسائل البريد الالكتروني الدعائية دون طلب وبشكل يزعج المتلقين . كما اشرنا الى استغلال مواقع الانترنت للتصرفات غير القانونية وغير المشروعة كنشر المواد الاباحية وادارة انشطة المقامرة ، او القيام باشطة الغسيل الالكتروني للاموال ، واشرنا ايضا الى ظاهرة الارهاب الالكتروني وتحديدا استغلال الانترنت للوصول الى النظم والشبكات المحلية لاجل الحاق الاذى والخوف والتهديد بافراد المجتع ومؤسساته الحيوية. وهذه الانشطة بمعمومها هي ما ارتأينا ان نضعها في نطاق وتحت عنوان انشطة الانترنت غير المشروعة المتصلة بالمحتوى المعلوماتي الضار ، وانشطة التصرف المعلوماتي غير القانوني او غير المشروع ، ولكن هذا لا يعني اننا نخرج هذه الانشطة من تصنيفاتها التي اوردناها سابقا ، لكننا وجدنا ان الجامع بينها استغلال الانترنت ذاتها لارتكاب هذه الانشطة او المساس بمواقع المعلومات على الانترنت وامن البريد الالكتروني او استثمار مواقع الانترنت والبريد الالكتروني في انشطة غير مشروعة .

## الفرع الثالث: تحديات التصرف غير القانوني على شبكة الانترنت.

ان الانترنت تغير بشكل سريع ومتنام طريقة الاتصال والتعليم البيع والشراء وتلقي الخدمات ، وبقدر ما تقدم خدمة وفوائد للمجتمع فان الاعتماد عليها في خدمة الانشطة غير القانونية يتزايد يوما بعد يوم ، ويتزايد استخدام الانترنت في التصرفات غير القانونية شأنه شأن ذات التصرفات غير القانونية في العالم الحقيقي . ان استراتيجيات وسياسات الجهات الرسمية التي تتعلق بالانترنت والتجارة

الالكترونية تبحث عن تشجيع القطاع الخاص لقيادة هذه الانشطة ولوضع تشريعات ذات طبيعة تقنية مؤسسة على ان الانترنت اهم وسيطة اتصال وتجارة على المستوى الداخلي والخارجي .
لهذه الاسباب فان الرئاسة الامريكية مثلا أنشات فريق عمل في حقل التصرفات غير القانونية يرأسة النائب العام ، من اجل تقييم التشريعات الفدرالية القائمة ومدى كفايتها لتغطية التصرفات غير القانونية على شبكة الانترنت ، واستظهار الوسائل والاليات المطلوبة للجهات القانونية من اجل فعالية ملاحقة وتحري والتحقيق في مثل هذه التصرفات ، ومن اجل استخدام الوسائل التعليمية والتدريبية لتخفيف مخاطر هذه التصرفات ، واستنادا الى هذه الاهداف وضع فريق العمل استراتيجية من ثلاثة اقسام تتعلق بالتصرفات غير القانونية ، وتوصلت الى ثلاثة خلاصات اساسية تبعا لكل قسم : –

1 – ان أي تنظيم للتصرفات غير القانونية على شبكة الانترنت يتعين ان يستند الى قاعدة اساسية وهي ضمان ان التصرفات عبر الخط تعامل بنفس الطريقة للتصرفات خارج الخط ، وبشكل يأخذ بعين الاعتبار المصالح الاجتماعية كالخصوصية وحماية الحريات المدنية .

2 – جهات تنفيذ القانون عليها ان تعي وبشكل خاص الطبيعة التقنية للانترنت وان تتدرب وتتأهل للتعامل مع مثل هذه السلوكيات ، الى جانب الحاجة الى وسائل ومقدرات تحقيق جديدة على المستوى الفدرالي والمحلي وفي ميدان التعاون الدولي لمواجهة هذه التصرفات .

3 – يتعين الاستمرار بدعم القطاع الخاص وتطوير ادواته للتنظيم الذاتي للانترنت مثل اخلاقيات عالم التكنولوجيا ( CYBERETHICS ) والمعايير التقنية والقواعد الاعلانية وغيرها التي من شأنها ان تعلم مستخدمي الانترنت لحماية انفسهم وعلى الاقل تقليل المخاطر من الانشطة غير القانونية .

ان التصرفات غير القانونية على وعبر شبكة الانترنت في تزايد ملحوظ ، والامثلة عليها يصعب تقصيها جميعا ، ففي 7 نيسان 1999 ارسل احد زائري مجلة اخبار مالية تدار من قبل مؤسسة ياهو رسالة بريد الكتروني تحت عنوان اخبار البيع ، تتضمن ان شركة PAIRGAIN قد تم شرائها من شركة (اسرائيلية) وتضمنت الرسالة مدخلا الى احد المواقع التي تعرض خدمات جديدة وتشير الى مزيد من التفاصيل حول هذا الخبر ، وبمجرد انتشار الخبر فان اسهم الشركة قد ارتفعت 30 سنت، ونمت عمليات التداول وازدادت بنحو 7 مرات ، لكن كان هناك مشكلة ، وهي ان هذا الخبر مصطنع وغير صحيح ، والموقع الذي يظهر انه يتضمن تفاصيل بشانه هو ايضا موقع وهمي ، وعندما

انتشر خبر ان المعلومات السابقة غير صحيحة انخفضت اسعار الاسهم بشكل مريع ، ملحقة خسائر مالية ضخمة بالعديد من المستثمرين الذين اشتروا تلك الاسهم استنادا الى الخبر الاول ، وبعد اسبوع من هذه الواقعة تمكنت وكالة التحقيقات الفدارلية الامريكة FBI من اعتقال رجل من شمال كرولاينا ، وقد اعتبر هذا الشخص اول محتال – وطبعا لم ولن يكون الاخير – في حقل الاسهم المالية يستخدم وسيلة احتيال مواقع الانترنت ، وقد تم ملاحقة هذا الشخص من خلال عنوان الانترنت IP ، وتم اتهامه بالاحتيال عن طريق نشر معلومات مزورة حول اسهم الشركات المساهمة ، وقد اقيم ت ضده ايضا دعوى مدنية للتعويض عن الاضرار التي الحقها با لم سرتثمرين ، وفي اب 1999 تم الحكم عليه بالسجن لمدة خمسة سنوات والزامه بدفع مبلغ 93 الف دولار .

ان الانترنت شأنها شأن غيرها من التقنيات الجديدة ، تعد قيمة إضافية للمعرفة والأداء وا لادارة الفاعلة في مختلف حقول النشاط الإنساني وفي مقدمتها التجارة الالكترونية، ويمكن استخدامها لمزيد من الفوائد الاجتماعية والاقتصادية والسياسية والثقافية ، ولكن ها تستخدم ايضا لالحاق الضرر بالمجتمع وبالقيم الاجتماعية فالتقنيات الجديدة تخلق عادة تصرفات وسلوكيات جديدة وتقدم وسائل جديدة لارتكاب الانماط الجرمية والافعال الضارة ، وهذا القول ينطبق على كل تقنية جديدة ، فالتلفون فتح الباب امام انماط جرمية جديدة ( كالاحتيال عن بعد بواسطة الهاتف ) اضافة الى ما قدمه من تسهيل لارتكاب الانماط الجرمية القديمة (انشطة الازعاج ) . ولا تختلف الانترنت عن التقنيات الاخرى لؤلائك الذين يسعون الى ارتكاب الأفعال غير القانونية ، ففي عام 1999 على سبيل المثال، تعرضت انظمة عشرات الآلاف من مستخدمي الكمبيوتر الى الإصابة بفيروس ميلسا (MELISSE ) وانواع اخرى من الفيروسات التي انتشرت حول العا لم عبر البريد الالكتروني والانترنت ، وأدت إلى الإضرار بالملفات وتدمير الأنظمة وألحقت بالشركات ملايين الدولارات من الخسائر ، وفي فترة لاحقة ايضا تعرضت كبرى مواقع الانترنت التجارية الى انشطة هجمات انكار الخدمة DENIAL-OF-CERVICE ATTACKS كما كانت العديد من المواقع هدفا الى انشطة PAGE-GACKING التي من شأنها ان تجعل المواقع ومحركات البحث تعمل لغير المشتركين وفي غير ما يطلب .

ان الانترنت اضافة الى ما تقدم ، مثلت ايضا وسيلة جديدة لارتكاب انشطة جرمية تقليدية بطرق اكثر تعقيدا ويسرا بالنسبة للجناه ، كما هو الحال بالنسبة للاحتيال FRAUD ، وكذلك توزيع

المواد الاباحية وترويج الدعارة PORNOGRAPHY ، وبيع الاسلحة والمخدرات وغيرها من انشطة الاجرام المنظم ، وكذلك انشطة التوزيع غير المصرح به وغير القانوني لبرامج الحاسوب وغيره من مصنفات الملكية الفكرية ، وفي غالبية الاحوال فان انشطة الانترنت غير المشروعة تقود الى انشطة عنف مادية ، اضافة الى المخاطر التي يمكن ان يتعرض لها امن التجارة الالكترونية في ظل التزايد الرهيب في هذا الحقل ، كل ذلك يضع المشرعين والمنفذين وجهات الصناعة وجهات القانون وجهات ملاحقة الجرائم امام تحديات كبيرة .

كما اوضحنا فيما سبق وعلى نحو تفصيلي ، فان تعريف جريمة الكمبيوتر يختلف ليس فقط في حقل التقنية او القانون وانما في مختلف فروع البحث تبعا للمراد بالتعريف والغرض من استخدامه ومما استفدناه من تناول هذا الموضوع فيما سبق ، ان كل جريمة ترتكب بواسطة الكمبيوتر لا تكون بالضرورة جريمة كمبيوتر ، فعلى سبيل المثال اذا قام شخص بسرقة رمز الدخول للهاتف وبواسطته تمكن من اجراء مكالمات دولية بعيدة ، فان الرمز المسروق يجري فحصه والتعرف عليه من قبل الكمبيوتر قبل اجراء المكالمة، وبرغم ذلك فان مثل هذه الجريمة تعامل على انها احتيال وليست جريمة كمبيوتر ، وبكثير من القضايا لا يمكن تبويبها ضمن الطوائف المتعلقة بجريمة الكمبيوتر ، وقد تجد موقعها الطبيعي في جرائم الاتصالات التقليدية التي نصت عليها قوانين الاتصالات ، عوضا عن الخلاف الكبير والغير مستقر حتى الان بشأن طوائف جرائم الكمبيوتر والخلط التي قد يحصل بين جرائم تتشابه السلوكيات فيها ويمكن وصفها بذات الوصف لكن احداها جريمة كمبيوتر والاخرى ليست كذلك ، فعلى سبيل المثال فان محاسب البنك الذي يقوم بسرقة مبلغ من الصندوق يعد مختلسا ، كذلك فان محاسب البنك الذي يقوم بكتابة برنامج كمبيوتر من شأنه سرقة اجزاء النقد الصغيرة من الحسابات المختلفة وتدويرها ونقلها الى حساب في بنك اخر عن طريق ان ظمة نقل الالكتروني للاموال يعد مختلسا ايضا من زاوية استيلائه على اموال بحكم ادارتها ، ومع ان كلتا الجريمتين تتصلان بالانظمة البنكية وبمعرفة نظم العمل والرقابة ، فان الثانية تعد جريمة الكمبيوتر على خلاف الاولى ، ووفقا لما سبق لنا ايضاحه حول خصائص ومحل ومتطلبات جريمة الكمبيوتر .

والكمبيوتر – كما اسلفنا ايضا – قد يلعب احد ثلاثة ادوار في الحقل الجنائي ، فالكمبيوتر اولا قد يكون الهدف TARGET للجريمة ، وهذا يحصل عندما يكون السلوك موجها للحصول الى المعلومات بدون تصريح ، او الحاق الضرر بالمعطيات او بنظام الكمبيوتر او شبكة الكمبيوتر ،

فالفيروسات والديدان التقنية التي تطلق من قبل اله اكرز مثال على هذا النمط . والكمبيوتر ثانيا قد يكون وسيلة ارتكاب الجرم ، كما هو الحال بانشطة الاحتيال والتزوير وقد يكون الكمبيوتر ثالثا بيئة ارتكاب الجرم كما هو الحال بتخزين معلومات مروجي المخدرات كالاسماء والتواريخ والكميات لتخزن بالصورة الالكترونية بدلا من الاوراق ، وكل دور من هذه الادوار قد يكون موجودا في حالة جنائية واحدة وقد يتم استخدام الكمبيوتر لاكثر من دور في الجرم الواحد .

ومن اوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية ، عندما تكون السرية CONFIDENTEALETY والتكاملية او السلامة INTEGRETY ، والقدرة او التوفر AVAILAPILITY هي التي يتم الاعتداء عليها ، بمعنى ان توجه هجمات الكمبيوتر الى معلومات الكمبيوتر او خدماته بقصد المساس بالسرية او المساس بالسلامة والمحتوى والتكاملية ، او تعطيل القدرة والكفاءة للانظمة للقيام باعمالها ، وهدف هذا النمط الاجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله ، بهدف السيطرة على النظام دون تخويل ودون ان يدفع الشخص مقابل الاستخدام (سرقة خدمات الكمبيوتر ، او وقت الكمبيوتر ) او المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر وغالبية هذه الأفعال الجرمية تتضمن ابتداءا الدخول غير المصرح به الى النظام الهدف UNAUTHORIZED ACCESS والتي توصف بشكل شائع في هذه الايام بأنشطة الهاكرز كناية عن فعل الاختراق HACKING .

والافعال التي تتضمن سرقة للمعلومات تتخذ اشكالا عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء ، وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء ، فالكمبيوترات مخازن للمعلومات الحساسة ، كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها ، وهذه تمثل هدفا للعديد من الجهات بما فيها ايضا جهات التحقيق الجنائي والمنظمات الارهابية وجهات المخابرات والاجهزة الامنية وغيرها ، ولا يتوقف نشاط الاختراق على الملفات والانظمة غير الحكومية ، بل يمتد الى الانظمة الخاصة التي تتضمن بيانات قيمة ، فعلى سبيل المثال قد يتوصل احد المخترقين للدخول الى نظام الحجز في احد الفنادق لسرقة ارقام بطاقات الائتمان ، وتتضمن بعض طوائف هذا النمط انشطة السرقة والاعتداء على الملكية الفكرية ، كسرقة الأسرار التجارية واعادة انتاج ونسخ المصنفات المحمية وتحديدا برامج الحاسوب . وفي حالات اخرى فان افعال الاختراق التي تستهدف انظمة المعلومات الخاصة تستهدف منافع تجارية او ارضاء اطماع شخصية كما ان الهدف في هذه

الطائفة يتضمن انظمة سجلات طبية وانظمة الهاتف وسجلاته ونماذج تعبئة البيانات للمستهلكين وغيرها .

## الفرع الرابع : جرائم الانترنت التي تستهدف الاطفال ( انشطة المواد الاباحية )

إن الاطفال والمراهقين يصبحون ضحايا لجرائم الانترنت بشكل متزايد ، ويكون ذلك في الغالب الاعم بسبب ثقتهم بالاخرين وبسبب غياب التوجيه او الرقابة في كثير من الاحيان ، ولانه لا تتوفر لديهم الخبرة والدراية الكافية لتقدير المخاطر .

وابرز انماط الجرائم التي تستهدف الاطفال عبرالانترنت تتمثل بما يلي :

1 – اقحام الاطفال باتصالات عبرالخط يكون غرضها انشطة جنسية Sexual acts.

2 – استخدام الانترنت لترويج وانتاج وتوزيع مواد دعارة الاطفال 3 Child pornography

– استخدام الانترنت لاجبار الشباب والاطفال على ممارسة افعال الدعارة وتشجيعهم لتبادلها

4 – اقحام الاطفال في انشطة سياحية تستهدف اغراض جنسية كالسفر للمشاركة في انشطة غير اخلاقية سواءا لكسب مادي او لتحقيق منافع شخصية.

5 – تنسيق وتنظيم الانشطة الجنسية الواقعية او الاتصالات الجنسية باستخدام البريد الالكتروني أو التلفون او انتقال الشخص فعلا الى مكان مادي لاجراء هذه الانشطة الجنسية .

6 – توزيع المواد الجنسية غير المطلوبة اصلا ، حيث وبمجرد الاتصال بالانترنت او فتح البريد الالكتروني او الدخول على بعض المواقع المشروعة، تظهر مواد جنسية وصور خلاعية دون ان يكون الشخص قد طلبها .

7 – انشطة الابتزاز وتشويه السمعة والتهديد الموجهة للشباب والاطفال عبرالرسائل الالكترونية سواءا تتصل باغراض جنسية او جرمية او غيرها .

ان حجم مشكلة المواد الاباحية بوجه عام ، والمواد والانشطة الجنسية المتصلة بالاطفال والقصر بوجه خاص ، يتزايد بشكل غير عادي ، ووفقا لتقديرات حديثة فان واحدا من كل خمسة شباب قد توصل مع احد مواقع المواد الجنسية على الانترنت ، وان واحدا من كل ثلاثة وثلاثين شاب تلقى

عرضا لانشطة جنسية بشكل او بأخر ، وان كل واحد من اربعة شباب وصلته مواد جنسية غير مطلوبة ، وان كل واحد من سبعة عشر شاب تلقى تهديدات او ابتزازات او غيرها من المواد المسيئة ، ذلك كله خلال عام 2000 وفقا للدراسة التي اجراها مكتب ضحايا الجريمة التابع لوزارة العدل الامريكية .

## المطلب الثاني :جريمة غسل الاموال عبر الوسائل الالكترونية

ظهر اصطلاح (غسل الأموال) لأول مرة في اتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع في المخدرات والتي عقدت في فينا عام 1998[1]، وقد نص في المادة الثالثة منها على أن غسل الأموال يتمثل إما في تحويل الأموال أو نقلها مع العلم بأنها من نتاج جرائم المخدرات، أو في إخفاء أو تمويه حقيقة الأموال أو مصدرها أو في إكتساب أو حيازة أو استخدام الأموال مع العلم وقت تسليمها أنها من حصيلة جريمة من الجرائم المنصوص عليها في الإتفاقية.

وغسل الأموال يقصد به ببساطة إخفاء مصدر المال الإجرامي وظهوره بمظهر المال الناتج عن عمليات مشروعة، وقد بلغ حجم الأموال المغسولة في العالم في الآونة الأخيرة ثلاثمائة مليار دولار.

وقد تبنى القانون النموذجي الصادر عن الأمم المتحدة عام 1955[2] اتجاهين خرج بهما على

---

**1 .** Convention des Nations Unies contre le traffic illicite de stupéfiants et de substances psychotropes – Vienne 1988.

وقد وقعت مصر على هذه الإتفاقية.

**2.** Modèle de le'gislation, programme des Nation Unies pour le contrôle international des drogues (PNUCID), Modèle de loi relative au blanchement de l'argent de la drogues 1995.

القواعد العامة في النظرية العامة للجريمة، أولهما هو تجريم الأعمال التحضيرية بنصه في المادة 23 منه على أن (الأعمال التمهيدية والعمليات التمويلية التي يتم تنفيذها عن عمد وترتبط بالجرائم السابق ذكرها في المادة 20 يجب أن يعاقب عليها بنفس طريقة العقاب على الجريمة نفسها).

وثانيهما أنه عاقب على الشروع في الجريمة بذات العقوبة المقررة للجريمة التامة، فنص في المادة 21 منه على أن (محاولة ارتكاب أي من الجرائم المذكورة في المادة 20 سوف يكون عقوبتها بنفس عقوبة الجريمة التامة). وقد كانت اتفاقية فينا عام 1988 قد اخذت بذات الإتجاه الأخير، وساير المشرع المصري – أيضا – هذه النظرية ونص في المادة 14 من القانون رقم 80 لسنة 2002 على المساواة في العقاب بين الجريمة التامة والشروع.

ولا شك أن غسل الأموال يؤدي إلى آثار اقتصادية سلبيية مباشرة وغير مباشرة وعلى وجه الخصوص في الدول النامية ولعل ابرزها عدم استقرار سعر الصرف وسعر الفائدة نتيجة صعوبة تسجيل المتحصلات من عمليات غسل الأموال ضمن حسابات الناتج القومي والتي يترتب عليها بالضرورة دخول بيانات نقدية مضللة تؤدي إلى صعوبة وضع خطط فعالة للتنمية الإقتصادية، وتؤدي عمليات غسيل الأموال من ناحية اخرى إلى تعميق التفاوت بين الطبقات وعدم استقرار اسواق المال ونقص العملات الاجنبية وإنخفاض

الإنتاج القومي، وتفاقم مشكلة البطالة ذلك لأن الأموال المغسولة تبحث عن الربح السريع فلا تخلق فرص عمل مستديمة.

وجريمة غسل الأموال ذات الطابع الدولي، اتجه مرتكبوها إلى ممارسة السلوك الإجرامي التقليدي والسلوك الإجرامي الحديث الذي يواكب تطور تكنولوجيا المعلومات والاتصالات مما يمكن أن نطلق عليه السلوك الإجرامي الإلكتروني، وهو ما نتعرض له من خلال المطلبين الاول السلوك الاجرامي التقليدي و المطلب الثاني السلوك الاجرامي التقليدي.

أن غسل الأموال هو (كل سلوك ينطوي على إكتساب أموال أو حيازتها أو التصرف فيها أو إدارتها أو حفظها أو استبدالها أو إيداعها أو ضمانها أو إستثمارها أو نقلها أو تحويلها أو التلاعب في

قيمتها إذا كانت متحصلة من جريمة من الجرائم المنصوص عليها في القانون مع العلم بذلك متى كان القصد من هذا السلوك إخفاء المال أو تمويه طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقة أو الحيلولة دون اكتشاف ذلك أو عرقلة التوصل إلى شخص من ارتكب الجريمة المتحصل منها المال.

تحليل : من خلال تتبع نصوص قانون مكافحة غسل الأموال تتوافر الملاحظات الآتية:

إن جريمة غسل الأموال تفترض بالضرورة وقوع جريمة سابقة عليها هي الجريمة التي تحصل منها المال المراد غسله وهو بمثابة ركن مفترض في جريمة غسل الأموال وهو ارتكاب جريمة أولية يعقبها جريمة تابعة.[1]

1. أن المشرع بدأ من حيث انتهى الآخرون، فوسع في نطاق الجرائم الناتج عنها المال المراد غسله ولم يقصرها على مجرد جرائم المخدرات وتوابعها ولكنه أدخل فيها جرائم اخرى مستهديا في ذلك بالاتفاقيات الدولية المتتابعة ذات الصلة ومعيارها الجرائم الخطيرة الناتج عنها أموال قذرة طائلة والتي تكون هدفا للجناة لغسلها وإخفاء مصدرها غير المشروع وهو سلوك محمود من المشرع، وقد يتبادر إلى الذهن لأول وهلة أن المشرع قد حدد الجرائم الأولية على سبيل الحصر، إلا أن النص ترك المجال مفتوحا لدخول طائفة أخرى من (الجرائم المنظمة التي يشار إليها في الاتفاقيات الدولية التي تكون الدولة طرفا فيها) واشترط أن تكون هذه الجرائم معاقبا عليها في كلا القانونين الوطني والأجنبي.

2.أن جريمة غسل الأموال هي جريمة عمدية ولا يتصور أن ترتكب بطريق الخطأ أو الإهمال فقد اشترط المشرع ان يكون مرتكب الجريمة (عالما) بأن الأموال المغسولة محل جريمة من الجرائم التي عددها المشرع، وتقوم الجريمة في مجال ركنها المعنوي على القصد الجنائي العام الذي يتمثل في

---

**1.**د. هدى حامد قشقوش – جريمة غسيل الأموال في نطاق التعاون الدولي – 2003 ص 19.

العلم والإدارة، فلا بد أن يعلم الجاني أن الأموال المغسولة متحصلة من أحدى الجرائم الأولية المنصوص عليها واتجاه إرادته إلى تطهيرها. وبالإضافة إلى هذا القصد العام فإننا نذهب إلى أن المشرع تطلب – أيضا – توافر قصد خاص لدى الجاني يتمثل في نية إخفاء المال أو تمويه طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقته أو الحيلولة دون اكتشاف ذلك أو عرقله التوصل إلى شخص من ارتكب الجريمة المتحصل منها المال [1]

## الفرع الأول : السلوك الإجرامي التقليدي:

عدد المشرع صور السلوك الإجرامي في جريمة غسل الأموال على نحو جامع لكل ما يتصور عملا قيام الجاني به في مجال هذه الجريمة وهي:

اكتساب أو حيازة أو التصرف أو إدارة أو حفظ أو استبدال أو إيداع أو ضمان أو إستثمار الأموال المتحصلة من احدى الجرائم التي نص عليها المشرع، وهي صور من السلوك نصت عليها اتفاقيات دولية لمكافحة جرائم غسل الأموال، اقترنت بضرورة العلم بمصدر الأموال محل هذا السلوك، وطبقا للنظرية العامة للجريمة فإنه يتصور وقوع هذه الأفعال بالمساهمة التبعية للجريمة في إحدى صور الإشتراك في الجريمة.

نقل أو تحويل الأموال مع العلم بأنها متحصلة من جريمة، اما عن نقل المال فيقصد به الحركة المادية التي تنقل المال من مكان إلى مكان اخر، وقد يكون هذا النقل داخليا في اطار الحدود الإقليمية

**1.** ومع ذلك اكتفى المشرع الدولي في اتفاقية فينا عام 1988 بتوافر القصد الجنائي العام عندما نص في المادة 3/35 من الاتفاقية على أنه يجوز الاستدلال على العلم (من الظروف الواقعية والموضوعية على العلم أو النية أو القصد المطلوب) مما يعني أنه لم يشترط سوى القصد العام.

للبلد الواحد، كما قد يكون وهو الغالب الأعم عبر الحدود إلى دول اخرى قد تكون مجاورة أو بعيدة وتتخذ هذه الصورة الأموال الهاربة من الرقابة على التعامل بالنقد الاجنبي أو لاسباب استثمارية أو لغير ذلك. أما تحويل الأموال فإنه يتمثل في أجراء عمليات مصرفية أو غير مصرفية سواء عن طريق مؤسسات مالية رسمية كالبنوك أو مؤسسات مالية غير رسمية يكون الغرض منها في كل الأحوال تحويل المال إلى شكل اخر سواء من عُمْلَه محلية إلى عُمْلَه عالمية أو من عُمْلَه إلى منقول ثمين، أو غير ذلك من الاشكال التي تؤدي إلى قطع الصلة الظاهرة بين المال ومصدره حتى يبدو كما لو كان مالا ناتجا عن مصدر اخر غير الجريمة.

## الفرع الثاني: السلوك الإجرامي الإلكتروني.

مع التطور المذهل في تكنولوجيا المعلومات والاتصالات فإن الجرائم المنظمة التي تتسم بالطابع الدولي تستغل هذا التطور في ابتكار اسآليب جديدة للسلوك الإجرامي يتمكن من خلاله الجناة من ارتكاب جرائمهم وهم بمنأى عن المراقبة والمتابعة والضبط، وهو الامر الذي يؤدي إلى صعوبة دور الجهات المكلفة بضبط الجرائم وتتبع مرتكبيها. ولم تكن جريمة غسل الأموال بمنأى عن هذا التطور بل تطور السلوك الإجرامي للجناة فيها، ومن أهم صور هذا السلوك هو الإستعانة بالوسائط الإلكترونية في غسل الأموال ويظهر ذلك من المراحل التي تمر بها هذه الجريمة على النحو التالي:

### أولا : مراحل الجريمة الإلكترونية

### المرحلة الاولى: مرحلة الإيداع Le placement

وهي المرحلة التي تلي الحصول على الأموال القذرة من الجرائم التي نص عليها المشرع. وهي مرحلة ركود للمال، ويقصد به وضعه في مكان معين لفترة معينة من الزمن يقصد به وضعه في مكان معين لفترة معينة من الزمن بقصد توافر فكرة نسيان مصدره، وقد يكون سلوك الجاني في هذه المرحلة متمثلا في فتح حساب أو حسابات بنكية باسم حقيقي أو مستعار وشراء اسهم في مؤسسات تجارية أو مالية وعلى وجه الخصوص الاسهم لحامله التي لا تشير إلى اصحابها ومن ثم إلى مصادرها، أو شراء منقول أو عقار له قيمة كبيرة والاحتفاظ به لفترة من الزمن قبل التصرف فيه.
وتقدير الفترة الزمنية التي يتطلبها ركود المال أمر تحكمه الظروف ويختلف من حالة إلى اخرى ومن بلد

إلى آخر، إلا أن المال يظل متربصا باللحظة المناسبة التي يتحرك فيها إلى المرحلة التالية دون إمكانية تتبعه أو ضبطه.

## المرحلة الثانية: التكديس L'empilage

وفيها يخرج المال القذر من مكمنه، ويدخل في المرحلة الثانية أو كما يقال عنها مرحلة الغسيل الأولى وذلك بوضع المال في مشروعات قد تكون حقيقة كمشروعات عقارية ضخمة كالقرى الساحلية أو شركات وهمية في البلاد التي لا تفرض قيودا على حركة رأس المال بحيث يصعب تتبع مصدر أموالها[1] وهذه المرحلة يقصد من خلالها تضليل الجهات الرقابية عن مصدر الأموال غير المشروع بإتخاذ أسلوب التمويه أو التعتيم، ويمكن أن يتم ذلك عند القيام بأعمال مصرفية معقدة ينتقل بها المال عن بعد من حساب إلى حساب اخر ومن مصرف إلى مصرف اخر ومن قارة إلى قارة اخرى آليكترونيا، ويذكر ان احد الاشخاص من محترفي برامج الحاسب الآلي تمكن من تصميم برنامج يتم فيه تحريك الحساب المودع في احد البنوك إلى حساب اخر، ومن بنك إلى بنك اخر عبر القارات الخمس، يعمل تلقائيا كل ربع ساعة ولمدة ثلاث سنوات هي الحد الاقصى لعقوبة جريمة غسل الأموال في بلده فيما لو ضبط، بحيث يبدأ العمل فور ضبطه ولا يمكن ايقاف البرنامج إلا بشفرة خاصة يحتفظ بها.

---

**1**.Thony Jean (Francois), les politiques législatives de lutte contre le blanchement en Europ., tev pen et Dr. Pen no 4oct Dec. 1997, P.309

### المرحلة الثالثة: الإندماج L'inteGration

وهي المرحلة الاخيرة في عملية غسل الأموال أو هي مرحلة غسل الأموال الثانية والأخيرة، وفيها يندمج المال القذر في الأموال المشروعة ويدخل في مجال الإقتصاد القومي، ويتخذ مظهرا قانونيا مشروعا، وعلى سبيل المثال فإن المشرعات التي سبق إخفاء المال فيها في المرحلة الأولى يتم بيعها وتصبح ظاهريا أموالها مشروعة ذلك أن حصيلة مشروعات حقيقية، والرصيد الذي ينتقل من مصرف إلى اخر ومن مكان إلى اخر تتوقف حركته ويخرج إلى حلبه الاقتصاد على اساس انه حصيلة اعمال تجارية مصرفية.

## ثانيا : الأساليب الحديثة لغسل الأموال

كما قدمنا اتجه الجناة إلى استخدام الوسائط الإلكترونية لارتكاب جريمة غسل الأموال لتطيهر المال من مصدره غير المشروع والدخول به في دائرة الأموال المشروعة، ويمكن بإستخدام هذه الوسائط تحريك المال عن بعد في مختلف مراحل غسل الأموال سواء في مرحلة فتح الحساب في أحد المصارف على سبيل المثال عن طريق الحاسب الآلي مستعينا بشبكة الإنترنت مع اختيار اسم مستعار أو شفرة أو رموز معينة، ثم يحرك المال من مكان إلى مكان حتى لا تتمكن أي جهة كانت من تتبعه ثم يكدس المال في مشروعات وهمية بأن يعلن على شبكة الإنترنت عنها ويفتح باب المساهمة العامة عن طريق اسهم محددة القيمة تدخل إلى حساب المشروع إلكترونيا عن طريق فتح صفحة خاصة Side لتلقي هذه الأموال التي تدخل إليه مختلطة بأمواله غير المشروعة فتغسلها جزئيا ثم يعلن بعد مرور وقت معين عن تصفية هذا المشروع زعما بتعرضه لخسائر ويعيد توزيع الحصص على أصحابها مع هامش الفائدة المتفق عليها، ويسحب أمواله القذره على هذه المرحلة باعتبارها ناتجا عن مشروع، ويبدأ في المرحلة الثالثة والأخيرة في استثمار هذا المال في مشروعات حقيقية تدخل في دائرة الاقتصاد القومي، ويمكن تصور القيام بهذه الامور من خلال الاستعانة بما يلي:

**1) وساطة البنوك** :وهي الطريقة الأكثر شيوعا في مجال غسل الأموال سواء بالطريقة التقليدية أو بالطريقة الإلكترونية، وتبدأ طبقا لمراحل غسل الأموال المتعارف عليها بالإيداع وتنتهي بالاستثمار.

**2) الايداع**: وتسبق هذه المرحلة، مرحلة أخرى مفترضة وهي فتح حساب وهناك بعض الأنظمة التي

تتبعها البنوك بإمكانية فتح الحساب إلكترونيا عن طريق الدخول على شبكة الإنترنت، بملء إستمارة حدد نموجها البنك ويمكن التوقيع عليها إلكترونيا، وفيها يختار العميل ما يشاء من أسماء حقيقية أو وهمية أو حتى مجرد رموز سواء اكانت رقمية أو حروف وتنتهي عملية فتح الحساب عند هذا الحد، وقد لا يقتصر الأمر على فتح حساب واحد فقط بل قد تتعدد الحسابات البنكية في بنوك مختلفة ودول مختلفة.

ومرحلة الإيداع الآليكتروني قد لا تتناسب مع غسل الأموال ذلك ان هذا النوع من الإيداع يتم بمبالغ ضئيلة لا تتناسب مع حجم المال المغسول، لذلك فإنه في الغالب الأعم يتم الإيداع بالطريق المختلط التقليدي والإلكتروني معا.

**3) أستثمار الأموال القذرة** : ويلاحظ أنه بمجرد إيداع الأموال القذرة في البنوك، فإن البنوك تساهم بصورة أو بأخرى في غسلها دون أن يتوافر لها حقيقة مصدرها، ذلك ان البنوك بحسب طبيعة نشاطها تستثمر أموال المودعين في مشروعات مختلفة تدر عليها أرباحا تستطيع من خلالها أن تؤدي للعملاء الفوائد المتفق عليها، ومن ثم فإن الأموال القذرة تختلط مع أموال المودعين على وجه العموم ويتم استغلال المال كوحدة واحدة في الاستثمار.

ومع ذلك فإن مودع الأموال القذرة قد يستثمرها طبقا للانظمة التي يضعها البنك، وذلك بطلب قروض بضمان هذه الودائع وهو امر يدر على البنك ربحا حاصله الفرق بين فائدة الإيداع وفائدة الإقراض، ولا يشترط بطبيعة الحال أن يتم الاقتراض من ذات البنك الذي اودع فيه المال المغسول، بل يمكن طلب القرض من بنك اخر بضمان الوديعه، وقد يكون هذا البنك في دولة اخرى غير دولة البنك المودع لديه، والأموال المقترضه هي بطبيعة الحال أموالا نظيفة يمكن من خلالها الاشتراك في مشروعات أو شراء ممتلكات تبدو في صورة مشروعة تماما.

**4) السحب الإلكتروني**: ويمكن لصاحب الحساب أن يحصل من البنك المودع لديه على كارت ممغنط يستطيع بموجبه أن يسحب الأموال إلكترونيا من اي مكان في العالم، والذي يحدث عملا أن غاسل الأموال إذا وضع ماله بعملات محلية ليس لها سعر صرف مناسب بالقياس إلى العملات الإجنبية ذات الغطاء القوي كالدولار والاسترليني واليورو مثلا، فإنه يلجأ إلى الدول التي تتعامل بهذه

العملات ويسحب أمواله إلكترونيا خارج الحدود دون مخاطرة تذكر والثانية أنه يمكن فتح حساب جديد في الخارج بعملة قوية ومصدر ظاهره مشروع.

**5) التجارة الإلكترونية** : تبعا لتطور تكنولوجيا الإتصالات والمعلومات فقد انتشرت في الآونة الاخيرة ظاهرة التجارة الإلكترونية عبر الإنترنت وفيها لا يشترط تواجد اطراف العقد في المواجهة، ولا يشترط تنفيذ التزامات العقد في ذات المكان، وقد وافقت لجنة الأمم المتحدة للقانون التجاري الدولي UNCITRALعلى نموذج لمشروع قانون موحد للتجارة الإلكترونية في 16 ديسمبر 1996، وعلى الرغم من ان المشرع لم يضع تعريفا محددا لمفهوم التجارة الإلكترونية والتي تتم بواسطة نقل المعلومات بين جهازين للحاسب الآلي وفقا لقواعد معينة متفق عليها سواء بالنسبة للعرض أو الطلب أو التعاقد أو التنفيذ[1]

وفي مشروع قانون التجارة الإلكترونية المصري جاء في مادته الأولى تعريف للتجارة الإلكترونية بأنها (كل معاملة تجارية تتم عن بعد باستخدام وسيلة إلكترونية). وقد فرض المشرع على المعلن بطريق التجارة الإلكترونية التزامات محددة ببيان أسمه وعنوانه والسلعة أو الخدمة أو القيمة وقيمة الجمارك التي تحصل عليها ومكان وتاريخ التسليم وجهة اعتماد التوقيع الإلكتروني.

ولا شك أن أحد الأساليب المتبعة في غسل الأموال هي وسيلة التجارة الإلكترونية ولا نقصد بذلك مجرد الحصول على سلع استهلاكية، بل المقصود بذلك عقد الصفقات المالية الضخمة مع الشركات الكبرى ثم إعادة طرحها في الاسواق، كصفقات السيارات أو العقارات أو المعادن الثمينة على سبيل المثال[2]

---

**1** . د. مدحت عبد الحليم رمضان – الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة – 2001 ص 10 وما بعدها.

**2**. د. محمد حسام محمود لطفي – الاطار القانوني للمعاملات الإلكترونية – 2002 ص 7 وما بعدها.

## الفرع الثالث : الجرائم التقليدية التي ترتكب بإستخدام وسائل تقنية فنية

تتعدد هذه الجرائم، وبالنظر إلى كونها ترتكب باستخدام وسائل فنية، فإننا سوف نقصر حديثنا على جريمة الاستيلاء على الأموال عن طريق الاحتيال. (التحويل الإلكتروني غير المشروع للأموال). وفيما يتلاعب الجاني في البيانات المختزنة في ذاكرة الحاسب الآلي أو في برامجه وفقاً لأساليب متعددة، بهدف تحويل كل أو بعض أرصدة الغير أو فوائدها إلى حسابه.

### أ / الاحتيال على نظام الحاسب الآلي

الاحتيال هو كل تظاهر أو إيحاء يكون صالحاً لإيقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة النصب هو من جازت عليه حيلة الجاني فانخدع بها وسلمه ماله.

وتباينت إتجاهات التشريعات المقارنة في شأن الإجابة عن تساؤل محله هل يمكن ممارسة أفعال الاحتيال على الحاسب الآلي وإيقاعه في الغلط؟

تستهدف التشريعات التي أمدت نطاق تطبيق نصوص في مجال النصب على النصب المعلوماتي، الحد من جرائم التلاعب في البيانات المعالجة إلكترونياً بواسطة الحاسبة الآلي.

### ب / الاستيلاء على نقود كتابية أو بنكية [1]

إن نشاط الجاني في جريمة النصب مركب لا بسيط، فهو يتكون من فعلين مختلفين، هما الاحتيال والاستيلاء. وأول الفعلين يتقدم الثاني في الزمن ويفضي إليه بحكم المنطق، ومحل الاستيلاء في جريمة النصب هو المال المنقول والذي حدده المشرع المصري في المادة 336 عقوبات بأنه "نقود أو عروض أو سندات دين أو سندات مخالصة أو متاع منقول " ويتحقق الاستيلاء على المال في هذه الجريمة بتسليم المجني عليه المال بمحض إختياره إلى الجاني تحت تأثير الغلط الذي أوقعه فيه فعل الاحتيال[2]

---

**1**. راجع د. محمد سامي الشوا، مرجع سابق، ص 170

**2**. راجع د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، ط 3، 1990، ص 861

ولا يرتب الإستيلاء الناشئ عن الاحتيال على الحاسب الآلي أدنى مشكلة إذا كان محل الاستيلاء نقوداً أو أي منقول آخر له قيمة مادية، كأن يتم التلاعب في البيانات الداخلة أو المختزنة بالحاسب أو برامجه، بواسطة شخص ما كي يستخرج الحاسب بإسمه أو بإسم شركائه، شيكات أو فواتير بمبالغ غير مستحقة يستولى عليه الجاني أو يتقاسمها مع شركائه.

ويدق الأمر عندما يكون محل هذا الاستيلاء نقوداً كتابية أو بنكية، أي أن في هذا الفرض يتم الاستيلاء على المال عن طريق القيد الكتابي، وصورة ذلك أن يتلاعب شخص في البيانات المخزنة في الحاسب كي يحول بعض أرصدة الغير أو فوائدها إلى حسابه[1]

وهنا يثور التساؤل : هل حدث استيلاء مادي على المال أم لا؟

إتجه عدد محدود من الدول، كما هو الحال في كندا وهولندا وسويسرا وإنجلترا ومعظم الولايات المتحدة الأمريكية إلى اعتبار النقود الكتابية – وعلى الرغم من طابعها غير المحسوس – من قبيل الأموال التي تصلح لأن تكون محلاً لجرائم السرقة والنصب وخيانة الأمانة[2]

وعلى النقيض ذهبت بعض التشريعات – كما هو الحال في ألمانيا واليابان – إلى عدم إعتبار النقود الكتابية بمثابة مال مادي، ولكن ينظر إليها بوصفها من قبيل الديون والتي يستحيل أن تكون محلاً للاختلاس أو السرقة.

أما التشريع الفرنسي فإن القضاء الفرنسي إبتدع نظرية التسليم المعادل، ومؤداها أن مجرد القيد الكتابي والذي لا يقتضي تسليم شيء مادي أياً كان، يعد من قبيل التسليم المعادل. وتلقف الفقه الفرنسي نظرية التسليم المعادل التي أرستها محكمة النقض الفرنسية [3] وقام بتطبيقها على جميع

---

**1**.راجع د. محمد سامي الشوا، مرجع سابق، ص 131.

**2**.المرجع السابق، ص 132.

**3**. راجع د. محمد سامي الشوا، مرجع سابق، ص 134، والمراجع المشار إليها في هامش 1 من ذات الصفحة، ود. جميل عبد الباقي الصغير القانون الجنائي، والتكنولوجيا الحديثة، الجرائم الناشئة عن الحاسب الآلي، 1992، دار النهضة العربية، ص 116 وما تلاها، و د. هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة بأسيوط 1992، ص 282 وما تلاها .

أفعال التلاعب في عملية البرمجة، أو في البيانات المدخلة إلى الحاسب الآلي، والتي تؤدي إلى إلغاء رصيد دائن، أو من باب أولى خلق رصيد دائن بمبالغ غير مستحقة وتتعدد الأساليب المستخدمة في هذا الشأن، فقد يحدث ذلك عن طريق إلتقاط أمر التحويل بواسطة الجاني، أو تزيفه بالأمر بتحويل نفس المبلغ بحسابه الخاص، أو عن طريق التلاعب في عملية البرمجة بغرض تحويل فوائد حساب شخص ما إلى حساب الفاعل، وأخيراً عن طريق انتحال الفاعل لشخصية الغير ومباشرته لعملية تحويل النقود وبالتالي فإن الدفع يتم بمجرد القيد الكتابي، وهو يعادل تسليم النقود .

## ج / جريمة التزوير

نصت المادة 341 ع على ان يعاقب بالحبس مدة لاتقل عن ثلاث سنوات كل موظف يضع اثناء ممارسة مهامه وثيقة مزورة في كليتها او جزء منها او زور وثيقة صحيحة ، ما يهمنا في هذا الصدد محل جريمة التزوير لان هذه الاخيرة من من الجرائم ذات القالب الحر التي لم يحدد المشرع فيها شكلا معنيا للسلوك الاجرامي في لكنه حدد محل هذا السلوك بالوثيقة دون أن يعرفها او يحدد مضمونها تاركا للفقة والقضاء هذه المهمة.

فالوثيقة هي مجموعة من المعاملات والرموز التي تعبر تعبيرا اصطلاحيا عن مجموعة مترابطة من الافكار والمعاني الصادرة عن شخص او اشخاص معينين ، وتكمن القيمة الحقيقية لها ليس في مادتها او ما تحتويه بل تكمن فيما لهذا التعبير من دلالة اجتماعية [1].

فجوهر جريمة التزوير هو الاخلال بالثقة العامة التي اراد المشرع حمايتها في هذه الوثيقة لما لها من اثار قانونية باعتبارها وسيلة للإثبات[2].

ولما كان ذلك ، فإن قوة الوثيقة في الاثبات هى جوهر الحماية الجنائية لها ومن هنا ذهبت بعض الآراء الفقهية الى أن كل مادة تصلح للاثبات يجوز أن تكون محلا للتزوير مهما كان شكلها او مساحتها ولا اهمية للمادة المستعملة في الكتابة يستوى ان تكون مصنوعة من خشب او جلد[3] فاذا

---

**1**.. محمود نجيب حسني – شرح قانون العقوبات – القسم الخاص – الجرائم المضرة بالمصلحة العامة – دار النهضة العربية – القاهرة 1972 ص 322

**2** . محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية – القاهرة 1994 ص 155

**3** . حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الاسكندرية مصر 1991 ص 116

كانت فكرة التوسع في مفهم الوثيقة مطروحة في الفقة الجنائي قبل ظهور جرائم المعلوماتية فإن هذا التوسع يبدو أكثر الحاحا في ظل الفراغ التشريعي لمواجهة جرائم التزوير المرتكبة بواسطة الحاسب الالي ، الأأن هذا الاتجاه واجه نقداً شديداً حيث ذهب جانب من الفقة الفرنسي قبل صدور القانون رقم 19 لسنة 1988 الخاص بالغش المعلوماتي الى رفض اعتبار التعبير الواقع على الاسطوانات الممغنطة تزويراً، استنادا الى اعتبارين اولهما انتفاء الكتابة ،لان التغيير انصب على نبضات الكترومغناطيسية ،والثاني هو عدم التيقن من صلاحيتها في الإثبات [1]. يؤيد هذا الرأي قياس ذلك على انتفاء التزوير في التغيير الذي يطرأ على الصوت المسجل، والعلة هي انعدام عنصر الكتابة ، بالإضافة إلى أن النبضات الالكترومغناطيسية تمثل جزءا من ذاكرة الآلة او برنامج تشغيلها وهو ما يمكن ان يتحقق معه الإتلاف او التقليد إذا توافرت شروطهما، وقد بدأ الفكر القانوني الحديث يقبل فكرة الوثيقة الاليكترونية استنادا الى ان المادة التي تصنع منها الوثيقة ليست عنصرا فيها.

ان مجاراة التقديم العلمي والتكنولوجي تتطلب تجاوز المفهوم التقليدي للوثيقة أو حصره في الورق المكتوب. ويمكن لنا في هذه الحالة أن نجد سندا لهذه الفكرة ومنطلقا لها ان المشرع المدني في الاصل رغم أخذه بمبدأ سيادة الدليل الكتابي على غيره من طرق الإثبات إلا أنه أورد عليه بعض الاستثناءات فقبل الإثبات بالبينة فيما كان يجب اثباتها كتابة في حالات حددتها المواد 387 289 391 من القانون المدني الليبي وهي اتفاق الاطراف على الاثبات بالبينة أو وجود مانع يحول دون الحصول على الدليل الكتابي فإذا اتفق الاطراف على الاثبات بالبينة يكون على القاضي ان يعتد بها استنادا الى عدم تعلق القواعد الموضوعية في الإثبات بالنظام العام ، مما يمكن القول معه على امكانية اتفاق الأطراف على الاثبات بالوسائل الاليكترونية وهو ما يعد ايذانا ببداية عصر الوثائق الالكترونية.

1. محمد سامي الشوا – المرجع السابق ص 155

## الفرع الرابع : الجرائم المستحدثة في مجال المعلوماتية باستخدام وسائل تقنية فنية و مدى تكييفها القانوني و تنظيمها التشريعي:

### أولا : الجرائم المستحدثة في مجال المعلوماتية باستخدام وسائل تقنية فنية:

سبقت الإشارة إلى أن من الجرائم المستحدثة في مجال إختراق شبكات المعلومات، والاستيلاء على المعلومات الموجودة في قواعد البيانات، والدخول أو البقاء في الأنظمة المعلوماتية بطريق غير مشروع، التجسس على البيانات، وأخيراً ما يعرف بسرقة الحاسب الآلي[1] .ونجتزء من هذه الجرائم مثالاً هو اختراق شبكات المعلومات (الولوج غير المسموح به في نظم المعلومات.

أدى ربط الحاسبات الآلية بعضها ببعض عن طريق شبكات المعلومات إلى سرعة انتقال المعلومات من جهة، وإلى سهولة التطفل عليها من جهة أخرى عن طريق استخدام "المودم" حيث يسمح هذا الجهاز للمتطفلين من أي مسافة يتواجدون فيها بالولوج إلى الحاسبات الآلية المستهدفة، ودون أي مساس مادي بحق ملكية الغير أو ترك أي أثر يدل على إنتهاك المعلومات أو نسخها [2]

ونظراً لجسامة هذا النوع من التعدي، فقد حرصت دولاً كثيرة على إرساء مبدأ حماية سلامة نظم المعلومات لديها وبغض النظر عن مبدأ حماية سرية البيانات المعالجة أو المتداولة .

وبالرغم من أهمية هذه الحماية، فإن ثمة صعوبات في تطبيق النصوص التقليدية. ذلك أن غالبية الأنظمة القانونية لا تستهدف النصوص التقليدية التي تجرم التصنت على المكالمات التليفونية والتقاط المراسلات المتبادلة، سوى تسجيل المحادثات أو الإتصالات الشفوية أي التي تتم بين شخصين فأكثر. وعلى سبيل المثال أن المادة 716 المستحدثة من قانون العقوبات الإيطالي يقتصر

---

1. راجع د. محمد سامي الشوا، مرجع سابق، ص 204 وما تلاها.
2. المرجع السابق، ص 204.

تطبيقها على الاتصالات التي تجري بين شخصين، وهذا هو الحال أيضاً من القوانين العقابية الألمانية والسويسرية والهولندية والمصرية. وأيضاً في الولايات المتحدة حيث يستهدف القانون الفيدرالي الخاص بمراقبة المكالمات التلفونية الصادر سنة 1968 الإتصالات الشفوية التي تتم بواسطة أنظمة الإتصالات البعدية، ودون أن يستطيل ذلك إلى البيانات المتدفقة بين الحاسبات الآلية [1]

بينما يذهب قانون العقوبات الكندي عكس ذلك، حيث تجرم المادة 178 منه إلتقاط المراسلات التي تتم بين الحاسبات الآلية، ولكن بشرط أن يكون هناك إتصال شفوي بين شخصين أو عن طريق أنظمة الاتصالات البعدية، ومن ثم لا تسري هذه المادة على الإتصالات التي تجري بين حاسبين آليين يخصان شخص واحد، أو على الاتصالات التي تجري بين حاسبين آليين، أو على الاتصالات المتبادلة داخل نظام معلوماتي واحد.

والعقبات التي تثار عند تطبيق النصوص الجنائية التقليدية على الأنماط المستحدثة لظاهرة الغش المعلوماتي ما زالت أكثر وضوحاً في مجال "مجرد" الولوج غير المسموح به في أنظمة معالجة وتخزين البيانات تعني مجرد "الولوج غير المسموح به في حاسب آلي، فعل التواجد به بدون إحداث أدنى ضرر لصاحبه، سوى الإطلاع على المعلومات المخزنة به وبدون غرض محدد[2]

أما عن الحلول التشريعية، فإن المشكلة في هذا المجال هي معرفة ما إذا كان يجب تنظيم الولوج في المعلومات والبيانات، أم يجب حماية المعلومات لذاتها، أو أن يعمل بالحلين معاً في نفس الوقت، على إعتبار أن التعدي على البيانات والمعلومات وما يتحقق من لحظة التعدي – على النظام المعلوماتي.

بيد أن المشكلة الاكثر جسامة هي معرفة ما إذا كان من الملائم تجريم مجرد الوجود في الأنظمة، أم يجب أن يقترن هذا الأخير بأفعال أخرى كتعديل معلومات أو حيازتها أو إستخدامها أو إحداث ضرر بها.

---

**1** . راجع د. محمد سامي الشوا، مرجع سابق، ص 205.

**2** . راجع د. محمد سامي ا شوا، مرجع سابق، ص 206.

إتجهت بعض الدول إلى النص في تشريعاتها على تجريم فعل الولوج في المعلومات أو البرامج المخزنة في أجهزة المعالجة الإلكترونية للمعلومات. ومن هذه الدول السويد والدنمارك[1]

أما الولايات المتحدة، فإن التشريع الفيدرالي الصادر سنة 1984 بحذر الولوج بدون تصريح في الحاسبات الآلية المستخدمة من قبل الحكومة الفيدرالية والبنوك[2]

أما التشريع الفرنسي، فإن القانون الفرنسي الصادر في 5 يناير 1988 إستحدث بموجب المادة 2/462 عقوبات، جريمة الولوج غير المشروع في نظم المعلومات والتي تنص على أن يعاقب.....كل من ولج أو تواجد بطريق الغش في كل أو جزء من نظام مبرمج للبيانات. "وتشدد العقوبة إذا ما ترتب على ذلك إلغاء أو تعديل للبيانات التي يحتويها النظام أو إتلاف لوظيفة هذا النظام[3]

ويستهدف هذا النص في المقام الأول – حماية الولوج في نظم المعلومات، لا حماية حق الملكية ذاته، وهو بذلك فراغاً تشريعياً هائلاً في القانون الفرنسي، ومن جهة أخرى استجابة لرغبة ملاك الأنظمة المعلوماتية [4].

## ثانيا : التكييف القانوني لهذه الأنماط من السلوك

ولقد تدخل القانون العربي النموذجي بالنص مع تجريم الصور السابقة والاستيلاء على الاموال فنص في المادة 6 على انه كل من استخدم بطاقة ائتمانية للسحب الالكتروني من الرصيد خارج حدود رصيده الفعلي أو باستخدام بطاقة مسروقة او تحصل عليها بايه وسيلة بغير حق أو استخدام أرقامها في السحب او الشراء و غيرها من العملات المالية مع العلم بذلك وهو ما يعني ان هذا النص قاصرا على توفير الحماية لغيرها من البطاقات لتقدير الدولة.

---

1 . راجع د. محمد سامي الشوا، مرجع سابق ص 207 وما تلاه.
2 . راجع د. محمد سامي الشوا، مرجع سابق ص 207 وما تلاه.
3 . راجع د. محمد سامي الشوا، مرجع سابق ص 208.
4. راجع د. محمد سامي الشوا، مرجع سابق ص 210.

اما اتفاقية بودابست السابق الإشارة اليها فقد نصت المادة 8 منها و الخاصة بالتحايل المرتبط بالحاسب computer related frau على معاقبة أي شخص يتسبب باي خسائر مادية للغير عن طريق تعديل أو محو أو إيقاف لأي بيانات مخزنة في أي نظام معوماتي أو عن طريق أي تدخل فيه، وبذلك تتوفر الحماية الجنائية اللازمة للأموال في مواجهة السلوك المرتكب بالحاسب الآلي.

اذا كانت جرائم الاموال المرتكبة بواسطة الحاسب الالي تواجه فراغا تشريعيا في ليبيا فإن المشكلة الحقيقة في نظرنا بالنسبة لهذه الجرائم لا تتمثل في الفراغ التشريعي بقدر ما هي كامنة في طرق ضبطها وإثباتها، وهو ما يرجع الى افتقاد الاثار التقليدية التي قد تتركها أي جريمة في الجريمة المعلوماتية، فالبيانات يتم إدخالها باشرة في الجهاز دون ان تتوقف على وجود وثائق او مستندات لانه كثيرا ما يكون هناك برامج معدة ومخزنة سلفا على الجهاز ولا يكون عليه سوى ادخال البيانات في الاماكن المعدة لها كما هو الحال بالنسبة للمعاملات المصرفية والمؤسسات التجارية الكبرى ويمكن في هذه الفروض اقتراف جرائم الاختلاس والتزوير فتفقد الجريمة اثارها التقليدية. فالجريمة المعلوماتية ترتكب في مسرح خاص هو يتمثل في عالم اقتراضي مفرغ cyberspace وهو ما يختلف كليا عن المسرح الذي ترتكب فيه الجرائم في صورتها التقليدية حيث تطبق القواعد العامة لانتداب الخبراء في اقتفاء اثار الجناة ، الذين يرتكبون جرائم تتكون من سلوك مادي ملموس وله محل مادي ملموس ايضا ، مما لا يتناسب ونوع الخبرة المطلوبة لمعاينة المسرح السيبيري للجريمة المعلوماتية المرتكبة في الفضاء الالكتروني. فالخبرة المطلوبة للتحقيق في الجريمة المعلوماتية يجب ان تكون على درجة عالية من الكفاءة العلمية او العملية أيضا ، وهو ما يوجب أن يكون الخبير في الجريمة المعلوماتية ملما بأدق تفاصيل تركيب الحاسب وعمل الشبكات المعلوماتية والأماكن المحتملة للأدلة كالمواضع التي يمكن ان تحتفظ بآثار الاختراق و توقيته ، و البرامج المستخدمة في أي عملية تمت اثناء الاختراق ، بالإضافة إلى إمكانية نقل الأدلة الى أوعية أخرى دون تلف.

يجب الإشارة أيضا إلى ان ملاحقة الجرائم المعلوماتية لا يتطلب رفع كفاءة الخبراء فقط بل أنها تحتاج الى رفع كفاءة مأموري الضبط القضائي بصفة عامة لان مأمور الضبط القضائي أول شخص يكتشف الجريمة ويتصل بمسرحها والمسئول الأول عن التحفظ على اي اثر يتركه الجاني بعد ارتكابه للجريمة ،مما يستوجب ان يكون المتعامل الأول مع النظام المعلوماتي على درجة من الكفاءة تسمح له

بالتحفظ على هذه الأدلة لأن أي خطأ في التعامل الأولى مع هذه الأجهزة قد يؤدي الى محو الأثر أو الأدلة.

اما اتفاقية بودابست السابق الاشارة اليها فقد أشارت في القسم الإجرائي منها في المادة 16 إلى أنه (على الدول الأعضاء العمل على تطبيق أنظمة فنية لحماية البيانات المخزنة مع الزام العاملين في أي نظام معلوماتي بحفظ كل العمليات المنطقية التي تجري على الأجهزة لمدة لا تقل على 90 يوما) ، وهو ما يعني ان الاتفاقية تشترط مستوا معيناً للكفاء الفنية في العمل بهذه التقنية ، مما يعني اننا نحتاج إلى برنامج وطني متكامل لرفع مستوى كفاءة العمل بهذه التقنية قبل الحديث عن امكانية تطبيق هذه المعاهدة.

## ثالثا : التنظيم التشريعي للوثائق الالكترونية

استجابت العديد من دول العالم الى الاتجاه السابق واعترفت بحجية المستندات الالكترونية في الاثبات ومن ثم الى اعتبارها محلا لجريمة التزوير وقد كانت المملكة الاردنية سباقة في ذلك حيث اصدرت قانون الاوراق المالية المؤقت رقم 23 لسنة 1997 الذي نص في المادة 2/24 على ان تعتبر القيود المدونة في سجلات البورصة و حساباتها سواء كانت مدونة يدويا او الكتروني ا او أي وثائق صادرة عنها دليلا على تداول الاوراق.

اما بالنسبة لتجريم تزوير الوثائق الالكترونية فقد كان القانون الفرنسي رقم 19 الصادر في يناير 1988 اولى التشريعات التي جرمت تزوير المستندات المعلوماتي فنص في المادة 5/462 على أن ( كل من ارتكب افعالا تؤدي الى تزوير المستندات المعلوماتية ايا كان شكلها باي طريقة تؤدي الى حدوث ضرر للغير فإنه يعاقب بالسجن من سنه الى خمس سنوات وغرامه لا تقل عن 20.000 فرنك ) ونصت الفقرة السادسة من ذات المادة على معاقبة كل من استخدم بتبصير المستندات المعلوماتية المزورة طبقا للفقرة السابقة ، ولم يكتف المشرع الفرنسي بذلك بل انه نص على امكانية ارتكاب جريمة التزوير خطا لان التغيير والتحريف للمعلومات المخزنة خطأً وإن كان غير متصور في المستندات والوثائق التقليدية الا انه كثيرا ما يحدث في المجالات المعلوماتية لان الدخول الى الانظمة المعلوماتية لا يحدث دائما بشكل متعمد فمن الممكن ان يحدث بشكل غير معتمد نتيجة الدخول الخاطئ إليه وهو ما يجب النص عليه في تجريم التزوير في المستندات المعلوماتية.

اما القانون العربي النموذجي فقد نص على أن كل من غير في البيانات المخزنة في المستندات المعالجة آليا أو البيانات المخزنة في ذاكرة الحاسب الآلي أو على شريط أو اسطوانة ممغنطة أو غيرها من الوسائط التي يعاقب عليها الانون وهو متروك لكل دولة على حدة كما نصت المادة 8 منه على تجريم استخدام المستندات المعالجة آليا مع العلم بتزويرها .

تجدر الإشارة إلى أن كل حالات السرقة والاحتيال تتم عن طريق تزوير البيانات لنجد أننا أمام حالة من حالات تعدد الجرائم فالأمثلة التي سبقت الإشارة إليها في الفقرة الخاصة بالسرقة سواء كانت بتصميم برنامج معد خصيصا إو عن طريق إجراء عمليات تحويل غير مشروعة للأرصدة بخلق حسابات دائنة وهمية كلها لا تتم إلا بتزوير في البيانات المخزنة آليا لنجد ان معظم الحالات يتحقق فيها التعدد المعنوي للجرائم خاصة مثل التلاعب الذي يتم في الأرصدة المصرفية لان عمليات التحويل غير المشروعة تتم عن طريق تعديل في البيانات والأسماء او تعديل في البرامج المعلوماتية المعالجة لهذه البيانات.

فإذا كان السلوك الإجرامي في هذه الحالة متمثلا في تعديل البرامج و البيانات يترتب عليه تحويلات مالية غير مشروعة فإن السلوك او الفعل يظل واحدا يتحقق به اكثر من نموذج تجريمي في هذه الحالة وهو ما يوجب تطبيق احكام التعدد المعنوي والارتباط بين الجرائم.

تجدر الاشارة الى ان هذا التوسع في تفسير مفهوم الوثيقة لا يغني عن ضرورة تدخل المشرع لمواجهة التزوير المرتكب بالحاسب الالي على المستندات والوثائق الالكترونية لان المسالة تحتاج اولا الى الاعتراف بحجية هذه المستندات الالكترونية في الإثبات قبل تجريم تحريفها ، بالاضافة الى ان تجريم التعديل في هذه البيانات يجب أن يخضع لعقوبات أشد من عقوبة التزوير التقليدية نظرا لاختلاف حجم الضرر والخسائر الناتجة عن تحريف هذه البيانات وتزويرها.

وقد نصت اتفاقية بودابست في المادة 7 على بتجريم اي تبديل او محو او اخماد لأي بيانات مخزنة في اي نظام معلوماتي يؤدي إلى إنتاج بيانات غير حقيقية -in authentic data- لغرض اسعمالها لأغراض قانوية على أنها صحيحة و ذلك سواء كانت فورية القراءة من عدمها whether or not the data is directly readable and intelligible

وهو ما يقطع الجدل حول قابلية المستند للقراءة بالعين المجردة ، و اعتبار المستند الإليكتروني وثيقة قابلة للقراءة ، مشمولة بالحماية الجنائية .

يتضح لنا أن الجريمة المعلوماتية ثتير مشكلات عديدة في تطبيق النصوص القانونية الحالية ، فإن وجد النص القانوني وأمكن اعمال المطابقة بينه و بين السلوك المرتكب لا نجد العقوبة تتناسب وحجم الخسائر الناتجة عن ارتكاب مثل هذه الجريمة ،واذا امكن اعمال المطابقة وكانت العقوبة رادعة فإننا نواجه عقبة كبيرة في عمليات ضبط هذه الجرائم واثباتها لان القواعد التقليدية للإثبات وضعت لتواجه سلوكا ماديا يحدث في العالم الفيزيائي physical world , ولا تتناسب لإثبات جريمة مرتكبة في عالم اليكتروني أو فضاء سيبراني افتراضي غير ملموس يتكون من ذبذبات والموجات غير المرئية. وهو ما يحتم ضرورة التدخل التشريعي لتنظيم هذه المسألة عنطريق الاعتراف لقوة المستندات الإليكنروني في الإثبات ،و اعتبارها من قبيل الوثائق قبل النص على تجريم تزويرها أو التعديل فيها و تحريفها حسب الأحوال.

## المبحث الثاني:

## التحديات الإجرائية للجريمة الواقعة على المواقع الإلكترونية

اتضح لنا من الفصل السابق أن الجريمة الواقعة على المواقع الإلكترونية ترتكب باستخدام التقنية المعلوماتية مما يعني أنها ترتكب في فضاء افتراضي مفرغ cyberspace ، سواء ارتكبت عبر شبكة الإنترنت أم في داخل نطاق ذات المؤسسة التي يتم الاعتداء عليها، أو ارتكاب الجريمة من خلالها، و تعرضنافي الفصل السابق أيضاً إلى المشكلات الموضوعية التي تثيرها هذه الجرائم في تطبيق القواعد التقليدية لقانون العقوبات الذي صيغت جل نصوصه ونظمه الأساسية لتواجه سلوكاً مادياً يرتكب في عالم مادي ملموس، فإذا كان ذلك هو حال القواعد الموضوعية للتجريم و العقاب ، فما هو حال القواعد الإجرائية لهذا الفرع من القانون الجنائي ؟ وهو ذلك الفرع الذي يتأسس في كل النظم القانونية المختلفة على مبدأ دستوري هو الشرعية ،أي شرعية التجريم و العقاب ، الذي تنبثق عنه قاعدة الشرعية الإجراءائية ، و ما يميز هذه الجريمة هو أنها ترتكب في مسرح اليكتروني أو مجال مفرغ يختلف كلياً عن المسرح التقليدي الذي ترتكب فيه الجريمة حيث يتم الاستدلال عليها وضبطها و اثباتها بالوسائل التقليدية المتمثلة في اجراءات الاستدلال و التحقيق ، فهي اجراءات صيغت لضبط و اثبات جرائم ترتكب في عاالم ملموس مادياً ، يلعب فيه السلوك المادي الدور الأكبر و الأهم، وهنا يثور التساؤل حول مدى صلاحية هذه الإجراءآت لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس ؟ أما إذا ارتكبت الجريمة عبر الشبكة العنكبوتية الدولية (الانترنت) تزداد العقبات القاونية صعوبة ، فلا نكون أمام مشكلات اجرائية تخص ضبط الجريمة و اثباتها فحسب ، بل نجد انفسنا أمام مشكلة أكثر تعقيداً تتمثل في تحديد الاختصاص القضائي المرتبط بتحديد القانون الواجب التطبيق على هذه الجريمة ، فقواعد الاختصاص القضائي التقليدية صيغت لكي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة ، وهي قواعد ترتكز على مبدأ الإقليمية ، وهو ما يرتبط بسيادة الدولة على إقليهما ، فلا يكون الخروج عليه بقبول اختصاص قضائي أجنبي إلا في حالات استثنائية يجب النص عليها صراحة ، وهنا تثور امامنا مدى امكانية الاعتماد على هذه القواعد لتحديد الاختصاص القضائي لجريمة ترتكب في مجال تنعدم فيه الحدود الجغرافية ، وكثيرا ما يكون مرتكبيها في بلاد مختلفة و من حنسيات متعددة، و كثيرا ايضا ما يتعلق السلوك الاجرامي

باكثر من دولة : الدولة التي ارتكب فيها السلوك و الدولة التي تم فيها القبض على الجاني و تلك التي حدثت فيها النتيجة الاجرامية و هو ما يتطلب منا التطرق الى مشكلات ضبط الجريمة المعلوماتية و اثباتها في مطلب أول قبل التطرق إلى الحديث عن مشكلات الاختصاص بنظر الجريمة المعلوماتية في مطلب ثانٍ .

## المطلب الأول : ضبط الجريمة المعلوماتية و اثباتها

يعتمد ضبط الجريمة و اثباتها في المقام الأول على جمع ألادلة التي حدد المشرع وسائل اثباتها على سبيل الحصر ، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية ، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية ، و تتمثل في وسائل الاثبات الرئيسية في و في المعاينة و الخبرة و التفتيش و ضبط الأشياء المتعلقة بالجريمة ، أما غيرها من وسائل الاثبات كالاستجواب و المواجهة و سماع الشهود فهي مرحلة تالية من إجراءات التحقيق و جمع الأدلة ، ولما كنا بصدد تناول الجريمة المعلوماتية و ما تثيره من مشكلات إجرائية ، فسنتعرض للمشكلات القانونية التي يثيرها اثبات هذه الجرائم دون غيرها من الاجراءات كالاستجواب و المواجهة و سماع الشهود ، لأن هذه الأخيرة تتم في مواجهة البشر ، أما المعاينة و الخبرة و التفتيش ،فهي إجراءات فنية محلها الأشياء لا الافراد وهو ما يهمنا في هذا الموضوع .
لما كان ذلك فسوف نقسم هذا المطلب إلى فرعين ، نتناول في الأول الحديث على حجية المخرجات الاليكترونية في الاثبات الجنائي ،قبل أن ننتقل لتناول اشكاليات المعاينة و الخبرة في المسائل المعلوماتية في الفرع الثاني.

### الفرع الأول: حجية المخرجات الإليكترونية في الاثبات:

تخضع المحررات كغيرها من الأدلة التي تقدم أثناء نظر الدعوى إلى تقدير المحكمة حيث يسود مبدأ حرية القاضي في تكوين عقيدته، وهو ما يختلف فيه القاضي المدني حيث يتقيد هذا الاخير بطرق معينة في الاثبات ، فالقاضي الجنائي له مطلق الحرية في تقدير الدليل المطروح أمامه ،وله أن يأخذ

به أويطرحه ولا يجوز تقييده بأي قرائن أو افتراضات[1] .

ولما كانت المحررات أحد ألأدلة التي قد يلجأ اليها القاضي في الاثبات فهي تخضع كغيرها من الادلة لتقدير المحكمة ، الا إذا كان الاثبات متعلقاً بمواد غير جنائية ، ففي هذه الحالة يكون على القاضي الجنائي أن يتقيد بطريق الاثبات المحددة في ذلك الفرع من القانون مثال ذلك حق الملكية في جريمة السرقة ، والعقود التي تثبت التصرف في الحق في جريمة خيانة الامانة أو صفة التاجر في جريمة التفالس بالتدليس[2].

وهنا تثور مشكلة مدى حجية المخرجات الاليكترونية في الاثبات الجنائي في هذه الحالات ، فللمخرجات الاليكترونية انواع مختلفة ، فهي تتنوع بين مخرجات ورقية ، و مخرجات لاورقية و هي المعلومات المسجلة على الأوعية الممغنطة كالاشرطة و الاقراص المرنة Floppy Disk القرص الصلب Hard Disk وغيرها من الاوعية التي اصبحت في تطور مستمر حتى وصلت الى اقراص الflash discs التي اصبحت تتميز بسعات كبيرة للتخزين، خاصة أنه تواجهنا مشكلة اساسية تتعلق بصعوبة التمييز بين المحرر و صورته أو بين الاصل و الصورة ، ذلك لأننا نتعامل مع بيئة اليكترونية تعمل بالنبضات و و الذبذبات و الرموز و الأرقام وهو ما يستحيل معه تطبيق القواعد الخاصة بالمحررات العرفية [3]

ولما كان المشرع لا يزال عازفاً عن التدخل التشريعي في هذه المسألة فلا نجد بداً من تطبيق القواعد العامة في هذا الصدد ، ولما كان ذلك لايزال يعتمد على مبدأ سيادة الدليل الكتابي على غيره من الادلة ولا يجوز الاعتماد على الدليل غير الكتابي في غير المسائل الجنائية ،الا على سبيل الاستئناس ، ولا يخفى ما يؤدي ذلك من تقييد للقاضي الجنائي لأن الإثبات في المسائل الجنائية كثيراً ما يعتمد على مسائل غير جنائية ، وهو ما سبقت الاشارة اليه عند تناول جريمة التزوير في هذا البحث التي اعتمدت على مدى اعتبار هذه الاوعية من قبيل المستندات او المحررات موضوع جريمة التزوير ،

---

**1**. مأمون سلامة – الاجراءات الجنائية في التشريع الليبي – ج 2ط2000- منشورات المكتبة الجامعة – ص151.

**2**. مأمون سلامة – المرجع السابق – ص160

**3**.احمد شرف الدين- حجية الرسائل الاليكترونية في الاثبات – شبكة المعلومات القانونية العربية – East Law .com - 2007

فمواجهة الجرائم المعلوماتية لا تتأتى الا عن طريق نظام قانوني متكامل أهم عناصره التدخل لضبط

المعاملات و التجارة الاليكترونية وضفاء الحجية القانونية على المستندات الاليكترونية شأنها شأن المستندات الورقية ، حتى يتاح للقاضي الجنائي الاعتماد عليها و اتخاذها دليلاً جنائياً ، كغيره من الادلة ، وقد كان المشرع التونسي من السباقين بين أقرانه على المستوى العربي في هذا المجال، حيث صدر في تونس قانون التجارة و المعاملات الاليكترونية الذي اعترف للمستندات الاليكترونية سنة 2000 بحجيتها في الاثبات ، كما أصدرت امارة دبي قانون التجارة الاليكترونية سنة 2002 ، وتبعهما بعد ذلك المشرع المصري سنة 2004 الذي اصدر قانون نظم التوقيع اليكتروني ، وتجدر الاشارة في هذا الصدد إلى القانون العربي النموذجي السابق الاشارة اليه سنة 2003 ، وكل هذه القوانين اعطت للمستند الاليكتروني ذات الحجية التي يتمتع بها المحرر الورقي ، تجدر الاشارة ايضاً إلى أن لجنة الأمم المتحدة للقانون التجاري الدولي United Nation Commission on International Trade Law (UNCITRAL) على هذه الحجية و قد كان ذلك سنة 2000 أما القانون العربي النموذجي فنص في المادة الأولى منه على تعريف الكتابة بأنها كل(عملية تسجيل للبيانات على وسيط لتخزينها ) ، و المقصود بالوسيط في هذه الحالة هو الوسيط الاليكتروني لأن الوسيط الورقي المتمثل في الأوراق التقليدية لا يحتاج إلى تعريف ، وإن كنا نتحفظ على استخدام عبارة الوسيط دون تحديده بالاليكتروني ، مادام الأمر متعلقاً بالتجريم و العقاب، أما المادة 6 من قانون الاونسترال النموذجي السابق الاشارة اليه .

اذا كان المشرع التونسي يعد سباقاً إلى اللحاق بهذا التطور التشريعي فإن المشرع السنغافوري أصدر قانوناً للاثبات أقر فيه حجية المستندات المعلوماتية في الاثبات منذ سنة 1997م وهو ما يبين مدى تأخرنا في مواكبة هذا التطور.

## الفرع الثاني : الخبرة و المعاينة في الجرائم المعلوماتية

تعتبر كل من الخبرة و المعاينة أكبر العقبات التي تواجه الاثبات في الجرائم المعلوماتية، فالمعاينة اجراء بمقتضاه ينتقل المحقق الى مكان وقوع الجريمة ليشاهد اثارها بنفسه ، فيقوم بجمعها وجمع أي شيء يفيد في كشف الحقيقة ، وتقتضي المعاينة اثبات حالة الأشخاص و الأشياء الموجودة بمكان الجريمة و رفع الآثار المتعلقة بها كالبصمات و الدماء و غيرها مما يفيد التحقيق ، و المعاينة تكون شخصية إذا تعلقت بشخص المجني عليه ، أو مكانية اذا تعلقت بالمكان الذي تمت فيه الجريمة ،

ووضع الشهود و المتهم و المجني عليه ، أما المعاينة العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة وقد يقتضي الامر الاستعانة بخبير للتعرف على طبيعة المادة او نوعها إذا كان ذلك يحتاج لرأي المتخصص ، وفي هذه الحالة يتم ارسال هذه الاشياء الى الخبير لنكون امام بصدد اجراء آخر من اجراءات التحقيق و هو الخبرة ، فالخبرة هي أحد أهم وسائل جمع الأدلة ، يلجأ اليها المحقق عند وجود واقعة مادية أوشيء مادي يحتاج االتعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الاثبات.

يثور التساؤل هنا عن مدى امكانية معاينة الجريمة المعلوماتية ، من حيث انتقال المحقق لأي مكان ليثبت حالة الامكنة و الاشياء و الاشخاص ووجود الجريمة مادياً ، فهل يكون للجريمة المعلوماتية وجود مادي يمكن للمحقق معاينته؟ نجد في هذه المادة أن المشرع سن هذا النص لضبط جريمة لها وجود مادي محسوس في العالم الخارجي، وما يؤكد ذلك هو أن القانون 09-04 إدراك المشرع بمدى الصعوبة التي تواجه المحققين والقضاة في البحث عن الدليل الإلكتروني ،وهنا نصطدم بالعقبة الاساسية أمام معاينة الجريمة المعلوماتية التي ترتكب داخل الفضاء المعلوماتي أو السيبراني ، فالمحقق في هذه الحالة يتعامل مع بيئة مليئة بالنبضات الاليكترومغناطيسية و البيانات المخزنة داخل نظام معلوماتية شديدة الحساسية ولا يتعامل مع أوراق او اسلحة أو اشياء قابلة للربط وهو ما يؤكد القواعد الاجرائية التقليدية سنت لتواجه سلوكاً ماديا يرتكب بواسطة الات و ادوات قابلة للربط و التحريز .

أما السلوك الاجرامي في الجريمة الواقعة على المواقع الإلكترونية، فهو عبارة عن بيانات مخزنة في نظام معلوماتي يتطلب اثباته انتقال محقق متخصص حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الاسطوانة الصلبة الخاصة بالجهاز ، ويجب على المحقق أو ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة. وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الانترنت ،ولكي ينجح المحققون في عملهم يجب أن يقتفوا أثر الاتصالات منذ الحاسب المصدر إلى الحاسب أو المعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل ودولة. كما يقتضي ذلك ايضاً ان يعمل المحقق على الوصول إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات. من أين صدرت؟ ومن الذي يحتمل إجراؤها ، بالاضافة الى ضرورة المام المحقق بالحالات التي يكون عليه فيها

التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الاسطوانة الصلبة للحاسب ، والاوقات التي يستخدم فيها برامج استعادة المعلومات التي تم الغاؤها[1]

فالمحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملماً بمهرات هذه التقنية ، مثل القدرة على استخدام براج Time stamp وهي البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الاجرامي، لأن ذلك لا يكون متاحاً في جميع الانظمة المعلوماتية ،أما الخبير ففي هذه الحالة يجب ان يكون ملماً بمهارات تحليل البيانات و مهارات التشفير cryptanalysis skills التي تتيح له فك الرموز استعادة البيانات لملغية .

ولما كانت الجرائم ترتكب عبر الشبكة الدولية فقد نصت المادة 23 على أن (تتعاون كل الأطراف، وفقاً لنصوص هذا الفصل، على تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وكذلك بشأن الحصول على الأدلة في الشكل الإلكتروني لمثل هذه الجرائم) كما نصت المادة 30 من الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على : أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله. كما أشارت المادة 31 إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف

---

**1.** Recommandations sur le dépistage des communications électroniques transfrontalière dans le cadre des enquêtes sur les activités criminelles www G8 Mont tremblant Canada 21 mai 2002. اشار اليه أ.د. صالح أحمد البربري دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية -الموقعة في بودابست في 2001/11/3- www.arablawinfo.com@

عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة 29 من الاتفاقية .

وهو ما نصل معه الى حقيقة مؤداها اننا نواجه اليوم اخطر مظاهر العولمة ، فالتعاون الدولي في المجال الجنائي لم يعد مقتصراً على نظام الانتربول ، فأصبح على الدولة أن تستخدم بروتوكولات موحدة لنظم التخزين و الحماية المعلوماتية كما حدث على مستوى الاتصالات الهاتفية ، لأن التعاون بين دولة واخرى سوف يتم بين أجهزة الخبرة الجنائية بشكل مباشر وبطريقة متشابكة ، وهو مانصل معه إلى ان تطوير البنية التحتية المعلوماتية لأي دولة اليوم اصبح ضرورة ملحة ، ومطلباً أساسياً قد يترتب على غيابه انعزال الدولة وصيرورة نظامها المعلوماتي – اذا كان متواضعاً – مباحاً لمجرمي المعلوماتية .

نخلص من كل ما تقدم إلى أن الخبرة و المعاينة الجنائية في الجرائم المعلوماتية اليوم تحتاج إلى ادارة خاصة يعمل بها متخصصون في أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية ، وهوما يتطلب انشاء ادارة خاصة للخبرة و المعاينة في الجرائم المعلوماتية ، ولا يجب الاكتفاء بمجرد تدريب القائمين على إدارة الخبرة الجنائية ، أما رجال القضاء و النيابة والضبطية القضائية فلا شك أنهم يحتاجون للتدريب على استخدام مهارات الحاسب لآلي و و الموسوعات القانونية التي تتطلب ربط كافة المؤسسات القضائية بقواعد بيانات قانونية مثل أحكام المحاكم و القوانين المختلفة ، لتوفير امكانية استخدام موسوعات القوانين و مجموعات الأحكام القانونية العربية المختلفة و تعليمات النائب العام ، لرفع مستوى الكفاءة القانونية لدى رجال القضاء و النيابة العامة .

## المطلب الثاني : الاختصاص بنظر الجريمة المعلوماتية

خلصنا من المبحث السابق إلى عدم كفاية القواعد التقليدية للخبرة و المعاينة ، وعدم ملاءمتها لاثبات الجرائم المعلوماتية ، فهل تستجيب القواعد الخاصة بتحديد نطاق تطبيق القانون من حيث المكان ، فكيف يمكن تحديد مكان وقوع الجريمة المعلوماتية ؟ واذا كانت هذه الجريمة ترتكب في مجال افتراضي غير محدد جغرافياً فهل يمكن ربط هذه الجريمة بدولة ما دون اخرى ؟ لما كان ذلك فإن الاجابة على هذا التساؤل تتطلب ضرورة الحديث عن لامركزية الفضاء امعلوماتي في فرع أول ، قبل تناول التعاون الدولي لملاحقة الجريمة المعلوماتية في الفرع الثاني

### الفرع الأول : لامركزية الفضاء و عالمية الجريمة المعلوماتية .

فقدت الحدود الجغرافية كل اثر لها في الفضاء الشبكي او الآلي ، فهو لا يعترف بالحدود الجغرافية حيث يتم تبادل البيانات في شكل حزم الكترونية توجه الى عنوان افتراضي ليس له صلة بالمكان الجغرافي ، فهو فضاء ذو طبيعة لا مركزية DESSENTRALI ZED NATURE و يمكن اجمال اهم خصائصه في عدم التبعية لاي سلطة حاكمة .فالفضاء الالي : نظام الكتروني معقد لانه عبارة عن شبكة اتصال لا متناهية غير مجسدة و غير مرئية متاحة لاي شخص حول العالم و غير تابعة لاي سلطة حاكمة فالسلوك المرتكب فيها يتجاوز الاماكن بمعناه االتقليدي له وجود حقيقي وواقعي لكنه غير محدد المكان لكنه حقيقة واقعا .

فالشبكة عالمية النشاط و الخدمات لا تخضع لاي قوة مهيمنة الا في بدايتها حيث كان تمويل هذه الشبكة حكوميا يعتمد على المؤسسة العسكرية الامريكية، أما الان فقد اصبح التمويل ياتي من القطاع الخاص حيث الشركات الاقليمية ذات الغرض التجاري التي تبحث عن كافة السبل للاستفادة من خدماتها بمقابل مالي [1].

والجريمة المرتكبة عبر شبكة الانترنت جريمة تعبر الحدود و القارات ،و هو ما يدرجها ضمن موضوعات القانون الجنائي الدولي[2] ، الذي يقابل القانون الدولي الخاص في القانون المدني ، و هو

---

1. منير الجنبهي – ممدوح الجنبهي – صراخ الانترنت وسائل مكافحتها – المرجع السابق –ص 9
2. فتوح الشاذلي – القانون الدولي الجنائي – دار المطبوعات الجامعية – الاسكندرية – 2001 – ص 34

ذلك الفرع من القانون الذي يحدد ضوابط مجالات التعاون الدولي في مجال مكافحة الجريمة بالتزام الدول الموقعة على الاتفاقيات بالعمل بقتضاها في مكافحة الجريمة .

و قد ازدادت اهمية القانون الجنائي الدولي بعدما تطورت الجريمة المنظمة في وقت تقلص فيه المفهوم التقليدي للسيادة ، حيث اتسع نظام المعاهدات الدولية لمكافحة الجرائم العابرة للحدود فالجانب الدولي للجريمة المعلوماتية لا يعد عنصرا من عناصرها كما هو الحال في الجريمة الدولية بل يعد هو نطاقها المكاني .

ان القواعد العامة التي تحكم نطاق تطبيق النصوص الجنائية – التي تتمثل في مبدأ اقليمية النص الجنائي و الاستثناءات الواردة عليه – تقتضي تطبيق النص الجنائي على كل الجرائم الواقعة في اقليمه ، الا في احوال خاصة نص عليها المشرع في المواد 4 و ما بعدها تبين حالات يطبق فيها القانون الليبي على جرائم ارتكبت خارج اقليمه .

## الفرع الثاني : التعاون الدولي لملاحقة الجرائم المعلوماتية :

يعتمد النظام القانوني السابق على جريمة ترتكب في مكان قابل للتحديد الجغرافي ، اما الجريمة المعلوماتية فهي جريمة ترتكب في مسرح غير قابل للتحديد الجغرافي، الا انه يضم اكبر تجمع إنساني يتميز بارتباط و تشابك معقد ، و تتمثل اهم خصائصه في خلق آليات خاصة لفرض الالتزامات و الاذعان لها مثل قطع الاتصال على مخترقي بعض القواعد او طردهم من المنتديات ، لكن هذا التجمع الانساني الضخم يفتقر الى المعايير الاخلاقية المشتركة .

و هو ما حدا المجلس الاوروبي الى عقد اتفاقية بوداست COUNCILالسابق الاشارة اليها ، و التي قدمت صورا لمكافحة هذه الجرائم و نصت المادة 22 منها على "أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التي يراها لازمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقاً لما هو وارد في المواد من 2 إلى 11 من الاتفاقية الحالية عندما تقع الجريمة :

أ- داخل النطاق المحلي للدولة :

ب- على ظهر سفينة تحمل علم تلك الدولة.

ج- على متن طائرة مسجلة في هذه الدولة.

د- بواسطة أحد رعاياها، إذا كانت الجريمة معاقباً عليها جنائياً في المكان الذي ارتكبت فيه أو إذا كانت الجريمة لا تدخل في أي اختصاص مكاني لأي دولة أخرى.

ولكل طرف أن يحتفظ لنفسه بالحق في عدم تطبيق، أو عدم التطبيق إلا في حالات وفي ظل شروط خاصة، قواعد الاختصاص المنصوص عليها في الفقرة الأولى (ب و د) من هذه المادة أو في أي جزء من هذه الفقرات.

و تنص الفقرة 4 من المادة على عدم استبعاد اي اختصاص ينعقد للقضاء الوطني طبقا للقانون المحلي الفقرة 5 تنص على انه في حالة حدوث تنازع في الاختصاص فان يجب ان يتم حله بالتشاور بين الدول الاطراف حول المكان الاكثر ملائمة . كما افردت الاتفاقية بندا خاصا لضرورة التعاون بين الدول.

و لم ينص القانون العربي النموذجي بشان الجرائم المعلوماتية على اي قواعد لتحديد الاختصاص بنظر هذه الجرائم. فان كان الفقه الجنائي اليوم قبل فكرة تطبيق القانون الاجنبي لمواجهة الجريمة عبر الوطنية ما أظهر ضرورة تجاوز فكرة تلازم الاختصاص الجنائي القضائي و التشريعي فيلزم من باب اولى قبول هذه الفكرة و التوسع فيها بالنسبة لجرائم ترتكب في الفضاء السيبراني الذي يتجاوز الحدود و القارات ، و بذلك نصل الى ضرورة التفكير في وضع ضوابط اسناد جنائية لتحديد الاختصاص الموضوعي و الاجرامي بعد ان تصنف الى فئات مختلفة تشكل كل فئة فكرة مسندة تتضمن المصالح الواجب حمايتها جنائيا على المستوى العالمي لوضع ضوابط اسناد تشير الى القانون الواجب التطبيق.

الا أن هذه القواعد يجب ان تتم صياغتها في اطار اتفاقات دولية لأن الجريمة الدولية لا يمكن مواجهتها إلا بالتعاون الدولي ، و هو اهم ما جاء في اتفاقية بودابست بشكل يسمح بتبادل التعاون سواء كان ذلك على مستوى جمع الأدلة أو تسليم المجرمين وهو ما يعني ان المجتمع الدولي مقبلا على توسع في مجال التعاون القضائي الذي يتوقع أن يتم بين الاجهزة القضائية و و الامنية بشكل مباشر نظراً لأن عامل الوقت في حفظ الادلة المعلوماتية سوف يكون حرجاً ومتطلباً لسرعة الانجاز.

# الفصل الثاني :
# جهود المشرع الجزائري للحد من الجريمة

# الفصل الثاني :

# جهود المشرع الجزائري للحد من الجريمة الواقعة على المواقع الإلكترونية

## مقدمة

لقد صاحب التطور الذي شهده العالم في الفترة الأخيرة من القرن الماضي في شتى المجالات تطورا هاما وخاصة في مجال الاتصالات فيما يتعلق بالتقنيات المعلوماتية والتي تزايد التعامل بها و ذلك لسرعتها ولما توفره من وقت وجهد .

ولقد كانت المعلومات المتولدة عن التفاعلات البشرية محدودة إلى حد كبير ولم يمثل حجمها أي مشكلة أمام جمعها وتخزينها , ولكن مع تقدم البشرية , تزايد كم المعلومات وأصبحت الطرق التقليدية لجمع المعلومات عاجزة عن تلبية الاحتياجات بكفاءة وفعالية , وأصبح من الضروري وجود وسائل أكثر تطورا لحماية وجمع هذه المعلومات.

فظهر ما يعرف بالآلات الحاسبة في القرن 17 ابتكرها كل من **بليز باسكال** و **ويلهلم ليبينيز** , ولم تكن مبرمجة[8] ويعد نول الحياكة الذي ابتكره **josephmarie jacquard** في نهاية القرن 18 جد الآلات المبرمجة , حيث يمكن بر مجته بفضل بطاقات مثقبة تحدد رسمه النسيج في عام 1860.

وفي الثلاثينات تصور **شارل باباج** في 1822[9] ( وهو عالم رياضيات انجليزي ) آلة للقيام بالعمليات الحسابية بصورة آلية , فهذه الآلة دلت على البنية الهندسية للحاسب الحديث , وبعد عقد من الزمن , رسمت عالمة الرياضيات **ادالو فلاس** طرائق حساب لهذه الآلة , وفي عام 1937 صمم عالم المنطق البريطاني **آلان تورينغ** آلة غير مادية تتكون من شريط يتحرك عليه قلم يمكنه من كتابة إشارات مختارة أو محوها.

**1**- د . محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديد النشر ،جامعة الإسكندرية ،2004 ، التهميش 2 ، 13 ص .

**2** – عفاف شمدين ، الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات ، الطبعة 1 ، دمشق ، 2003 ، ص 68 .

-و أثناء الحرب العالمية [1] ظهرت الآلات الرائدة الحقيقية للحاسبات وكانت الآلات ضخمة ومخصصة لإجراء العمليات الحسابية العسكرية وفي عام 1949 ادخل عالم الرياضيات **جون فون فيومان** البرامج المسجلة في الاواكر و ليس على بطاقات مثقبة.

وظهر ما يسمى ب "الحاسب الآلي" أو الكمبيوتر وهو جهاز قادر على استيعاب كم هائل من المعلومات ويمكنه استرجاعها بسرعة فائقة ودقة متناهية وتزايد استخدامها و استهلاكها وتطورها وأصبحت مصدر قوة اقتصادية و سياسية لمن يحسن استعمالها ، هذا من جهة .

- من جهة أخرى و منذ حوالي 50 سنة و بعد غزو روسيا للفضاء و بدء السباق نحو التسلح النووي في عهد الحرب الباردة طرح في أمريكا بقوة مشكل كيفية ضمان استمرارية الاتصالات بين السلطات الأمريكية في حال نشوب حرب نووية ووضع القوات الأمريكية على استعداد لأي اعتداء عسكري[2]

و على هذا كلفت شركة حكومية تدعى RND بدراسة هذه المسالة الإستراتيجية و محاولة إيجاد حل لها و دارت الدراسة حول وجوب بناء شبكة لا مركزية

" DISTRIBUTED COMMUNICATION NET WORK "

تعتمد مبدأ تحويل الرسائل الالكترونية و تقسيمها إلى وحدات تسمى الحزم PAKETS يمكن للمرسل إرسالها عبر مجموعة من العقد NODES ثم تجمع هذه الحزم لدى المستقبل لتشكل رسالة .

و في عام 1969 نفذت وزارة الدفاع الأمريكية مشروع هذه الشبكة عمليا و أسمتها " اربانت"[10][4]

ADVENCED RESEARCH PROJECT AGENCY ARPANET

إذ ربطت هذه الشبكة مجموعة من الجامعات الأمريكية عبر أربعة عقد مكونة من أجهزة كمبيوتر عملاقة , و تجلت فائدتها في نقل المعلومات بسرعة هائلة بين تلك الأجهزة .

---

**1**. عام 1974 استخدم فين سيرف كلمة انترنت لأول مرة في ورقة قدمها إلى مؤتمر حول بروتوكولات التحكم في الاتصال .

**2**. منير و ممدوح محمد الجنيهي ، امن المعلومات الالكترونية ،دار الفكر الجامعية ، الإسكندرية ، 2006 ، ص 7 .

و مع زوال خطر الحرب , بدأت الدعوى للاستعمال السلمي لهذه التقنيات وانقسم المشروع إلى شبكتين إحداهما احتفظت باسمها الرئيسي "اربانت" وكذا بغرضها الذي انشات من اجله , و الثانية سميت "ميلنت" و خصصت للاستخدامات السلمية المدنية .

فأصبحت هذه التقنيات في متناول الجميع خاصة بظهور الشبكة المعلوماتية الدولية على يد مهندس الاتصالات الانجليزي TIM BERNERRS LEE[1] .

و منذ ذلك الوقت و عدد مستخدمي الانترنت في تزايد مستمر , ولم يقتصر استعمال هذه التقنيات في الأبحاث العسكرية والجامعية بل تعدتها إلى الأعمال التجارية و هذا في أوائل السبعينات عبر ما يسمى ب TELNET .

و في سنة 1972 ظهرت خدمة البريد الالكتروني التي ابتكرتها شركة BBN إذ قدمه احد مبرمجيها "راي توملينسون" أول برنامج للبريد الالكتروني E-MAIL [2] ، الذي أصبح أهم وسائل الاتصالات عبر الانترنت.

و في أواخر السبعينات كان بإمكان الناس حول العالم الدخول عبر الشبكة في نقاشات حول مواضيع متفرقة عبر ما يسمى بالمجموعة الإخبارية " NEWS GROUP"، و مع ظهور شبكات أخرى تقدم خدمات E-MAIL ونقل الملفاتFTP ، إضافة إلى NSF NET [3].

التي طورتها ، بدأ انتشار استخدام مصطلح الانترنت–في أوائل الثمانينات – على أنه مجموعة من الشبكات المختلفة التي ترتبط فيما بينها بواسطة مجموعة من البروتوكولات التحكم بالإرسال و التي طورتها وزارة الدفاع الأمريكية لإتاحة الاتصالات عبر الشبكات مختلفة الأنواع .

و مع بداية التسعينات ظهرت واجهة تستخدم النصوص و تعتمد القوائم "MENUS " للوصول

---

**1**. نبيلة هروال ،الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دار الفكر الجامعية ، الطبعة 1، الإسكندرية ،2007 ،ص8 .

**2**. منير ممدوح محمد الجنيهي ، المرجع السابق ، ص 08 .

**3**. NSF = NATIONAL SCIENCE FOUNDATION

إلى المعلومات عبر العالم وتدعى هذه الواجهة" COPHER " و لكن الثورة الحقيقية في عالم الانترنت كانت ظهور شبكة الويب العالمية [1] WWW وهي خدمة سهلة تعتمد في عرض المعلومات على النصوص و الصور والصوت و الفيديو مما ساعدها على الانتشار ومضاعفة سرعة خطوط الاتصالات و في هذه الفترة ظهرت الشركات الموفرة لخدمة الانترنت عبر شبكة الاتصال الهاتفي و توالى ظهور هذه الشركات منها ما يقدم بحوث و منها ما يقدم لغات لبرمجة و تطوير المواقع , إضافة لظهور التجارة الالكترونية (التعاملات المالية عبر الشبكة) .

– وبالموازاة مع ذلك ، ظهرت تقنيات مستحدثة و متقدمة مثل : CD-DVD إضافة لظهور منافذ استثمارية جديدة تهتم بتصنيع هذه الآلات كما أنتجت علاقات قانونية في مجالات فروع القانون المختلفة خاصة القانون الجنائي .

ورغم ما تقدمه هذه التقنيات من خدمات هامة ومفيدة لأقصى الحدود في جميع القطاعات خاصة ما يتعلق بنقل المعلومات وتنظيم المعاملات بين الأفراد .إلا أنها تعتبر سلاح ذو حدين فهي من جهة تسهل رفع كفاءات وقدرات الإنسان والحفاظ على أمنه وراحته واستقراره ومن جهة أخرى فقد أدت إلى تطوير وتحديث وتسهيل استغلالها لارتكاب جرائم لم يكن يعرفها الإنسان من قبل ,هذا ما جعلها محل اهتمام الباحثين القانونيين والمشرع والقضاة.

فقد استحدثت صور وطرق جديدة ومتطورة من الجرائم الفنية والتي تعتمد على الحاسوب كأداة لارتكابها وهي ما يسمى ب "جرائم الانترنت و الكمبيوتر".

حيث تظهر أهمية هذا الموضوع من منطلق حداثة استخدام الكمبيوتر وغلوب الصبغة العلمية التي تدخل في مجال رجال القانون .

– فمن الناحية العملية :

فان إساءة استخدام المعلوماتية بارتكاب جرائم عن بعد,تكون محلا لإثارة الإشكال في تكييف

1. WWW= WORLD WIDE WEB

الاعتداء إن كان جريمة أم لا.

كما تثير مسالة الاختصاص القضائي والقانون الواجب التطبيق على الجرائم المرتكبة عبرها.

إضافة لمشكلة تحديد الإجراءات الجزائية المتبعة في ملاحقة مرتكبيها وكيفية إثباتها.

- أما من الناحية الاقتصادية:

فان جرائم المعلوماتية تؤدي إلى التأثير سلبا على حجم التجارة الالكترونية ومبادلاتها مما يؤدي لضياع الحقوق وانتهاكها .

- اجتماعيا: يستفيد منها من لهم أموال في القيام بأعمالهم ، والإرهاب في توزيع أفكارهم.

- سياسيا: تستعملها الجماعات الضاغطة من طرف العابثين لنشر أفكارهم التي تتناسب مع مصالحهم

- نظريا: فهي تدرس مدى كفاية النصوص الجنائية لمنع مثل هذه الجرائم ومدى ردع مرتكبيها, وهل تفي الإجراءات الجنائية في تحقيق غايتها أم يلزمها تعديل؟

إن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية فرض حلها البحث في الأوضاع القانونية القائمة ومدى ملائمتها لمواجهة هذه المشاكل، ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم، فانه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا مستهجنة وعلى مستوى عال من الخطورة الإجرامية .

فما مدى إمكانية استعانة القاضي بقانون العقوبات التقليدي لتوفير الحماية لهذه القيمة الاقتصادية الجديدة ألا وهي أموال الإعلام الآلي في ظل النصوص التقليدية ؟ خاصة وان المشرع لم يكن في ذهنه وقت وضع النصوص التقليدية هذا النوع من الاستثمار الجديد، وهنا تكمن خطورة المحاولة لان القانون الجنائي له مبادئه وأصوله وعلى رأسها مبدأ الشرعية والذي يتفرع عنه مبدأي التفسير الضيق وخطر القياس في مجال التجريم .

فالإشكال المطروح: هل يستطيع القاضي الجزائي من خلال النصوص الحالية لجرائم الأموال تحقيق حماية جزائية معلوماتية دون الإطاحة بالمبادئ الراسخة التي يرتكز عليها القانون الجنائي ؟ ولهذا الغرض ارتأينا تركيز دراستنا على نقطتين أساسيتين وهما :

1 -مدى اعتبار المعلوماتية موضوع لجرائم الأموال.

مدى خضوع المعلوماتية للنشاط الإجرامي لجرائم الأموال

- **أين المشرع الجزائري من كل هذا ؟**

## المبحث الأول : من خلال النصوص التقليدية (الكلاسيكية)

### المطلب الأول: مواجهة الجريمة المعلوماتية من خلال جرائم الأموال المقررة في قانون العقوبات الجزائري

إن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية فرض حلها البحث في الأوضاع القانونية القائمة ومدى ملائمتها لمواجهة هذه المشاكل، ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم، فانه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا مستهجنة وعلى مستوى عال من الخطورة الإجرامية .

فما مدى إمكانية استعانة القاضي بقانون العقوبات التقليدي لتوفير الحماية لهذه القيمة الاقتصادية الجديدة ألا وهي أموال الإعلام الآلي في ظل النصوص التقليدية ؟ خاصة وان المشرع لم يكن في ذهنه وقت وضع النصوص التقليدية هذا النوع من الاستثمار الجديد، وهنا تكمن خطورة المحاولة لان القانون الجنائي له مبادئه وأصوله وعلى رأسها مبدأ الشرعية والذي يتفرع عنه مبدأي التفسير الضيق وخطر القياس في مجال التجريم .

فالإشكال المطروح: هل يستطيع القاضي الجزائي من خلال النصوص الحالية لجرائم الأموال تحقيق حماية جزائية معلوماتية دون الإطاحة بالمبادئ الراسخة التي يرتكز عليها القانون الجنائي ؟ ولهذا الغرض ارتأينا تركيز دراستنا على نقطتين أساسيتين وهما :

2 -مدى اعتبار المعلوماتية موضوع لجرائم الأموال.

3 -مدى خضوع المعلوماتية للنشاط الإجرامي لجرائم الأموال .

**الفرع الأول : مدى اعتبار المعلوماتية موضوع لجرائم الأموال :**

لتحديد مدى إمكانية إخضاع الاعتداءات الواردة على أموال الإعلام الآلي للنصوص التقليدية لجرائم الأموال وجب :

**أولا : مدى انطباق وصف المال على المعلوماتية :**

يقصد بالمال ألمعلوماتي الحاسوب بكل مكوناته وهو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واسترجاعها عند الطلب وهو يتكون من كيانين :

-كيان مادي

-كيان معنوي

ويضم الكيان المادي الأجهزة المادية المختلفة وهي جهاز الإدخال، جهاز الإخراج ووحدات التشغيل المركزية التي يتم من خلالها معالجة المعلومات وتخزينها و إخراجها. أما الكيان المعنوي فيشمل البرامج المختلفة التي تتحقق من خلالها قيام الحاسب بوظائفها المختلفة بالإضافة إلى المعلومات المطلوب معالجتها بالفعل [1]

فإذا كانت الأجهزة المادية للحاسبات لا تحتاج إلى نصوص خاصة لحمايتها جزائيا إذ تشملها نصوص

---

**1** – د. محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة غريب، القاهرة 1984، ص 217.

**2** – أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة للطباعة والنشر ، الجزائر 2006 .

الجرائم التقليدية ، فالأمر يختلف بصدد الكيان المعنوي لتلك الحاسبات لان جرائم الاعتداء على الأموال يشترط بشأنها عادة أن يكون موضوعها شيئا ماديا ، وطبيعة الكيان المعنوي ليس كذلك وعليه فالسؤال يطرح حول مدى اعتبار الكيان المعنوي للحاسوب مالا.[2]

المال هو كل ما يصلح أن يكون محلا للحق ذو القيمة المالية والشيء هو محل الحق ،وتقسم الأشياء، إلى أشياء مادية وأشياء غير مادية أو معنوية، علما بان الأموال من وجهة النظر التقليدية لا ترد على أشياء مادية ولهذا كان تعريف المال بصدد جرائم الأموال بأنه " كل شيء مادي يصلح لان يكون محلا حق من الحقوق المالية" [1]

ولكن مع التطور ازدادت الأشياء المعنوية عددا وتفوق بعضها من حيث قيمتها على الأشياء المادية مما استدعى البحث عن معيار أخر غير طبيعة الشيء الذي يرد عليه الحق المالي حتى يمكن إسباغ صفة المال على الشيء المعنوي.

ومن هذه الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسب الآلي –هذه البرامج تكون عادة مثبتة على دعامة أو حامل SUPPORT –مثل الأقراص أو الشرائط الممغنطة من البلاستيك أو الورق المقوى أو أي مادة أخرى .

والبرنامج المستقل عن دعامته لا جدال في انه شيء معنوي وبالتالي لا يصدق عليه وصف المال طبقا للتحديد التقليدي للاموا ل الذي يشترط أن يكون محله شيئا ماديا، أما إذا سجل البرنامج أو نقش

---

[1] – د. احمد عبد الرزاق السنهوري ، الوسيط في شرح القانون المدني ، حق الملكية ، الجزء الثاني ، دار إحياء التراث العربي ، بيروت 1952، ص 09 .

على دعامته فان تلك الدعامة بما عليها من برامج تصلح لان تكون محلا لجرائم الأموال على الرغم من أن الدعامة منفصلة عن البرنامج تعتبر ضئيلة القيمة إذا ما قيست بقيمة البرنامج وعلى الرغم أيضا من أن الاعتداء عليها ليس في غاية في ذاته، وإنما الباعث على ذلك هو البرنامج نفسه لا دعامته ومع ذلك لا تأثير لهذه البواعث في القانون الجنائي [1]

ويعتبر الاعتداء على الدعامة في هذه الحالة قد وقع على شيء مادي مما يصلح تكييفه حسب النشاط الإجرامي بإحدى جرائم الأموال التي يتطابق نموذجها مع هذا النشاط ، أما إذا وقع الاعتداء على البرنامج مستقلا عن دعامته ،فان الأمر يختلف حيث يكون قد وقع على شيء معنوي ،هذا الشيء المعنوي لابد وان تثبت له صفة المال أولا حتى يمكن البحث بعد ذلك في مدى إمكانية وقوع جرائم الأموال عليه .

وقد انقسم الفقه في هذا الصدد إلى اتجاهين:

- **الاتجاه الأول**: الفقه المؤيد لإضفاء وصف المال على البرنامج

يرى جانب من الفقه أن المعلومات صالحة لان تكون محلا للاعتداء عليها طالما كانت هذه المعلومات تعكس الرأي الشخصي لصاحبها ولا تتوقف عند نطاق المعلومات العامة ، وذلك على أساس أن هذه المعلومات صادرة عن صاحبها أي أنها ترتبط بشخصيته وهو الذي فكر فيه ،أو هذا يعني أنها من الحقوق اللصيقة بشخصية صاحبها ،وهذه المعلومات ذاتها هي موضوع هذا الحق ومن خصائصها القابلية للانتقال وهذا يعني أن هناك طرفا أخر يستقبل هذه المعلومات ،ومن هنا تنشا علاقات إما بينها وبين صاحبها وأما بين صاحبها والغير، فالمعلومات باعتبارها نتاجا ذهنيا لمن يعطيها شكل

[1] – د. علي عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999، ص7.

المعلومة فهي تعد محور العلاقات مثل تلك التي تنشا بين المالك وبين ما يملك فيكون له نقلها وإيداعها وحفظها وتأجيرها وبيعها. ومن أمثلة هذه المعلومات برامج الحاسب الآلي ،إذ أن هذه البرامج ترتب حقوقا لصاحبها وتخول له إبرام عقود متعلقة بها مثل الإيجار والبيع والحفظ وأي صورة أخرى من صور الاستغلال، لان من خصائصها القابلية للانتقال .

كل هذه التصرفات والحقوق هي التي دفعت جانبا من الفقه إلى القول بان المعلومات مال ليس فقط لوجود علاقة حق استئثار خاص عليها، وإنما أيضا لأنها تعتبر قيمة اقتصادية، فهي تطرح في السوق للتداول مثلها في ذلك مثل أي سلعة ولها سوق تجاري يخضع لقوانين السوق الاقتصادية .

وإذا كان الفقه التقليدي قد استبعد المعلومات من طائفة الأموال على أساس أنها غير مادية أي أن عدم مادية المعلومات هو الذي أدى إلى عدم الاعتراف لها بصفة المال فان الفقه الحديث يرى على العكس أن المعيار في اعتبار الشيء مالا ،ليس على أساس ماله من كيان مادي وإنما على أساس قيمته الاقتصادية، وان القانون الذي يرفض إصباغ صفة المال على شيء له قيمة اقتصادية هو بلا جدال قانون ينفصل تماما عن الواقع [1]

ومادامت البرامج في جوهرها معلومات معالجة بطريقة ما ولها قيمة اقتصادية فانه يجب معاملتها على أنها مال[2].ما يؤكد هذا المعنى أن المشرع الحديث يعترف لصاحب هذه المعلومات بما يطلق عليه الحق في الملكية الفكرية ،ولولا أن المعلومات مالا ما كان المشرع ليستطيع التسليم لها بهذا الحق، وان كانت طبيعة هذه الملكية محل جدل فقهي[3].فإنها على كل حال نوع من الملكية أو الحق الذي لصاحبه في القليل الحق في احتكار استغلال هذا المال غير المادي أي المعلومات والتي منها برامج الحاسب الآلي .

---

**1**– أمال قارة، المرجع السابق، ص 18.

**2**. أمال قارة، المرجع السابق، ص 18

**3** . د. عبد الرشيد مأمون، الحق الأدبي للمؤلف، النظرية العامة وتطبيقاتها، دار النهضة العربية، القاهرة 1978.

- **الاتجاه الثاني**: الفقه المعارض لإضفاء وصف المال على البرنامج

الجانب الأخر من الفقه يرى عدم صلاحية المعلومات لان تكون محلا للاعتداء عليها ، حيث ذهب جانب من الفقه في فرنسا إلى أن المعلومة في حالتها المجردة والفكرة في حد ذاتها لا تقبل التملك والاستئثار ،وان تداولها والانتفاع بها من حق الكافة دون تمييز ومن ثم لا يمكن أن تكون محلا للملكية الفكرية[1]

ويفرق البعض الأخر بين المعلومات والبيانات التي تمت معالجتها الكترونيا فيرون أن الأولى باعتبار أن عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها ، لها طبيعة غير مادية ولا سبيل من ثم إلى اختلاسها أما البيانات التي تمت معالجتها الكترونيا، فتتحدد في كيان مادي يتمثل في نبضات أو إشارات ممغنطة يمكن تخزينها على وسائط معينة ونقلها واستغلالها وإعادة إنتاجها فضلا عن إمكانية تقديرها كميا وقياسها فهي إذن ليست شيئا معنويا كالحقوق والآراء والأفكار بل شيئا له في العالم الخارجي المحسوس وجود مادي وفقا لهذا الرأي فان المعلومات إذا لم تعالج أليا عن طريق الحاسب لا تعتبر من قبيل الأموال الخاضعة للحماية الجنائية باعتبار أن هذه المعالجة تتم في صورة نبضات الكترونية ،مما يمكن القول معه بأنه لعملية المعالجة تلك تتحول من أموال معنوية إلى أموال مادية، الأمر الذي يخضعها للنصوص التقليدية لجرائم الأموال ،ويأخذ نفس حكمها البيانات المخزنة سواء في برامج الحاسب أو في ذاكرته وبالتالي تأخذ برامج وبيانات الحاسب وحكم الأموال عليه وبالتالي تتمتع بالحماية الجنائية المقررة لها .

إن اعتبار المعلومات مالا قابلا للتملك أو الاستغلال كما سبق أن وضحنا يزيل أمامنا عقبة كبيرة

**1** . د. هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الكاتبة ، أسيوط ،طبعة 1995 ،ص 256-257 .

تسمى التملك. هذا النوع من الأموال إلى مجموعة الأموال التي يحميها القانون الجنائي والتي تتمثل في ضرورة أن يكون المال موضوع جرائم الاعتداء على الأموال شيئا منقولا مملوكا للغير، فانه يمكن إسباغ حماية النصوص التقليدية عليه وذلك على أساس أن هذه النصوص جاءت عامة ولم يشترط أن تقع جرائم الأموال على منقول مادي .وعليه يكون من المتصور أن تقع هذه الجرائم على مجال غير مادي طالما اعترف لها بصفة المال وقابلية التملك .وقد سايرت هذا الاتجاه محكمة النقض الفرنسية في العديد من أحكامها[1] 1-2 مدى برامج الحاسب استنادا إلى هذه الصفة تحت مفهوم الشيء الذي يصبح محلا لجرائم الأموال ؟

**ثانيا : مدى اعتبار المعلوماتية مالا بصدد جرائم الأموال :**

ذكرنا في الفرع السابق أن برامج الحاسب وفقا للفقه الراجح ينطبق عليها وصف المال فإذا كانت المعلومات شيئا منقولا لا مملوكا للغير إلا أنها شيء غير مادي فهل تدخل البرامج استنادا إلى هذه الصفة تحت مفهوم الشيء الذي يصلح محلا لجرائم الأموال ؟

**أ / مدى اعتبار البرنامج مالا بصدد جريمة السرقة :**

طبقا للمادة 350 من قانون العقوبات الجزائري فان "كل من اختلس شيئا غير مملوك له يعد سارقا " نص المادة 350 لم يشترط صراحة ضرورة أن يكون المال موضوع الجريمة ماديا مما يجعل وقوع جريمة السرقة على مال معنوي أمرا لا يصطدم بمبدأ شرعية الجرائم والعقوبات .

يجد هذا الرأي تسويغه في أن الشيء وهو محل السرقة حسبما يصفه نموذجها في التشريع الجزائري لا يقتصر لورود لفظه بغير نعت أو تخصيص على الأشياء المادية المجسمة فحسب بل يشمل الأشياء غير المادية كذلك، وهذا التفسير الراجح فقها ، ولكن يبقى اعتبار البرنامج كمحل للسرقة غير قطعي ومن باب الإمكان لا غير .

1. د. علي عبد القادر القهوجي، المرجع السابق، ص 23.

**ب/ مدى اعتبار البرنامج كمحل لجريمة النصب :**

طبقا للمادة 372 من قانون العقوبات الجزائري فان "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل بالفوز بأي شيء أو في وقوع حاد أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20000 دج ".

نستنتج من نص المادة 372 بأنه ليس كل شيء مادي ومنقول يصلح أن يكون محلا لجريمة النصب بل يجب أن يكون ضمن الأشياء التي عددتها المادة 372 على سبيل الحصر.

تجدر الإشارة إلى أن النص على المنقول ورد دون تحديد لطبيعته ودون أن يقيده المشرع بان يكون ماديا مما يسمح بتفسير هذا النص على نحو يسمح بدخول برامج الحاسب ضمن الأشياء التي تقع عليها جريمة النصب إلا انه حتى وان أخذنا بهذا التفسير، نصطدم بعدم وجود نشاط مادي ملموس يحصل به التسليم والاستلام ،وحتى على فرض أن التسليم قد تم ،فان المجني عليه لا يحرم من حيازة البرنامج والبيانات التي تبقى تحت سيطرته التامة .

**ج/ مدى اعتبار البرنامج كمحل لجريمة خيانة الأمانة :**

طبقا للمادة 376 من قانون العقوبات الجزائري " كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو ابراءا لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير اجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة ...."

يستنتج من نص المادة 376 إن الاختلاس يقع على مال منقول سلم إلى الجاني بمقتضى عقد من عقود الأمانة، وعليه لا تقع جريمة خيانة الأمانة على غير المنقولات المادية.

وقد حددت المادة 376 الأشياء التي تصلح محلا لهذه الجريمة وهي على سبيل الحصر أوراق تجارية ، نقود بضائع ،أوراق مالية ، مخالصات ،محررات تتضمن أو تثبت التزاما أو ابراءا وعليه فان إخضاع الاعتداءات الواردة على المال ألمعلوماتي إلى نصوص خيانة الأمانة يثير بعض المشاكل القانونية نظرا للطبيعة غير المادية للقيم في حقل الجريمة المعلوماتية .

الحل الوحيد هو الاقتداء بما اخذ به القضاء الفرنسي باعتباره بعض القيم في المجال ألمعلوماتي من قبيل ( البضائع) أي التوسع في مفهوم البضاعة، وعليه فان تطبيق نصوص خيانة الأمانة في مجال المعلوماتية يكون في نطاق محدود ومن باب الإمكان لا غير .

**د/ مدى اعتبار البرنامج كمحل لجريمة الإتلاف :**

طبقا للمادة 407 من قانون العقوبات الجزائري "كل من خرب أو اتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا بعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 500 إلى 5000 دج".

كما تنص المادة 412 من قانون العقوبات الجزائري "كل من اتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة وذلك بواسطة مواد من شانها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من500 دج إلى 5000 دج"

بالرجوع إلى نص المادة 412 نجدها قد حددت الأشياء الخاضعة للإتلاف وبالتالي فإنها تشمل المكونات المادية للحاسوب سواء بوصفها أجهزة أو بضائع .كما أن الكيان المنطقي يمكن أن يخضع لهذا النص ألتجريمي باعتباره مالا بالنظر لما له من قيمة اقتصادية .

**الفرع الثاني : مدى خضوع المعلوماتية للنشاط الإجرامي لجرائم الأموال :**

المطروح للبحث هو مدى خضوع برامج الحاسب الآلي أو المعلومات بصفة عامة للسلوك الإجرامي الذي يتحقق به الركن المادي في جرائم السرقة والنصب وخيانة الأمانة والإتلاف.

**أولا : مدى خضوع المعلوماتية للنشاط الإجرامي في جريمة السرقة :**

بالنسبة للنشاط الإجرامي المكون لجريمة السرقة وهو الاختلاس وبتطبيقه على برامج الحاسب الآلي أو المعلومات المعالجة بصفة عامة ، نلاحظ أن الجاني وان كان يدخل في ذمته ما استولى عليه من برامج إلا انه في نفس الوقت لم يخرج هذه البرامج من ذمة صاحبها الشرعي إذ تظل رغم مباشرة أفعال الاختلاس عليها تحت سيطرة هذا الأخير دون انتقاص من محتواها ، كما يلاحظ إن الاستيلاء على البرامج باعتبارها معلومات لا يتصور من الوهلة الأولى إلا على انه انتقال لهذه المعلومات من ذهن إلى ذهن أو من ذاكرة إلى ذاكرة[1] وهذه عقبة ثانية ويلاحظ ثالثا أن المعلومات التي تحويها البرامج من طبيعة غير المادية أي أنها شيء معنوي فكيف يتصور أن يرد فعل الاختلاس الذي هو من طبيعة مادية على شيء معنوي وهذه عقبة ثالثة. نتيجة لهذه العقبات فليس من السهل بسط أحكام السرقة على برامج الحاسب الآلي وخاصة في الحالات التالية :

**أ/ سرقة المعلومات عن طريق النسخ غير المشروع للبيانات المخزنة الكترونيا:**

أي عن طريق إعادة إنتاج الوثيقة أو الدعامة التي تحتويها، لمحاولة بسط أحكام السرقة على حالات النسخ غير المشروع يمكننا اعتماد ما توصل إليه الاجتهاد القضائي الفرنسي في هذا الصدد بإعلانه صراحة أن المعلومات التي نسخت أو أعيد إنتاجها هي التي سرقت كما انه لم يخرج عن مبدأ الشرعية الجنائية وحافظ على مبدأ مادية الاختلاس وعلاوة على ذلك فان إقرار الحكم باختلاسه المعلومات عن طريق إعادة إنتاج المستند الذي يحويها يحمل في طياته ثروة مستترة ولكنها عميقة لأنها تسمح بالعقاب على إعادة الإنتاج الذي لا يمكن أن يقع تحت طائلة جريمة التقليد .

1- د. علي عبد القادر القهوجي، المرجع السابق، ص 95.

وتجدر الإشارة إلا انه لا يجب الخلط بين جريمة سرقة المعلومات عن طريق النسخ غير المشروع وبين جريمة التقليد لان السرقة تحوي البيانات في ذاتها، بينما تنصب الحماية التي يكفلها المشرع للمصنفات بتجريم تقليدها على طريقة التعبير عن أفكار المؤلف **1** .

**ب/ سرقة وقت الآلة :**

يكيفها فقهاء القانون الجنائي على أنها سرقة استعمال ، وفي هذه الحالة ليس من السهل بسط أحكام جريمة السرقة على وقت الآلة لان المشرع الجزائري لا يأخذ بما يسمى سرقة الخدمة وعليه تتطلب تدخلا تشريعيا على غرار ما فعل المشرع الفرنسي بتجريمه البقاء غير المشروع في نظام المعالجة الآلية للمعطيات ، فإذا كانت هذه الجريمة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة إلا أنها تحقق أيضا وبصورة غير مباشرة حماية للمعلومات ذاتها .

**ج/ الالتقاط الذهني للبيانات :**

كأن يقوم شخص بالتقاط معلومات ظهرت على شاشة الحاسب وقام بحفظها و اختزانها في ذاكرته ، هذا المسلك يمكن أن يكون اختلاسا رغم انه لم يرد على ذات مادة المستند وإنما اقتصر الشيء المختلس على مضمون المستند مع بقائه في حيازة صاحبه لان هذا المضمون شيء منقول مملوك للغير منحصر في منفعة المستند كجزء من حق صاحبه في ملكيته ، إلا إن المشرع الجزائري لا يأخذ بسرقة الاستعمال وعليه ضرورة تدخل تشريعي يشمل حالتي الالتقاط الذهني للبيانات وحالة سرقة المعطيات دون استنساخها ودون المساس بسلامتها أو أصالتها [2]

**1** . – أمال قارة، المرجع السابق، ص 26.

**2**. – أمال قارة، المرجع السابق، ص 23.

**د/ تكييف الالتقاط الهوائي للبيانات المعالجة أو المنقولة الكترونيا :**

من المعلوم أن الطاقة والقوى الطبيعية أو الصناعية تعد من الأموال المنقولة وتصلح لان تكون محلا للسرقة إلا انه لا يمكننا أن نطبق أحكام سرقة الطاقة على الإشعاعات والموجات والنبضات المنبعثة من الحاسب الآلي أثناء تشغيله رغم أنها كهربائيا قابلة للقياس والتقدير الكمي وذات قيمة [1]

ولهذا نخلص لعدم وقوع السرقة في الحالات السابقة لان طبيعة البرامج والمعلومات تأبى تحقيق الأخذ أو الاختلاس بمعناه الدقيق المسلم به في جريمة السرقة والذي يعني الاستيلاء على الحيازة الكاملة للشيء بدون رضا مالكه أو حائزه السابق لأنه إذا تصورنا وقوع الاختلاس من خلال النسخ أو التصوير على المعلومات فان هذه المعلومات الأصلية ذاتها تظل في نفس الوقت كما كانت من قبل تحت سيطرة صاحبها الأصلي ولا تخرج من حيازته ، ولما كان قانون العقوبات الجزائري لا يجرم سرقة الاستعمال بصفة عامة ، فان المخرج الوحيد لا يكون إلا بتدخل صريح من المشرع، لتفادي الجدل حول سرقة المعلومات وسرقة وقت الآلة أو سرقة استعمال الأصل وتحقق حماية مباشرة للبرامج والمعلومات .

**ثانيا : مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي في جرائم النصب وخيانة الأمانة والإتلاف :**

**أ / بتطبيق النشاط الإجرامي لجريمة النصب في المجال ألمعلوماتي :**

نجد أن لجوء الجاني إلى إحدى الطرق الاحتيالية وحمل المجني عليه على تسليمه دعامة مادية مثبتا عليها احد البرامج ثم استيلاء الجاني عليها فان النشاط الإجرامي في جريمة النصب يتحقق .لكن هل من المتصور أن يتحقق النشاط الإجرامي لجريمة النصب من خلال الطرق الاحتيالية التي يلجا إليها الجاني والتي يترتب عليها وقوع المجني عليه في غلط يدفعه إلى أن ينقل إليه شفويا أي عن طريق القول

---

**1**.د. هشام رستم ، المرجع السابق ، ص 456 .

محتويات برنامجه الذي يلتقطه الجاني ويحفظه في ذاكرته ؟

هل النقل من خلال القول يعادل التسليم بناء على غلط منصوص عليه في م 376 من قانون العقوبات؟ وهل التقاط أو سماع الجاني للمعلومات يعادل الاستيلاء ؟

لا يوجد نشاط مادي يتحقق به التسليم والاستلام في جريمة النصب ، وحتى لو فرضنا جدلا إمكانية وقوع التسليم والاستلام، فانه لن ينتج عن ذلك حرمان المجني عليه من المعلومات التي نقلها بالقول بل تظل تحت سيطرة من نقلها وفي حوزته وهو أمر وان كان يتفق وطبيعة البرامج والمعلومات إلا انه لا يتفق و طبيعة النشاط الإجرامي في جريمة النصب وهذا يعني عدم صلاحية البرامج للخضوع للنشاط الإجرامي في جريمة النصب .

**ب / بتطبيق النشاط الإجرامي لجريمة خيانة الأمانة في المجال ألمعلوماتي :**

نجد انه تطبيق نسبي فلا جدال في وقوع جريمة خيانة الأمانة بالنسبة للدعامات المثبتة عليها البرامج والمعلومات وذلك في الحالة التي يقوم فيها الأمين بنسخ البرنامج لحسابه الخاص متجاوزا الاتفاق الذي يربطه بصاحب البرنامج إذ يتحقق بهذا النسخ فعل الاستعمال والذي يقصد به استخدام الأمين للمال استخداما يستنزف قيمته كلها أو بعضها مع بقاء مادته على حالها إلا انه من الصعب القول بقيام جريمة خيانة الأمانة في حالة البرامج والمعلومات المستقلة عن الدعامة وذلك لعدم إمكانية قيام النشاط الإجرامي للجريمة ألا وهو التسليم بناء على عقد من عقود الأمانة لعدم وجود نشاط مادي مجسم يتحقق به فعل الاستلام، مما يحول دون صلاحية البرامج والمعلومات للخضوع للنشاط الإجرامي في جريمة خيانة الأمانة [1].

**ج/ بتطبيق النشاط الإجرامي لجريمة الإتلاف في المجال ألمعلوماتي :**

نجد أن المشرع الجزائري لم يقيد النشاط الإجرامي في جريمة الإتلاف بوسيلة معينة إذ هي من الجرائم ذات القالب الحر ولهذا لا يوجد ما يحول دون وقوع جريمة الإتلاف على برامج الحاسب الآلي

---

1- أمال قارة، المرجع السابق، ص 45-60

خاصة وان المشرع الجزائري لم يحدد طريقة بعينها لوقوع الجريمة ولم يحدد نتيجة وحيدة محددة لقيامها، فانه من المتصور أن يتجه الجاني بنشاطه الإجرامي إلى البرنامج والدعامة المسجل عليهما معا ،أو إلى البرنامج فقط دون الدعامة، وقد تقع الجريمة عن طريق الاتصال المباشر بالجهاز كما قد تقع من خلال الاتصال عن بعد .

وعليه فان جريمة الإتلاف المنصوص عليها في قانون العقوبات تحقق حماية جنائية كاملة لبرامج الحاسب على خلاف باقي جرائم الأموال التي توفر حماية نسبية فقط.

## المطلب الثاني : مواجهة الجريمة المعلوماتية من خلال قانون الملكية الفكرية الجزائري

نظرا لنسبية الحماية المقررة من خلال النصوص التقليدية في قانون العقوبات الجزائري ارتأينا البحث في مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية ،وسنفصل في ذلك من خلال نقطتين أساسيتين :

1 -الحماية في إطار قانون الملكية الصناعية

2 -الحماية في إطار قانون الملكية الأدبية والفنية

### الفرع الأول : مواجهة الجريمة المعلوماتية من خلال قانون الملكية الصناعية

**أولا : من خلال أحكام العلامات التجارية.**

ينظمها الأمر 06/03 المؤرخ في 2003/07/19 المتعلق بالعلامات المعدل والمتمم للأمر 57/66 المؤرخ في 1966/03/19 المتعلق بعلامات المصنع والعلامات التجارية والمعدل للأمر رقم 223/67 المؤرخ في 1967/10/19 المتضمن أحكام العلامات التجارية و العلامات التجارية هي كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات ،ويشترط في العلامة أن تكون مميزة وجديدة وغير مخالفة للنظام والآداب

السؤال المطروح: هل تستفيد برامج الحاسب الآلي من الحماية الجنائية للعلامات التجارية ؟

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجا أصحاب البرامج إلى وضع الاسم مقترنا به.

الحماية بإحكام العلامات التجارية قد تكون فعالة بالنسبة للنسخ البسيط، لكن ليس الأمر كذلك بالنسبة للنسخ المعقد.

**ثانيا : من خلال أحكام براءة الاختراع .**

عرفت المادة 02 من الأمر 07/03 الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية. وبشان الشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي:

- ✓ شرط الابتكار
- ✓ شرط الجدة
- ✓ القابلية للتطبيق الصناعي
- ✓ المشروعية

في حال توافر هذه الشروط يتحصل المخترع على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية .

السؤال المطروح هل تستفيد برامج الحاسب من الحماية بواسطة براءات الاختراع ؟

التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع لأحد سببين أساسين هما:

- إما تجرد البرامج من أي طابع صناعي
- إما صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة فليس من الهين توافر شرط الجدة في البرمجيات وليس من الهين إثبات توافر هذا الشرط، إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة

للاختراع المقدم الطلب بشأنه أم لا ، الأمر يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال الذي تتولى بحثه.

و الجهة المكلفة بتقرير توافر شرط الجدة في الجزائر هي المعهد الجزائري لحماية الملكية الصناعية إذ يأخذ المشرع الجزائري بمبدأ الجدة المطلقة [1] الذي يتنافى مع وجود أية سابقة دون تحديد زماني أو مكاني، إنما يشرط أن تتوافر علانية هذه السابقة .

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة الاختراع ، ويتمثل هذا التحفظ في الإجراءات المعقدة للحصول على البراءة والتكلفة العالية والمدد الطويلة التي يستغرقها هذا التسجيل ، فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة سنوات بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر وعليه بمكن للغير الوصول إلى سر البرنامج واستغلاله قبل صدور البراءة .

وتجدر الإشارة إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا للمادة 07 من الأمر 07/03 المتضمن براءة الاختراع " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب ".

**الفرع الثاني : مواجهة الجريمة المعلوماتية من خلال قانون الملكية الأدبية والفنية الجزائري**

نظم المشرع الجزائري قانون الملكية الأدبية والفنية بمقتضى الأمر 14/73 المؤرخ في 1973/04/03 المعدل والمتمم بمقتضى الأمر 10/97 المؤرخ في 1997/03/06 المعدل والمتمم

---

**1** – الأمر 07/03 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع المعدل للأمر 17/93 المؤرخ في 1993/12/07 المتعلق بحماية الاختراعات المعدل للأمر 54/66 في 1963/03/03 المتعلق بشهادات المخترعين وإجازات الاختراع .

بموجب الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة.

لتحديد مدى خضوع برامج الحاسب الآلي للحماية المقررة بمقتضى قانون حق المؤلف الجزائري وجب مناقشة نقطتين أساسيتين :

**أولا : مدى اعتبار البرنامج كموضوع من موضوعات حق المؤلف الجزائري :**

موضوع حق المؤلف هو" المصنف الأدبي والفني" وقد عرف المشرع الجزائري المصنف في المادة الأولى من الأمر 14/73 كما نصت المادة 2 من الأمر 14/73 على أن المصنفات التي تشملها حماية حق المؤلف هي كالتالي:

- الكتب والمنشورات وغيرها من المؤلفات الأدبية والعلمية والفنية
- المحاضرات والخطب والمواعظ والمؤلفات الأخرى المماثلة
- مؤلفات الدراسة والدراسات الموسيقية
- مؤلفات الألحان الإيقاعية والمسرحيات الإيمائية المعبر عنها كتابة أو بطريقة أخرى
- أعمال التصوير والرسم والهندسة والنحت والنقش والطباعة الحجرية
- مؤلفات الفنون التطبيقية
- الصور والخرائط الجغرافية والتصميمات والرسوم والأعمال التشكيلية الخاصة بالجغرافيا والهندسة المعمارية أو العلوم
- المؤلفات الفلكلورية وبصفة عامة المؤلفات التي هي جزء من التراث الثقافي التقليدي الجزائري .

إذن فالمشرع الجزائري لم ينص صراحة من خلال الأمر 14/73 على حماية البرامج المعلوماتية في إطار حق المؤلف، لكن رغم عدم التنصيص فان بعض المختصين يرون إمكانية الحماية واردة بدليل الصياغة المرنة عند ذكر المصنفات المشمولة بالحماية.

أي يمكن إسباغ الحماية على برامج الحاسوب كمصنفات فكرية ضمن عمومية نص المادة 2 الواردة في شان المصنفات التقليدية المحمية .

فنص المادة 2 وان كان لم يذكر صراحة برامج الحاسوب ضمن المصنفات المحمية لحماية حق المؤلف إلا أن صياغتها قد جاءت في صورة عامة ، هذا التعداد ورد على سبيل المثال لا الحصر .

ومنعا لأي لبس ،كان من الأفضل النص على البرامج صراحة ضمن قائمة المصنفات المحمية، وهذا مافعله المشرع الجزائري في تعديل قانون حق المؤلف بمقتضى الأمرين 10/97 – 05/03 حيث ادمج برامج الإعلام الآلي ضمن المصنفات الأصلية [1].

من استقراء الأمرين 10/97-05/03 المعدل والمتمم للأمر 14/73 نستخلص مايلي :

– مجموعة المصنفات والأساليب والقواعد، كما يمكن أن يشمل الوثائق المتعلقة بسير ومعالجة المعطيات [2]

– إن مدة الحماية تحدد من 25 سنة إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية "بارن" التي حددت كمدة للحماية 50 سنة .

– تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية (المادة 151 الأمر 10/97) إذ كان في السابق التعدي على الملكية الفكرية يخضع للمواد 394/390 من قانون العقوبات لكنها أخرجت بموجب الأمر 10/97 من مظلة قانون العقوبات وأصبح لها تجريم خاص إذ أن قانون العقوبات كان يقرر بموجب المادة 390 الغرامة كعقوبة للاعتداء على حق المؤلف بينما الأمر 10/97 يقرر عقوبتي الحبس والغرامة .

تجدر الإشارة إلى أن هذه المستجدات التي اعتمدها المشرع الجزائري من خلال الأمرين 10/97 – 05/03 تعود لأسباب أهمها الانضمام إلى المنظمة العالمية للتجارة هو المصادقة على اتفاقية بارن وهو مافعلته الجزائر بموجب المرسوم الرئاسي 341/97 .

---

**1** – المادة 04 الأمر 10/97 "تعتبر على الخصوص كمؤلفات أدبية أو فنية محمية ما يأتي المصنفات الأدبية المكتوبة مثل المحاولات الأدبية والبحوث العلمية والتقنية والروايات والقصص والقصائد الشعرية ومصنفات وقواعد البيانات ".

**2** –المادة 05 الأمر 10/97 "تعتبر أيضا مصنفات محمية الأعمال الآتية مجموعات المعلومات البسيطة التي تتأتى أصالتها من انتقاء مواردها أو تنسيقها أو ترتيبها ".

متوافقة مع الاتفاق لتفادي الاستعمال المتعسف لحقوق الملكية الفكرية من طرف حائزي الحقوق واللجوء إلى تصرفات تمس بالتجارة أو تضر بعقود نقل التكنولوجيا .

ومن أهم ما ورد في اتفاق جوانب الملكية الفكرية المتعلقة بالتجارة [1] هو ما ورد في نص المادة 10 أن برامج الإعلام الآلي سواء كانت في صورة برنامج مصدر أو الصورة المنقوشة فهي محمية على أساس أنها مصنفات أدبية ،كما أن الاتفاقية حول الإجرام ألمعلوماتي نصت على تجريم الاعتداءات على حق المؤلف والحقوق المجاورة تطبيقا لأحكام اتفاق جوانب الملكية إذا ارتكبت هذه الاعتداءات عن طريق نظام معلوماتي في نطاق تجاري.

**ثانيا : مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي لجرائم التقليد في التشريع الجزائري :**

قانون حق المؤلف يوفر الحماية الجزائية لمصنفات الإعلام الآلي بعد إدماجها صراحة ضمن المصنفات المحمية. في السابق كانت أفعال التعدي على حقوق الملكية الأدبية والفنية معاقب عليها في قانون العقوبات المواد( 390 إلى 394) غير أن هذه المواد ألغيت بمقتضى المادة 165 من الأمر 10/97.

الملاحظ أن الاعتداءات على حقوق المؤلف أخرجت بموجب الأمر 10/97 من تحت مظلة قانون العقوبات، حيث كان منصوصا عليها في القسم التاسع المعنون بجنح التعدي على الملكية الأدبية والفنية من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال. لكن حاليا أخرجت من نطاق قانون العقوبات وأصبح لها تجريم خاص في إطار قانون حق المؤلف .

وتجدر الإشارة إلى الأمر 10/97 فقد شدد في العقوبات المقررة للاعتداءات على حقوق المؤلف مقارنة بالعقوبات المنصوص عليها في قانون العقوبات (المادة 75 الأمر 14/73) تحيل إلى المادة

**1**.اتفاق بين المنظمة العالمية للتجارة والمنظمة العالمية للملكية الفكرية ابرم في 1994/04/15.

390 من قانون العقوبات تقرر الغرامة كعقوبة للاعتداء على حق المؤلف بينما الأمر 10/97 يقرر عقوبتي الحبس والغرامة .

**أ / جرائم التقليد وبرامج الحاسب الآلي في التشريع الجزائري :**

مادام المشرع الجزائري قد ادمج برامج الحاسب الآلي ضمن قائمة المصنفات المحمية عن طريق القانون المتعلق بحق المؤلف ، فان أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج يشكل فعلا من أفعال التقليد ، وقد نص المشرع الجزائري في الأمر 10/97 على جريمة التقليد والجرائم المشابهة لها .

تنص المادة 149 من الأمر 10/97 (المادة 151 الأمر 05/03) عن وجود جنحة التقليد في الحالات التالية:

الكشف غير المشروع عن مصنف أدبي أو فني

المساس بسلامة مصنف أدبي أو فني

استنساخ مصنف أدبي أو فني بأي أسلوب من الأساليب في شكل نسخ مقلدة أو مزورة

استيراد نسخ مقلدة أو تصديرها

بيع نسخ مزورة من مصنف أدبي أو فني

تأجير مصنف أدبي أو فني مقلد أو عرضه للتداول

نستنتج من هنا ستة جرائم تعتبر من جنح التقليد ويمكن تصنيفها إلى ثلاث[1]:

**الصنف الأول**: الجنح المتعلقة بالحق المعنوي للمؤلف

الكشف غير المشروع من مصنف أدبي أو فني (م22 الأمر 05/03)

المساس بسلامة المصنف الأدبي أو الفني (م 25 الأمر 03 /05)

**الصنف الثاني**: الجنح المتعلقة بالحق الأدبي للمؤلف

**1**. د. عكاشة محي الدين، محاضرات في الملكية الأدبية، ديوان المطبوعات الجامعية، الجزائر 2001، ص 48.

– استنساخ مصنف بأي أسلوب من الأساليب في شكل نسخ مقلدة، هذا الصنف من جرائم التقليد هو الأكثر شيوعا في المجال ألمعلوماتي أي عملية استنساخ البرامج (النسخ غير الشرعي)

– الإبلاغ الغير شرعي للمصنف فطبقا للمادة 150 من الأمر 10/97 يعد مرتكبا لجنحة التقليد كل من يقوم بإبلاغ المصنف الأدبي أو الفني للجمهور عن طريق التمثيل أو الأداء العلني أو البث السمعي البصري أو بواسطة التوزيع أو أية وسيلة أخرى لبث الإشارات الحاملة للأصوات أو الصور و الأصوات معا أو بأي نظام من نظم المعالجة المعلوماتية [1].

**الصنف الثالث:** الجنح المشابهة لجنحة التقليد والمتمثلة في:

استيراد النسخ المقلدة وتصديرها

بيع نسخ مزورة من المصنف ( برنامج)

تأجير مصنف ( برنامج) مقلد أو عرضه للتداول

الجنحتين المتعلقتين بالمساعدة والمشاركة في المساس بحقوق المؤلف والرفض عمدا دفع المكافأة المستحقة بمقتضى الحقوق المقررة للمؤلف

نخلص من هذه الأصناف الثلاث أن جريمة التقليد تتضمن اعتداء على احد الحقوق المالية أو الأدبية دون موافقة المؤلف، والقصد الجنائي في جريمة التقليد مفترض.

الاعتداء على الحق المالي :

1 -الاعتداء على حق النسخ (المواد 41-46-53-54 الأمر 05/03) إن استنساخ المصنف هو إمكانية استغلال المصنف في شكله الأصلي أو المعدل بفضل تثبيته المادي على أية دعامة أو بكل وسيلة تسمح بإبلاغه وبالحصول على نسخة أو أكثر من كامل المصنف أو جزء منه ونطاق الحق في الاستنساخ واسعد جدا سواء بالنسبة لمصنف المستنسخ أو لأسلوب الاستنساخ والمصنف المستنسخ

28- د. عكاشة محي الدين، المرجع السابق، ص 45.

يمكن إن يكون في شكل برنامج إعلام ألي .

2- الاعتداء على حق المؤلف في إبلاغ المصنف للجمهور (المادة 150 الأمر 05/03) ويعتبر الإبلاغ عموميا حينما يبقى خارج الإطار العائلي بالمفهوم الدقيق ويحتوي حق الإبلاغ على كل إبلاغ سواء كان مباشرا أو غير مباشر عن طريق تثبيتات كالاسطوانات أو الفيلم أو الفيديو ... الخ

3- الاعتداء على حق المؤلف في تحويل البرنامج أي حق المؤلف في استغلال مصنفه وفي ترخيص انجاز مصنفات مشتقة كالاقتباسات والترجمات والتعديلات .... الخ [1].

الاعتداء على الحق الأدبي :

1 - الاعتداء على حق مؤلف البرنامج في الكشف عن برنامجه في الوقت وبالطريقة التي يراهما مناسبين.

2 -الاعتداء على الحق في سلامة المصنف إذ يحمي المشرع جنائيا حق المؤلف في تعديل وتحوير أو تغيير أو حذف أو إضافة ترد على البرنامج من شخص أخر دون إذن من المؤلف، فمن يرتكب احد الأفعال السابقة يتوافر في حقه النشاط الإجرامي لجريمة التقليد .

**ب / الجزاءات المقررة لجرائم التقليد :**

العقوبات المقررة للاعتداءات على حقوق الملكية الأدبية والفنية محددة في المواد 153-156-157-158-159 من الأمر 05/03 .

كانت في السابق تتناولها المواد 390 إلى 394 من قانون العقوبات غير أن أحكام هذه المواد ألغيت بمقتضى المادة 165 من الأمر 10/97 المعدل والمتمم بالأمر 05/03 إذ أخرجت من تحت مظلة قانون العقوبات وأصبح لها تجريم خاص في إطار قوانين حقوق المؤلف.

تجدر الإشارة إلى انه تم التشديد في العقوبات على النحو التالي:

1 - د. عكاشة محي الدين، المرجع السابق، ص 46.

للقاضي أن يطبق كعقوبة أصلية الحبس من 06 أشهر إلى 03 سنوات وغرامة قدرها 500 ألف دج إلى 01 مليون دج سواء تمت عملية النشر في الجزائر أو في الخارج .

للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لإقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف (البرنامج) وكل النسخ المقلدة والمصادرة تدبير تكميلي.

وتأمر الجهة القضائية بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك وكذلك الإيرادات موضوع المصادرة للمؤلف أو أي مالك حقوق أخر لتكون عند الحاجة بمثابة تعويض

للقاضي إن يضاعف العقوبات المقررة وذلك في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى 06 أشهر، وإذا اقتضى الحال تقرير الغلق النهائي

تجدر الإشارة إلى إجراء هام يتم أثره اكتشاف جريمة التقليد وهو مايسمى بالحجز الناتج عن التقليد يمكن بواسطته لمؤلف البرنامج المحمي أو ذوي حقوقه المطالبة بحجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع أو التقليد ،وذلك حتى في غياب ترخيص قضائي أو انه إيقاف لأية عملة جارية ترمي إلى الاستنساخ غير المشروع للبرنامج أو حجز الدعائم المقلدة والإيرادات المتولدة عن الاستغلال غير المشروع للمصنفات .

- نصت المادتان 145، 146 على أن من اختصاص ضباط الشرطة القضائية معاينة انتهاك حقوق المؤلف وهم مؤهلون بصفة تحفظية بحجز النسخ المقلدة من المصنف أو من دعائم المصنفات ولكن بشروط:

1 – النسخ المقلدة يجب أن تكون موضوعة تحت الحراسة ليس من طرف ضباط الشرطة القضائية ولكن من الديوان الوطني لحقوق المؤلف والحقوق المجاورة.

2- المحضر الذي يثبت بان النسخ المقلدة المحجوزة يجب أن تقدم لرئيس الجهة القضائية المختصة إقليميا.

---

**1**. د. عكاشة محي الدين، المرجع السابق، ص 48.

- كما يختص بعملية الحجز الأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف والحقوق المجاورة لكن بشروط :

1- يشترط من الأعوان المحلفين وضع النسخ المقلدة تحت حراسة الديوان الوطني لحقوق المؤلف والحقوق المجاورة .

2- الإخطار الفوري لرئيس الجهة القضائية المختصة إقليميا بمحضر مؤرخ وموقع قانونيا يثبت النسخ المقلدة المحجوزة [1]

رغم اعتراف المشرع الجزائري لبرنامج الحاسب الآلي بصفة المصنف المحمي إلا انه اغفل نقاطا هامة نظرا لوجود بعض المفاهيم التقليدية لحقوق المؤلف لا تتماشى مع طبيعة برنامج الحاسب الآلي نجملها فيما يلي:

1- قرن المشرع الحماية المقررة لحق المؤلف بضرورة الإيداع ، بحيث لا يضفي هذا القانون حماية على البرنامج الذي لم يتم إيداعه ، وان كان من الأفضل أن يربط المشرع هذه الحماية بتاريخ الانتهاء من الابتكار أو تاريخ النشر و التوزيع لأول مرة أسوة بما سار عليه المشرع الفرنسي و تماشيا مع نصوص اتفاقية بارن كما انه من الأجدر وضع نظام خاص بإيداع برامج الحاسب الآلي[2]

2-مدة حماية المصنفات هي 50سنة بعد الوفاة طبقا لتوصيات معاهدة برن ، هذه المدة طويلة نسبيا وليس من مصلحة المجتمع و تقدمه احتكار أفراد لتلك المعرفة التكنولوجية الحديثة مددا طويلة فالاحتكار في تطبيقات الإعلام الآلي يجب أن يكون قصير المدة كما هو الحال في جميع الوسائل التطبيقية .

3- ضرورة وضع معيار حصول الاعتداء على حقوق المؤلف البرنامج أو أي صاحب حق فيه ، يجب أن يكون هذا المعيار مختلفا عن معايير حقوق الملكية الفكرية التقليدية لتحديد الاعتداء لان خضوع

---

**1** - د. عكاشة محي الدين، المرجع السابق، ص 49.

**2** - أمال قارة، المرجع السابق، ص93.

البرامج لنفس المعايير التقليدية يعني أننا لا نحمي البرامج إلا بصورة الاعتداء المباشر الذي يتمثل بالنسخ المجرد فيجري التحقق من الاعتداء في مدى التشابه الظاهر بين العمل الأصلي والعمل المنسوخ ، لكن برامج الحاسب قد تكون بصورة تظهر متطابقة تمام التطابق ولكنها تؤدي إلى نتائج تختلف عن بعضها كما أن هناك برامج تكتب بصورة قد تظهر أنها مختلفة تماما ولكنها تأتي بنفس النتائج ، وتطبق معيار قانون حق التأليف السابق يؤدي في مثل هذه الأحوال إلى تقرير الاعتداء في الأول حيث لا يوجد اعتداء وتقرير عدم الاعتداء في الثانية حيث أن هناك اعتداء بالفعل [1].

4-تسري الحماية علي مصنفات الجزائريين سواء نشرت هذه المصنفات في الجزائر أو في الخارج أخذا بالمعيار الشخصي.أما بالنسبة لمؤلفات الأجانب فنفرق بين المؤلفات التي لم يسبقها أن نشرت والتي تنشر للمرة الأولى في الجزائر ، وهي تتمتع بنفس الحماية التي تتمتع مؤلفات الجزائريين وهذا معيار إقليمي أما مؤلفات الأجانب التي نشرت في الخارج من قبل فإنها لا تتمتع بالحماية إلا على أساس المعاملة بالمثل .

وعليه ضرورة تنسيق الجزائر مع باقي الدول فيما يتعلق بالمصنفات المعلوماتية نظرا لكثرة تداولها ،واعتمادا على المذكرة الإيضاحية للنصوص النموذجية التي وضعتها المنظمة العالمية للملكية الفكرية التي تقصر الحماية على واقعة النقل المادي للبرامج بل نصت صراحة على صلاحية النقل المعنوي لها عن طريق شبكات الحاسب التي تربط العديد من الدول ويطلق عليها شبكات الانترنت .

5- عادة ما تكون المصنفات المعلوماتية عبارة عن مصنفات يتعدد مؤلفوها المساهمون في إيداعها وهي عبارة عن مصنفات مشتركة أو جماعية خاصة تلك المبرمجة من قبل مؤسسات ضخمة بمساهمة عدة اختصاصيين محللين ومبرمجين .

بالنسبة للمشرع الجزائري نص على المصنف المشترك للأشخاص الطبيعية المشاركة في انجازه لكن

1. د.عكاشة محي الدين، المرجع السابق، ص 51.

نظرا لكون عملية الاستثمار الاقتصادي الذي يتطلب انجاز المصنفات المعلوماتية مرتفع جدا في بعض الحالات أو بالاعتماد على هذه الأسس ولضمان الاستقلال الكافي لهذا المصنف كان من الأجدر أن يأخذ المشرع الجزائري بما سارت عليه الدول الانجلوساكسونية التي تمنح للمنتج صفة المؤلف ولا تمنحها لغيره من المشاركين تجنبا لمشكلة اعتراض المؤلفين لاستغلال المصنف .

كان من الأجدر في هذا الإطار أن يضع المشرع نصا خاصا بالمصنفات المشتركة في مجال الإعلام الآلي كما هو الحال بالنسبة للمصنفات السمعية البصرية .

نخلص إلى انه نظرا لقصر أحكام العلامات التجارية ونصوص براءة اختراع في مواجهة الجريمة المعلوماتية ، ونظرا لكون قانون الملكية الأدبية والفنية ورغم اعتراف المشرع الجزائري لبرامج الإعلام الآلي وقواعد البيانات بصفة المصنف المحمي إلا انه لا يخفى علينا أن الحماية الجزائية للبرامج من خلال حق المؤلف تنصب بصفة أساسية على شكل البرنامج أو مضمونه ألابتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرنامج . لهذا السبب كان البحث عن نوع أخر ينضم إلى الحماية السابقة من الحماية الجزائية لهذه البرامج في مثل هذه الحالات ،ولذلك فلا مفر من ضرورة اللجوء إلى استحداث نصوص تجريمية خاصة بالمعلوماتية وذلك ما اعتمده المشرع الجزائري في مشروع تعديل قانون العقوبات الجزائري باستحداث فصل خاص بالاعتداءات على أنظمة المعالجة الآلية للمعطيات .

## المبحث الثاني: من خلال النصوص القانونية المستحدثة (قانون 15/04)

لما كانت الحاجة ملحة و ضرورية لحماية المال ألمعلوماتي، فقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لهذا الغرض، و قد استجابت عدة دول لهذا الاتجاه منها الولايات المتحدة الأمريكية، كندا، ألمانيا، النرويج و فرنسا...الخ .

و بالنسبة للتشريع الجزائري، فقد تدارك المشرع الجزائري مؤخرا – ولو نسبيا– الفراغ القانوني في مجال الإجرام ألمعلوماتي و ذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات ، لكن تجدر الإشارة إلى أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية، و أغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي و

المتمثلة في التزوير ألمعلوماتي، و لذلك ارتأينا و حتى لا تكون دراستنا لموضوع الحماية الجزائية ناقصة أن نتعرض للاعتداءات الواردة على المعلوماتية من خلال المطلبين التاليين :

المطلب الأول : الاعتداءات الماسة بالأنظمة المعلوماتية

المطلب الثاني : الاعتداءات الماسة بمنتوجات الإعلام الآلي

**المطلب الأول : الاعتداءات الماسة بالأنظمة المعلوماتية**

تشير الإحصائيات إلى وقوع ما بين 200 إلى 250 اعتداء يوميا على الأنظمة المعلوماتية في الجزائر[1] إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية ، استدعى تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي فدوليا وضعت أول اتفاقية حول الإجرام ألمعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام ألمعلوماتي[2] أما على المستوى الوطني,فقد استدرك المشروع الجزائري الفراغ القانوني من خلال التعديل الأخير لقانون العقوبات الذي تم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم156/66 بقسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات " ويشمل المواد من 394 مكرر إلى 394 مكرر 7.

الجرائم الماسة بالأنظمة المعلوماتية وان كانت تختلف في أركانها و عقوباتها إلا أن ما يجمعها أنهما تحقق حماية جزائية تنظم المعالجة الآلية للمعطيات ,أي أن القاسم المشترك بينهما هو نظام المعالجة الآلية ،ولذلك فان دراسة تلك الجرائم تقتضي منا أولا توضيح وبيان مفهوم نظام المعالجة الآلية للمعطيات.

**الفرع الأول : مفهوم نظام المعالجة الآلية للمعطيات**

يمثل نظام المعالجة الآلية للمعطيات المسالة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث

---

**1** – آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة و النشر، الجزائر 2006 .

**2** – الاتفاقية الدولية حول الإجرام ألمعلوماتي التي أبرمت بتاريخ: 2001/11/08 من طرف المجلس الأوروبي و تم وضعها للتوقيع منذ تاريخ:2001/11/23.

في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام . فان ثبت تخلف هذا الشرط الأولي ,لا يكون هناك مجال لهذا البحث, ويؤدي توافر هذا الشرط إلى الانتقال إلى المرحلة التالية وهي بحث توافر أركان أية جريمة من الجرائم السابقة , إذ أن هذا الشرط يعتبر عنصر لازما لكل منها , ولذلك يكون من الضروري تحديد مفهوم نظام الآلية للمعطيات .

نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن انه تعبير متطور يخضع للتطورات السريعة و المتلاحقة في مجال فن الحاسبات الآلية[1] ولذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات فأوكل بذلك مهمة تعريفه كل من الفقه و القضاء.

## 1. تعريف نظام المعالجة الآلية للمعطيات[2] .

الاتفاقية الدولية للإجرام ألمعلوماتي قدمت تعريف للنظام ألمعلوماتي في مادتها الثانية على النحو التالي:

Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnecté ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement ou tonatisé de données.

أما الفقه الفرنسي فقد عرفه كما يلي:

كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة البرامج والمصطلحات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهما معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية .

بناء على التعريفات السابقة, تخلص إلى أن تعريف نظام المعالجة الآلية للمعطيات يعتمد على عنصرين:

– العنصر الأول: مركب يتكون من عناصر مادة ومعنوية مختلفة ترتبط بينهما نتيجة علاقات توحدهما

---

**1**– د. علي عبد القادر القهوجي، المرجع السابق، ص 119–120.

**2** .أنظر المادة 01 من الاتفاقية الدولية للإجرام ألمعلوماتي.

نحو تحقيق هدف محدد.

– العنصر الثاني: ضرورة خضوع النظام لحماية فنية.

**2. مكونات نظام المعالجة الآلية للمعطيات :**

العناصر المادية والمعنوية التي يتكون منها المركب ومثال ذلك:الذاكرة، البرامج، المعطيات, أجهزة الربط... الخ. هذه العناصر واردة على سبيل المثال لا الحصر.

وهذا يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال , وعلى ذلك لا يتوافر نظام المعالجة الآلية للمعطيات ,ولا تقع بالتالي أي جريمة من جرائم الاعتداء عليه المنصوص عليها إذا وقع الاعتداء على برامج معروضة للبيع , أو على جهاز حاسب لم يدخل الخدمة أو على عنصر مودع بالمخازن، أو على قطع الغيار، أو على الأجهزة التي مازالت في حالة التجربة، أو حتى الأنظمة التي خرجت من الخدمة تماما و لكن على العكس من ذلك، تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل أو حتى لو كان النظام كله في حالة عطل تام، و كان يمكن إصلاحه.

و تقع الجريمة أيضا إذا وقع الاعتداء على عنصر يشكل جزءا من أنظمة متعددة، فإذا تصورنا عدة أنظمة ترتبط فيما بينها بأجهزة اتصال و وقع اعتداء على جهاز حاسب آلي في نظام من تلك الأنظمة المرتبطة، فإن الجريمة تقع في هذه الحالة. و إذا كان الدخول إلى هذا الجهاز مشروع ،فإن البحث في توافر الجريمة يتوقف على ما إذا كانت توجد علاقة سببية بين هذا الدخول المشروع و الاعتداء المفروض على الأنظمة ككل ،و ومدى حسن اوسوء نية المتدخل كما تقع الجريمة إذا وقع الاعتداء على شبكة الاتصال التي تربط بين أكثر من نظام ،لان تلك الشبكة تعتبر عنصر في كل نظام من الأنظمة التي تربط بينهما [1]

**1** - د. علي عبد القادر القهوجي، المرجع السابق، ص 121.

### 3.ضرورة خضوع النظام لحماية فنية [1]:

يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص حاليا شبكة الانترانت فهم يسعون لتامين سرية الرسائل الالكترونية وسرية البيانات المتناقلة وخاصة بالأعمال التجارية الرقمية . ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة ، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الالكترونية .

و تنقسم الأنظمة إلى ثلاثة أنواع :

أنظمة مفتوحة للجمهور.

أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية.

أنظمة قاصرة على أصحاب الحق فيها و تتمتع بحماية فنية.

و مقتضى تطبيق هذا العنصر أن النوع الثالث فقط من تلك الأنظمة هو الذي يتمتع بالحماية الجنائية أما النوع الأول و الثاني فلا يتمتعان بتلك الحماية، و هناك من يصرون عليه لأن الحماية الجزائية في نظرهم يجب أن تقتصر على الأنظمة المحمية. فنيا لأنه من الطبيعي في نظرهم، أن ما يقوم بالاستغلال يضع الوسائل الفنية اللازمة لمنع الغش و أن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، و ليس من يهمل منهم في توفير الحد الأدنى لحماية أمواله ، و يكون دور القانون الجنائي في هذه الحالة دور وقائي و هذا أيضا هو ما يتفق و سياسة المشرع الجنائي و ما نلاحظه من المفهوم العام للحماية الجزائية للملكية.

بالرجوع إلى النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات لا تتضمن شرط الحماية الفنية و خرجت تلك النصوص الخالية منه تماما. و من المبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص المطلق، أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك. و لا يوجد في حالتنا نص خاص يقيد إطلاق النص أو يخصص عمومه، و لذلك فإن عدم ذكر

---

**1**- أمال قارة، المرجع السابق، ص 103.

المشرع لشرط الحماية الفنية يعني أن المشرع أراد استبعاده. هذا بالإضافة إلى أن الحماية الجزائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا.

و تطبيقا لذلك، فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا بوجود حماية فنية و لكن إذا نظرنا للوقائع ، نلاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية، بالإضافة إلى أن وجود مثل تلك الحماية يساعد على إثبات أركان الجريمة و بصفة خاصة الركن المعنوي[1].

**الفرع الثاني : الأركان الأساسية**

و تتمثل هذه الأركان فيما يلي :

**أولا : الركن المادي :**

يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات و التي هي:

أ /الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

ب/ الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.

ج /الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتوجات النظام و سنتعرض إليها بالتفصيل فيما يلي:

**أ / الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:**

نصت عليه المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة

1. د. علي عبد القادر القهوجي، المرجع السابق، ص 123.

الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج".

كما نصت عليه المادة 02 من الاتفاقية الدولية للإجرام ألمعلوماتي.

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

**الصورة البسيطة:**

* **فعل الدخول** : لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، و في نفس الاتجاه إلى جهاز الحاسب الآلي و إنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات. و لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، و لذلك تقع الجريمة بأية وسيلة أو طريقة و يستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[1] .

* **فعل البقاء Le maintien [2]** :

قد يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام، و يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام و قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، وقد يجتمعان. و يكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا.و من أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده و ينسحب فورًا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي. و يكون البقاء جريمة إذا تجاوز المتدخل المدة

---

**1** – د. علي عبد القادر القهوجي، المرجع السابق، ص 121.

**2** – د. علي عبد القادر القهوجي، المرجع السابق، ص 133.

المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية و الإطلاع فقط و يتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، و التي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة، و قد يجتمع الدخول غير المشروع و البقاء غير المشروع معا و ذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام ، و يدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، و يتحقق في هذا الفرض الاجتماع المادي للجرائم و إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضا و بصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة ، و ذلك بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له الحق السيطرة على النظام، و يقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج[1].

كما يمكن أن تطبق على الاستخدام غير المشروع البطاقات الممغنطة إما لسرقتها أو التزوير ثم استخدامها أو حتى إذا استخدمها صاحبها في سحب مبالغ دون أن يكون لديه رصيد كاف، أو عند عدم وجود الرصيد و تكون الجريمة في هذه الحالة هي جريمة البقاء غير المشروع داخل النظام بشرط أن يكون صاحب البطاقة يعلم مقدما بأنه ليس له رصيد كاف و يمكن أيضا تطبيقها على التصنت على المحادثات الهاتفية طالما أن أرقام الهواتف معالجة آليا في نظام خاص بها. هذه الجريمة تعد جريمة سلوك مجرد، أي أنها تقع و تكتمل بمجرد الانتهاء من السلوك المكون لها و هو الدخول أو البقاء دون أن يطلب المشرع في نموذجها القانوني حسب نصوص التجريم أية نتيجة إجرامية[2]

---

**1**- آمال قارة، المرجع السابق، ص 111.

**2** – د. جميل عبد الباقي الصغير، جرائم التكنولوجيا الحديثة، دار النهضة العربية، ص28.

**الصورة المشددة:**

نصت المادة 394 مكرر 3/2: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظمة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 دج إلى 150000 دج".

نصت المادة 394 مكرر 3/2 قانون العقوبات على ظرفين تشدد بهما عقوبة جريمة الدخول و البقاء داخل النظام، و يتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام و إما عدم صلاحية النظام لأداء وظائفه ، و يكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع و تلك النتيجة الضارة، و لا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب مثل هذا الشرط يكون غير معقول ، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة. كما لا يشترط أن تكون تلك النتيجة مقصودة، أي على سبيل الخطأ غير ألعمدي، فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه و بين الجريمة العمدية الأساسية و هي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتفاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

**ب / الاعتداء ألعمدي على سير نظام المعالجة الآلية للمعطيات:**

نصت عليه المادتين 05 و 08 من الاتفاقية الدولية للإجرام ألمعلوماتي [1]

لم يورد المشرع الجزائري نصا خاصا بالاعتداء ألعمدي على سير النظام و اكتفى بالنص على الاعتداء ألعمدي على المعطيات الموجودة بداخل النظام و ربما يجد ذلك تفسيره في أن الاعتداء على المعطيات

---

**1**- آمال قارة، المرجع السابق، ص 114.

قد يؤثر على صلاحية النظام للقيام بوظائفه، و قد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات و الاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية. فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء ألعمدي على النظام، أما إذا كان الاعتداء الذي وقع على المعطيات غاية فإن الفعل يشكل جريمة الاعتداء ألعمدي على المعطيات.

سبق و أن ذكرنا أن الاعتداء على سير النظام الناجم عن الدخول أو البقاء غير المشروع لا يشترط أن يكون مقصودا، لكن الإشكال المطروح أن أفعال الاعتداء على سير النظام الناجمة عن الدخول المشروع للنظام تفلت من العقاب خاصة مع عدم وجود نص خاص بالاعتداء ألعمدي على سير النظام.

يتمثل هذا السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات من أداء نشاطه العادي و المنتظر منه القيام به، و إما في فعل إفساد نشاط أو وظائف هذا النظام، و لا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية جهاز الحاسب الآلي نفسه، شبكات الاتصال، أجهزة النقل ...الخ، أما المعنوية مثل البرامج و المعطيات.

**ج / الاعتداءات العمدية على المعطيات:**

نصت عليها المادة 03،04،08 من الاتفاقية الدولية للإجرام ألمعلوماتي ، كما نص المشرع الجزائري عليها في المادة 394 مكرر2 في قانون العقوبات «يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها».

**الصورة الأولى: الاعتداءات العمدية على المعطيات الموجودة داخل النظام**

النشاط الإجرامي في جريمة الاعتداء ألعمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية[1]:

---

1. آمال قارة، المرجع السابق، ص 114.

* الإدخال L'intrusion.

*المحوL'effacement.

*التعديل Modification.

لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي. و أفعال الإدخال و المحو و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل و هذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد و هو المعطيات أو المعلومات التي تمت معالجتها آليا و التي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات، و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزءا منه.

لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام أو تلك التي دخلت، و لم يتخذ حيالها إجراءات المعالجة الآلية، أما تلك التي في طريقها إلى المعالجة حتى و لو لم تكن المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية، و يكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال.

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

و عمومًا التلاعب في المعطيات الموجودة داخل النظام يتخذ إحدى الأشكال التالية :

**– الإدخال L'intrusion**:

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، و يتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هاته الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي و ذلك حين يستخدم رقمه الخاص و السري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، و كذلك الحامل الشرعي لبطاقة الائتمان و التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له و بصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب« فيروس...الخ» يضيف معطيات جديدة .

**– المحو L'effacement** :

يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة و الموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

**– التعديل Modification**:

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام و استبدالها بمعطيات أخرى، و يتحقق فعل المحو و التعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات و برنامج الممحاة Gomme d'effacement أو برنامج الفيروسات بصفة عامة[1]، و هذه الأفعال المتمثلة في الإدخال و المحو و التعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى و لو تضمن

**1** – آمال قارة، المرجع السابق، ص 122.

الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لأن كل تلك الأفعال لا تنطوي لا على إدخال و لا على تعديل بالمعنى السابق.

- **الصورة الثانية: المساس ألعمدي بالمعطيات خارج النظام**

وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها من خلال تجريمه السلوكات التالية:

1 -نص المادة 394 مكرر2 يستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

2 -نص المادة 394 مكرر 2/2 يجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال، أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة،الجوسسة،الإرهاب، التحريض على الفسق ...الخ.

**ثانيا : الركن المعنوي**

إن الركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية تتخذ صورة القصد الجنائي إضافة إلى نية الغش.

**أ / الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:**

الولوج و التجول و البقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا تما عمدا.

المادة 02 من الاتفاقية الدولية للإجرام ألمعلوماتي تسمح للدولة العضو أن تشترط بأن ترتكب الجريمة عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله.

جريمة الدخول أو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم و الإرادة.

فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء و أن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام و البقاء فيه، و عليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصريه العلم و الإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى و لو كان الباعث هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظام[1] .

بالنسبة لنية الغش تبدو من خلال الغش الذي يتم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام، بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام.

في الحقيقة أن الدخول و البقاء بالغش لا يتضمن معنى خرق الجهاز الرقابي للنظام، إنما يظهر من خلال الولوج دون وجه حق إلى النظام إلاّ أن الجهاز الرقابي ما هو إلاّ وسيلة لإثبات أن الدخول للنظام غير مرخص به.

**ب / الاعتداءات على سير نظام المعالجة الآلية للمعطيات :**

إن هذه الجريمة جريمة عمدية ، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير ألعمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء الغير مشروع داخل النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة [2] .

**1** – د. علي عبد القادر القهوجي، المرجع السابق، ص 136-137.

**2** – د. علي عبد القادر القهوجي، المرجع السابق، ص142.

**ج / الاعتداءات العمدية على المعطيات:**

جريمة الاعتداء ألعمدي على المعطيات جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه ألجرمي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أن ليس له الحق في القيام بذالك وانه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته [1] .

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذالك واتجاه الإرادة إليه ، وان كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا انه ليس عنصرا في الجريمة .

**ثالث: استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية :**

وذلك إما بالتصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية.

حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان للمعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية .فان هذا الاستخدام يجب أن يكون عمدا وبطريق الغش أي بتوافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش.

**الفرع الثالث : الجزاءات المقررة**

وسنتناول فيما يلي الجزاءات التي قررها المشرع الجزائري لهذا النوع من الإجرام الحديث .

طبقا للمادة 13 من الاتفاقية الدولية للإجرام ألمعلوماتي فإن العقوبات المقررة للإجرام ألمعلوماتي يجب أن تكون رادعة وتتضمن عقوبات مالية للحرية ، والتي تتمثل في عقوبات أصلية وعقوبات تكميلية

---

**1** – د – علي عبد القادر القهوجي، المرجع السابق، ص145

تطبق على الشخص الطبيعي ، كما توجد عقوبات تطبق على الشخص المعنوي بناءا على تبني مبدأ مسالة الشخص المعنوي الواردة في المادة 12من الاتفاقية.

**أولا : العقوبات المطبقة على الشخص الطبيعي :**

**أ / العقوبات الأصلية :**

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

* **الدخول والبقاء بالغش (الجريمة البسيطة)**: العقوبة المقررة هي 3 أشهر إلى سنة حبس و 50000 دج إلى 100000 دج غرامة (المادة 394 مكرر) .

* **الدخول والبقاء بالغش (الجريمة المشددة)**: تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة ،وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر02-03 ) .

* **الاعتداء ألعمدي على المعطيات** : طبقا لنص المادة 394 مكرر 2 فالعقوبة المقررة للاعتداء ألعمدي على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 2000000 دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، العقوبة المقررة هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000 دج إلى 5000000 دج .

**ب / العقوبات التكميلية:**

نصت المادة 394 مكرر 3 قانون العقوبات على العقوبات التكميلية إلى جانب العقوبات الأصلية و المتمثلة في:

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

**ج / الظروف المشددة:**

أ/ نصت المادة 394 مكرر /2-3 على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول و البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

في الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر ،و في الحالة الثانية تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج .

هذه الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول والبقاء غير المشروع علاقة سببية للقول بتوافره.

ب/ نصت المادة 394 مكرر 3 على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام

**ثانيا : العقوبات المطبقة على الشخص المعنوي :**

مبدأ مساءلة الشخص المعنوي وارد في المادة 12 من الاتفاقية الدولية للإجرام ألمعلوماتي ، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة

التامة أو الشروع فيها ،كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.

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

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

أ/ الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

ب/واحدة أو أكثر من العقوبات الآتية:

حل الشخص المعنوي

غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات

الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات

المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.

مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

نشر أو تعليق حكم الإدانة.

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

بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394 مكرر 4 قانون العقوبات 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

**ثالثا : عقوبة الاتفاق الجنائي:**

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام ألمعلوماتي وقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5 ، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار ،حيث تنص المادة 394 مكرر 5 من قانون العقوبات : " كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل اوبعدة أفعال مادية ،يعاقب بالعقوبات المقررة بالجريمة ذاتها ".

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

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

وشروط المعاقبة على الاتفاق الجنائي بمن استخلاصها من نص المادة 394 مكرر 5 م قانون العقوبات، والتي هي:

مجموعة أو اتفاق.

بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.

تجسيد هذا التحضير بفعل مادي.

فعل المشاركة في هذا الاتفاق.

القصد الجنائي.

فبالنسبة لمجموعة أو الاتفاق يستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي، كما.يستوي. أن يعرف أشخاص الاتفاق بعضهم بعضا كما في العصابة أم تكون مجرد مجموعة

من الأشخاص، لا يعرف أحدهم الأخر من قبل و لكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي ، المهم أن يتم الاتفاق بين شخصين على الأقل ، فإذا ارتكب الشخص العمل التحضيري المادي شخص واحد بمفرده أو بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر.

وتكاثف الجهود لا يكفي بل يجب أن يكون بهذه تحضير جريمة من جرائم الماسة بالأنظمة المعلوماتية بمعنى أن الاتفاق يجب أن يكون له هدف إجرامي منذ البداية فعليه فإنشاء نادي للمعلوماتية بهدف التكوين أو التسلية العلمية يحول نشاطه لأهداف إجرامية لا يقع تحت طائلة المادة 394 مكرر 5 من قانون العقوبات .

الجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي الجنح الماسة بالأنظمة المعلوماتية وعليه لا يعاقب استنادا لهذا النص الاتفاق بهدف ارتكاب جنحة تقليد البرامج المعاقب عليها بنصوص حق المؤلف وحقوق المجاورة.

التحضير لا يكفي بل يتم تجسيده بفعل مادي، الأمر يتعلق بأعمال تحضيرية مثل تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان على كلمة مرور mots de passe أو رمز الدخول code d'accès. الخ.

فعل المشاركة في الاتفاق إذ أن المجرم بنص المادة 394 مكرر5 ليس الاتفاق وإنما المشاركة من طرف شخص طبيعي أو معنوي فبمجرد الانضمام إلى الاتفاق غير كافي بل يجب توافر فعل إيجابي للمشاركة.

توافر القصد الجنائي لدى أعضاء الجماعة والمتمثل في توافر العلم لدى كل منهم بأنه عضو في الجماعة الإجرامية وأن تتجه إرادة كل عضو أي تحقيق نشاط إجرامي معين وهو العمل التحضيري.

**رابعا : عقوبة الشروع في الجريمة :**

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام ألمعلوماتي وتبناه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص.

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

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

بعض التشريعات المقارنة بما فيها التشريع الفرنسي أخرجت جنحة الاتفاق الجنائي لتحضير جرائم ماسة بالأنظمة المعلوماتية من نطاق الشروع لأنها تعتبر أن في ذلك مساس بالنظرية العامة في القانون الجنائي ،لأن التحضير للجرائم الذي يتم في إطار اتفاق أو مجموعة تشكل في حد ذاتها محاولة أو عمل تحضيري مما يؤدي إلى تبني فكرة الشروع في الشروع .

## المطلب الثاني :الاعتداءات على منتوجات الإعلام الآلي – التزوير ألمعلوماتي–

إن الدعامات المادية للحاسب الآلي قد احتلت مكانة المحررات والصكوك ونظرا لأهمية وخطورة ما تحتويه من بيانات والتي قد تكون محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها، والذي من شأنه إحداث أضرار مادية أو معنوية[1].كتزوير المستخرجات الإلكترونية كالأوراق المالية أو السحب على الجوائز.

جريمة التزوير في المجال ألمعلوماتي من اخطر صور غش المعلوماتية نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسب الآلي الآن والذي اقتحم كافة المجالات وأصبحت تجري من خلال كم هائل من العمليات ذات الآثار القانونية الهامة والخطيرة والتي لا يصدق عليها وصف " المكتوب" في القانونين المدني والجنائي ، وقد أثار هذا الوضع الشك حول دلالتها في الإثبات وحول إمكانية وقوع جريمة التزوير العادية ولهذا كان التدخل التشريعي ذو أهمية بالغة.

تجدر الإشارة إلى أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير ألمعلوماتي، ربما إقتداء بما فعله المشرع الفرنسي الذي أخضع أفعال التزوير ألمعلوماتي للنصوص العامة للتزوير وذلك بعد أن قام بتعديله بجعل موضوع التزوير أي دعامة مادية وليس محررا، الفرق أن النصوص الواردة في قانون العقوبات الجزائري الخاصة بالتزوير تجعل التزوير يرد على محرر وعليه لا يمكن إخضاع أفعال التزوير ألمعلوماتي للنصوص العامة للتزوير كما هو عليه الحال في التشريع الفرنسي مما يستدعي تدخلا تشريعيا ، إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير ألمعلوماتي

**الفرع الأول : مفهوم منتوجات الإعلام الآلي**

سنعرض من خلال هذا العنوان التفرقة بين مفهومين هما المستند المعالج أليا والمستند ألمعلوماتي

**أولا : المستند المعالج أليا[1] :**

يقصد بالمستند في الاصطلاح القانوني كل دعامة مادية (مكتوب أو أي شيء) تصلح لأن تكون عليها معلومات أو أراء والتي هي غير مادية، أو هي الشيء المادي الذي يمكن أن يدون عليه شيء معنوي، ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز (قرص ،أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية، ويستوي بعد ذلك أن

**1** - أمال قارة، المرجع السابق، ص 193.

يكون هذا الشيء قد خرج من الآلة و ثم تصنيفه أو تخزينه أو أنه مازال بداخلها انتظارا لاستخراجه أو تعديله .

المستند المعالج أليا هو كل دعامة مادية مهيأة لاستقبال المعلومات والتي تسجل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية للمعلوماتية أي من خلال نظام المعالجة الآلية للمعلومات ,بعبارة أخرى يقصد بالمستند المعالج آليا الدعامة المادية التي تم تحويل المعطيات المسجلة عليها لغة الآلة[1].

**ثانيا : المستند ألمعلوماتي :**

وهو ذلك المستند غير المعالج آليا وتعتبر مستندات معلوماتية الأوراق المعدة لتسطير المعلومات عليها والأقراص الممغنطة التي لم يسجل عليها أي شيء بعد ،والملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرامج ،وكذلك أيضا البطاقات البنكية التي لم تدخل الخدمة بعد وهذه إن كان مسجلا عليها معلومات مكتوبة بخط اليد أو مطبوعة أو محفورة ،إلا أنه لم يتم معالجتها بعد، إذ أنها مازالت في مرحلة الإعداد فقط .

**الفرع الثاني : مدى خضوع منتوجات الإعلام الآلي لنصوص التزوير**

الاعتداء على منتوجات الإعلام الآلي يتجسد في فعل التزوير ألمعلوماتي الذي نصت عليه المادة 7 من الاتفاقية الدولية للإجرام ألمعلوماتي إذ أن التلاعب في المعطيات الذي ينتج عنه معطيات غير أصلية يعد تزويرا .

الإشكال المطروح هو هل بمكن تطبيق نصوص التزوير الواردة في قانون العقوبات الجزائري على الاعتداءات الماسة بمنتوجات الإعلام الآلي ؟

للإجابة على هذا التساؤل وجب التطرق إلى مدى انطباق وصف المحرر على البيانات المعالجة آليا ومدى خضوعها لفعل تغيير الحقيقة.

---

**1**- أمال قارة، المرجع السابق، ص 135

**أولا: مدى انطباق وصف المحرر على منتجات الإعلام الآلي:**

موضوع جريمة التزوير هو المحرر والمحرر في مضمونه كتابة مركبة من حروف أو علامات تدل على معنى أو فكرة معينة، وإمكانية القراءة البصرية لمحتواه، وهو ما تفرضه نصوص التزوير التقليدية، وعليه يمكن إجمال خصائص المحرر في ثلاث نقاط:

أن يتخذ المحرر شكلا كتابيا ويجب إدراك مضمون المحرر بالنظر إليه أو لمسه وإذا استحالت قرأته فلا يصلح وسيلة للإثبات و لا عقاب على مااحتواه من تغيير.

أن تكون الكتابة منسوبة لشخص معين .

أن يحدث المحرر أثارا قانونية.

فهل يعتبر البيان المعالج آليا من قبيل المحررات التقليدية التي يسري عليها النص الجنائي الخاص بالتزوير ؟ بإسقاط المفهوم التقليدي للمحرر على مجال المعالجة الآلية للبيانات ، نجد أن تغيير الحقيقة الذي يكون محله الأشرطة الممغنطة لا تقع به جريمة التزوير في المحررات وذلك لعدم وجود عنصر الكتابة فجريمة التزوير تشترط الكتابة فأي تغيير في الوعاء ألمعلوماتي لا يعتبر تزويرا لانتفاء هذا الشرط .

الفقيه (DEVEY) يقرر أن الكتابة مطلب تقليدي في جرائم التزوير، لكن تجدر الإشارة إلى أن بعض الفقه الفرنسي يرى إمكانية تغليب روح النصوص واعتبار ما يظهر على شاشة الحاسب شكلا مستحدثا للمحرر[1] .

الفقه البلجيكي يرى أن نصوص التزوير في المحررات يمكن أن تنطبق في حالة ظهور المعلومات التي تم تزويرها في المستخرجات الورقية .

كما أن جانبا من الفقه السوري يرى تطبيق نصوص التزوير عندما تكون البيانات قد سجلت على أسطوانة أو شريط ممغنط بحيث يعتبر محررا.

وتغيير الحقيقة فيه يعد تزويرا وذلك بسبب انتقال المعلومات و المعطيات المخزنة إلى جسم مادي له سمات المحرر المكتوب و الذي يمكن قراءته بالعين باستخدام الحاسب للكشف على محتواه من قبل الغير فالعبرة بالمادة التي دوّن عليها.

و قد ذهبت بعض التشريعات كمصر (المادة 211) إيطاليا (المادة 485) بلجيكا (المادة 190) فنلندا وسويسرا إلى اشتراط وجود المحرر بمفهومه التقليدي لتطبيق جريمة التزوير، بان يكون محتوى الوثيقة أو الوعاء قابلا للمشاهدة البصرية، فلا يشمل ذلك البيانات المخزنة الكترونيا.

وقد عمدت بعض التشريعات الحديثة لمواجهة القصور في النصوص التقليدية ، إلى استحداث نصوص تجريمية جديدة أو إدخال تعديلات على التشريعات التقليدية، من أجل المعاقبة على جريمة التزوير الواقعة على المستندات المعلوماتية، حفاظا على الثقة الواجب توافرها في المستندات المعلوماتية . ومن أمثلة هذه التشريعات التشريع الفرنسي الذي استحدث نصا خاصا بالتزوير ألمعلوماتي و هو المادة 9/462 من قانون العقوبات وذلك بموجب تعديل 1988، غير أنه و بموجب تعديل 1994 تراجع المشرع الفرنسي عن موقفه وألغى النص الخاص بالتزوير ألمعلوماتي، و أخضعه لنصوص التزوير التقليدية.

وكان السبب الذي أدى إلى إلغاء النص الخاص بالتزوير ألمعلوماتي هو أن إفراد جرائم التزوير الواقعة على المستندات المعلوماتية سوف يكون من غير جدوى مادام مفهوم التزوير غير واضح،وهو ما دفع بالمشرع الفرنسي إلى إدراج تعريف للتزوير في نص المادة 441 من قانون العقوبات التي أصبحت تشمل كل صور التزوير الحديثة التي تنشأ عن استخدام الحاسب الآلي ،كما أن الغاية من تجريم أفعال التزوير هو حماية الثقة العامة، التي تنشأ من تعامل الأفراد بالمحررات بمفهومها التقليدي ، ووضع نص خاص بالتزوير

---

**1**. أمال قارة ،المرجع السابق ،ص137

ألمعلوماتي يحقق حماية للنظام ألمعلوماتي فقط دون الحفاظ على الثقة العامة، وعن طريق وضع نص خاص بالتزوير ألمعلوماتي تخرج المحررات المعلوماتية من المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها، لذلك فإن إلغاء النص يخضع المحررات المعلوماتية إلى النصوص التقليدية الخاصة بالتزوير ،بالمفهوم الجديد للمحررات .

أما بالنسبة للتشريع الجزائري فيعد من التشريعات التقليدية ، حيث أدرج النصوص الخاصة بتزوير المحررات في الأقسام الثالث والرابع و الخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد 124 إلى 229 التي تشترط المحرر لتطبيق جريمة التزوير ،ولم يتخذ أي موقف لتوسيع مفهوم المحرر من أجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير ، وكان من الأفضل لو أضاف المشرع الجزائري في باب التزوير في المحررات نصا يعرف فيه التزوير .

وعليه نقترح إضافة نص إلى باب التزوير في المحررات يعرف فيه التزوير على النحو التالي: كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن الفكر.

وهذا النص قد يكون أشمل حيث يمكن أن تدرج فيه جميع المستندات المعلوماتية حتى وإن كانت غير معالجة آليا، وهو ما يتضمن حماية جزائية فعالة لكافة المنتجات المعلوماتية.

**ثانيا : مدى خضوع منتوجات الإعلام الآلي للنشاط الإجرامي لجريمة التزوير:**

النشاط الإجرامي لجريمة التزوير يتمثل في فعل تغيير الحقيقة و يعني استبدالها بما يخالفها وإذا انتفى هذا التغيير انتفى التزوير و المقصود هو تغيير الحقيقة القانونية النسبية وليس تغيير الحقيقة الواقعية المطلقة، إذ يكفي لتغيير الحقيقة الذي تتطلبه جريمة التزوير أن يكون هناك مساس بحقوق الغير، أو مراكزهم القانونية الثابتة في تلك المحررات، وعليه يمكن تصور تغيير الحقيقة في نطاق المعالجة المعلوماتية بالتلاعب في المعطيات مما يؤثر على أصالتها [1].

و تجدر الإشارة إلى أن تحويل البرامج أو قواعد البيانات لا يعد تزوير و إنما يقع تحت طائلة نصوص التقليد الواردة في قانون حق المؤلف و الحقوق المجاورة.

لا يتصور وقوع فعل تغيير الحقيقة من خلال طرق التزوير المعنوية – و التي كما هو معروف– لا تتحقق إلا أثناء تكوين المستند بالنسبة إلى للجريمة محل البحث.

بينما من المتصور وقوع فعل تغيير الحقيقة بالنسبة لهذه الجريمة من خلال طرق التزوير المادية ،ولكن بشرط أن يكون التزوير لاحقا على نشأة المستند الأصلي و الحقيقي المعالج آليا فلا تتحقق تلك الجريمة من خلال فعل تغيير الحقيقة باستخدام طريقة التزوير المادية أثناء نشأة المستند على خلاف جريمة التزوير العادية[2].

نخلص إلى أن المشرع الجزائري رغم تداركه من خلال القانون 15/04 و المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام ألمعلوماتي وذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة، إلا أنه أغفل تجريم الاعتداءات الواردة على منتوجات الإعلام الآلي، فلم يستحدث نصا خاصا بالتزوير ألمعلوماتي ،و لم يتبنى الاتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

**الفرع الثالث : القانون الجديد: مشروع قانون :الوقاية من الجريمة الإلكترونية.**

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

إن مشروع القانون جمع بين القواعد الإجرائية المكملة لقانون الإجراءات المدنية، وبين القواعد الوقائية

---

**1** – أمال قارة، المرجع السابق، ص 139.

**2**– د. علي عبد القادر القهوجي، المرجع السابق، ص155.

التي تسمح بالرصد المبكر للاعتداءات المحتملة مع التدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

وقد منح نص المشروع دورا ايجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم وكشف مرتكبيها حيث تنص المادة الثالثة منه على وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

ونص مشروع القانون على أربع حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية، عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

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

وعلى هذا الأساس، يجوز للجهات القضائية وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي. ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها.

ولأجل إشراك مزودي خدمات الإنترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم التكنولوجية، يلزم مشروع القانون هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة

بمحتوى الاتصالات في حينها، وبوضع المعطيات الملزمين بحفظها. وتشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات المستعملة في الاتصال، والخصائص التقنية وتاريخ وزمن ومدة كل اتصال، والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وعناوين المواقع المطلع عليها.

أما بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعلومات التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه، على أن يلتزم متعاملو الهاتف بالاحتفاظ بالمعطيات لمدة سنة ابتداء من تاريخ التسجيل.

ويتضمن مشروع القانون أيضا إجراءات عقابية حيث أنه ولتفادي أي تهرب من التزامات القانون، يسلّط هذا الأخير على الأشخاص الطبيعيين الذين يعرقلون سير التحريات القضائية عقوبة السجن من خمس إلى ست سنوات وغرامة مالية تتراوح ما بين خمسة ملايين إلى خمسين مليون سنتيم، مع معاقبة المؤسسات المخالفة بالغرامات المالية المنصوص عليها في قانون العقوبات.

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

**الخاتمة:**

وفي الأخير نخلص القول بان دراسة موضوع الجرائم الواقعة على المواقع الالكترونية لها أهمية بالغة كونها تساهم بالتعريف بنوع جديد من الجرائم والتي بدئت بالظهور و الانتشار في معظم المجتمعات و ترتبط ارتباطا وطيدا بالتكنولوجيا هذا ما أدى إلى تميزها عن الجرائم التقليدية المعروفة.

و لا شك أن القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الأعلام و الاتصال و مكافحتها وتعديل قانون العقوبات بموجب الأمر 04-15 كانت لهما أهمية تدارك الفراغ التشريعي الذي كان يعتري القانون الجزائري وذلك من خلال حسم المشرع الجدل الفقهي القائم حول طبيعة المعلوماتية باعتبارها مالا من نوع خاص باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآليات المعطيات فالفصل الثالث من الباب الثاني من الكتاب الثالث من المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات لكون أن القسم السابع ورد تحت الكتاب الثالث المتعلق بالجنايات و الجنح ضد الأموال .

جاء هذا التعديل كقفزة نوعية في مجال التشريع بحث واكب التشريعات المقارنة بتجسيده معظم الأحكام الاتفاقية الدولية للإجرام ألمعلوماتي من خلال تجريم أفعال الدخول و البقاء الغير مشروع داخل النظام ألمعلوماتي و تحديد العقوبة إذا ترتب عن ذلك مساس بالمعطيات تغييرها أو حذف أو زيادة ، على أساس اعتبار المعطيات المعلوماتية من خلال الفقرة ج من المادة الثانية من قانون 09-04 تشمل برامج التشغيل.

كما أن المشرع الجزائري قد تبنى مسؤولية الشخص المعنوي و وسع نطاق العقوبة بتجريم الشروع في هذه الجرائم بتجريم حتى الأعمال التحضيرية في إطار الاتفاق الجنائي.

بالرغم من مزايا هاذين القانونين إلا أنهما لا يخلوان من العيوب و النقائص و الانتقادات الملاحظة من خلال معالجتنا لهذا الموضوع نذكر منها:

-عدم ذكر المشرع الخصائص التي يجب أن تتوفر عليها المعلومة حتى تتمتع هذه الأخيرة من الحماية ، و المتمثلة في صفات التحديد و الابتكار و السرية و الاستئثار فلو ذكر ذلك صراحة لكان أحسن.

- هناك قصور في تعريف المشرع الجزائري للجرائم المعلوماتية و ذلك بعدم تحديده لصور السلوك الإجرامي ودور المنظومة المعلوماتية في نشاط المجرم ، و ذلك ما ارتأيناه في أحكام المادة 02 من القانون 09-04 التي نصت على أن الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية ،و بما انم بدا الشرعية يحكم المجال الجزائي يجب تحديد بدقة الأفعال المجرمة، إذ أنه لو قال كل اعتداء على نظام المعلوماتي أو كل اعتداء يتم باستخدام النظام المعلوماتي و كان له دور رئيسي في السلوك المجرم.
- باعتبار الجريمة المعلوماتية هي جريمة بدون حدود ، فقد تبقى إشكاليتها قائمة من حيث الاختصاص و المتابعة و الإثبات فمن هنا يستوجب للدول التدخل على محورين أولهما داخلي أي من حيث ملائمة تشريعاتها مع هذا النوع الجديد من الجرائم و ثانيها دولي عن طريق إبرام اتفاقيات دولية جماعية ، من هنا حاول المشرع الجزائري على المستوى الداخلي التعامل مع هذا النوع من الجرائم و ذلك بسنه قانون 04-15 و 09-04 لكن لا زالت مبادرته على المستوى الدولي قاصرة.
- بالرجوع إلى الامر03-05 المتعلق بحق المؤلف و الحقوق المجاورة ، تطبيقات الإعلام الآلي ضمن المصنفات المحمية من خلال المادة الرابعة، إلا أن هذه الحماية المقررة بموجب هذا الأمر قاصرة لكون مفاهيم التقليدية لحق المؤلف لا تتماشى مع خصوصيات برامج الحاسب الآلي ومن ثم وجب تعديل قانون الملكية الأدبية و الفنية فيما يخص تقليص مدة الحماية من خمسين سنة بعد وفاة المؤلف بما يتماشى و طبيعة برامج الحاسب الآلي و هذا مع التطور السريع الذي تشهده المعلوماتية و تقرير نصوص تجريمية خاصة لكل مساس بالمعلوماتية مراعاة لطبيعتها الخاصة.
- زد على ذلك عدم تجريم المشرع الجزائري التزوير المعلوماتي فلهذا يجب تدارك الأمر كي لا يكون هناك فراغ تشريعي من خلال استحداث نص خاص به أو بتوسيع مجال التزوير عن طريق توسيع مفهوم المحرر .

- أهمل المشرع تقرير نصوص خاصة للأفعال التي يكون النظام المعلوماتي وسيلة مسهلة لارتكابها كالجرائم الأخلاقية و الإرهابية المرتكبة عبر الأنظمة المعلوماتية فلذلك يتعين عليه مراجعة هذا الأمر.
- كما أنه بالإمكان تكوين فرق من الضبطية متخصصين في مجال المعلوماتية وقضاة متخصصين في مجال الجرائم المعلوماتية على غرار ما هو معمول به في الدول المتقدمة .
- وفي الأخير و رغم جهود المشرع الجزائري لسد الفراغ التشريعي لمواجهة هذه الجرائم إلا أن نصوصه لا تزال ناقصة خاصة فيما يتعلق بالاعتداءات على الأموال المعلوماتية "التزوير المعلوماتي".

# قائمة المراجع

## المراجع باللغة العربية:

### 1.القوانين الدولية :


- اتفاقية مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية ، رقم ( 63 / 55 )، الصادرة عن هيئة الأمم المتحدة ، الجلسة العامة 81 ديسمبر 2000.
- مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة و العدالة الجنائية، البند الثامن من جدول الأعمال المؤقت ، التطورات الأخيرة، في استخدام العلم و التكنولوجيا من جانب المجرمين و السلطات المختصة في مكافحها بما فيها الجرائم الحاسوبية ، المنعقد بالبرازيل 12-19 أبريل 2010، رقم 09 / 213 A/Conf .
- مؤتمر هيئة الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المعلوماتية عبر الوطنية، المنعقد بفينا في 18-22 أكتوبر 2010، رقم 5 , CTOC/Cop/2010/crp.


### 2.النصوص القانونية:


- الأمر 10/97 المؤرخ في 1997/03/06 المتعلق بحق المؤلف و الحقوق المجاورة ، الجريدة الرسمية عدد 13 صادر في 12-03-1997.
- الأمر 07/03 المتعلق براءات الاختراع، الجريدة الرسمية العدد 44 صادرة في 23-07-2003.
- الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 44 صادرة في 23-07-2003.
- الأمر 04-15 مؤرخ في 10-11-2004 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 الصادرة في 10-11-2004.
- الأمر رقم 09-04 المؤرخ في 05-02-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، الجريدة الرسمية عدد47 لسنة 2009.
- الأمر 03-06 مؤرخ في 19 جويلية 2003، المتعلق بالعلامات الجديدة عدد 44 صادر في 23 جويلية 2003.

## 3. الكتب :


- آمال قارة : الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة الجزائر 2006.
- أحمد فتحي سرور : نظرية البطلان في قانون الإجراءات الجزائية .رسالة دكتوراه سنة . 1959 جامعة القاهرة.
- د .احمد فتحي سرور ، الحماية الجنائية لأسرار الأفراد في مواجهة النشر، رسالة .ماجستير، كلية الحقوق ، جامعة القاهرة1991
- د .إسحاق إبراهيم منصور المبادئ الأساسية في قانون الإجراءات الجزائري .ديوان .المطبوعات الجامعية 1979
- إيهاب فوزي السقا :جرائم التزوير في المحررات الإلكترونية، دار الجامعة الجديدة 2008.
- د .جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة2001
- .د .خالد إبراهيم ممدوح، الجرائم المعلوماتية دار الفكر الجامعي ط1 2009
- .د .رأفت منير : فيروس الحاسبات و طرق الوقاية، مجلة المهندسين القاهرة1990
- مسيس بنهام :النظرية العامة للقانون الجنائي، منشأ المعارف لإسكندرية1995
- زيبحة زيدان : الجريمة المعلوماتية في التشريع الجزائري و الدولي .دار الهدى. الجزائر .ط2011
- سامي صادق الملا :اعتراف المتهم .ط1 1982
- سليمان عبد المنعم : النظرية العامة لقانون العقوبات، دار الجامعة الجديدة الإسكندرية 2000.
- طارق إبراهيم الدسوقي عطية : الأمن المعلوماتي النظام القانوني للحماية المعلوماتية. 2009، دار الجامعة الجديدة .ط1
- عادل قورة .محاضرات في قانون العقوبات، القسم العام –الجريمة، ديوان .المطبوعات الجامعية 1992

- عبد الفتاح بيومي حجازي : مكافحة جرائم الكمبيوتر و الإنترنت في القانون العربي النموذجي، دار الفكر الجامعي الإسكندرية2006
- عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة الإسكندرية1997
- د .عبد الله اوهايبية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومة للطباعة و النشر والتوزيع2008
- د .عبد الله عبد الكريم عبد الله الحماية القانونية لحقوق الملكية الفكرية على شبكة الأنترنت .دار الجامعة الجديدة.
- عفيفي كامل عفيفي :جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة والقانون، منشورات الحلبي الحقوقية / طبعة ثانية 2007 .
- علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب و الأنترنت .دار الجامعة الجديدة 2008
- د . عمر الفاروق الحسيني، تأملات في بعض صور الحماية الجنائية لنظام الحاسب الآلي، ماي 1991. تقرير مقدم إلى اتحاد المصارف العربية في دورته التدريبية التي عقدت في القاهرة بتاريخ 1991/09/25
- عمر محمد بن يونس :الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي. رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، سنة 2004
- فوزية عبد الستار :شرح قانون العقوبات القسم الخاص، دار النهضة العربية 1988.
- د .محمد امين الشوابكة، جرائم الحاسوب و الانترنت، الجريمة المعلوماتية، دار الثقافة 2009.ط 1
- محمد زكي أبوعامر :الإجراءات الجنائية، الجامعة الجديدة/الطبعة الثامنة2008
- محمد علي العريان : الجرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية 2004
- نائلة عادل محمد فريد قورة :جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية2005

- نعيم مغبغب : حماية برامج الكمبيوتر الاساليب و الثغرات دراسة في القانون المقارن، منشورات الحلبي الحقوقية ط1 2006
- نهلا عبد القادر المومني :الجرائم المعلوماتية .رسالة ماجيستر، دار الثقافة للنشر و التوزيع، طبعة 2، 2010.
- هدى حامد قشقوش :جرائم الحواسب الإلكترونية في التشريع المقارن، دار النهضة العربية القاهرة 1992
- هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة /الطبعة الرابعة 1994
- هلالي عبد الله أحمد :تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي دار النهضة العربية القاهرة2000
- جرائم الكمبيوتر والإنترنيت لمحمد أمين الرومي، الطبعة 2003،
- احمد عبد الرزاق السنهوري ، الوسيط في شرح القانون المدني ، حق الملكية ، الجزء الثاني ، دار إحياء التراث العربي ، بيروت 1952.
- د. علي عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999.
- – محمد الولادي" جرائم الحاسوب وحقوق المؤلف" يوم دراسي منظم بتعاون بين وزارتي العدل والاتصال. 28 أبريل 99 .


**4. المقالات :**


- بشرى النية، " حماية الحاسوب عن طريق قواعد القانون الجنائي حماية للمصالح الخاصة والنظام العام، مقال منشور بالمجلة المغربية لقانون الأعمال والمقاولات، العدد7، 2005.
- محمد بوطيبة حماية برامج الحاسوب طبقا لقانون 00- 2 المنظم لحقوق المؤلف والحقوق المجاورة، مقال منشور بمجلة القضاء والقانون، العدد 150، 2004.

- فايز بن عبد الله الشهري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنيت، الدليل الإلكتروني للقانون العربي arablawinfe .
- تركي محمد الوطيان، جرائم الحاسب الآلي: دراسة نفسية تحليلية، هذا المقال موجود على الموقع / WWW.Minshawi.COM. PDR other/
- عبد القادر دوحة، محمد بن حاج الطاهر " مدى مواكبة المشرع الجزائري لتطور الجريمة الالكترونية" الملتقى الوطني الأول ، النظام القانوني للمجتمع الالكتروني، المركز الجامعي خميس مليانة، معهد العلوم القانونية والادارية، 09-10 مارس 2008.


**4. المذكرات:**


- صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، مذكرة لنيل شهادة الماجستير في القانون ، تخصص قانون دولي للاعمال ، جامعة مولود معمري –تيزي وزو 2013.
- سمية مزغيش ، جرائم المساس بالأنظمة المعلوماتية ، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق ، تخصص قانون جنائي، جامعة محمد خيضر –بسكرة 2014.


**5.المراجع باللغة الأجنبية:**


- la criminalité informatique sur l'Internet, journal of Law ñ 1- val 26, mars 2002, p : 45 . Mohammed ----
- Bouchaib RMAIL, la criminalité informatique, criminalité a double dimension :internationale, thèse pour l'obtention du grade de ducteur en droit privé- option : droit des affaires, faculté des sciences juridiques, économiques et sociales- fés, 2005.

- Philippe JOUGLEDX, droit des médias, faculté de droit d'aix- Marseille, dans le thème : « la criminalité dans le cuber- espace », 1999, p : 25 et suivants. oteyom.

# فهرس المحتويات

## الفصل الأول:

## المكافحة الموضوعية و التحديات الإجرائية للجريمة الواقعة على المواقع الإلكترونية

## الفصل الثاني

## جهود المشرع الجزائري للحد من الجريمة الواقعة على المواقع الإلكترونية