**وزارة التعليم العالي والبحث العلمي**

**جامعة أحمد دراية – أدرار -**

**كلية الحقوق والعلوم السياسية**

**قسم الحقوق**

# الحماية الجنائية لنظام المعالجة الآلية للمعطيات

## - دراسة مقارنة -

**رسالة مقدمة لاستكمال متطلبات الحصول على شهادة دكتوراه الطور الثالث**

**تخصص قانون جنائي**

**إعداد الطالب**

الطيبي البركه

**الأستاذ المشرف**

الدكتور حاج سودي محمد

| لجنة المناقشة | | | |
|---|---|---|---|
| أ.د بن عومر محمد الصالح | أستاذ التعليم العالي | جامعة أدرار | رئيسا |
| د. حاج سودي محمد | أستاذ محاضر قسم "أ" | جامعة أدرار | مشرفا ومقررا |
| أ.د يوسفات علي هاشم | أستاذ التعليم العالي | جامعة أدرار | مناقشا |
| د.كابوية رشيدة | أستاذ محاضر قسم "أ" | جامعة أدرار | مناقشا |
| أ.د ماينو جيلالي | أستاذ التعليم العالي | جامعة بشار | مناقشا |

**الموسم الجامعي: 2021/2020**

# بسم الله الرحمن الرحيم

﴿ صُنْعَ ٱللَّهِ ٱلَّذِيٓ أَتْقَنَ كُلَّ شَيْءٍ ۚ إِنَّهُۥ خَبِيرٌۢ بِمَا تَفْعَلُونَ ﴾ سورة النمل: بعض من الآية رقم 88

برواية ورش عن نافع

# إهداء

إهدي هذا العمل المتواضع

إلى أبي رمز العطاء رحمه الله

وإلى أمي عنوان المحبة والحنان أطال الله في عمرها

وإلى رفيقة دربي زوجتي الغالية

وإلى أملي المتجدد في الحياة أولادي عبدالحي، يونس، مريم.

وإلى من أشد بهم أزري إخوتي

وإلى كل الأهل والأقارب وجميع الإصدقاء.

طالب دكتوراه

الطيبي البركه

# شكر وتقدير

أول الشكر وآخره إلى العليم الخبير الذي منحني الصبر والقوة ووفقني لإتمام هذا العمل العلمي المتواضع

ثم أتوجه بجزيل الشكر والإمتنان إلى الدكتور حاج سودي محمد لقبوله الإشراف على هذه الرسالة، إذ لم يبخل علي بإرشادته ونصائحه وتوجيهاته القيمة لإثراء هذا العمل رغم مشاغله الكثيرة.

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه الرسالة دون أن أنسى شكر كل من قدم لي يد العون من قريب أو بعيد في إنجاز هذا العمل

طالب دكتوراه

الطيبي البركه

# قائمة أهم المختصرات

| الرمز | الكلمة |
|---|---|
| ج ر ج ج | الجريدة الرسمية للجمهورية الجزائرية |
| ب ط | بدون طبعة |
| ب س ن | بدون سنة نشر |
| ط | الطبعة |
| ص | الصفحة |
| ص ص | من الصفحة إلى الصفحة |
| ع | العدد |
| P | Page |
| Ed | Edition |
| JORF | Jornal officiel de la Rèpublique Francaise |
| N° | Numèro |
| Art | Article |

# مقدمة

**مقدمة:**

شهد العالم منذ منتصف القرن العشرين ثورة جديدة أصطلح على تسميتها بالثورة المعلوماتية وذلك إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن، ومما لا شك فيه أنه نتيجة للتقنيات العالية التي تقوم عليها قد تركت آثاراً ايجابية وشكلت قفزة حضارية نوعية في حياة الأفراد والدول، حيث تعتمد القطاعات المختلفة في الوقت الحالي في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظراً لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها ومن تم نقلها وتبادلها بين الأشخاض والجهات والشركات والمؤسسات المختلفة داخل الدولة الواحدة وبين عدة دول، إضافة الى أنها تعد مستودعا لكم هائل وضخم من البيانات والمعطيات الشخصية والإقتصادية والمالية والعسكرية، وتعتبر الشبكات الإلكترونية بمختلف أنواعها ممرا لنقلها من مركزها الى كافة أنحاء العالم، مما جعل نطاقها لا يقتصر على المستوى المحلي بل يتعداه الى المستوى الأقليمي والدولي.

إلا أن هذا الجانب الإيجابي للأنظمة المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية العالية والمتمثلة في إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبصورة تضر مصالح الأشخاص والجماعات.

كما أن الإستخدام المتزايد للأنظمة المعلوماتية وبالرغم من ما تحققه من فوائد جمة في مجال الرقي والتقدم التكنولوجي والأنساني إلا أنه أدى الى كثير من المخاطر التي تهدد الدول والأشخاص وتمس بمعطياتهم ذات الطابع الشخصي في مجال عالم مفتوح لكل أنواع الجرائم المعلوماتية التي يصعب حصرها أوتعدادها.

وضمن طائفة هذه الجرائم المعلوماتية المتعددة الصور نجد جرائم المساس بأنظمة المعالجة الآلية للمعطيات والتي بدورها جاءت كنتيجة للتطور التكنولوجي الهائل الذي أصبح يربط العالم بشبكة معلوماتية عنكبوتية أمتدت الى كافة إنحاء العالم.

وتعد جرائم نظم المعالجة الآلية للمعطيات من الجرائم المعلوماتية المستحدثة باعتبارها تشكل نمطا جديدا من الجرائم العابرة للحدود وذات طبيعة خاصة وترتكب عبر أساليب إجرامية حديثة وتحصي جميع السلوكات غير المشروعة المرتكبة ضد أمن نظام

المعلوماتية أو المعطيات المدرجة ضمن هذا النظام بواسطة عمليات إلكترونية، والذي يقوم على ثلاثة مبادئ وهي:

1- ضمان سرية المعطيات المدرجة ضمن نظام المعالجة الآلية للمعطيات: بحيث لا يمكن الدخول إليها إلا من قبل الأشخاص المسموح لهم بذلك سواء لكل النظام أو جزء منه فقط.

2- ضمان تكامل المعطيات وسلامة محتواها: ويتم ذلك من خلال الحفاظ على سلامة المعلومات وكمال المعلومات المخزنة في النظام، بحيث لا يقوم هذا الأخير بحرق هذه المعلومات أو يسمح لأي شخص ماكر غير مخول بإجراء أي تعديل عليها.

3- توافر المعطيات: ويعني ذلك أن يقوم نظام المعالجة الآمن بالحفاظ على المعلومات متوافرة ويسمح بالوصول الموثوق إلى هذه المعلومات عند الحاجة إليها من قبل الأشخاص المخولين.

وترتكب من طرف مجرم معلوماتي كانت أهم خاصية له في السابق عند بدايات الكتابات الأولى عن الجريمة المعلوماتية هي الذكاء، ولكن بمرور عشريتين تغيرت الأوضاع وأضحى كل رجل عادي يعرف أبجديات بسيطة في إستعمال جهاز الحاسوب، يمكن له إرتكاب إي جريمة معلوماتية قد نتصورها تقع على شبكة الأنترنت، نظرا لتوافر برامج وتطبيقات مجانية تسهل له إرتكابها، وإنتشار العديد من المواقع الإلكترونية، المدونات ومواقع الدردشة التي تشرح بكيفيات مبسطة طرق القرصنة والإحتيال وغيرها من الجرائم المعلوماتية، والأكثر من ذلك هو إنتشار برامج تخفي آثار الجريمة ومعالمها مما يجعل من الصعب جدا التعرف على مرتكبها([1])

ومن خلال ما تم ذكره وجب التصدي فنيا وتشريعيا لتلك السلوكات غير المشروعة ودرء تلك المخاطر والتهديدات التي تمس بالنظام المعلوماتي للموازنة بين حاجيات المجتمع لجمع وتخزين ومعالجة البيانات إلكترونيا وضمان حماية هذه المعلومات من الإستخدام غير المشروع، وكذا إيجاد السبل الكفيلة للحد من الإعتداءات التي تقع عليها،

[1]- مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات(ماهيتها، صورها، الجهود الدولية لمكافحتها)- دراسة مقارنة-، دار الخلدونية، الجزائر، ط 1439هـ-2018م ، ص 41.

لا سيما وأن مهمة تقرير الحماية الجزائية للمعلوماتية مهمة صعبة لتشعب الجوانب المتعلقة بها، واتسامها بطبيعة علمية تقنية وفنية.

واختلفت وجهات نظر الفقهاء والمشرعين والقضاة فيما يخص أمر الحماية الجنائية المقررة للنظم المعلوماتية من خلال نصوص الملكية الفكرية أو من خلال نصوص جرائم الاموال أو من خلال نصوص مستحدثة.

فعلى الصعيد الدولي تم خلق آليات قانونية للحماية الجنائية من جرائم نظام المعالجة الآلية للمعطيات بسن عدة إتفاقيات دولية للحد من مخاطرها التي تمس بالأشخاص والممتلكات، ومن أهما إتفاقيتان هما:

1- إتفاقية بودابست: شهدت العاصمة المجرية بودابست بتاريخ 22 نوفمبر سنة 2001، ميلاد أولى المعاهدات الدولية في مكافحة جرائم الأنترنيت التي تبلور التعاون والتضامن الدولي في محاربتها، وتسمى إتفاقية الإجرام السبيري"الإجرام عبر الأنترنت" وقد صدرت هذه الإتفاقية عن المجلس الأروبي، وقعت عليها 30 دولة ودخلت حيز التنفيذ إبتداء من أول يناير 2007، كما إشتملت على عدة جوانب من جرائم الأنترنت.

2- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات: هي التي وافق عليها مجلس وزراء الداخلية والعدل العرب في إجتماعها المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 21 ديسمبر 2010([1]).

وعلى الصعيد الداخلي سارعت العديد من دول العالم الى إتخاذ التدابير اللازمة لمواجهة هذه النوعية من الجرائم، فبعض الدول حرصت على أن تضمن تشريعاتها هذه النوعية من الجرائم إما عن طريق تحديثها وإدماجها في قوانين العقوبات أو عن طريق النص عليها إستقلالا في تشريعات خاصة أو مستقلة أو عن طريق الجمع بين مختلف الأساليب السابقة.

ومن أهم التشريعات الغربية التي نصت على جرائم نظام المعالجة الآلية للمعطيات من خلال تحديث قوانينها وإدماجها في قوانين العقوبات هي التشريع الفرنسي الذي تيقن بأن التصدي الفعال لجرائم نظام المعالجة الآلية للمعطيات لن يكون إلا من خلال سن

---

1- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، ، دار المطبوعات الجامعية، مصر، ط الأولى، سنة 2019، ص 7، 8.

نصوص عقابية وإجرائية خاصة بهذه الجرائم وإدخاله عدة تعديلات على إجراءات المتابعة والتحقيق والإثبات التقليدي لمحاصرة هذه الجرائم.

فكانت أولى المحاولات لمد سلطان قانون العقوبات لحماية المال المعلوماتي بفرنسا من طرف وزير العدل سنة 1985، عندما تقدم بمشروع قانون عقوبات جديد أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان" الجرائم في المادة المعلوماتية" يتكون من ثمانية مواد من 1/307 إلى 8/307، لكن هذا المشروع لم يجد سبيله للتطبيق.

ثم كانت محاولة ثانية تقدم بها النائب Jacque Cod frain([1]) ونواب آحرون إلى الجمعية الوطنية في الخامس من أغسطس عام 1986 بإقتراح مشروع قانون عن الغش المعلوماتي fraude informatique، هذا الإقتراح حاول تعديل وتطويع بعض النصوص القائمة في قانون العقوبات، والتي تتناول جرائم تقليدية كالسرقة وخيانة الأمانة والتزوير والإتلاف والإخفاء، فتعددت بذلك المناقشات حول هذا المشروع في البرلمان الفرنسي ووصلت ثلاث مرات أمام الجمعية الوطنية ومرتين أمام مجلس الشيوخ، وطال أمدها حتى أستغرقت عام ونصف لتسفر في النهاية عن إقرار قانون تشابه إلى حد كبير مع المشروع الأول الذي تقدم به وزير العدل عام 1985، وتم إدماجه في قانون العقوبات الفرنسي ليشكل الباب الثالث من الكتاب الثالث من القسم الثاني منه متعلقا بالجرائم المعلوماتية وذلك في المواد من 2/462 إلى 9/462([2]).

وأصدر المشرع الفرنسي فيما بعد قانون العقوبات الفرنسي الجديد الصادر سنة 1992([3]) الذي طبق إعتبارا من أول مارس 1994، وأضاف فصلا ثالثا للباب الثاني من القسم الثالث من قانون العقوبات تحت عنوان إنتهاكات نظم المعالجة الآلية للبيانات

---

[1]- قود فران هو أحد نواب البرلمان الفرنسي الذي عدل بصفة نهائية رفقة نواب آخرين نظرة المشرع الفرنسي حول إعتبار الأنظمة المعلوماتية عبارة عن مال في حد ذاته ولا بدا على قانون العقوبات أن يحميه من المساست غير المشروعة، أنظر: محمد علي سويلم، مرجع سابق، ص 50.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الأسكندرية، ب ط، 2007، ص 66،67.

[3] -Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur, JORF n° 0298 du 23 décembre 1992.

بموجب المواد من 1/323 الى8/323، والذي شهد فيما بعد عدة تعديلات في هذا المجال أبرزها سنة 2004 وكان آخرها سنة 2015.

كما نصت العديد من التشريعات الغربية على جرائم نظام المعالجة الآلية للمعطيات في تشريعات خاصة أو مستقلة، ومن أهمها التشريع السويدي الذي يعتبر أول من سن تشريعا ضد جرائم الأنترنت أو جرائم المعلوماتية، لا سيما التزوير المعلوماتي، بإصداره قانون البيانات السويدي عام 1973 الذي عالج قضايا الدخول غير المشروع للبيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها، والتشريع الدنماركي الذي سن قانون مكافحة جرائم الحاسب الآلي والأنترنت الدنماركي عام 1985 الذي شمل في فقراته العقوبات المحددة لجرائم الحاسب الآلي، وكذلك التشريع الأمريكي الذي أصدر قانون الإحتيال وإساءة إستخدام الحاسب الآلي سنة 1986، بالإضافة إلى المشرع البريطاني الذي أصدر قانون إساءة إستخدام الحاسب في 29 يونيو سنة 1990 ودخل حيز التنفيذ إعتبارا من 29 أوت 1990([1]).

أما بالنسبة لبعض التشريعات العربية التي نصت على جرائم نظام المعالجة الآلية للمعطيات من خلال تحديث قوانينها وإدماجها في قوانين العقوبات نذكر من بينها المشرع القطري الذي عدل قانون العقوبات القطري رقم 11 لسنة 2004 المؤرخ بتاريخ 10 ماي 2004([2])، بحيث أضاف فصلا خامسا للباب الثالث من الكتاب الثالث تحت عنوان جرائم الحاسب الآلي بموجب المواد من 370 الى 387.

فضلا عن ذلك، فإن العديد من التشريعات العربية هي الأخرى نصت على جرائم نظام المعالجة الآلية للمعطيات في تشريعات خاصة أو مستقلة، ومن أهمها المشرع السوذاني الذي أصدر قانون جرائم المعلوماتية سنة 2007، والمشرع المغرب الذي أصدر القانون رقم 03-07 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات لسنة

[1]- هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، دار النهضة العربية، ط الأولى، 1997، ص 108.

[2]- قانون رقم 11 المؤرخ في 10 ماي 2004، المتضمن قانون العقوبات القطري، جريدة رسمية، ع 7 المؤرخة في 30 ماي 2004.

2007، والمشرع السعودي الذي أصدر قانون نظام مكافحة جرائم الأنترنت الصادر بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8هـ بناء على قرار مجلس الوزراء رقم 79 بتاريخ 1428/3/7هـ، والذي طبق إعتبارا من 26 مارس 2008، ويتكون من 16 مادة([1])، والمشرع العماني الذي أصدر المرسوم السلطاني العماني رقم 12 لسنة 2011 المتضمن قانون جرائم مكافحة تقنية المعلومات([2])، وكذلك المشرع البحريني الذي أصدر القانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات([3])، والمشرع الكويتي الذي سن القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، وكذا قرار السلطة الفلسطيني الذي صدر بموجب القانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية([4])، وأخيرا أصدر المشرع المصري القانون رقم 175 لسنة 2018([5]) بشأن مكافحة جرائم تقنية المعلومات([6]).

أما بالنسبة للتشريعات التي نصت على جرائم نظام المعالجة الآلية للمعطيات عن طريق الجمع بين مختلف الأساليب السابقة أهمها التشريع الجزائري الذي أعتمد على إستراتيجية مزدوجة لمواكبة تطور جرائم نظام المعالجة الآلية للمعطيات، بحيث أنه قام من جهة بتعديل العديد من التشريعات الجزائية ( العقوبات والإجراءات) وجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والإتصال، بداية بوضعه نصوص خاصة لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 04-15 المؤرخ في 10

---

[1]- نظام مكافحة الجرائم المعلوماتية رقم 17 الصادر بتاريخ 2007/03/26 ، الجريدة الرسمية، مجموعة الأنظمة السعودية.

[2]- مرسوم سلطاني رقم 12 الصادر بتاريخ 2011/02/06، بشأن قانون مكافحة جرائم تقنيات المعلومات، الجريدة الرسمية لسلطنة عمان، العدد 929.

[3]- القانون البحريني رقم 60 لسنة 2014، بشأن جرائم تقنية المعلومات، الجريدة الرسمية البحرينية، المؤرخة في 9 أكتوبر 2014، العدد 3178.

[4]- القرار الفلسطيني بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية، الصادر في مدينة رام الله بتاريخ 24 يونيو 2017م.

[5]- قانون رقم 175 لسنة 2018، بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية المصرية، العدد 32 مكرر (ج) الصادرة بتاريخ 2018/08/14.

[6]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، دار المطبوعات الجامعية، مصر، ط الأولى،سنة 2019، ص 12،13.

نوفمبر 2004، المتضمن تعديل قانون العقوبات([1])، باعتبارها مال معلوماتي من نوع خاص باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات في الفصل الثالث من الباب الثاني من الكتاب الثالث من المواد 394 مكرر الى 394 مكرر 8 من قانون العقوبات المعدل بالقانون 16-02 المؤرخ في 19 يونيو سنة 2016([2]) لكونه ورد تحت الكتاب الثالث المتعلق بالجنايات والجنح ضد الاموال، مستحدثا فيه جملة من النصوص جرم من خلالها الإعتداءات الواردة على نظم المعالجة الآلية للمعطيات وحدد لكل فعل منها ما يقابله من الجزاء، وقام الى جانب ذلك بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة لجرائم نظام المعالجة الآلية للمعطيات، وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 06 جوان 1966، المتضمن قانون الإجراءات الجزائية([3]).

ومن جهة ثانية قام المشرع الجزائري بسن قوانين أخرى خاصة أكثر إنسجاما مع الطبيعة المميزة لجرائم نظام المعالجة الآلية للمعطيات بإستحداثه القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها([4])، والذي يجمع بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة بتحديد مصدرها والتعرف على مرتكبها، وكذا القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع

---

[1]- قانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، ج ر ج ج، ع 71 المؤرخة في 10 نوفمبر سنة 2004، ص 11.

[2]- قانون رقم 16-02 مؤرخ في 14 رمصان عام 1437 الموافق 19 يونيو سنة 2016، يتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 والمتصمن قانون العقوبات، ج ر ج ج، ع 37.

[3]- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 06 جوان 1966، المتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 84 المؤرخة في 24 ديسمبر 2006.

[4]- قانون 09-04 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتهما، ج ر ج ج، ع 47، المؤرخة في 16 غشت سنة 2009.

الشخصي([1])، والذي يحوي مجموعة من الضمانات التي تحمي البيانات الشخصية للشخص الطبيعي وتضمن عدم المساس بحياته الخاصة، وإلى جانب ذلك صدر المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي سنة 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية([2])، باعتبارها أداة الدولة في مجال الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها.

وعلى هذا الأساس فأن موضوع الأطروحة المتعلق بالحماية الجنائية لنظام المعالجة الآلية للمعطيات يتمحور حول أن يكون النظام هو من تقع عليه الجريمة (موضوع الجريمة) ولا ترتكب بواسطته (وسيلة لإرتكابه)، وأن يكون معالج آليا وليس يدويا، كما أنه يحتوي على معطيات عديدة بغض النظر عن نوعها، شريطة أن تكون مدرجة فيه أو لها علاقة به، وذلك من خلال دراسة مقارنة للتشريع الجزائري بالتشريعين الفرنسي والمصري، وكذا مدى مسايرته لإتفاقية بودابست والإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وتتجلى أهمية هذه الدراسة في كونها تتعلق بمطلب أساسي ينشده جميع مستخدمي نظام المعالجة الآلية للمعطيات سواء كانوا أشخاص أو مؤسسات أو هيئات وهو ضمان حماية جنائية خاصة لأمن النظم المعلوماتية ولكافة المعطيات التي تحتويها، في الوقت الذي يتنامى فيه الإعتماد على هذه النظم في جمع ونقل المعلومات والبيانات الخاصة بالأشخاص الطبيعيين والمعنويين وتخزينها ومعالجتها، وظهور ما يعرف ببنوك المعلومات، بحيث أصبحت المعلومات المخزنة في تلك النظم عرضة لمخاطر إساءة الإستخدام والوصول إليها بطرق غير مشروعة، أكثر من إي وقت مضى إذا ما تم مقارنتها بالوضع التقليدي الذي تكون فيه المعلومات والبيانات في سجلات ورقية تحفظ في خزائن خلف أبواب مغلقة.

كما أن تطور جرائم المساس بأنظمة المعالجة الآلية للمعطيات أدى بشكل كبير إلى تزايد فرص ارتكابها، لذا كان من الضروري دراسة هذا الموضوع من أجل تسليط الضوء

---

1- قانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعين في مجال المعطيات ذات الطابع الشخصي، ج ر ج ج،ع 34، المؤرخة في 29 ديسمبر سنة 2018.

2- مرسوم رئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر ج ج، ع 04، المؤرخة في 26 جانفي سنة 2020 م.

على هذه الجريمة باعتبارها تتميز بعنصري السرعة والدقة، وكونها تمس بالفرد والدولة بمؤسساتها العامة والخاصة، وليس على المستوى الداخلي فحسب بل يمتد أثرها على المستوى الدولي مما جعل دول العالم تلجأ الى إبرام إتفاقيات دولية ثنائية ومشتركة لمواجهة هذه الجرائم، ولعل أبرزها إتفاقية بودابست والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لتواكب بها التطور المستمر لهذه الأنظمة التي ينتج عنها ظهور أنواع جديدة من الجرائم.

كما يستمد موضوع الدراسة أهميته لما له من إنعكاسات هامة من الناحية العملية في جميع دول العالم على بيئة التعاملات الإلكترونية في كافة المجالات سواء كانت تجارية أو مصرفية أو إدارية أو غيرها.

ولقد وقع اختياري على هذا الموضوع بسبب تقنية هذا الموضوع وصعوبة تمييز جرائم نظام المعالجة الآلية للمعطيات عن غيرها من الجرائم المشابهة لها كالجرائم المعلوماتية والإلكترونية أو جرائم الأنترنت، إضافة إلى ميلي الشخصي للكتابة في مثل هذه المواضيع، هذا بالنسبة للأسباب الذاتية.

أما بالنسبة للأسباب الموضوعية تتمثل في ضرورة الوقوف على هذا النمط من الجرائم الذي بدأ يغزو مجتمعنا الجزائري وله مخاطر عدة تمس بجميع مناحي الحياة، المدنية والسياسية والإقتصادية والعسكرية، ومعرفة مدى قدرة النصوص القانونية في الحد من جرائم نظام المعالجة الآلية للمعطيات سواء كانت هاته النصوص مدمجة في قانون العقوبات أو في نصوص قانونية مستقلة لمكافحة هذا النوع من الجرائم.

وتبعا لذلك سأعالج في هذه الدراسة مسألة الحماية الجنائية لنظام المعالجة الآلية للمعطيات، وذلك من خلال دراسة الأحكام القانونية الخاصة بالنظام، وفحص قدرة النصوص الموضوعية والإجرائية على توفير الحماية الجنائية اللازمة للمعطيات المدرجة ضمن نظام المعالجة الآلية للمعطيات سواء كانت عامة أو شخصية، في ظل قصور الحماية الفنية لنظام المعالجة الآلية للمعطيات، بالإضافة إلى القيمة الاقتصادية الكبيرة لبعض المعطيات التي يحتويها، وهذا وفق الإشكالية التالية:

**ما مدى كفاية الحماية الجنائية بشقيها الموضوعية والاجرائية في الحد من جرائم المساس بنظام المعالجة الآلية للمعطيات؟**

ويتفرع عن هذه الإشكالية إشكاليات جزئية تتمثل في:

- ما هو النظام المقصود بالحماية الجنائية من الإعتداءات غير المشروعة؟
- وكيف تتم حماية المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات من أي تهديدات تمس مصالح الأشخاص والدول؟
- وما هي الإجراءات والتدابير الكفيلة للحد من جرائم المساس بنظام المعالجة الآلية للمعطيات؟

وباعتبارها تأتي في إطار الدراسات القانونية فقد تم الاعتماد على المنهج التاريخي والتحليلي والمقارن حيث تم إتباع المنهج التاريخي الذي يساهم في التعرف على ماضي الجرائم المعلوماتية بشكل منظم وموضوعي يساعدنا على الإلمام بمفاهيم الأنظمة المعلوماتية عبر مراحل التاريخ المختلفة، وإتباع المنهج التحليلي لتحليل النصوص القانونية التي أقرها المشرع الجزائري والتشريعات المقارنة في هذا المجال وتحليل المخاطر الناجمة عن جرائم المساس بنظام المعالجة الآلية للمعطيات ودواعي الحماية الجنائية منها، واتباع المنهج المقارن نظرا لكون موضوع الدراسة هو دراسة مقارنة، وأن الدول الاجنبية هي السباقة في سن قوانين في هذا المجال، وإنشئت هيئات دولية وإقلمية لمكافحة هذا النوع من الإجرام، فيظهر ذلك جليا من خلال مقارنة التشريع الجزائري مع التشريعات الأخرى ومدى مسايرته لها، وأهمها التشريع الفرنسي وبعض التشريعات الأخرى.

ومن أهم الدراسات السابقة في هذا الموضوع هي دراسات جامعية في شكل بحوث دكتواره وماجستير، ولعل أبرزها مذكرة ماجستير في القانون الجنائي بعنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات للطالبة جدي نسيمة بكلية الحقوق جامعة وهران للموسم الجامعي 2014/2013، وقد تناولت الباحثة في هذه الدراسة صور جرائم نظام المعالجة الآلية للمعطيات وكيفية قمع مرتكبي هذه الجرائم دون التطرق إلى الشق الإجرائي، وهو ما سنتناوله في دراستي بالبحث في الحماية الجنائية بشقيها الموضوعي والإجرائي، ودراسة أخرى للدكتور مناصرة يوسف بعنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات( ماهيتها، صورها، الجهود الدولية لمكافحتها)-دراسة مقارنة-، وهي عبارة عن كتاب صاد عن دار الخلدونية، الجزائر، سنة 2018، حيث تطرق الباحث في دراسته

للشق الموضوعي من الحماية الجنائية لجرائم نظام المعالجة الآلية للمعطيات مبرزا أهمية الإتفاقيات الدولية في مكافحة هذا النوع من الجرائم وذلك دون ذكر آليات البحث والتحري المستحدثة في الكشف عن جرائم نظام المعالجة الآلية لمعطيات، وهو ما سنتطرق إليه في دراستي من خلال البحث في الشق الإجرائي للحماية.

بالإضافة إلى وجود دراسة للأستاذة رشيدة بوكر بعنوان جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، وهي عبارة عن كتاب صادر عن منشورات الحلبي الحقوقية، بيروت، لبنان، سنة 2012، حيث تطرقت الباحثة في دراستها إلى آليات الحماية الموضوعية من جرائم نظم المعالجة الآلية للمعطيات في التشريع الجزائري والتشريعات المقارنة وكذا آليات البحث والتحري المستحدثة في الكشف عن جرائم نظام المعالجة الآلية لمعطيات, وأيضا دراسة أخرى للطالب ربيعي حسن في الحقوق بعنوان آليات البحث والتحقيق في الجرائم المعلوماتية بكلية الحقوق جامعة باتنة للموسم الجامعي 2016/2015، وقد تناول الباحث في هذه الدراسة بعض آليات البحث والتحقيق في الكشف عن الجرائم المعلوماتية، وذلك دون تطرقهما إلى الآليات الدولية الإجرائية لمكافحة هذا النوع من الجرائم، وهذا ما سنتاوله في دراستي في الباب الثاني بعنوان الحماية الإجرائية لنظام المعالجة الآلية للمعطيات، وأيضا هناك دراسة أخرى للطالبة رابحي عزيزة في القانون الخاص بعنوان الأسرار المعلوماتية وحمايتها الجزائية بكلية الحقوق جامعة أبوبكر بلقايد تلمسان للموسم الجامعي 2018/2017، وقد تناولت الباحثة في هذه الدراسة بعض التدابير الإجرائية المقررة لمكافحة جرائم نظام المعالجة الآلية للمعطيات دون التطرق إلى أهم التدابير الوقائية المستحدثة لمكافحة هذا النوع من الإجرام.

وعليه من خلال الدراسات السابقة في هذا الموضوع سأحاول الوقوف على أهم النقائص التي شابت هاته الدراسات المشار لها أعلاه، من خلال محاكاة التشريعات الدولية والداخلية سيما التشريعين الجزائري والفرنسي، وذلك بالتطرق إلى أهم آليات الحماية الجنائية المقررة لمكافحة جرائم نظام المعالجة الآلية للمعطيات مع الإلمام بكافة جرائم النظام والتركيز على الآليات المستحدثة للبحث والتحري في الكشف عن هذا النوع من الجرائم، هذا من جهة.

ومن جهة أخرى إلى وجوب تشديد الحماية الجنائية على طائفة معينة من المعطيات تمثلت في المعطيات الشخصية التي أولت لها التشريعات المقارنة أهمية كبيرة، وسن لها المشرع الجزائري مؤخرا قانون خاص رقم 18-07 المؤرخ في 10 يونيو 2018، يهدف إلى حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ويقر مجموعة من الضمانات التي تحمي البيانات الشخصية للشخص الطبيعي وتضمن عدم المساس بحياته الخاصة.

وتكمن الصعوبات المتعلقة بهذا الموضوع في صبغته الفنية فلا يكفي في معالجته أن يكون الباحث متخصصا في القانون بل يجب أن يكون على دراية بالجوانب الفنية للحواسيب والنظم المعلوماتية.

ومن العراقيل الأخرى التي واجهتني هي نقص المراجع المتخصصة في جرائم نظام المعالجة الآلية للمعطيات إذ يتناولها العديد من الباحثين في فرع أو مطلب باعتبارها جزء من الجرائم المعلوماتية.

ولمعالجة الإشكاليات السابق طرحها إرتأيت أن تكون دراسة موضوع الحماية الجنائية لنظام المعالجة الآلية للمعطيات بشقيها الموضوعي والإجرائي دراسة تحليلية نقدية مرتكزة على بيان الأحكام الموضوعية لنظام المعالجة الآلية للمعطيات في التشريعات المقارنة والتركيز عليها في التشريع الجزائري من خلال حماية جنائية لهذه المعطيات المدرجة في نظام المعالجة الآلية للمعطيات بصفة عامة والمعطيات ذات الطابع الشخصي بصفة خاصة.

وفي الشق الإجرائي ترتكز الدراسة على القواعد الإجرائية الخاصة بهذه الجرائم بوجودها في بيئة إفتراضية، والتطرق الى التدابير المستحدثة في التحري والكشف عن هذه الجرائم، وكذا الآليات الإجرائية الدولية الفعالة لمكافحة هذا النوع من الإجرام.

وعلى هذا الأساس قسمت دراستي إلى مقدمة وفصل تمهيدي وبابين وخاتمة تحمل نتائج وإقتراحات الدراسة.

يتناول الفصل التمهيدي الإطار المفاهيمي لنظام المعالجة الآلية للمعطيات وقسمته الى ثلاثة مباحث يتناول المبحث الأول مفهوم نظام المعالجة الآلية للمعطيات والمبحث

الثاني خصصته لعناصر نظام المعالجة أما المبحث الثالث تناولت فيه أهمية الحماية الجنائية لنظام المعالجة الآلية للمعطيات.

أما الباب الأول تطرقت فيه للحماية الموضوعية لنظام المعالجة الآلية للمعطيات وقسمته الى فصلين تناولت في الفصل الأول حماية المعطيات ذات الطابع الشخصي مع أبراز صورها وآليات الحماية أما الفصل الثاني خصصته لأركان جرائم نظام المعالجة الآلية للمعطيات مبرزا فيه أهم الجرائم التي تمس سواء بنظام المعالجة الآلية للمعطيات في حد ذاته أو بالمعطيات المدرجة ضمن نظام المعالجة الآلية.

والباب الثاني تطرقت فيه للحماية الإجرائية لنظام المعالجة الآلية للمعطيات وقسمته الى فصلين تناولت في الفصل الأول التدابير المستحدثة للبحث والتحري في الكشف عن جرائم نظام المعالجة الآلية للمعطيات مبرزا فيه أهم الآليات التي تساهم في الكشف عن مرتكبي هذه الجرائم أما الفصل الثاني خصصته للآليات الإجرائية الدولية لمكافحة جرائم نظام المعالجة الآلية للمعطيات وتم التطرق فيه إلى الإختصاص القضائي الدولي والمساعدة القضائية الدولية المتبادلة.

# الفصل التمهيدي

# الإطار المفاهيمي لنظام المعالجة الآلية للمعطيات

إن التطور التكتولوجي الهائل في مجال المعلوماتية وما يتطلبه من ضرورة القيام بمهام توفير وجمع ومعالجة وتبادل المعلومات في نفس الوقت أدى الى أبتكار أنظمة المعالجة الالية للبيانات أو المعطيات، والتي تقوم على مجموعة من العناصر أو المكونات المترابطة التي تعمل معا لتحقيق هدف معين، وهو معالجة المعطيات،

وبداية قبل التطرق الى أوجه الحماية الجنائية لهاته الأنظمة سنتناول في الفصل التمهيدي بيان مفهوم نظام المعالجة الآلية للمعطيات( المبحث الاول) وعناصر نظام المعالجة الآلية للمعطيات( المبحث الثاني) وأهمية الحماية الجنائية لنظام المعالجة الآلية للمعطيات ( المبحث الثالث)

## المبحث الاول: ماهية نظام المعالجة الآلية للمعطيات

أن البحث في ماهية نظام المعالجة الآلية للمعطيات يستلزم ضرورة البحث عن مفهوم نظام المعالجة الآلية للمعطيات( مطلب أول) وتمييزه عن غيره من المصطلحات المشابهة له ( مطلب ثاني)

### المطلب الأول : مفهوم نظام المعالجة الآلية للمعطيات

من أجل فهم حقيقة نظام المعالجة الآلية للمعطيات كنظام وجب الوقوف أولا على تعريف النظام بصفة عامة( فرع أول) وعلى تعريف نظام المعالجة الآلية للمعطيات بصفة خاصة ( فرع ثاني).

#### الفرع الأول : تعريف النظام

عرف سكودربك شارلز وآخرون النظام حسب مدخل النظم بأنه مجموعة من الأجزاء التي ترتبط ببعضها ومع البيئة المحيطة وهذه الأجزاء تعمل كمجموعة واحدة من أجل تحقيق أهداف النظام([1]).

وهو مصطلح مشتق من الكلمة اللاتينية systema التي تعني الكل المركب من عدد من الأجزاء، ووفقا للمعجم الشامل "universalis encyclopedia" فأن النظام هو عنصر مركب يتم تشكيله من عدة وحدات متميزة متصلة مع بعضها البعض بواسطة عدد من العلاقات التي تنشأ لتحقيق التفاهم والترابط بين هذه المكونات والوحدات المختلفة.

وفي معجم "la rousse" في الجزء (10) منه فقد تم تعريف النظام بأنه يتحقق في مفهومين:

- الأول: أعتبار النظام مجموعة من العناصر التي تمارس وظائفها من خلال علاقتها بطريقة مماثلة.
- الثاني: يقصد بالنظام مجموعة الأوامر التي تتم بوسائل متعددة من أجل الحصول على نتائج محددة.

---

1- حرية شعبان محمد الشريف، مخاطر نظم المعلومات المحاسبية الإلكترونية، رسالة مقدمة للحصول على درجة الماجستير في المحاسبة والتمويل، كلية التجارة- الجامعة الإسلامية غزة، 2006، ص 25.

وليس هناك تعريف دقيق للنظام لدى أهل الإختصاص بسبب تعدد الإستعمال ووجود أنطمة كبيرة تضم بداخلها أنظمة أصغر منها، والنظام كمفهوم علمي عام لا يختلف من مجال لآخر وإنما النظام ذاته يختلف بإختلاف المجال الذي ينتمي إليه([1]).

ومن تم فإن مصطلح نظام مصطلح واسع ولا يقتصر على البرامج والتطبيقات الحاسوبية، فكل شيء يعيش أو يتحرك ويتفاعل مع إي شيء آخر يعتبر نظاما بحد ذاته، ويعد أيضا جزءا من نظام أكبر، فالانسان يعتبر نظاما وكل الأجهزة المكونة له ( الجهاز التنفسي، الجهاز الهضمي) تعتبر جزئية الآلية، السيارة، الحاسوب كلها أنظمة.

ويعرف النظام بأنه مجموعة من الأجزاء المترابطة والتي تعمل معا لتحقيق هدف معين، أو هو عبارة عن مجموعة من العناصر أو الأجزاء أو الوظائف مترابطة مع بعضها البعض وتتكامل في حدود واضحة من أجل إنجاز مهمة أو وظيفة معينة لتحقيق هدف معين، وتعتبر أجزاء النظام مكملة لبعضها البعض فأن توقف أحدها يؤدي الى توقف وظيفة معينة وقد يؤدي الى توقف النظام الكلي كاملا([2])، و يتكون النظام من أربعة أجزاء رئيسية وهي:

-المدخلات: ما يدخل إليه من البيئة المحيطة.

-المعالجة: تحويل المدخلات الى مخرجات كالسلع والخدمات والمعلومات.

-المخرجات: جميع ما يخرج من النظام كنتيجة للمعالجة الى البيئة المحيطة والمستفيد.

-التغذية العكسية: العنصر الذي يتولى مهمة المقارنة بين مخرجات النظام الفعلية والمخطط له.

وقد يكون النظام بشكل عام نظام فرعي لنظام أكبر منه، وفي الوقت نفسه يحتوى على أنظمة فرعية أصغر تكون النظام مثل المنظمة، جسم الانسان و غيرها، كما أن للنظام عدة أنواع، من بينها نظم المعلومات وهو الذي يقوم يدويا أو آليا بجمع المعلومات وتنظيمها وتخزينها ومعالجتها وعرضها في أشكالها ( البيانات الخام، البيانات المحللة،

[1]- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، لبنان، ط الاولى، 2012، ص 49،50.

2- ياسر مطيع، محمد نصر الله، حمزة الغولة، طه عثمان، أكرم أبوزر، مفاهيم أساسية في تحليل و تصميم نظم المعلومات، مكتبة المجمع العربي للنشر والتوزيع، دار اجنادين للنشر و التوزيع، الطبعة الأولى، عمان، الاردن، سنة 2006، ص 9، 10.

المعرفة، النظم الخبيرة) وبأي وسيلة من الوسائل التقنية والمرئية والضوئية، ويبرز البعد الحقيقي لنظم المعلومات الحديثة من خلال إستخدام تقانات المعلومات التي تسمح بوساطة الحواسيب بجمع كمية كبيرة من البيانات وتخزينها و معالجتها بسرعة و دقة عالية([1])

وإن معالجة المعطيات التي هي عبارة مجموعة من العمليات التي تحول المعطيات إلى معلومات([2]) تحتاج الى آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها، وهي تنقسم الى ثلاثة أنواع:

-**المعالجة الميكانيكية:** وتتم هذه المعالجة للبيانات عن طريق بعض الأجهزة الأقل تطورا من الناحية الفنية والتقنية والتي سبقت ظهور الحاسب الالي أساس الثورة المعلوماتية الحالية مثل الآلة الكاتبة، والتي كانت تستخدم في الكتابة الى وقت قريب، وأجهزة المحاسبة اليدوية التي كانت تستخدم في محلات التجارة، والتي تعمل بصورة يدوية.

-**المعالجة الآلية للبيانات**: وهو ما يقوم به الحاسب الالي من معالجة البيانات وحفظها وتخزينها وإخراجها عن طريق مجموعة من الوحدات والأجهزة التي تعمل بصورة مجتمعة لهذه الغاية([3])، كما أن هذا المصطلح في البداية كان يقتصر على تحرير النصوص، فتوسع عندما أصبحت البرامج تضم مجموعة كبيرة من التطبيقات، ليشمل تحرير النصوص ورقمنتها وإدخالها وتحليلها وكذلك إنتاجها.

والمعالجة الآلية للمعطيات وفق ما هو متعارف عليه في المجال التقني "مجموعة من العمليات المترابطة والمتسلسلة بدءا من جمع المعطيات وإدخالها إلى نظام المعالجة

[1]- محمد دباس الحميد، ماركو ابراهيم نينو، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، الأردن عمان، الطبعة الأولى ، سنة 2007، الصفحات: 15،16،17،18.

[2]- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، ، مرجع سابق، ص54.

[3]- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع الجزائري والمقارن، ماجستير في القانون، الطبعة الأولى، دار الفكر الجامعي، الأسكندرية، سنة 2008، ص 263.

الآلية ومعالجتها وفقا للبرامج التي تعمل به نظم المعالجة الآلية وصولا إلى تحليلها وإخراجها بصورة معلومات"([1]).

-**المعالجة المختلطة**: ويقصد بها المعالجة التي تتم عن طريق جيل من الآلات الكاتبة المتطورة والتي تتمتع بميزتي المعالجة الآلية واليدوية في آن واحد، بحيث تكون عبارة عن آلات كاتبة لها ذاكرة معلوماتية تستطيع بها الاحتفاظ بالمعلومات التي تمت كتابتها وكذلك تعديلها وإخراجها عند الحاجة.

وإستنادا لأرجح الأقوال الفقهية فأن المعالجة الآلية للبيانات أوالمعلومات تشمل كل من المعالجة الآلية وكذلك المختلطة، وبالتالي فأن كلمة الآلية ذاتها تدخل في مصطلح المعلوماتية أو المعالجة الآلية للبيانات الذي يتكون من شقين الشق الأول كلمة معلومة و الشق الثاني هو كلمة آلي([2]).

وعليه، يمكن القول بأن كلمة الآلية تجعلنا نفكر في النظام المعلوماتي ذاته كنظام حركي يتحرك بدينامكية محددة، أما كلمة المعلوماتية فتبين لنا نتاج عمل هذا النظام المتمثل في الوثائق المعلوماتية بانواعها المختلفة.

**الفرع الثاني : تعريف نظام المعالجة الآلية للمعطيات**

أن غالبية المشرعين تجنبوا الخوض في مسألة وضع تعريف تشريعي لنظام المعالجة الآلية للمعطيات تاركين مهمة ذلك الى الفقه والقضاء، وأتجه معظمهم إلى تعريف النظام المعلوماتي في حد ذاته، نظرا لكون التعريف التقني للنظام المعلوماتي يتفق مع تعريف نظام المعالجة الآلية للمعطيات.

فعلى المستوى الدولي عرفت إتفاقية بودابست النظام المعلوماتي في المادة الاولى التي نضمنت عدت تعريفات من بينها:

- تعريف النظام المعلوماتي الذي يتمثل في الجهاز الذي يتكون من مكونات مادية ومكونات منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية([3]).

---

[1]- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق، ص 53.

[2]- بلال أمين زين الدين، مرجع سابق، ص 264.

[3]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها، دار النهضة العربية، القاهرة، الطبعة الأولى، سنة 2007، ص 18.

ومنه فأن الشرح التفسيري لإتفاقية بودابست في الفقرة 23 يعتبر نظام المعلومات جهاز مكون من معدات وبرامج قائمة للمعالجة الآلية للبيانات الرقمية ويمكن أن تكون منفردة أو متصلة مع أجهزة مماثلة أخرى داخل الشبكة.([1]).

وعرف النظام المعلوماتي من طرف الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010([2])، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014([3])، بأنه" مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".

أما على الستوى الداخلي فقد عرفت العديد من التشريعات العربية النظام المعلوماتي، ومن أهمها:

1- المشرع المصري: عرف النظام المعلوماتي على أنه:"مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية"([4])

2- المشرع الأردني: عرفه من خلال قانون المعاملات الالكتروني الإردني رقم 85 لسنة 2001، بنص المادة 02 الفقرة 10 على أنه" النظام الالكتروني المستخدم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو تجهيزها على أي وجه آخر"([5])

---

[1]- مناصرة يوسف، مرجع سابق، ص 34.

[2]- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، الشبكة القانونية، العربية www.arablegalnet.org ، ص2.

[3]- مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، يتضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 12 ديسمبر سنة 2010، ج رج ج، ع 57، المؤرخة في 28 سبتمبر سنة 2014.

[4]- المادة 1 من قانون رقم 175 لسنة 2018.

[5]- قانون رقم 85 لسنة 2001، الجريدة الرسمية للمملكة الأردنية الهاشمية رقم 4524 الصادرة بتاريخ 2001/12/31، ص 6010.

3- المشرع البحريني: عرف نظام تقنية المعلومات على أنه:" أداة أو مجموعة أدوات متصلة أو ذات صلة ببعضها، ويقوم واحد منها أو أكثر بمعالجة آلية لبيانات وسيلة تقنية المعلومات وفقا لبرنامج"([1])

4- المشرع السعودي: عرف المشرع السعودي النظام المعلوماتي في المادة الأولى من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية الصادر بتاريخ 2007/03/26 بأنه" مجموعة برامج وأدوات معدة لمعالجة البيانات وإدراتها وتشمل الحاسبات الآلية"([2])

5- المشرع العماني: حيث عرف النظام المعلوماتي من خلال نص المادة الاولى من قانون سلطنة عمان رقم 2011/12، الخاص بمكافحة جرائم تقنيات المعلومات الصادر بتاريخ 2011/02/06، على أنه" مجموعة برامج وأدوات تستخدم في معالجة وإدارة البيانات والمعلومات الإلكترونية"([3]).

6-المشرع الجزائري: عرف المشرع الجزائري النظام المعلوماتي في المادة 02 الفقرة ب من القانون رقم 09-04، تحت عنوان المصطلحات التي نصت على ما يلي: "يقصد في مفهوم هذا القانون بما يأتي:

...-ب- منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،...."([4])، ومثال ذلك المنظومة المعلوماتية المركزية لوزارة العدل التي تم إستحداثها بموجب المادة 2([5]) من القانون رقم 15-03، المؤرخ في أول فبراير سنة 2015، والمتعلق بعصرنة العدالة.

---

[1]- قانون بحريني رقم 60 لسنة 2014، بشأن جرائم تقنية المعلومات، الجريدة الرسمية، العدد 3178، الصادر بتاريخ 2014/10/09، ص 06.

[2]- المادة 1 من نظام مكافحة الجرائم المعلوماتية رقم 17 الصادر بتاريخ 2007/03/26.

[3]- المادة 1 من المرسوم السلطاني العماني رقم 12 الصادر بتاريخ 2011/02/06، بشأن قانون مكافحة جرائم تقنيات المعلومات.

[4]- المادة 2 الفقرة ب من القانون رقم 09-04.

[5]- نصت المادة 2 من القانون رقم 15-03 المؤرخ في أول فبراير سنة 2015، والمتعلق بعصرنة العدالة، على إستحداث المنظومة المعلوماتية المركزية لوزارة العدل، بقولها:" تحدث منظومة معلوماتية مركزية للمعالجة الآلية

ويختلف موضوع النظام المعلوماتي بحسب إختلاف الزاوية التي ينظر فيها آزاء الإعتداء الموجه ضد أحد مكونات النظام المعلوماتي، فمن ناحية قد يكون هذا الأخير نفسه هو وسيلة للجريمة المعلوماتية وأداة لتنفيذها، ومن ناحية أخرى قد يكون هو موضوعا للجريمة المعلوماتية أو محلا لها.

- **النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها**: ففي هذه الحالة نجزم أننا بصدد جرائم تقليدية بحتة يكون فيها النظام المعلوماتي أو جهاز الحاسوب هو أداة إرتكاب الجريمة المعلوماتية ووسيلة تنفيذها، ففي هذه الحالة يمكن للجاني إستخدام الحاسوب لإرتكاب جرائم السرقة أو النصب أو خيانة الأمانة أو تزوير المحررات المعلوماتية عن طريق التلاعب في الحاسوب.

**-النظام المعلوماتي موضوعا للجريمة المعلوماتية أو محلا لها**: فالجرائم المعلوماتية في هذا النوع تتفق والجرائم التقليدية البحتة من ناحية وجود إعتداء على المكونات المادية للنظام المعلوماتي فتشمل جرائم سرقة، إتلاف وتخريب لهذه المكونات أو الشبكات، أما إذا كان الإعتداء واقع على البرامج والمعطيات، أي الجانب المعنوي عن طريق السرقة أو التقليد أو محو أو تغيير أو إضافة في المعطيات أو إفشاء لمحتوياتها يتفق وهي التي يمكن التعبير عنها بجرائم المساس بأنظمة المعالجة الآلية للمعطيات([1])، مثل إستخدام نظام المعالجة الآلية للمعطيات للمساس بنزاهة الإمتحانات والمسابقات([2]).

وعليه، فإنه إذا كان النظام المعلوماتي هو المستهدف في الجريمة المرتكبة نكون أما جرائم نظام المعالجة الآلية للمعطيات.

---

للمعطيات تتعلق بنشاط وزارة العدل والمؤسسات التابعة لها وكذا الجهات القضائية للنظام القضائي العادي والنظام القضائي الإداري ومحكمة التنازع"، ج ر ج ج، ع 06، المؤرخ في 10 فبراير سنة 2015، ص 4.

[1]- مناصرة يوسف، مرجع سابق، ص 19،20.

[2]- نصت المادة 253 مكرر 7 من القانون رقم 20-06 المؤرخ في 28 أبريل سنة 2020، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966، والمتضمن قانون العقوبات، على إستعمال نظام المعالجة الآلية للمعطيات كوسيلة من الوسائل الماسة بنزاهة الإمتحانات والمسابقات، بقولها:" تكون العقوبة الحبس من خمس (5) سنوات إلى عشر (10) سنوات والغرامة من 500.000 دج إلى 1.000.000 دج، إذا أرتكبت الأفعال المنصوص عليها في المادة 253 مكرر 6:...

- باستعمال منظومة للمعالجة الآلية للمعطيات.."، ج ر ج ج، ع 25، المؤرخ في 29 أبريل سنة 2020، ص 12.

ويعرف جانب من الفقه الفرنسي "نظام المعالجة الآلية للمعطيات بأنه"هو كل وحدة أو مجموعة من الوحدات القادرة على معالجة أو تخزين البرامج والمعلومات أو أجزاء الدخول أو الخروج أو الارتباط والتي تهدف الى نتيجة محددة في هذه المجموعة وتكون موضوعا للحماية بنظام الأمن"([1])

ويؤخذ على هذا التعريف أنه لم يحدد النتيجة التي ينبغي أن يسعى النظام الى تحقيقها، وأشترط في وحدات النظام التي يتكون منها إما أن تكون قادرة إما على معالجة أو على تخزين البرامج و المعلومات دون أن يتطلب الإرتباط بينها، ويترتب على ذلك إلا يشترط في الوحدة حتى تكون من ضمن مدلول النظام أن تكون من وحدات الخزن حتى ولو لم يتم تشغيلها، بل يكفي تهيئتها لتحقيق الدخول للمجرم حتى بحاسب آلي لم يدخل الخدمة ولم يتم تشغيله بعد لمجرد أنه من الوحدات القادرة على معالجة المعلومات.

على خلاف الأخذ بمفهوم مجلس الشيوخ الفرنسي الذي يشترط في الوحدة لكي تعد من مكونات النظام أن تكون في حالة تشغيل أو أشتغال باعتباره السبيل الى إتصالها، مما يترتب عليه أن الدخول لا يمكن أن يتحقق إلا في حالة أن تكون هذه الوحدات مرتبطة، ولا تكون كذلك إلا عند تشغيلها وأن تكون قادرة على ذلك أي عند تهيئتها للإتصال بوحدات النظام الأخرى، وعلى أساس ذلك يتحقق الدخول حتى في الوحدات التي قد تم إيقافها عن العمل بصورة غير نهائية لعطل أصابها يمكن إصلاحه أو تم توقيفها كالاعتداء الذي يقع خارج ساعات التشغيل والذي يعالجه البعض تحت جريمة سرقة ساعات العمل([2]).

وعرف الفقيه خالد ممدوح إبراهيم أيضا نظام المعالجة الآلية للمعطيات بأنه:" مجموعة العناصر المتداخلة والمتفاعلة مع بعضها البعض والتي تعمل على البيانات والمعلومات ومعالجتها وتخزينها وبثها وتوزيعها بغرض دعم صناعة القرارات والتنسيق وتأمين السيطرة على المنظومة إضافة لتحليل المشكلات للموضوعات المعقدة"

[1]- قال بهذا التعريف السيناتور الفرنسي thyraud أمام مجلس الشيوخ في جلسة مناقشة مشروع قانون المتعلق بالمعلوماتية المعطيات والحريات.

[2]- محمد حماد مرهج الهيتي، مقال بعنوان جريمة الدخول الى النظام الآلي لمعالجة المعطيات عن طريق الغش، مجلة كلية الحقوق، جامعة النهرين، المجلة 9، العدد 10، السنة محرم 1427-شباط 2006، ص 99.

ومن خلال هذا التعريف يستخلص أن لنظام المعالجة أربع نشاطات وهي:

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

2-المعالجة: تحويل البيانات المدخلة من شكلها الأولي إلى نتائج ومعلومات مفهومة وقابلة للإستخدام، ومن هذا المنطلق فالجزء المعالج بالجهاز (processin) يعتبر الأساس في نظام الكومبيتر.

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

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

أما على المستوى الدولي فإن الاتفاقية الدولية للإجرام تقنية المعلومات( إتفاقية بودابست) عرفت نظام المعالجة الآلية للمعطيات بموجب الفقرة (أ) من المادة الاولى من الفصل الاول بعنوان المصطلحات على أنه" كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين باداء معالجة آلية للبيانات"

وما يلاحظ على هذا التعريف أنه أشار فقط إلى العناصر المادية التي يتكون منها نظام المعالجة الآلية للمعطيات وهي كل آلة بمفردها أو مع غيرها من الآلات المتصلة، وأغفل ذكر العناصر المعنوية التي تمثل روح النظام ألا وهي البرامج والمعطيات.

وفي مشروع القانون العربي الموحد لمكافحة سوء إستخدام تكنولوجيات المعلومات والاتصالات في صيغته المعدلة نجد في مادته الاولى تعريفا لنظام المعالجة الآلية للمعطيات على أنه:" كل مجموعة مركبة من وحدة أو عدة وحدات للمعالجة سواء كانت

[1]- جدي نسيمة، مرجع سابق، ص 16،17.

متمثلة في ذاكرة الحاسوب وبرامجه أو وحدات الادخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة"([1]).

وعلى المستوى الداخلي عرف مجلس الأمة الفرنسي نظام المعالجة الآلية للمعطيات في الجريدة الرسمية، مجلس الأمة، 4 نوفمبر 1987، صفحة 3656 كما يلي:

هو كل مجموعة منسجمة تتكون من وحدة أو عدة وحدات معالجة، ذاكرة، وبرامج، ومعطيات، وحدات إدخال وإخراج، وإتصال بين هذه المكونات التي تؤدي الى إعطاء نتيجة محددة وهذه المجموعة تكون محمية تقنيا بموجب أي وسيلة أو مكنزم إئتمان.([2])

كما عرف مجلس الشيوخ الفرنسي بمناسبة تعديله قانون العقوبات نظام المعالجة الآلية للمعطيات بصورة أكثر وضوح بأنه: هو كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تكون كل منها الذاكرة، المعطيات، أجهزة الإدخال والإخراج أجهزة الربط التي تربط بينها مجموعة من العلاقات التي عن طريقها تم تحقيق نتيجة معينة، وهي معالجة المعطيات، على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية.([3])

أن تعريف نظام المعالجة الآلية للمعطيات وفقا للتشريع الفرنسي ومجلس الشيوخ الفرنسي يشترط بالضرورة توفر في آن واحد مكونات مادية ( ما ملموس في الجهاز و له دور مهم في تشغيل النظام) + مكونات معنوية ( البرامج و المعطيات الموجودة داخل النظام)، وأن المساس بهاته الأنظمة لا يعنيها المساس بالمكونات المادية وحدها أو المكونات المعنوية وحدها، ويفهم ذلك من خلال المواد العقابية حول المساس بالأنظمة التي لا تحمي المكونات المعزولة مادية وحدها أو معنوية وحدها، وإنما تحمي مجموعة منسجمة تهدف الى تحقيق نتيجة معينة، وهي معالجة المعطيات.

---

[1]- سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية- تخصص العلوم جنائية، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر - باتنة، الموسم 2013/2012، ص ص: 43-45.

[2]- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري و المقارن، رسالة ماجستير شعبة القانون الجنائي، كلية الحقوق- جامعة قسنطينة، الموسم 2013/2012، ص 20.

[3]- جدي نسيمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق-جامعة وهران، الموسم 2014/2013، ص 17.

كما إن جرائم نظام المعالجة الآلية للمعطيات قد تم تقديم تعريف لها أثناء المناقشات البرلمانية في فرنسا إلا أنها لم تقبل مخافة أن يرتبط النص التجريمي بحالة عابرة للتطور التقني والتكنولوجي وتصبح بدون معنى ويكون هذا التعريف لا يتماشى مع التطور التقني.

ومن تم فإنه أصبح لدى الإجتهاد القضائي والمحاكم الفرنسية مفهوم جد موسع لتعريف نظام المعالجة الآلية للمعطيات فشبكة الإتصال تلكوم عبارة عن نظام، شبكة البطاقات البنكية عبارة عن نظام، القرص الصلب عبارة عن نظام، كمبيوتر منفصل عبارة عن نظام وكذلك الشبكة وحاليا الشبكة اللاسلكية ويفي Wifi(Wireiess Fidelity) التي تسمح بالإتصال عبر ناقلات لاسلكية من أجهزة الإتصال لربطها الى الأنترانت أو الأنترنت، هو نظام معالجة آلية للمعطيات، وعدا أيضا الإجتهاد القضائي الجزائري الناقل التسلسلي العام ( serial BUS(Universal USB كنظام للمعالجة الآلية للمعطيات([1] ).

أما بالنسبة للمشرع الجزائري بداية لم يورد تعريفا لنظام المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، وتجنب التقيد بتعريف محدد له بحجة أن العناصر المعنوية التي يتكون منها النظام( المعطيات والبرامج) في حالة تطور تكنولوجي هائل وتخضع للتطورات السريعة والمتلاحقة، وتقوم على أساس العالم الافتراضي الذي لا يزال في بدايته، كما أن هذا المصطلح يعد تعبيرا فنيا يخرج من مجال تكوين رجال القانون.

إلا أن المشرع الجزائري أستدرك هذا التأخر بعد خمس(5) سنوات، بصدور القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، وذلك بموجب أحكام المادة الثانية(2)، تحت عنوان المصطلحات التي نصت على ما يلي: "يقصد في مفهوم هذا القانون بما يأتي:

أ-الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الالكترونية..."([2])، وهو تعريف واسع

[1]- مناصرة يوسف، مرجع سابق، ص33.

[2]- المادة 2 من القانون 09-04.

وشامل لجميع الجرائم المعلوماتية البحثة ممثلة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات وكل الجرائم المرتكبة بوسيلة معلوماتية إو إتصال إلكتروني، وهي عبارة أيضا عن تعريف ينصب على وصف للسلوك المجرم مرتبط بالمنظومة المعلوماتية وثانيها ربطها بوسيلة إرتكابها المنحصرة في المنظومة المعلوماتية أو نظام للإتصالات الإلكترونية، بل أكثر من ذلك أن هذا التعريف حاول أن يحيط بجميع الجرائم التي من الممكن أن تقع في هذه البيئة، وهي إحاطة الهدف منها تجنب حصر هذه الجريمة في مجال ضيق يسمح بإفلات العديد من صورها من دائرة التجريم([1])، كالجرائم التي تستعمل فيها تلك الأنظمة كدعامة للجريمة ومن أمثلتها في القانون الفرنسي الجرائم المتعلقة بالأخلاق والجرائم المتعلقة بالصحافة([2]).

وعليه فأن كل مجموع معلوماتي مهما كان حجمه وطريقة ربطه مع غيره وطريقة معالجته المرصودة تشكل نظاما، إذ لا يهم الحجم ولا الأهمية، والذي يهم هو طريقة الربط، ويظهر من تعريف القانون الجزائري رقم 09-04 السالف الذكر أن دوام ذلك غير لازم، وتدخل في التجريم القراءة غير المصرح بها للمعلومات الموجودة على بطاقة الإئتمان كذلك يعتبر غشا لأن هذه البطاقات جزء من نظام صالح لكي يقرأ ويسجل المعلومات على شريحة عندما يوضع في إتصال معه، كذلك القرص المرن القابل للعزل والنقل الذي يحمل شريحة برامج خاصة تقرأ من جهاز قارئ خاص فهذا القرص يشكل نظاما مع هذا القارئ([3]).

فالنظام دائما يتطلب الوجود المتزامن للإجهزة والبرامج، والقانون لا يعنى عادة بالهجمات التي توجه للإجهزة المادية البحثة لوحدها كالدعامات والروابط، وكذلك لا يعنى بالدخول في مجموع برامجي بحث كتفكيك البرامج ونسخها...الخ ذلك أن النصوص

[1] -رشيدة بوكر، مرجع سابق، ص 44.

[2] - بوبرقيق عبدالرحيم، مقال بعنوان مفهوم أنظمة المعالجة الآلية للمعطيات في الجرائم المحددة في المواد 394 مكرر إلى 394 مكرر 2 من قانون العقوبات الجزائري، مجلة الدراسات والبحوث القانونية، جامعة المسيلة، المجلة 4، العدد 1، جوان 2019، ص 362.

[3] - محمد خليفة، مرجع سابق، ص 26.

القانونية التي تحمي نظم المعالجة الآلية ومعلوماتها لا تحل في هذه الحالة محل القواعد التقليدية التي تنظم الإتلاف والتقليد.([1])

ومن خلال ما سبق يستنتج أن مصطلح نظام المعالجة الآلية للمعطيات مصطلح ينطبق على أي نظام مهما كان مسماه يحتوي على مجموعة من العناصر مرتبطة مع بعضها البعض تهدف الى تحقيق نتيجة معينة، وهي معالجة المعطيات، أي لا بدا أن يكون هناك ترابط وصلة بين وحدات النظام و توحدها أو تحاول توحيد جهودها نحو تحقيق الهدف المقصود، والوحدة التي لا تتوفر فيها هذه الصفات تخرج من مدلول نظام المعالجة الآلية للمعطيات، ويترتب على ذلك أن المساس بالمكونات مادية معزولة أو معنوية معزولة لا تشكل مساسا بالنظام إلا إذا كانت جزء من النظام أو لها علاقة مباشرة أو غير مباشرة به، ولا تشكل جريمة إلا إذا كانت هذه المكونات المادية أو المعنوية تشارك في تطبيقات فعلية داخل نظام كامل أو لها القدرة على ذلك و يكون لها دورا في تحقيق الغاية الأساسية وهي معالجة المعطيات و يدخل في ذلك: شبكة الانترنت، البريد الالكتروني، موقع الانترنت، بطاقات الكترونية، بطاقة الائتمان البنكية، القرص النقال والمرن والمضغوط، الاشرطة الممنغطة.... وهي كلها تعد أنظمة معلوماتية.

وعليه، فإن الدخول الى برنامج من أجل تعديله أو تحويله الى إستعمال غير الاستعمال المخصص له لا يشكل جريمة نظام المعالجة الآلية للمعطيات إلا إذا كان هذا البرنامج يشارك في تطبيق فعلي داخل نظام كامل، ذلك أن البرنامج المعزول لا يأخذ تكييف النظام، وكذلك الشأن بالنسبة لأي من المكونات التي تشكل جزءا من النظام، كما لو وقع الاعتداء على برامج معروضة للبيع.

ولا يدخل أيضا في مفهوم نظام المعالجة الآلية المعلومات المخزنة والتي لا توجد بالمعالجة، أي التي تعتبر كالأرشيف فالدخول عليها لا يمثل دخولا الى نظام المعالجة

[1]- يعيش تمام شوقي، خليفة محمد، مقال بعنوان نظام المعالجة الآلية المعطيات كأساس للحماية الجزائية في التشريع الجزائري، مجلة جيل للأبحاث القانونية المعمقة، مركز جيل البحث العلمي، العام الثالث، العدد 25، مايو 2018، ص 18.

الآلية للمعطيات، ذلك أن الاموال المعلوماتية المعزولة لا تطبق عليها عموما إلا القواعد التقليدية([1])

إضافة الى أن المواد العقابية المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات الجزائري، المعدل والمتمم بموجب القانون رقم 04-15، لاتحمي مكونات النظام المعزولة مادية أو معنوية وحدها، وأنما تحمي مجموعة منسجمة ومتصلة مع بعضها البعض ومرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وهذا ما يستفاد من المادة 2 من القانون 09-04 السالفة الذكر

اما بالنسبة للجرائم التي تقع خارج النظام وتكون وسيلة لارتكاب الجريمة وليس موضوعا للجريمة أو محلا لها، كجرائم السرقة والنصب والتزوير المعلوماتي فتطبق عليها النصوص التقليدية الواردة في قانون العقوبات المعدل والمتمم.

وفي الأخير يمكن القول أن نظام المعالجة الآلية للمعطيات هو تعبير يطلق على أي نظام مهما كان مسماه أو حجمه أو طريقة ربطه، يحتوي على مجموعة من المكونات المترابطة مع بعضها البعض والتي تعمل على تحقيق نتيجة معينة وهي معالجة المعطيات.

**المطلب الثاني : تمييز نظام المعالجة الآلية للمعطيات عن المصطلحات المشابهة له**

أن مصطلح نظام المعالجة الآلية للمعطيات يرتبط إرتباطا وثيقا بالجريمة المعلوماتية، وبالبرامج والمعطيات باعتبارهما أهم عنصرين في النظام، وتختلف جرائم النظام عن جرائم المعطيات الشخصية وجرائم الأنترنت، لذلك سنقوم بتمييزه عن الجريمة المعلوماتية ( الفرع أول) وعن البرامج و المعطيات ( الفرع ثاني) وعن جرائم المعطيات الشخصية ( الفرع الثالث) وعن جرائم الأنترنت ( الفرع الرابع)

**الفرع الأول : تمييز نظام المعالجة الآلية للمعطيات عن الجريمة المعلوماتية**

بالرغم من أن المشرع الجزائري لم يقم بسن نصوص صريحة وخاصة بالجرائم المعلوماتية إلا أنه أورد بعض الأحكام المتعلقة بها في القسم السابع مكرر من قانون

[1]- سعيداني نعيم، مرجع سابق، ص 45.

العقوبات بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات، لكنها تقتصر على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات([1]).

وإن للجريمة المعلوماتية عدة تعاريف تختلف بحسب الجانب الذي تقوم عليه، فالجانب التقني يعتمد على توافر المعرفة والدراية التقنية لدى شخص مرتكبها، ويعرفها بأنها نشاط إجرامي تستخدم فيه تقنية الحاسوب بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المقصود، أما الجانب القانوني يتولى التعريف بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة، وهناك جانب آخر يعرف الجريمة المعلوماتية بالنظر الى وسيلة إرتكابها أو موضوعها حسب توافر المعرفة بتقنيين المعلومات أو إستنادا لمعايير أخرى حسب القائلين بها([2]).

وقد أخذ الفقه باتجاهين في تعريفه للجريمة المعلوماتية: اتجاه أخذ بمفهوم واسع واتجاه آخر أخذ بمفهوم ضيق.

**الإتجاه الاول : المفهوم الواسع للجريمة المعلوماتية**

هذا الاتجاه أخذ به عدة فقهاء منهم تيادمان الألماني ودون باكر، والذين يوسعون من مفهوم الجريمة المعلوماتية لتشمل كافة أشكال السلوك غير المشروع الذي يرتكب باستعمال الحاسب الآلي، وتكون الأنظمة آداة لارتكاب الجريمة أو تكون المعلوماتية هدفا لها، ومن بين هذه التعريفات :

تعريف كلاوس تيادمان الذي عرفها بقوله" الجريمة المعلوماتية تشمل كافة أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الالي"([3])

وعرفها دون باكر بأنها" كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية ترتب عنه خسارة للمجني عليه أو مكسب يحققه الجاني"([4])

---

[1]- دليلة العوفي، مقال بعنوان إشكالية مواكبة الجزائر لمجتمع المعلومات من الفجوة الرقمية إلى الجريمة المعلوماتية، مجلة الحكمة للدراسات الإعلامية والإتصالية، المجلد 4، العدد 8، نوفمبر 2016، ص 8.

[2]- مناصرة يوسف، مرجع سابق، ص 24،28.

[3]- Tiedemann Kalus, fraude et autres délits d'affaires commis a l'aide d'ordinateurs éléctroniques, revus de droit penal et de criminologie(R.D.P.C), Bruxelles, A 64,N°7, juilliet 1984,P 61.

[4]- جدي نسيمة، مرجع سابق، ص 9.

وهناك جانب آخر ركز على الجانب الموضوعي في تعريفه للجريمة المعلوماتية باعتبارها تقع على الحاسب الآلي وفي داخل نظامه، منها تعريف الاستاذ روزنبلات بأنها" نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه.

كما تعرف" على أنها سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات" وتعرف أيضا بأنها" الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة إستخدام المخرجات إضافة الى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكومبيتر"([1])

وفي هذه المفهوم يعني أن الجريمة المعلوماتية هي كل الأفعال التي تنقل بالحاسب أو بالنظام المعلوماتي بوجه عام سواء كان ذلك النظام أو أحد مكوناته محل الإعتداء في هذه الجريمة أم كان هو آداتها ووسيلة في تنفيذها([2]).

وعليه فإن جرائم نظام المعالجة الآلية للمعطيات حسب هذا المفهوم الواسع، تقوم بغض النظر عما إذا كان النظام هو أداة الجريمة أو وسيلة لتنفيذها أو كان هو موضوع الجريمة أو محلا لها، وهو ذات المفهوم الذي تبناه المشرع الجزائري في تعريفه لجرائم تكنولوجيا الإعلام والإتصال التي تدخل ضمنها جرائم نظام المعالجة الآلية للمعطيات.

**الاتجاه الثاني: المفهوم الضيق للجريمة المعلوماتية**

يرى أصحاب هذا الاتجاه باقصاء الأفعال التي يستخدم فيها الحاسوب للإعتداء على الغير أو الاموال، وحصر مفهوم الجريمة في الجرائم الماسة بأنظمة المعلوماتية في حد ذاتها، وهم لا ينظرون للحاسب الآلي بوصفه أداة إرتكاب الجريمة المعلوماتية بل أن الجريمة تقع على الحاسوب ذاته وقد تقع داخل نظامه، ومن هذه التعريفات" أن جريمة الحاسوب هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه"، وهناك تعريف آخر

[1]- شنين صالح، الحماية الجزائية لبرامج الحاسب الآلي، مذكرة مكملة لنيل شهادة الماجستير في الحقوق تخصص قانون جزائي، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، الموسم 2007/2006، ص 16.

[2]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، دار المطبوعات الجامعية، مصر، ط الأولى،سنة 2019، ص 25.

أقترحته مجموعة من خبراء منظمة التعاون الإقتصادي والتنمية كأساس للنقاش في إجتماع عقد بباريس في عام 1982 وذلك لبحث الجريمة المرتبطة بالمعلوماتية وورد فيه أنه " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها"([1])، وهذا الاتجاه تزعمه الفقيه فراري الذي حصرها في الاعتداءات على الكيان المنطقي للمعلوماتية باعتبار الاعتداءات على العناصر المادية تطبق عليها النصوص الكلاسكية.([2])

كما يذهب بعض الفقه الجنائي الى القول بأن جرائم المساس بأنظمة المعالجة الآلية للمعطيات تشكل أهم الجرائم التي تتصل بالمعلوماتية وأكثرها إثارة للمشكلات القانونية فهي تتكون بصفة عامة من بعض الجرائم التقليدية التي تم إرتكابها بواسطة المعلوماتية فتكسب داخل هذا الإطار خصائص جديدة لارتباطها بالحاسب الآلي، والنظم المعلوماتية تتميز عن الصور التقليدية لها وتؤدي بالتالي الى صعوبة تطبيق النصوص التقليدية عليها وهي في ثوبها الجديد، ومن هذه الجرائم على سبيل المثال يمكن أن نتصور إرتكاب جرائم إرهابية، جرائم التزوير أو جرائم أخلاقية...بواسطة منظومة معلوماتية.([3])

أما بالنسبة للمشرع الجزائري فأنه قبل صدور القانون 09-04 السالف الذكر كانت الجريمة المعلوماتية تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات والتي تنصرف الى المعلومة والنظام الذي يحتوي عليها، اما بعد صدوره فقد تبنى المشرع تعريفا موسعا للجرائم المعلوماتية، واعتبر أنها تشمل بالإضافة الى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر الى 394 مكرر8 أي جريمة أخرى ترتكب أو يسهل إرتكابها بواسطة منظومة معلوماتية أو نظام للإتصالات الالكترونية، وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الافعال التي تكون فيها المنظومة المعلوماتية محلا

[1]- مناصرة يوسف، مرجع سابق، ص 29.

[2]- جدي نسيمة، مرجع سابق، ص 10.

[3]- سعيداني نعيم، مرجع سابق، ص 47.

للإعتداء بل توسع في نطاقها لتشمل إضافة الى ذلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لإرتكابها.

وحسب رأينا حسنا ما فعله المشرع الجزائري لما أخذ بالمعنى الواسع للجريمة المعلوماتية، وأخذ بعين الإعتبار الصعوبات التي تثيرها المصطلحات القانونية، لذلك تم إختيار عنوان القواعد الخاصة للوقاية من جرائم تكنولوجيا المعلومات والإتصال ومكافحتها حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمر بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا، إضافة الى أن التركيز على مجال الإعلام والإتصال يبين مقاصد النص الذي يهدف الى جعل المتعاملين في مجال الإتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الإجرام والوقاية منه([1]).

**الفرع الثاني :تمييز المساس بنظام المعالجة الآلية للمعطيات عن المساس بالمعطيات والبرامج**

تعتبر المعطيات والبرامج بمثابة الروح بالنسبة للحاسب، والعدوان عليها هو الذي يشكل جريمة معلوماتية بالمعنى الدقيق، مما يعني أن الإعتداء على نظام المعالجة الآلية للمعطيات معناه الإعتداء على البرامج والمعطيات باعتبارهما أهم عنصرين في نظام المعالجة بصفة عامة، وفي المكونات المعنوية له بصفة خاصة.

ومن أهم الجرائم التي تقع على برامج الحاسب الآلي هي نسخها غير المشروع عن طريق ما يسمى بالقرصنة المعلوماتية، وهذه الجريمة تختلط بنسخ معطيات غير مشروعة رغم أنهما يختلفان في المحل، فالأولى تقع على البرامج والثانية تقع على المعطيات.

فالمعطيات والبرامج بالرغم من أنهما جزء من نظام المعالجة الآلية للمعطيات إلا أن هناك تداخل كبير بينهما ويتجلى ذلك كثيرا في جريمة التلاعب بالمعطيات التي لا تتم إلا عن طريق التلاعب بالبرامج، وعليه تكون عملية التلاعب بالبرنامج جزء لا يتجزء من عملية التلاعب بالمعطيات لأن نظام المعالجة الآلية للمعطيات يتكون من برامج لهذه المعالجة، ووظائف الحاسب كلها تقوم على البرامج فالجريمتان متداخلتان، لكن الفيصل بين الجريمتان أن عملية التلاعب إذا توقفت على البرنامج في حد ذاته و لم

[1]- مناصرة يوسف، مرجع سابق، ص22.

تتعداه الى معطيات الحاسب فأنها تعتبر جريمة تلاعب بالمعطيات لأن التلاعب بالبرنامج كان مرحلة من مراحلها([1]).

هذا وأن كان بعض من الفقه يرى جدوى من التمييز والتفرقة بين المعطيات والمعلومات والبرامج، إلا أنه وفي الاتجاه المعاكس يرى جانب آخر من الفقه عدم وجود أهمية في التمييز بينها طالما أن المعلومات هي المعنى المستخلص من المعطيات بعد معالجتها، وأن البرنامج هو المستودع الذي يتم فيه معالجات هذه المعطيات، فالعلاقة بينها أذن هي علاقة الجزء بالكل، ولما كانت الغاية في المقام الأول هي حماية المعلومات فالكل يتمتع بنفس الحماية القانونية في إطار الجرائم المعلوماتية طالما أن هذه المعلومات موجودة داخل بيئتها الالكترونية.

كما أن المشرع الجزائري أدرج برامج الحاسوب ضمن مفهوم المعطيات ولم يأبه لهذا الجدل الفقهي من حيث التمييز بينهما، حيث نصت المادة الثانية (2) من القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في تعريفها للمعطيات أن هذه الأخيرة هي" أي عملية عرض للوقائع أو المعلومات بما في ذلك البرامج المناسبة التي من شأنها أن تجعل المنظومة المعلوماتية تؤدي وظيفتها"([2])

فضلا عن ذلك، فأن مصطلح المعلومات كثيرا ما يترادف مع مصطلح تكنولوجيا المعلومات أو تقنية المعلومات على الرغم من الإختلاف الموجود بينهما، فالمعلومات هي المضمون أو الرسالة الناتجة عن معالجة البيانات التي تم إدخالها بينما تكنولوجيا المعلومات هي الوسط المستخدم لإقتناء أو حفظ أو نقل المعلومات([3]).

[1]- محمد خليفة، مرجع سابق، ص 90.

[2]- سعيداني نعيم، مرجع سابق، ص 19.

[3]- رامي حليم، مقال بعنوان جرائم الإعتداء على أنظمة المعالجة الآلية للمعلومات، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجلد 1، العدد 1، سبتمبر 2009، ص 340.

**الفرع الثالث : تمييز جرائم نظام المعالجة الآلية للمعطيات عن جرائم المعطيات الشخصية**

لقد أدرك المشرع الجنائي الجزائري الدور الذي تلعبه معطيات الحاسب الآلي، فقام بوضع نصوص خاصة لحمايتها من إي إعتداء سواء بصفة عامة في جرائم نظام المعالجة الآلية للمعطيات بموجب القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، أو بصفة خاصة في جرائم المعطيات ذات الطابع الشخصي بموجب القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

كما أن المشرع الجزائري تماشيا مع المشرع الفرنسي أراد أن يوفر حماية خاصة للمعطيات الشخصية أو الإسمية نظرا لتعلقها بالحياة الخاصة للإنسان، ورغبة منه في حماية هذه الحياة الخاصة في مواجهة المعالجة الآلية للمعطيات المتعلقة بها وهي المعطيات الشخضية أو الإسمية المرتبطة أساسا بالشخص المخاطب بها، كإسمه وحالته الإجتماعية وموطنه وصحيفة السوابق القضائية الخاصة به، والتي ترتكز على تنظيم عملية المعالجة الآلية للمعطيات الشخصية إي المعطيات الإجرائية المتعلقة بهذه المعالجة، وتتعلق بنوع معين من المعطيات وهي المعطيات الشخصية أو الإسمية، والنص عليها يحمي هذه المعطيات من جانب معين وهو الجانب المتعلق بإجراءات المعالجة الآلية لهذه المعطيات في الأصل([1])، والتي تمثل حجر الزاوية لدولة القانون، ولا يمكن أن تقع معالجتها إلا في إطار الشفافية وإحترام كرامة الإنسان([2]).

أما المعطيات غير الشخصية أو العامة المدرجة ضمن نظام المعالجة الآلية للمعطيات فهي معطيات تتمتع بحماية عامة وتقوم على أسس موضوعية، و ترتبط أيضا بشتى مجالات الحياة غير تلك المتعلقة بشخص الإنسان، فقد تتعلق بالمال والإقتصاد أو

[1]- محمد خليفة، مرجع سابق، ص 108.

[2]-غزال نسرين، مقال بعنوان حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، المجلة الجزائرية للعلوم القانونية والسياسية ، جامعة بن يوسف بن خدة الجزائر، المجلد 56، العدد 01،جوان 2019، ص 121.

العلوم ...أو غير ذلك من المجالات، إضافة الى أن جرائم نظام المعالجة الآلية للمعطيات تكفل حماية عامة لكل المعطيات ومن كافة جوانبها الموضوعية.

كما أن هذه المعطيات ترد على الأشخاص الطبيعين سواء كانوا ممثليين لأنفسهم أو ممثلين لشخص معنوي، وأن كانت ليست من صنع من تتعلق به فهي خاضعة لسيطرته ومن تم لا يجوز للغير الإطلاع عليها إلا بموافقته الشخصية أو بأمر من السلطة العامة المختصة([1]).

**الفرع االرابع : تمييز جرائم نظام المعالجة الآلية للمعطيات عن جرائم الانثرنت**

تعرف جرائم الأنثرنت بأنها هي تلك الجرائم العابرة للحدود، والتي ترتكب بواسطة الأنثرنت أو عليها من شخص ذا دراية فائقة بها"([2])، ويستشف من هذا التعريف أن جرائم الأنثرنت قد تكون محلا للجريمة وقد تكون وسيلة لإرتكابها، وفي كلا الحالتين يشترط وجود جهازين كومبيوتر أو أكثر متصلين فيما بينهم عبر الأنترنت لإتمام أركانها.

أما بالنسبة لجرائم نظام المعالجة الآلية للمعطيات فهي تقع إذا وقع الإعتداء على شبكة الإتصال التي تربط بين أكثر من نظام، لأن تلك الشبكة تعتبر عنصرا في كل نظام من الأنظمة التي تربط بينها([3])، لذلك فهي يمكن أن تتم بواسطة شبكة الحاسب الآلي أو الأنترنت أو أي شبكة إلكترونية أخرى([4])، كما أن هذه الجرائم يشترط فيها أن تقع على النظام وليس بواسطته، أي بمعنى آخر أن يكون النظام محلا للجريمة وليس وسيلة لإرتكابها، وفقا لما هو منصوص عليه في المواد 394 مكرر الى 394 مكرر 8 من قانون العقوبات المعدل بالقانون 16-02 المؤرخ في 19 يونيو سنة 2016 .

---

[1]- محمد خليفة، مرجع سابق، ص 93.

[2]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنثرنت في مرحلة جمع الإستدلالات- دراسة مقارنة، دار الفكر الجامعي، الأسكندرية، مصر، سنة 2013، ص 54.

[3]- مزاولي محمد، مقال بعنوان المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الإلكترونية في القانون الجزائري، مجلة دراسات وأبحاث، جامعة عاشور زيان الجلفة، المجلد 1،العدد 1 ، سبتمبر 2009، ص 280،281.

[4]- نبيلة هبة هروال، مقال بعنوان ماهية جرائم الأنترنت، مجلة المعيار، المركز الجامعي تيسمسيلت، المجلد 3، العدد 5، جوان 2012، ص 212.

## المبحث الثاني : عناصر نظام المعالجة الآلية للمعطيات

لا يمكن تصور نظام المعالجة الآلية للمعطيات بدون حاسب آلي، وهو عبارة عن جهاز الكتروني مبرمج يستطيع أن يقوم بآداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعات كبيرة تصل الى عشرات الملايين من العمليات في الثانية بدرجة عالية من الدقة ولديه القدرة على التعامل مع كم هائل من البيانات وتخزينها وإسترجاعها عند الحاجة([1])، ويتكون من مجموعة أجهزة متكاملة مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة وفقالبرنامج موضوع مسبقا للحصول على النتائج المطلوبة([2]).

وإن نظام المعالجة الآلية للمعطيات يتكون من عناصر مادية ( مطلب أول) ومعنوية( مطلب ثاني) تربط بينها شبكات إتصال ( المطلب الثالث) توحدها نحو تحقيق المعالجة الآلية للمعطيات.

### المطلب الأول : العناصر المادية

يقصد بالعناصر المادية لنظام المعالجة الآلية للمعطيات جميع المكونات المادية الملموسة القابلة للإلتقاط والنقل واللازمة لعمله أو إشتغاله، وتتمثل هاته المكونات في ثلاثة وحدات وهي: وحدات الادخال( الفرع الأول) ووحدة المعالجة المركزية ( الفرع الثاني) ووحدات الاخراج( الفرع الثالث).

#### الفرع الأول: وحدات الادخال

هي الوحدات التي يمكن من خلالها للشخص القيام بادخال المعطيات المطلوب معالجتها الى وحدة المعالجة الرئيسية وهي المسؤولة عن إدخال المعطيات الى نظام المعالجة الآلية ومن أمثلها لوحة المفاتيح ومشغل الاقراص المغناطيسية أو مشغل شرائط التخزين أو الاقراص المغناطيسية الصلبة والفأرة، وتستخدم حاليا وحدات إدخال عالية الكفاءة والسرعة في إدخال المعطيات ومن أمثلتها إجهزة المسح الإلكتروني التي تقوم بقراءة الوثائق المكتوبة والخرائط المرسومة والصور التي تحولها الى إشارات ترسلها الى

[1]- جدي نسيمة، مرجع سابق، ص 18،

[2]- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية القاهرة، 1992، ص 19.

إجهزة نظام المعالجة الآلية لقراءتها والتعامل معها، كما توجد بعض الأجهزة الأخرى تستخدم للإدخال تتعرف على مطبوعات الحبر المغناطيسي تستخدم في البنوك، كما توجد وحدات للتعرف على الحروف والعلامات ضوئيا تستخدم في شركات الطيران والمؤسسات التجارية([1]).

**الفرع الثاني: وحدة المعالجة المركزية(الاساسية)**

تعتبر هذه الوحدة هي الأساس بالنسبة إلى جهاز الحاسب الآلي فإذا لم تكن موجودة فلا قيمة له، ولها دور رئيسي إذا تقوم بتنفيذ جميع العمليات اللازمة لتشغيل الجهاز([2])، وتتحكم في تدفق البيانات ومعالجتها وتخزينها([3])، ومن تم فهي التي تقوم بإنجاز كافة العمليات الحسابية بسرعة مذهلة تتلقى الأوامر عن طريق أجهزة الادخال ثم معالجتها وإخراجها بالكيفية التي يرغب بها مشغل الجهاز، كما تقوم بتنفيذ المعطيات من والى الوحدات المساعدة مع ضمان تحرك المعلومات من والى الذاكرة الرئيسية، ويعتبر المعالج من أكثر الأجهزة تعقيدا، حيث يحتوي على ملايين الترانزستورات والتي تترابط مع بعضها البعض بواسطة شعيرات معدنية من الزجاج المصهور والتي لها سمك أرق من سمك الشعرة الواحدة للإنسان، إذن فهي بمثابة العقل المفكر والمسيطر على باقي الوحدات المكونة لنظام المعالجة الآلية التي لا وجود لهذا النظام بدونها، وتنقسم وحدة المعالجة المركزية الى ثلاثة أقسام: وحدة التحكم ووحدة الحساب والمنطق ووحدة الذاكرة.

**أولا- وحدة التحكم:** وهي تعتبر بمثابة الدماغ بالنسبة للحاسب، ويمكن من خلالها إصدار الأوامر لجميع أقسام الحاسب وتنسيق فيما بينها من أجل القيام بالوظائف المطلوبة فيما بينها كلما كانت شريحة المعالج قوية كان النظام أسرع و أكثر كفاءة.

تنفذ المعالجات المصغرة تعليمات مختلفة التي تسح للجهاز الكومبيتر بالعمل، حيث يصدر كل جهاز إدخال وإخراج متصل بجهاز الكومبيتر تعليمات أو يتلقى تعليمات

---

[1]- رشيدة بوكر، مرجع سابق، ص 58،59.

[2]- عبدالرحمن جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي-دراسة مقارنة، أطروحة مقدمة لاستكمال متطلبات درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس فلسطين، 2008، ص 8.

[3]- حسن عماد مكاوي، تكنولوجيا الإتصال الحديث في عصر المعلومات، الدار المصرية اللبنانية، الطبعة الثانية، 1998، ص 74.

يعالجها المعالج بعد ذلك، تعد تلك الشريحة حقا هي الجهاز العامل الأساسي في النظام، حيث أنه يؤثر على كل شيء يفعله جهاز الكومبيتر، وتتنوع المعالجات وتختلف من حيث الآداء والسرعة([1])

**ثانيا -وحدة الحساب والمنطق:** هي جزء من وحدة المعالجة المركزية، وهي المسؤولة عن القيام بالعمليات الحسابية والمنطقية التي يعهد بها الى نظام المعالجة الآلية مثل عمليات الطرح والضرب والجمع، وكذا إجراء المقارنات بين المتغيرات المختلفة([2]).

وتتم على مستوى هذه الوحدة كل الحسابات والمقارنة والقرارات المنطقية وذلك بعد تغذيتها بالبيانات من وحدات الإدخال يتم أخذ البيانات المطلوبة من المدخلات وإجراء العمليات الحسابية والمنطقية عليها بواسطة الأوامر والتعليمات الصادرة من البرنامج المستخدم بغية الحصول على النتائج النهائية والتي يتم إرسالها إلى وحدة الإخراج للحصول على النتائج بالصور المناسبة مثل عرضها على الشاشة أو طبعها على الطابعة أو رسمها على راسم للمنحنيات أو تخزينها على وحدة تخزين خلفية أو أي أختيار آخر([3]).

**ثالثا -وحدة الذاكرة:** هي أي وحدة داخل الحاسب الآلي يمكن من خلالها تخزين المعطيات سواء بشكل مؤقت أو دائم، وسواء تمت عملية التخزين بواسطة المستخدم أو بواسطة الشركة المنتجة لمكونات الحاسب، وتتكون الذاكرة من مجموعة من الدوائر الإلكترونية التي تقوم بالإحتفاظ بالمعطيات والأوامر التي يحتاجها المعالج عند إجراء العمليات المختلفة وإرسالها عند الطلب، كما تحتفظ بالمعطيات الأساسية المطلوبة لنظام تشغيل جهاز الحاسب الآلي، ويمكن تقسيم الذاكرة إلى نوعين رئيسين وهما:

1- الذاكرة الداخلية: وتسمى كذلك internal memory لأن المستخدم لا يقوم بالتعامل مع هذا النوع من الذاكرة بشكل مباشر، إذ أن نظام التشغيل أو مصنفي أجزاء النظام هم من

[1]- رشيدة بوكر، مرجع سابق، ص 59

[2]- الغسلان عبد العزيز بن سليمان، جرائم الإعتداء على برامج الحاسوب-دراسة مقارنة، أطروحة مقدمة لاستكمال متطلبات درجة الماجستير، كلية المعهد العالي للقضاء، جامعة الأمام محمد بن سعود الإسلامية، الرياض-السعودية، 2000، ص 15.

[3]- محمد خليفة، مرجع سابق، ص 21.

يقومون بالتعامل مباشرة مع هذا النوع من أنواع الذاكرة، والذي ينقسم بدوره إلى عدة أصناف:

أ-**ذاكرة القراءة فقط:** وتعرف باسم rom إختصارا لتسميتها باللغة الإنجليزية readonly memory وتسمى أيضا بالذاكرة الدائمة، تسمح هذه الذاكرة بالقراءة منها فقط، كما أنها تحتفظ فقط بالمعطيات الأساسية التي يحتاجها الجهاز لبدء التشغيل مثل معلومات وحدات الإدخال والإخراج المتصلة بالجهاز كما تحتفظ بالمعلومات عن الشركة المصنعة([1])، ولا تفقد هذه الذاكرة محتوياتها بإنقطاع التيار الكهربائي([2]).

**ب-ذاكرة القراءة والكتابة:** وتعرف باسم ram إختصارا لتسميتها باللغة الإنجليزية readam access memory وتسمى أيضا بالذاكرة العشوائية أو الذاكرة المؤقتة أو الذاكرة المتطايرة أو ذاكرة العمل، وهي تستخدم في جميع أغراض التخزين أثناء تشغيل الحاسب([3])، فتعمل على تخزين المعلومات بصورة مؤقتة إستعدادا لمعالجتها أو تخزينها في وسائط التخزين الدائمة، وتحتفظ بجميع الملفات الرئيسية للبرامج عند البدء بتشغيلها، لذلك فأن حجم أو سعة هذه الذاكرة تعد من العوامل الرئيسية التي تؤثر على مدى فعالية النظام، فبعض البرامج تحتاج الى ذاكرة عالية لتشغيلها، وبغير ذلك يكون من الصعب إستخدامها.

**ج- ذاكرة القراءة فقط القابلة للبرمجة:** وتعرف باسم prom إحتصارا لتسميتها باللغة الإنجليزية prgrammable and read وهي تشبه rom في مكوناتها إلا أنها تختلف في أن ما يكتب عليها يتم بمعرفة شخص آخر ذو خبرة عالية قبل تركيبها في الجهاز.

**د- ذاكرة القراءة القابلة للبرمجة والحذف:** وتعرف باسم eprom إختصارا لتسميتها باللغة الإنجليزية erasable programmble read only هذا النوع من الرقائق من الممكن محوه والكتابة عليه مرات عديدة بإستخدام أداة خاصة تبعث تردد محدد من الموجات الضوئية ultraviolet(UV) light على الرقاقة فيمحو محتوياتها ويجهزها للكتابة عليها من جديد، وهذه الرقاقة تتكون أيضا من أسطر وعواميد وعند كل خلية تقاطع يوجد ترانزستوران مسؤولان عن شحن وتفريغ الخلايا.

---

[1]- رشيدة بوكر، مرجع سابق، ص 60،61.

[2]- علي حسن الطوالبة، الجرائم الإلكترونية،جامعة العلوم التطبيقية، مملكة البحرين،الطبعة ا، 2008، ص 19.

[3]- هلالي عبداللاه أحمد، مرجع سابق، ص 21.

**هـ - الذاكرة المخبأة:** وهي ذاكرة إلكترونية خاصة بالمعالج وعادة ما تكون بداخله، وهي تشبه ذاكرة الرام ولكنها أسرع منها فوقت الوصول يصل الى حوالي 20NC ويستخدمها المعالج في تخزين بعض المعطيات الخاصة والمتكرر إستخدامها ليسهل الرجوع إليها بسرعة فائقة([1]).

**2- الذاكرة الخارجية:** تتمثل في وسائط التخزين المختلفة التي يتعامل معها المستخدم بشكل مباشر، مثل Hard disk أو Floppy disk أو CD و الذاكرة الخارجية بمختلف أنواعها من أكثر الوسائل التي تساهم في نشر الفيروس بين المستخدمين عن طريق عملية تبادل المعطيات المصابة بالفيروس بإستخدام هذه الوسائط، فتنتقل العدوى للجهاز المتصل به.([2])

**الفرع الثالث: وحدات الاخراج**

هي التي تستخدم لإخراج البيانات والمعلومات المعالجة آليا داخل الحاسب الآلي والحيز الواقعي الملموس بأشكال وطلبات معينة([3])، أو هي الوحدات التي من خلالها يتم عرض نتائج العمليات التي إنتهى إليها الكومبيتر، وتم إدخالها إليه عن طريق وحدات الإدخال وإظهارها بأشكال مختلفة مرئية ومطبوعة، بحيث تقوم بنقل نتائج العمليات المختلفة التي تمت داخل نظام الحاسوب إلى الخارج بواسطة أجهزة الإخراج المتعددة([4])، ومن أمثلتها الطابعات والشاشات ومشغل الاقراص ووحدات الاصوات والسماعات ووحدات تخزين المعلومات على الأقراص الممنغطة أو على الشرائط الممنغطة.

يضاف الى هذه العناصر السابقة جميع التجهيزات التي تصنف كتجهيزات إتصال أصلا لكنها تستخدم ضمن التجهيزات السابقة لآداء مهام معينة كالمودم([5]) مثلا([1]).

---

[1]- رشيدة بوكر، مرجع سابق، ص 61،62.

[2]- محمد خليفة، مرجع سابق، ص 23.

[3]- جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية- دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، سنة 2010، ص 27.

[4]- سامي جلال قفي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي-دراسة مقارنة، دار شتات للنشر والبرمجيات، مصر، سنة 2011، ص 44.

[5]- كلمة مودم تعني إختصار لوظيفة تضمين الإشارت وإزالة تضمينها، وهوعبارة عن جهاز يحول نبضات الوصل والقطع الرقمية التي تمثل بيانات الحاسوب الى نغمات وصل وقطع تناظرية يمكن نقلها عبر شبكات الهاتف العادية،

**المطلب الثاني: العناصر المعنوية**

هي عناصر غير مادية تلعب دورا أساسيا في نظام المعالجة الآلية للمعطيات، و تعتبر بمثابة الروح بالنسبة لنظام المعالجة الآلية، وتتمثل في البرامج( الفرع الأول) والمعطيات (الفرع الثاني).

**الفرع الأول: البرامج**

يعرف البرنامج لغة بأنه لفظ يستخدم للإشارة إلى أهم مكونات الكيان المعنوي للحاسب الآلي وهي البرامج والمعلومات والبيانات([2])، وعرفه البعض بأنه مجموعة من التعليمات المتسلسلة التي تخبر الحاسوب ماذا يفعل أو أنه مجموعة من الأوامر والإرشادات والإيعازات التي تحدد لجهاز الحاسوب العمليات على وسيط Medi معين يمكن قراءته عن طريق الآلة، وبعد ذلك يمكن للبرنامج عن طريق معالجة البيانات أن يؤدي وظائف معينة ويحقق النتائج المطلوبة منه([3])، ومن تم فإنه يعد بمثابة العمود الفقري للحاسب ولا نبالغ إذا قلنا أنه يعتبر بالنسبة للحاسب بمثابة العقل للإنسان الذي يفكر به([4]).

ولبرنامج الحاسب الآلي مفهومان أحدهما ضيق والآخر واسع فأما المفهوم الضيق فينصرف إلى مجموعة من التعليمات الموجهة من الإنسان الى الآلة والتي تسمح لها بتنفيذ مهمة معينة، وأما المفهوم الواسع للبرنامج فهو يتضمن إضافة الى المفهوم الضيق

---

أنظر: رشيدة بوكر، مرجع سابق، ص 62، وعرفت أيضا بأنها الوسيلة التي تمكن أجهزة الحاسب الآلي من الإتصال مع بعضها البعض عبر خطوط الهاتف وقد تطورت المودم الى أجهزة إرسال الفاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها، أنظر: محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحوث مؤتمر القانون والكومبيتر والأنترنت، المجلد الثالث من 1 الى 3 مايو 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الطبعة الثالثة، 2004، ص 1060.

[1]- رشيدة بوكر، مرجع سابق، ص 62.

[2]- محمد هاشم ماقورا، مقال بعنوان الحماية الجنائية لبرامج الحاسب الآلي، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد1، سبتمبر 2009، ص 151.

[3]-رشيدة بوكر، مرجع سابق ، ص 68.

[4]- فتوح الشادلي، عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون- دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، ب س ن، ص 12.

وصف البرنامج وهو التقديم الكامل المفصل بصورة كافية لعمليات في شكل شفوي أو خطي أو غيره، بغية تحديد مجموعة التعليمات المشكلة لبرنامج الحاسب الآلي وصلة كل منها بالاخرى، كما يتضمن المستندات الملحقة وهي المستندات التي ليست ببرنامج الحاسب الآلي ولا بوصف له، تهدف الى تبسيط مفهوم وتطبيق البرنامج([1])، وهو ذات التعريف الذي أخذت به المنظمة العالمية للملكية الفكرية، والتي عرفت البرامج على أنها "مجموعة من التعليمات التي تصبح بعد نقلها مقروءة من قبل الآلة لأداء أو إنجاز وظيفة أو مهمة أو نتيجة معينة عن طريق آلة قادرة على معالجة المعلومات"([2]).

كما أن المشرع الفرنسي وأن كان لم يبين موقفه من تعريف البرنامج سواء في قانون العقوبات أو في إطار القانون رقم 690-85 المؤرخ في 3 يوليو سنة 1985 بشأن حقوق المؤلف والقوانين المعدلة له، إلا أن موقفه يعكسه القرار الوزاري الصادر عن وزير الصناعة والتعليم الوطني في 22 نوفمبر عام 1981 بشأن إثراء اللغة الفرنسية الذي أخذ بموجبه بالمفهوم الواسع للبرنامج([3]).

أما المشرع السوري فقد أدرج البرامج الحاسوبية بما في ذلك وثائق التصميم مثل نظيره المشرع الجزائري ضمن المصنفات المحمية، وذلك بموجب الفقرة(ب/9) من المادة (2)([4]) من الفصل الأول من القانون رقم 62 لعام 2014، المتعلق بحماية حقوق المؤلف والحقوق المجاورة السوري.

---

[1]- محمد خليفة، مرجع سابق، ص 25،24.

[2]-جدي نسيمة، مرجع سابق، ص 21.

[3]- نقلا عن: رشيدة بوكر، مرجع سابق، ص 73،72.

[4]- نصت المادة الثانية الفقرة ب النقطة التاسعة منها في الفصل الأول بعنوان محل حماية حقوق المؤلف من قانون حماية حقوق المؤلف والحقوق المجاورة السوري على ما يلي:" ب- تشمل الحماية جميع أشكال إنتاج العقل البشري سواء كانت شفهية أم خطية أم تصويرية أم رقمية ومهما كانت طريقة التعبير عنها ومنها بوجه خاص المصنفات الآتية:

9- البرامج الحاسوبية سواء كانت بلغة المصدر أم بلغة الآلة ومنها وثائق التصاميم ومجموعات المعلومات بإستثناء واجهة البرنامج والأفكاروالنظريات التي يقوم عليها"، أنظر: قانون حماية حقوق المؤلف والحقوق المجاورة السوري الذي صدر بالمرسوم رقم 62 لعام 2014 المؤرخ في 16 أيلول 2013، وبدأ به العمل بعد ستة أشهر من تاريخ نشره في الجريدة الرسمية للجمهورية السورية، ص2..

في حين لم يتطرق المشرع الجزائي الجزائري على غرار التشريعات الجزائية المقارنة الى تحديد مفهوما للبرنامج، والعلة في ذلك أن ما يدور من تعاريف مختلفة للبرامج لم تتناولها التشريعات الجزائية، وإنما تم ذلك في نطاق التشريعات التقليدية التي تنظم حقوق المؤلف.

وبالرجوع الى قانون حق المؤلف الجزائري([1])، نجد أن المشرع الجزائري قد وسع من قائمة المؤلفات المحمية حيث أدمج المصنفات المعلوماتية([2]) ضمن المصنفات الأصلية التي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي، فواكب بذلك العديد من التشريعات في معظم الدول التي إتجهت الى تعديل قوانين حقوق المؤلف، حيث أعتبر بموجب قانون حقوق المؤلف والحقوق المجاورة لاسيما في الفقرة (أ)([3]) من المادة الرابعة (4) والفقرة (2)([4]) من المادة الخامسة (5) منه الواردتين ضمن الفصل الأول بعنوان المصنفات المحمية مصنفات قواعد البيانات وبرامج الحاسب الآلي مصنفات محمية([5]).

ومن وجهة نظرنا، فإننا نؤيد الأخذ بالمفهوم الضيق للبرنامج، وذلك لأن الأخذ بالمفهوم الواسع من شأنه أن يضفي حماية على عناصر ليست جديرة بالحماية، إذ أن

---

[1]- الأمر رقم 03-05 المؤرخ في 19 جويلية سنة 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر ج ج، ع 44، المؤرخة في 2003/07/23.

[2]- من أهم المصنفات المعلوماتية أو تقنية المعلومات التي حظيت بإهتمام كبير من حيث وجوب الإعتراف بها وتوفير الحماية القانونية لها على مستوى العالم أجمع برامج الحاسوب (الكومبيتر) وقواعد البيانات والدوائر المتكاملة، أسماء النطاقات أو مواقع الأنترنت، ومحتوى المواقع من مواد النشر الإلكتروني نصوصا وصورا ومواد سمعية ومرئية (الوسائط المتعددة)، أنظر: رشيدة بوكر، مرجع سابق، ص 70

[3]- تنص الفقرة (أ) من المادة (4) من الأمر 03-05 المؤرخ في 19 يوليو سنة 2003، المتعلق بحقوق المؤلف والحقوق المجاورة على ما يلي: " تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي:

أ- المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية، والبحوث العلمية والتقنية والروايات، والقصص، والقصائد الشعرية، وبرامج الحاسوب، والمصنفات الشفوية مثل المحاضرات والخطب والمواعظ وباقي المصنفات التي تماثلها..."

[4]- تضمنت الفقرة (2) من المادة (5) قواعد البيانات فجاءت كما يلي:

" تعتبر أيضا مصنفات محمية الأعمال الآتية:

المجموعات والمختارات من المصنفات، مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للإستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، والتي تتأتى أصالتها من إنتقاء مواردها أو ترتيبها".

[5]- رشيدة بوكر، مرجع سابق، ص 70،71.

كثير من التعليمات الموجهة الى مستخدمي نظم المعالجة الآلية عادة ما يرفقها منتجو هذه البرامج ببرامج أخرى، وبالتالي لا يمكن أن تكون هذه التعليمات ضمن مفهوم البرامج، إضافة الى أن الأخذ بالمفهوم الضيق يعد متوافقا مع المفهوم العلمي الذي يجعل من البرنامج يؤدي وظائف معينة ويحقق النتائج المطلوبة منه.

وتصنف البرامج وفق مفهومها العلمي العام الى قسمين:

**أولا- برامج النظام:** وتقوم هذه البرامج بوظيفة إجرائية، حيث تسيطر على العمليات الأساسية للآداء الآلي داخل الحاسوب.

وبعض هذه البرمجيات يبنى داخل جهاز الحاسوب وبعضها يخزن على الأقراص الممغنطة ويجب شراؤه بشكل منفصل، ومن هذه البرمجيات لغات البرمجة([1]) والمترجمات([2]).

**ثانيا- برامج التطبيقات**: وتسمى برامج معالجة المعلومات وتقوم بتوجيه أقسام الحاسب الآلي ضمن النظام الذي وضع لها وفقا لأوامر البرامج التشغيلية المثبتة بالحاسب الآلي أو بلوحات مستقلة يجري إدخالها في نظام الكومبيتر، فهي تجعل النظام يستخرج نتائج معينة مطلوبة من المستخدم([3]) للإستفادة منها في عمله، وبذلك تكون وظيفة التطبيق الموضوعي هي المهمة الأساسية للبرامج التطبيقية([4]).

---

[1]- البرمجة هي عملية كتابة أو وضع البرامج، ولغات البرمجة هي عبارة عن تدوين مجموعة خاصة من العلامات أو الرموز يعبر بها عن البرنامج، فلغات البرمجة هي لغات مصطنعة، ولذلك فليس هناك حرية في التعبير كتلك التي تتميز بها اللغات الإنسانية، وهناك العديد من لغات البرمجة المستخدمة، ويتم تصميم كل منها لحل نوع خاص من المشكلات، ومن أهم لغات البرمجة المعروفة: فورتران، الكوبول، الباسكال، سي، جافا، أنظر: رشيدة بوكر، مرجع سابق، ص 69.

[2]- المترجمات: تعد كتابة برنامج نظام المعالجة الآلية بإحدى لغات البرمجة أيا كان محتواها لا بدا من ترجمته من لغته الأصلية المكتوب بها الى لغة الآلة حتى يتمكن جهاز نظام المعالجة الآلية من تنفيذه وتسمى هذه العملية بالترجمة، أنظر: المرجع نفسه، ص 69.

[3]- جدي نسيمة، مرجع سابق، ص 21.

[4]- مصطفى محمد عرجاوي، الحماية المدنية لبرامج الكومبيوتر في القوانين الوضعية، بحوث مؤتمر القانون والكومبيتر والأنترنت، المجلد الثاني من 1 الى 3 مايو 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الطبعة الثالثة، 2004، ص 369.

والبرامج التطبيقية لا تقع تحت حصر، ومن أمثلتها البرامج المستخدمة في البنوك والمؤسسات المالية لتؤدي وظائف معينة مثل مسك حسابات العملاء أو الربط بين فروع البنك([1]).

وعليه يمكن القول أن البرامج هي جزء أساسي في نظام المعالجة الآلية للمعطيات تقوم ببعث الحياة في الأجهزة بحيث أنه لا قيمة لهاته الأجهزة بدون برامج ولا فائدة من هذه البرامج بدون أجهزة.

**الفرع الثاني: المعطيات**

هي المعلومات التي تم تنظيمها ومعالجتها داخل نظام المعالجة الآلية للمعطيات وتخزينها بغية إسترجاعها عند طلبها، وكون المعطيات غير مادية لأنها عبارة عن نبضات الكترونية داخل الحاسب الآلي لا يمكن لمسها([2])، وقد سميت بهذا الاسم لأنها تعطى للحاسب الآلي لمعالجتها وتقديمها لمتلقيها كمعلومة مخرجة.

وعرفت إتفاقية بودابست المعطيات المعلوماتية([3]) بأنها" أي عمليات عرض للوقائع أو المعلومات أو المفاهيم في شكل معين جاهز لعملية المعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة لجعل منظومة معلوماتية تطبق وظيفة"، وتبنى المشرع الجزائري هذا التعريف في القانون 09-04 السالف الذكر في الفقرة ج من المادة (2) منه، بتعريفه للمعطيات المعلوماتية بأنها"أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها([4]).

وفي نفس السياق عرفت الإتفاقية الدولية للإجرام المعلوماتي المعطيات في المادة الأولى من الفصل الأول الفقرة ب على أنهاط عملية عرض للوقائع أو المعلومات أو

---

[1]- رشيدة بوكر، مرجع سابق، ص 69.

[2]- محمد خليفة، مرجع سابق، ص 25.

[3]- الشرح التفسيري لإتفاقية بودابست يبين بأن تعريف المعطيات المعلوماتية الوارد بها مأخوذ عن هيئة التوصيف العالمية الإيزو حيث جاءت الفقرة 25 من الشرح كالآتي: يقوم تعريف البيانات المعلوماتية على تعريف البيانات الذي أعدته هيئة الإيزو ويتضمن هذا التعريف كلمات " الذي يتهيأ الى المعالجة" ويعني ذلك أن توضع البيانات على شكل يسمح لنظام المعلومات بمعالجتها بصفة مباشرة، أنظر: مناصرة يوسف، مرجع سابق، ص 38.

[4]- مناصرة يوسف، مرجع سابق، ص 37،38.

المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكومبيتر لما في ذلك البرنامج المناسب لجعل منظومة الكومبيتر تؤدي وظائفها"([1]).

والمعطيات حسب الاستاذ j-p Buffelan هي سلسلة من أحرف مغناطيسية تترجم معلومات مسجلة، وعليه فهي بالنسبة له شكل معين تأخذه المعلومة بوضعها في قالب محدد، وهذا التعريف واسع ويجعل من المعطيات قالبا للمعلومات وشكلا لها، كون المعلومة في حد ذاتها هي الشكل الذي تتبلور فيه المعرفة، أما الأستاذ R. Gassin فيشرح المعطيات بمقارنتها مع مفهوم المعرفة ومفهوم المعلومات، فيرى بأن المعلومات هي المحتوى الإخباري للمعطيات، وهذه الأخيرة يعرفها بالرجوع الى القرار المؤرخ في 22 ديسمبر عام 1981 المتعلق بتنمية مصطلحات الإعلام الآلي بأنها تمثيل معلومة في شكل متفق عليه موجه لتسهيل معالجتها([2]).

ولكي تحظى هذه المعطيات بالحماية الجنائية لا بدا أن تكون محددة وسرية، ويظهر عنصر التحديد بالنسبة لجريمة التلاعب بمعطيات الحاسب الآلي، بوجود حدود للمعطيات التي يقع الإعتداء داخلها، أما عنصر السرية فيظهر بالنسبة لجريمة الدخول والبقاء غير المصرح بهما، باعتبار هذه المعطيات موجودة داخل نظام المعالجة الآلية للمعطيات، وأن هذا النظام مغلق وغير مفتوح للجمهور، ولا يتم الدخول إليه إلا بشروط معينة([3])، لذلك يجب التحقق من أن الشخص الذي يقوم باستخدام النظام هو ذلك الشخص المصرح له بالإستخدام وفقا للصلاحيات الممنوحة له والمتمثلة في الدخول على المعطيات والإطلاع والإضافة أو التعديل([4]).

كما أن هناك من ينطلق في تعريفه للمعطيات من إختلافها مع المعلومات فيعتبر الأولى تعبر عن الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض ولم تخضع بعد لعملية تفسير أو تجهيز للإستخدام، أما المعلومات فهي المعنى الذي يستخلص من المعطيات عن طريق العرف أو الإتفاق أو

[1]- جدي نسيمة، مرجع سابق، ص21.

[2]- مناصرة يوسف، مرجع سابق، ص 36.

[3]- محمد خليفة، مرجع سابق، ص 91.

[4]- أشرف السعيد أحمد، القرصنة الإلكترونية، مطابع الشرطة، مصر، ب ط، سنة 2013، ص 93.

الخبرة أو المعرفة، أو هي مجموعة من الأرقام والحروف أو الرموز المطلوب إدخالها الى الحاسب حتى يقوم بانتاج المعلومات المطلوبة([1])، ومن تم فإن المعطيات هنا هي المعلومات في حالة كمون وأن المعلومات هي معطيات في حالة تبلور، وبهذا التصور تكون المعطيات عبارة عن حقائق رقمية أو غير رقمية، أو مشاهدات واقعية لا تصورية، أو قياسات تتم بطريقة منهجية يمكن لآحاد الناس قراءتها وفهم دلالتها البسيطة دون الدخول في عمليات إستنتاجية وإستقرائية لدلالتها المعقدة سواء من حيث الربط بين أكثر من بيان منه([2]).

وعرفها الفقيه دون باركر بأنها:" مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل والإتصال أو للتفسير والتأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة([3]).

وقد يكون التلاعب بالمعلومة سببا في تغير الصورة التي توجد عليها، صحيح أن المعلومة تبقى ولكنها تكون بدون معنى، ومثال ذلك في حالة إدخال أحد البرامج الخبيثة الى نظام المعالجة الآلية، فأنه يتم تحويل المعلومة الى عدد من الحروف المبعثرة التي تتهاوى بسرعة كبيرة الى القاع مكونة كومة كبيرة من الحروف، وعلى الرغم من أن المعلومة مازالت موجودة إلا أنها فقدت كل أهمية لها([4]).

كما أن المعطيات والمعلومات يتفقان في أن كل واحدة منهما تحوي مضمونا معينا أي يتضمن فكرة معينة أو معرفة، لكن ما يميز كل واحدة عن الأخرى هو الصورة التي توجد في الواقع، فالمعطيات المقصودة هنا لا بدا أن تأخذ شكلا معينا، و ذلك بعد معالجتها داخل نظام المعالجة الآلية للمعطيات وأن مكانها هو هذا الأخير، اما المعلومات فقد يتم إدخالها الى الحاسب الآلي وتتم معالجتها في هذا النظام وبالتالي تصبح معطيات، كما إنها قد لا تأخذ شكلا معينا ببقائها مجرد أفكار ومعرفة داخل ذهن

[1]- المرجع نفسه ، ص 88.

[2]- رشيدة بوكر، مرجع سابق، ص 67.

[3]- جدي نسيمة، مرجع سابق، ص 21.

[4]- رشيدة بوكر، مرجع سابق، ص 83.

وفكر الانسان أو أنها لا تأخذ شكلا آخر يختلف عن الشكل الذي يقدمه لها نظام المعالجة الآلية للمعطيات.

وعليه يمكن القول أن كل معطيات هي معلومات وليس كل معلومات هي معطيات ذلك أن المعلومات لا تصبح معطيات إلا بعد معالجتها آليا وأن كان الكثير من الباحثين يطلق مصطلح المعلومات على الأثنيين معا.([1]).

ويميز بعض الفقه مثل نائلة عادل محمد فريد قورة في المؤلف جرائم الحاسب الاقتصادية بين المعلومات والبيانات فهذه الأخيرة تعبير عن الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة لها بينها و لم تخضع للتغيير أو الاستخدام وتخلو من المعنى الظاهري أحيانا اما المعلومات فهي المعنى الذي يستخلص من البيانات ([2])، أو هي البيانات المعالجة([3]).

اما الفرق بين المعطيات والبرامج يكمن في الوظيفة التي يؤديها كل واحد منهما، فالغاية من وجود المعطيات تكمن فيها في حد ذاتها إذ ليس لها دور في تشغيل الحاسب الآلي وإنما يعتبر هذا الأخير بمثابة مستودع تتم فيه معالجة هذه المعطيات وتخزينها ثم إتاحتها عند طلبها وإسترجاعها، اما البرامج فالغاية منها هي الوظائف التي تقدمها فليس مجرد الإطلاع على البرنامج وأخذ فكرة هو الهدف منه بل أن وجود الحاسب له دور وهو القيام بمختلف العمليات التي يحتويها نظام الحاسب، فهذا الأخير لا يقوم بعمله إلا عن طريق مجموعة من البرامج التي تسمح بالقيام بمختلف العمليات عند إعطائها اوامر بذلك، فقيمة المعطيات إذا والغاية منها تكمن فيما تحويه هي ذاتها، أما قيمة البرامج فتكمن فيما تقوم به من وظائف في تشغيل الحاسب الآلي، ولا غنى للمعطيات عن البرامج لأن إدخال المعطيات ومعالجتها وتخزينها وإسترجاعها يتطلب وجود برنامج خاص لمختلف هذه العمليات([4]).

---

[1]- محمد خليفة، مرجع سابق، ص 89.

[2]- جدي نسيمة، مرجع سابق، ص 22.

[3]- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق ، ص 54.

[4]- محمد خليفة، مرجع سابق، ص 90.

**المطلب الثالث: شبكات الإتصال**

وهي ذات طابع مادي تنقل المحتوى الغير مادي من المعطيات وتعمل على ربط الأجهزة والأنظمة المعلوماتية المختلفة على المستوى المحلي أو الدولي التي تخضع لسلطة وتسيير العنصر البشري ولعل أهمها حاليا هو شبكة الانترنت التي تربط مجموعة من أجهزة الكومبيتر ببعضها البعض لتستطيع تبادل المعلومات.([1]).

والشبكة هي عبارة عن مجموعة من أجهزة الحاسب وبعض الأجهزة الأخرى مرتبطة مع بعضها البعض للمشاركة في الموارد المتاحة مثل الطابعات والبرامج التطبيقية([2])، وتلك الرابطة يمكن أن تكون أرضية كالسلك أو الكابل، كما يمكن أن تكون لاسلكية مثل الراديو أو الأشعة الحمراء أو القمر الصناعي([3]) أو كليتهما معا أي السلكية واللاسلكية.

والشبكة يمكن أن تغطي منطقة صغيرة فتسمى بالشبكة المحلية Réseau locale ويرمز إليها ب: l.a.n إختصارا لتسميتها باللغة الإنجليزيةlocal area network وإستخدامها محدود بالعاملين فيها، والشبكة المحلية هي عبارة عن نظام إتصال المعلومات يسمح لعدد من الأجهزة المستقلة بالإتصال كل مع آخر في حيز معتدل، ومن خلال قنوات إتصال فيزيائية وبمعدل مرور معلومات معتدل، أما الشبكات الممتدة هي نفسها المحلية لكن مع وجود إختلافين جوهريين.

- الأول: هو المسافة التي قد تكون هنا بعشرات أومئات بل ربما بالآلاف الكيلومترات. -
- الثاني: هو وجود أجهزة خاصة تضطلع بمهمة تنظيم عملية الإتصال كنقاط مركزية في الشبكات الممتدة لكي تنجز مهامها في الإتصال كما لو كانت محلية وهذه الإجهزة

[1]-جدي نسيمة، مرجع سابق، ص 22.

[2]- مجدي محمد أبو العطاء، أمن المعلومات والأنترنت، شركة علوم الحاسب كمبيوساينس، مصر، سنة 2016، ص 144.

[3]- مصطلح القمر يعود من الناحية الجغرافيا الى جسم فضائي يصاحب ويدور جسم فضائي أكبر منه، فالقمر هو جسم تابع للأرض يدور حولها مثلا...بالإضافة الى الأقمار الطبيعية يوجد الآن ما يسمى بالأقمار الصناعية والتي تستعمل في الأغراض الأمنية والأهداف العلمية والإتصالات، والغرض من الأقمار الصناعية هو جمع المعلومات عن الأرض والشمس ونقلها الى الأرض، دراسة حالة الطقس، الإتصالات السلكية واللاسلكية للأغراض العسكرية وتصوير مواقع العدو، أنظر: رشيدة بوكر، مرجع سابق، ص 85.

تسمى بالأجهزة الموزعة، وتقوم هذه الموزعات بعملية الإتصال بين محطات العمل المنتشرة في الشبكة الممتدة.

كما يمكن أن تغطي منطقة كبيرة فتكون شبكة واسعة النطاق فتسمى الشبكة الواسعة النطاق أو الشبكة البعيدة المدى Réseau etendu ويرمز إليها برمز w.a.n إختصارا لتسميتها باللغة الإنجليزية wide area network وهي تقدم المعلومات والخدمات للعديد من المستخدمين ومنها الأنترنت، التي تعددت التسميات التي تطلق عليها مثل شبكة طرق المواصلات السريعة، شبكة الطرق الدولية للمعلومات..، وتعتبر من أكبر شبكات حواسيب موسعة تغطي جميع أنحاء العالم، تصل بين حواسيب شخصية وشبكات محلية، وشبكات عامة.

والأنترنت هي كلمة إنجليزية مركبة مختصرة مكونة من مقطعين i-ter إختصارا للكلمة الإنجليزية international وتعني دولي وnet إختصارا لكلمة network وتعني الشبكة([1])، وهي عبارة عن شبكة هائلة من أجهزة الكومبيوتر المتصلة فيما بينها بواسطة خطوط الإتصال العالمية([2]).

وشبكة الأنترنت أوجدها الجيش الأمريكي كوسيلة إتصال مستقلة وسريعة، وأنطلق العمل بها رسميا بتاريخ 1969/01/02 ثم إنتشر هذا المشروع في منتصف السبعينات وتبنته هيئات التدريس في الجامعات لتبادل البيانات العلمية والفنية وكان يسمى ARPA NET وهو إختصار ل" وكالة مشروعات البحوث المتقدمة"، إلا أن الإنتشار الحقيقي للأنترنت كان عام 1980، ومنذ ذلك التاريخ وهذه الشبكة في تطور وإنتشار([3])، وهذا بالرغم من أن الحكومة الأمريكية في البداية كانت ممثلة في وزارة الدفاع ثم المؤسسة القومية للعلوم هي المالك الوحيد للشبكة ولكن بعد تطور الشبكة ونموها لم يعد هناك مالك لها وأختفى مفهوم التملك ليحل محله ما أصبح يعرف بمجتمع الأنترنت الإفتراضي، كما أن تمويل الشبكة تحول من القطاع الحكومي الى القطاع الخاص.

---

[1]- رشيدة بوكر، مرجع سابق، ص ص 85-87.

[2]- رابحي أحسن، مقال بعنوان الجريمة الإلكترونية: النقطة"المظلمة" بالنسبة للتكنولوجية المعلوماتية، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد1، سبتمبر 2009، ص 100.

[3]- جدي نسيمة، مرجع سابق، ص 22،23.

وأن الأنترنت مهما تعددت تعريفاتها فإنها تدور حول مفهوم واحد وهو أن أنها عبارة عن شبكة تسمح بإنضمام شبكات معلوماتية ذات أنساق مختلفة في إطارها وذلك بفضل إستخدام البرتوكول الوحيد([1]) والبريد الإلكتروني والصفحات والمعلومات والآراء وكذلك بنوك المعلومات([2]).

ومع ذلك إختلف الفقه في فرنسا حول إعتبار شبكة الإتصالات ضمن النظام المعلوماتي بين ثلاثة إتجاهات.

فذهب الإتجاه الأول إلى رفض إعتبار أن تكون شبكة الإتصالات ضمن النظام المعلوماتي، وبالتالي لا تقع تحت طائلة النصوص العقابية التي تعاقب على التعديات على النظم المعلوماتي، مستندا في ذلك إلى أن القانون الفرنسي رقم (88-19) الصادر في 22 ديسمبر 1987 والنافذ في 5 يناير 1988 المتعلق بالجرائم المعلوماتية([3]) قد أورد فقط حماية المعلومات دون أن يعطي أي حماية لشبكة الإتصالات، وبالتالي فإنها لا تدخل ضمن الحماية المقررة للنظام المعلوماتي.

ويرى أصحاب الرأي الثاني أن الشبكات السلكية واللاسلكية وإن لم ينص على ذلك صراحة فإنها تعتبر من مكونات النظام المعلوماتي، وعليه فلا بدا من ضرورة وجود نظام أمني يحمي الشبكة من الإنتهاك بالدخول لإثبات سوء نية القائم بالمحاولة.

بينما ذهب رأي ثالث إلى أن الشبكة تدخل ضمن النظام وتحميها نصوص القانون التي تحمي النظام المعلوماتي، وهو ما تبناه المشرع الجزائري في القانون 09-04 المذكور سالفا في مادته الثانية في الفقرتين أ ود/1، والتي نصت على أنه:" يقصد في مفهوم هذا القانون بما يأتي:

---

[1]- أن مصطلح البروتوكولات يعني مجموعة من القواعد المتفق عليها دوليا وذلك لإقامة الإتصالات بين الحاسوبات المختلفة، وقد تنوعت أسماء هذه البروتوكلا تبين الأسماء الطريفة مثل جوبر والأسماء الطويلة المزعجة التي تم إختصارها، وأهمها بروتوكول التحكم في النقل، رشيدة بوكر، مرجع لسابق، ص 87.

[2]- بنوك المعلومات هي عبارة عن تكوين قاعدة بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض معينة، أنظر: نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات- دراسة مقارنة، مرجع سابق، ص 71.

[3]-Loi n°88-19 du 05 janvier 1988, relative à la fraude l'informatique , JORF du 06 janvier 1988 , (LOI GODFRAIN)

أ-الجرائم المتصلة بتكنولوجيات الإعلام والإتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

د- مقدمو الخدمات

1- أي كيان عام أو خاص يقدم لمستعمليه خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات([1]).

[1]- عمراني أحمد، مقال بعنوان الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في التشريع الجزائري والمقارن، مجلة الحضارة الإسلامية، جامعة وهران السانية، المجلد 13، العدد 16، ماي 2012، ص 597،598.

## المبحث الثالث:أهمية الحماية الجنائية لنظام المعالجة الآلية للمعطيات

لقد تعاظم الدور الذي يؤديه نظام المعالجة الآلية للمعطيات باعتباره مستودعا لكم هائل وضخم من البيانات والمعلومات الشخصية والاقتصادية والمالية والعسكرية، وأصبح عرضة للكثير من الإعتدءات التي تمس بسلامته مما أدى الى ظهور شركات متخصصة في صناعة برامج الحماية الفنية ونظم الأمان الهدف منها حماية هذه الأنظمة من الإختراقات والفيروسات، ورغم هذا التطور الذي بلغته هذه الصناعة فإن الإعتداءات لم تتوقف بل على العكس من ذلك ذهب مرتكبوها إلى تطوير تقنيات وسائل إرتكابهم لهذه الجرائم بما يحبط آمان هذه النظم و إلحاق أضرارا إقتصادية كبيرة بالدول والمؤسسات من خلال الولوج اليها بطرق غير مشروعة، الأمر الذي جعل المشرع الدولي والداخلي يتدخلان بوضع نصوص جديدة لتجريم مختلف أنواع العدوان على نظم المعالجة الآلية للمعطيات.

وعليه فإن أهمية الحماية الجنائية لنظام المعالجة الآلية للمعطيات تتجلى من خلال معرفة مبررات حماية نظام المعالجة الآلية للمعطيات(المطلب الأول) وخصائص جرائم نظام المعالجة الآلية للمعطيات وتقنيات إرتكابها( المطلب الثاني) وقصور الحماية الفنية للنظام ( المطلب الثالث).

### المطلب الأول: مبررات حماية نظام المعالجة الآلية للمعطيات

أن موضوع الحماية الجنائية لنظام المعالجة الآلية للمعطيات من أكثر المواضيع التي آثارت التشكيك حول قدرة النصوص الجنائية التقليدية على مسايرة واقع الثورة المعلوماتية لما أفرزته من تداعيات قانونية جنائية غير مسبوقة أصبحت تهدد مصالح الأشخاص والدول، ولعل ذلك يرجع أساسا الى الأسباب التالية:

#### الفرع الأول: أهمية المعطيات المدرجة في النظم المعلوماتية

إن التطورات التكنولوجية الحديثة لنظم المعالجة الآلية للمعطيات غيرت الكثير من المفاهيم القانونية التقليدية التي يصعب على رجل القانون فهمها باعتبارها أصبحت تدخل في عصر العولمة والتدويل والرقمنة، وتكون في بيئة رقمية إفتراضية أزآلت المسافات وتلاشت معها الحدود، فأصبحت العلومات بأشكالها المتباينة في البيئة الرقمية الهدف الرئيسي لمرتكبي جرائم تقنية المعلومات بصفة عامة، وذلك نتيجة للقيمة الإقتصادية

العالية التي تمثلها إذ تفوق قيمة الأموال المادية، إلا أن طبيعة هذه الأموال([1]) في حالتها المجردة من الوسائط المادية تثير عدة مشاكل في تحديد محل الجريمة باعتبارها مجرد إشارات الكترونية غير مرئية تنساب عبر أجزاء نظام المعالجة الآلية وشبكات الإتصال العالمية بصورة آلية وليست ذات كيان مادي([2]).

وأن المادة محل الوصف في هذا العصر الرقمي هي المعطيات المدرجة بأنظمة الحواسيب وأنظمة الإتصالات بمكوناتها المادية والمعنوية، وما نتج عن إستعمالها من سرعة فائقة في نقل وتخزين وتبادل المعلومات داخل شبكات المعلومات التي تربط بين مختلف الحاسبات الآلية في مختلف أنحاء العالم، أدت الى تقريب المسافات بين دول العالم وتسهيل التواصل بين مختلف الجنسيات وتطور عالم الإقتصاد والثقافة، وبروز موازين وتكتلات جديدة قوامها المعلومة فمن يملك المعلومة في وقتها يملك القوة([3])، الأمر الذي أحدث إنقلابا حقيقا وكبيرا على المفاهيم الجنائية التقليدية، وطرح السؤال حول قدرتها على التأقلم مع هذا التحول أم عجزها على ذلك وما إذا كان يتعين هجرها والبحث عن بدائل قانونية حديثة تواكب التطورات التقنية وما أفرزته من نظم معلوماتية لازمة للتعامل مع هذا الوسط الحديث([4]).

[1]- لم يحدد المشرع الجزائي الجزائري المقصود بالمال، وبالتالي كان لا بدا من الرجوع الى القانون المدني وبالتحديد الى المادة 682 منه التي عرفت المال بأنه" كل شيء خارج عن التعامل بطبيعته أو بحكم القانون" والشيء في نظر القانون كما عرفته هذه المادة هو ما يصلح لأن يكون محلا لحق من الحقوق المالية، وفي نفس المعنى عرفت المادة 83 من القانون المدني السوري المال بأنه" هو كل شيء خارج عن التعامل بطبيعته أو بحكم القانون يصح بأن يكون محلا للحقوق المالية" فالأموال من وجهة نظر الإتجاه التقليدي لا ترد إلا على الأشياء المادية لهذا كان تعريف المال بصدد جرائم الأموال على أنه" كل شيء مادي يصلح لأن يكون محلا لحق من الحقوق المالية"، أنظر: القانون المدني السوري الصادر بالمرسوم التشريعي رقم 84 بتاريخ 1949 والمطبق إعتبارا من 15 حزيران 1949، مكتبة محمد حسين النوري، دمشق-سورية.

[2]- رشيدة بوكر، مرجع سابق، ص 90.

[3]- مناصرة يوسف، مرجع سابق، ص 9.

[4]- حمودي ناصر، مقال بعنوان الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الاكاديمية للبحث القانوني ، المجلد 14، العدد2 لسنة 2016، ص 70.

**الفرع الثاني: إرتباط النظم المعلوماتية بالأنترنث**

أن البعد التقني الحديث للنظم المعلوماتية غير الكثير من المفاهيم القانونية التقليدية، وأحل مفاهيم أخرى محلها تصعب على رجل القانون فهمها وإدراكها، خاصة بحلول دعائم الكترونية رقمية أوجبت الإعتراف بها وإضفاء الحجية القانونية عليها مما آثار في الوقت ذاته مسألة حمايتها جنائيا، خاصة بعد أن أخذت الطابع الدولي باعتبارها شبكة دولية مفتوحة ترفض الإعتراف بالحدود وتأبى الخضوع لمفاهيم السيطرة والأمر والملكية، الأمر الذي أعجز أهم المبادئ التي يقوم عليها القانون الجنائي المتمثلة في الإختصاص المبنية على فكرة الحدود الأقليمية، لاسيما وأن الأنثرنت ليست ملكا لأي جهة ولا يسيطر عليها أي أحد أضغفت كثيرا بهذه المبادئ التي كانت متجذرة في السيادة الأقليمية للدولة، إضافة الى أن الأدوات والمعدات الإلكترونية المستحدثة قد يضيق بها الإنسان ذرعا لأنها ستصيبه بأذى وضرر ناجم عن الجرائم الحديثة التي تتمخض عنها، وسوف تسهل وتوسع من مجالات إنتهاك مكنون حياته الخاصة للحصول على أسراره الشخصية وأسراره المالية بل أن هذه الوسائل قد تنتهك كذلك الأسرار المهنية والإقتصادية للمؤسسات والشركات والبنوك([1])، ومن تم كان لزاما على هذه التطورات المعلوماتية أن تواكبها في نفس الوقت تطورات في المتطلبات القانونية لتجاوز قصور القواعد الجنائية التقليدية ومواجهة ظواهر إجرامية مستجدة سميت عموما بالإجرام المعلوماتي أو الإلكتروني أو الرقمي.

**الفرع الثالث: النظم المعلوماتية تتطلب أساليب مستحدثة للمواجهة**

إن النظم المعلوماتية للأنترنت شكلت موضوعا قانونيا جديدا للحماية، صاحبتها ظواهر إجرامية معلوماتية، تبين أنها في تطور مستمر وفي كل مرة تظهر بشكل جديد مسايرة بذلك االتقنيات والتطبيقات المستجدة، وتتم عبر أساليب إجرامية جديدة لم تألفها مبادئ القانون الجنائي التقليدي التي تبدو قاصرة في مواجهتها، وتفاديا لفكرة الفراغ التشريعي الذي يتيح إفلات الكثير من المجرمين من العقاب تعين البحث عن أساليب مستحدثة للمواجهة، خاصة وأن للنظم المعلوماتية أساليب تقنية وضعت لكي تتم من خلالها تبادل المعلومات المعالجة إلكترونيا، التي أضحت بدورها موضوعا للجريمة المعلوماتية هي

[1]- مناصرة يوسف، مرجع سابق، ص 41،42.

والنظم التي تعالجه، الأمر الذي يحتم إعادة التفكير في صياغة المفاهيم الجنائية التقليدية لأجل مواجهة ظاهرة الإجرام المعلوماتي بتطوير الظاهرة القانونية.

وما يزيد أيضا من خطورة هذه الجرائم إنها تنصب على قيم معنوية لا تلمسها الأيدي ولا تبصرها الأعين تتخطى حدود المكان في ظل إنفتاح شبكة الأنترنت وتجاهلها للحدود الجغرافيا للدول، إضافة الى إنها ترتكب من قبل أشخاص من أصحاب المعارف والمهارات الفنية، وفي الغالب من قبل المتخصصين في مجال المعلوماتية وعلى قدر عال من الاحتراف يضاف لذلك خفاء الجريمة المعلوماتية كونها تتم عبر نبضات الكترونية لا تجيد قراءتها سواء برامج الكومبيتر، كل ذلك في ظل غياب الكفاءات العالية وإنعدام الخبرة لدى الأجهزة الأمنية والقضائية([1]).

كما أن هذه الجرائم تتميز بحداثة أساليب إرتكابها وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو آثارها وهي تعتمد في الأساس على الخداع في إرتكابها والتضليل في التعرف على مرتكبيها وتحتاج لخبرة فنية يصعب على الخبير التقليدي التعامل معها([2]).

**الفرع الرابع: وجوب مقابلة تطور الفكر الإجرامي بتفعيل الفكر القانوني**

إن تطور الفكر الإجرامي لا بدا أن يقابله تفعيل الفكر القانوني، بحيث أن ظهور الأنثرنت وما أسفرت عنه من ظهور ظاهرة الإجرام المعلوماتي يستدعي بالضرورة وجود مواجهة جنائية جديدة وفعالة كونه إجرام يقع على إنتهاك المواقع المعلوماتية وسرقة بياناتها وأموالها الإلكترونية ووجوب أن يكون هناك تطور موازي ومواكب في الإطار القانوني خاصة في ظل واقع المعلوماتية الذي يتسم بالحركية والتحول الدائمين وظهور الحاجة الى الحماية الجنائية للنظم المعلوماتية والبيانات التي تتدوال عبرها([3]).

وإن مراجعة المراحل التطورية التي مرت به معالجة ظاهرة الجرائم المعلوماتية منذ نشأتها تبين أنها في تطور دائم ومستمر وفي كل مرة تظهر بشكل جديد مسايرة بذلك التقنيات والتطبيقات الجديدة، وورد في وثيقة لجنة منع الجريمة والعدالة الجنائية في

---

[1]- حمودي ناصر، مرجع سابق، ص .71

2- مسرة خالد الحمد، الدليل الرقمي ومعايير جودته، مركز الكتاب الأكاديمي، عمان، ط الأولى، سنة 2014، ص 101.

[3]-حمودي ناصر، مرجع سابق، ص 71.

دورتها العشرين بفيينا من 11الى 15 نيسان/أبريل 2011 البند6 من جدول الأعمال المؤقت إتجاهات الجريمة على الصعيد العالمي والمسائل المستجدة وتدابير التصدي في مجال منع الجريمة والعدالة الجنائية بالأمم المتحدة E/CN.15/2011/19، التي جاء في مضمونها أنه في ستينيات القرن العشرين عندما ظهرت الأنظمة المعلوماتية بالترانزيستور وأصبحت الحواسيب تلاقي مزيدا من الرواج تم التركيز في تجريم الأفعال المرتكبة على الأضرار المادية التي تلحق بالنظم الحاسوبية والبيانات المخزنة فيها، وأتسمت السبعينيات بالتحول من جرائم الممتلكات التقليدية التي تمس النظم الحاسوبية الى أشكال جديدة من الجريمة تشمل أمور منها الإستخدام غير المشروع للنظم الحاسوبية والتلاعب بالبيانات الإلكترونية.

وأفضى الإنتقال من المعاملات اليدوية الى المعاملات الحاسوبية الى نشوء شكل جديد من الجريمة وهو الإحتيال الحاسوبي، وفي الثمانينات زاد رواج الحواسيب الشخصية أكثر فأكثر، وكان من بين الآثار الجانبية لانتشار النظم الحاسوبية إزدياد الإهتمام بالبرامجيات الحاسوبية وبدء ظهور أول شكل من أشكال قرصنة البرامجيات الحاسوبية، وفي التسعينيات أدى التزايد السريع في مستخدمي الأنترنت الى ظهور أساليب جديدة من السلوك الإجرامي حولت الجريمة الإلكترونية الى جريمة دولية، وأتسم العقد الأول من القرن الحادي والعشرين مرة أخرى بأنتشار أساليب إجرامية جديدة ومعقدة للغاية في إرتكاب الجرائم مثل التصيد الإحتيالي والإعتداءات البوتنتية والإستخدامات المستجدة للتكنولوجيا مثل الإتصال عن طريق بروتوكول نقل الصوت عبر الأنترنت (VOLP) والحساب الإلكتروني السحابي([1]).

**المطلب الثاني: خصائص جرائم نظام المعالجة الآلية للمعطيات وتقنيات إرتكابها**

تتميز جرائم نظام المعالجة الآلية للمعطيات بعدة خصائص تميزها عن باقي الجرائم التقليدية( الفرع الأول) ويتم إرتكابها بواسطة تقنيات حديثة( الفرع الثاني)

**الفرع الأول: خصائص جرائم نظام المعالجة الآلية للمعطيات**

إن جرائم نظام المعالجة الآلية للمعطيات تمتاز بعدة خصائص سواء تلك المتعلقة بالمجرم المعلوماتي أو بطبيعة الجريمة في حد ذاتها باعتبارها تقع على المعطيات،

[1]- مناصرة يوسف، مرجع سابق، ص ص 44- 46.

وسهولة إرتكابها وطمس آثارها وعابرة للحدود الوطنية وصعوبة إكتشافها وإثباتها ولها عدة إضرار كما للضحية إيضا دور مهم فيها.

**أولا: إنها جرائم ترتكب من مجرم معلوماتي**

إن المجرم المعلوماتي يحيا وسط المجتمع ويمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى([1]) أي أنه ينتمي في أكثر الحالات إلى وسط إجتماعي متميز ويكون على درجة كبيرة من العلم والمعرفة([2])، لذلك فإن هذا المجرم لا يوجد له نموذج محدد بل هناك عدة نماذج لهؤلاء المجرمين الذين قد يستخدمون نظام المعلومات الإلكتروني في جرائمهم وقد يقومون بأفعال جرمية ضد نظام المعلومات الإلكترونية نفسه، ويرى عدد كبير من الباحثين الذين عنوا بالمجرم في الجريمة المعلوماتية أن هذا المجرم وأن كان يتميز ببعض السمات الخاصة إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه، وفي هذا السياق يرمز بعض الباحثين بكلمة skram الى مجموعة الخصائص التي تميز المجرم في جريمة تكنولوجيا المعلومات الحديثة بصفة عامة عن غيره من المجرمين، وهي تعني المهارة Skils، المعرفة Knowledge، الوسيلة Ressourcesk، السلطةAuthority، الباعث Motive.

1- **المهارة:** يرى الأستاذ باكر أن تنفيذ هذه الجرائم يتطلب قدرة من المهارة يتمتع بها الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال وعن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات الحديثة أو بمجرد التفاعل الإجتماعي مع الآخرين.

**2- المعرفة:** يقصد بها التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانية نجاحها وإحتمال فشلها، فالجناة عادة يمهدون لإرتكاب جرائمهم بالتعرف على المحيط الذي تدور فيه حتى لا يواجه بأشياء غير متوقعة من شأنها إفشال إفعالهم أو الكشف عنهم.

---

[1]- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الأسكندرية، ب ط، سنة 2004، ص 62.

[2]- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية-جامعة أبوبكر بلقايد، تلمسان، سنة 2011/2010، ص 23.

**3- الوسيلة:** يراد بها الأمكانيات التي يتزود بها الفاعل لإتمام جريمته والقدرة على الحصول على ما يحتاج إليه أو إبتكار الأساليب اللازمة لإتمام نشاطه الإجرامي.

**4- السلطة:** يقصد بها الحقوق أو المزايا التي يتمتع بها المجرم في جريمة تكنولوجيا المعلومات الحديثة والتي تمكنه من إرتكاب جريمته، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول الى نظام المعالجة الآلية([1]).

**5- الباعث:** يقصد بالباعث أو الدافع الرغبة في تحقيق المكسب المالي الذي يظل هو الباعث الأول وراء إرتكاب جرائم النظام، في حين يرى البعض الآخر أن الربح المادي لا يعد هو الباعث في أغلب الأحيان على إرتكاب هذه الجرائم وإنما هناك أمورا عديدة أخرى مثل الإنتقام من رب العمل والرغبة في قهر النظام وإختراق حاجزه الأمني([2]).

كما أن المجرم المعلوماتي ينقسم الى نوعين رئيسين:

- الأول يتمثل في الهواة المولعون بالمعلوماتية.
- الثاني محترفوا الجرائم المعلوماتية.

وأساس التميز بين النوعين هو الباعث أو الدافع الى إرتكاب الجريمة بينما هو سادج لدى النوع الأول لا يتعدى الرغبة في الإستطلاع والإستكشاف في حين أنه خبيث لدى النوع الثاني والذي قد يكون ماليا أو سياسيا أو غيره([3])

**ثانيا: إنها جرائم تقع على المعطيات المدرجة ضمن نظام المعالجة الآلية للمعطيات**

هي جرائم تستهدف معنويات وليست ماديات ملموسة وتقع على العمليات الإلكترونية المختلفة ويكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للمعطيات، فإذا وقعت جرائم معينة على هذه الجوانب المعنوية كجرائم السرقة أو الإختلاس أو الإستيلاء أو الغش أو التزوير أو الإتلاف فإنه قد يصعب التعامل معها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة.

---

[1]- ملياني عبد الوهاب، أمن المعلومات في بيئة إلكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية-جامعة أبوبكر بلقايد، تلمسان، سنة 2017/2016، ص 64،65.

[2]- سعدات، محمود فتوح محمد، بحث بعنوان خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات-جامعة الأمام محمد بن سعود الإسلامية، الرياض- المملكة العربية السعودية، نوفمبر 2015، ص45.

[3]- محمد خليفة، مرجع سابق، ص 33،34.

وأن جهات التحقيق والتحري أعتادت الإعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجزائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإلكترونيات الأمر مختلف فالمتحري أو المحقق لا يستطيع تطبيق إجراءات الإثبات التقليدية على المعطيات المعنوية التي لا تترك أية آثار تدل على مرتكبها، لا سيما وأن هذه المعطيات التي يتم تداولها بواسطة العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممنغطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحاسبات الآلية([1])

**ثالثا: إنها جرائم تتميز بصعوبة إثباتها وإكتشاف مرتكبها**

أن جرائم نظام المعالجة الآلية للمعطيات لا تكتشف في الغالب إلا بعد مرور زمن طويل، وهي ترتكب بخفة شديدة من دون أن يرى طرفا الجريمة بعضهما البعض، وهي نادرا ما تكتشف مباشرة من الضحية أو غيره، وتقع في الغالب من دون أن يدرك المجني عليه نفسه بوقوعه ضحية للجريمة المرتكبة، ولعل مما يزيد من صعوبة إكتشافها أن أغلب الضحايا لا يتوسلون ببرامج وأنظمة الحماية الفنية لحماية أنظمة المعلوماتية([2])، ذلك أن الرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة والعدد الذي تم إكتشافه هو رقم خطير، والفجوة كبيرة بين الجرائم المرتكبة والجرائم التي تم إكتشافها([3]).

كما يشكل الكم الهائل للبيانات التي يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلآف من الصفحات والتي قد لا تثبت كلها تقريبا شيئا على الإطلاق([4]).

ومن تم يقتضي أن تكون جهات التحري و التحقيق بل و المحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسبة الإلكترونية وطريقة تشغيلها وأساليب ارتكاب الجرائم

---

[1]- مناصرة يوسف، مرجع سابق، ص 40.

[2]- ملياني عبدالوهاب، مرجع سابق، ص 61.

[3]- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية-جامعة أبوبكر بلقايد، تلمسان، سنة 2012/2011، ص 48.

[4]- الديربي عبدالعال، محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، ط الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص340.

عليها أو بواسطتها مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها و ضبط الأدوات التي استخدمت في ارتكابها، لذلك فقد وجدت صعوبات جمة في كشف غموضها و إجراء التفتيش والضبط اللازمين أو التحقيق فيها على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الموارد من الناحية الفنية على نحو تمكينها من تحقيق المهمة المطلوبة وبكفاءة عالية.

ففي الفترة الأولى لظهور هذا النوع من الجرائم وقعت الشرطة في أخطاء جسيمة أدت إلى الأضرار بالإجهزة أو الملفات أو الإدلة الرقمية الخاصة بإثبات الجريمة، ونعطي مثالا لهذا الخطأ من عمل الشرطة بالولايات المتحدة الأمريكية فقد حدث أن طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة وقد حدث نتيجة ذلك أن تسببت دائرة الشرطة بدون قصد في إتلاف ما كان قد سلم من الملفات والبرامج([1])

إضافة الى أن إثبات الجرائم التي تقع على العمليات الإلكترونية بإستخدام الوسائل الإلكترونية سيتأثر بطبيعة هذه الجرائم وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم إكتشاف العديد من الجرائم في زمن إرتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد و بالمجتمع([2]).

**رابعا: إنها جرائم يكون للضحية دور مهم في إرتكابها**

أن الضحية في جرائم نظام المعالجة الآلية للمعطيات لا تعلم عنها شيئا إلا عندما تكون إنظمتها المعلوماتية هدفا لفعل غير مشروع، أو حتى عندما تعلم فهي تفضل عدم إفشاء الفعل([3]) حرصا على ثقة العملاء فلا تبلغ عن تلك الجرائم التي أرتكبت ضدها([1])،

---

[1]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية- دراسة مقارنة، ماجستير قانون، كلية الحقوق، جامعة الموصل، المكتب الجامعي الحديث، الأسكندرية، ب ط، ص19،20.

[2]- جورج أسحق حنين، دراسة عن الجرائم المعلوماتية و الإلكترونية عبر شبكة الأنترنت و سبل مواجهتها، الإدارة العامة المركزية للمعلومات الإحصائية، ص16.

[3]- حكيم سياب، مقال بعنوان السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد1، سبتمبر 2009، ص 231.

ذلك أنها تلعب دورا لا يستهان به في أغلبها، وهذا الدور قد لا تلعبه بإرادتها كما هو الحال عندما تكون شخصيتها غير متجلية أمام الجاني، وذلك عندما لا يرى أمامه إلا الحاسبات وما تحتويه أنظمتها من معطيات دون أن يدرك قيمتها وما قد تمثله في الواقع.([2]).

كما تلعب العلاقة بين الضحية والجاني دورها في حدوث الجريمة وذلك إذا كان الجاني يعمل لحساب الضحية، لا سيما إذا كان عارفا بخبايا أنظمة الكومبيتر والثغرات الأمنية فيها أو كان مؤتمنا على ذلك، كأن يكون هو المسؤول عن المركز المعلوماتي فيستغل مركز الثقة الذي يحوزه، والتعود على الدخول إلى هذه الأنظمة.

ويمكن للضحية أيضا في هذه الجرائم أن يقدم خدمات كبيرة لرجال الشرطة أو لسلطة التحقيق بتقديمه معلومات تحقق فائدة كبيرة في معرفة طبيعة الجريمة التي وقعت وأساليب إرتكابها والأدوات المستخدمة في إرتكابها والأشخاص المشتبه فيهم وبواعث الجريمة وما إذا كان هناك شهود أم لا([3]).

**خامسا: إنها جرائم تمتاز بكونها سهلة الإرتكاب وقليلة المخاطرة**

أن الجرائم التقليدية يحتاج مرتكبها الى قوة عضلية لتنفيذها عكس جرائم نظام المعالجة الآلية للمعطيات التي تحتاج الى قوة علمية وذكاء ومهارة ولا تحتاج من الوقت إلا ثوان أو دقائق معدودة في إرتكابها، وفي بعض الأحيان يكون الدافع لإرتكابها بغرض اللهو والتسلية أو تحقيق إنتصارات تقنية دون أن تكون لديه سوء نية في إرتكاب جريمة معينة([4])،

والمجرم المعلوماتي يرتكب هذه الجرائم لوحده دون الإستعانة بأي شخص آخر بحيث أنه يكون قادر على تنفيذ مخططه الإجرامي لوحده وهو جالس أمام الكومبيتر في

---

[1]- خيرات علي محرز، التحقيق في جرائم الحاسب، دار الكتاب الحديث، القاهرة، سنة 2012، ب ط، ص 68.

[2]- محمد خليفة، مقال بعنوان خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد1، سبتمبر 2009، ص 373.

[3]- علي عدنان الفيل، مرجع سابق، ص20

[4]- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية (دراسة نظرية وتطبيقية)، منشورات الحلبي الحقوقية، بيرقت-لبنان، ط الأولى، سنة 2005، ص 61.

منزله أو مكتبة أو مقهى للأنترنث ضد ضحية موجودة في دولة أخرى تبعد عنه آلاف الأميال دون جهد عضلي، وإنما يحتاج فقط إلى قدر معين من التفكير الذهني وبعض ضغطات الأزرار والحصول على الأجهزة والبرامج التقنية للتعامل مع النظام المعلوماتي والشبكة المعلوماتية، ومن تم فإن هذه الجرائم تمنح الجناة في الغالب فرصة سانحة لتخفيض تكاليف إرتكاب جرائمهم، وتكون مغرية للمجرمين عموما، لأنها تحقق أكبر قدرا ممكن من الأرباح بأقل قدر ممكن من التكلفة والجهد.

كما إن نسبة مخاطرة الجاني الناجمة عن إرتكاب مثل هذه الجرائم قليلة نسبيا بالمقارنة مع تلك الناجمة عن إرتكابه للجرائم التقليدية وهو غير معرض لخطر المواجهة المباشرة مع المجني عليه إو غيره ولا لخطر المواجهة المسلحة، خصوصا وأن هذه الجرائم لا تكتشف في الغالب إلا بعد مرور زمن طويل على إرتكابها([1]).

وهذه الآثار المتخلفة عن هذه الجرائم هي آثار إلكترونية، وهذه الآثار بدورها إنما هي عبارة عن نبضات إلكترونية غير مرئية بالعين المجردة فهي تصل في حجمها و شكلها ومكان تواجدها الى درجة شبه منعدمة بحيث أنه لا يمكن رؤيتها إلا من خلال الإستعانة بأجهزة ووسائل تقنية تظهرها للعيان، إضافة إلى أن ضخامة حجم وكم البيانات والملفات الإلكترونية المجرمة من بين ذلك الكم الهائل لفصلها عن تلك البريئة منها تؤدي في الغالب إلى إصطدام مهمة الإكتشاف بحق الأفراد في الخصوصية الشخصية([2])

**سادسا: إنها جرائم تمتاز بسهولة إخفاء وطمس آثارها**

أن أستعمال طائفة متنوعة من التكنولوجيا الجديدة مثل الهواتف الخلوية الرقمية والهواتف الساتلية( الفضائية) وغرف المحادثات عبر الأنترنت والتي يصعب إعتراضها بالنسبة لوسائل الإتصال القديمة وكذا إستخدام منتجات التشفير القوية التي تجعل المعطيات المعترضة أو المضبوطة يصعب أو يستحيل قراءاتها، وأصبحت الآن أكثر شيوعا كاستعمالات يمكن للجناة الحصول عليها وإستخدامها باعتبارها عناصر أساسية

[1]- ملياني عبدالوهاب، مرجع سابق، ص 59،60.

[2]- جاسم خريبط خلف، مقال بعنوان الدليل الجنائي في الجريمة المعلوماتية، قسم القانون، كلية شط العرب، الجامعة،ص09.

جاهزة للبريد الإلكتروني وكذا الهاتف الخلوي وغير ذلك من التكنولوجيات، ومثل هذه الأجهزة تكون لديها وقاية بالتشفير وبموانع الإختراق وغير ذلك من برامج الآمان([1]).

ومن الصعوبات التي يمكن أن تعترض عمليات الإثبات في الجرائم الإلكترونية سهولة محو أو تدمير أدلة الإدانة في فترة زمنية يسيرة، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها قي زمن قصير جدا، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم إستطاعة هذه السلطات إقامة الدليل ضده وبالتالي تنصله من مسؤلية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسبة الإلكترونية أو الشبكة أو في الأجهزة، ومن أمثلة ذلك قيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسبة الإلكترونية الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذه الحاسبة من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة([2]).

**سابعا: إنها جرائم عابرة للحدود الوطنية**

أن جرائم نظام المعالجة الآلية للمعطيات تتعدى حدود المكان ويصعب بالنسبة لنا حساب الزمان، ويزداد اللأمر تعقيدا إذا كانت الأنظمة المعلوماتية متصلة في شبكة مفتوحة كشبكة الأنترنت التي لا تعترف بالأقليمية والجغرافيا، والحقيقة أن مسألة الأقليمية بين الفعل وتحقق النتيجة من أكثر المسائل التي تثير إشكالات في مجال جرائم المعلوماتية وبشكل خاص الإجراءات الجزائية والإختصاص القضائي والقانون الواجب التطبيق([3]).

وهذه الخاصية مكنت مجرمي المعلوماتية من إرتكاب جرائم عن بعد، فيكون هناك تباعد كبير بين الجاني والمجني عليه في هذه الجرائم، وبالتالي بين الفعل الإجرامي

[1]- مناصرة يوسف، مرجع سابق، ص 40.

[2]- عبد العال الديربي، محمد صادق إسماعيل، مرجع سابق، ص 327.

[3]- مناصرة يوسف، مرجع سابق، ص 41.

والنتيجة الإجرامية حيث تتحقق الأخيرة في الغالب خارج حدود الدولة التي وقع فيها الفعل الإجرامي([1])

كما أن هناك أماكن متعددة في دول مختلفة قد تتأثر بجريمة تكنولوجيا المعلومات الحديثة الواحدة في آن واحد، فمكان وقوعها ليس بالضرورة موجودا على إقليم الدولة أو في نطاق اختصاص جهازها القضائي عند ظهور التأثيرات المادية للجريمة([2])، مما ينجم عنه السهولة في حركة المعلومات عبر الأنظمة التقنية الحديثة التي تمكن من إرتكاب هذه الجريمة عن طريق نظام معلوماتي إلكتروني موجود في دولة معينة، بينما يتحقق الفعل الإجرامي في دولة أخرى،

وإن الطبيعة التي تتميز بها تكنولوجيا المعلومات الحديثة كونها عابرة للحدود خلقت الكثير من المشاكل حول تحديد الدولة صاحبة الإختصاص القضائي بهذه الجريمة، وكذا القانون الواجب تطبيقه، بالإضافة الى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وبالتالي فإن الوصول الى للحقيقة بشأنها يستوجب الإستعانة بخبرة فنية عالية المستوى([3]).

كما تشكل الإجراءات الرسمية المعقدة والتي تستغرق وقتا ليس بالقصير في حالات المساعدة القانونية أو القضائية بين الدول، والتي تتعارض مع طبيعة الجرائم المعلوماتية التي تتطلب سرعة في التحقيقات حيث أن جزءا كبيرا من الأدلة في الجرائم المعلوماتية كما سبق الأشارة غير ملموس ويزول بسرعة، وهو ما يتطلب أن تكون إجراءات التحقيق وجمع الأدلة بصورة سريعة وآنية([4]).

**ثامنا: إنها جرائم تمتاز بخطورة الأضرار الناجمة عنها**

تتسم جرائم نظام المعالجة الآلية للمعطيات بالخطورة البالغة نظرا لإرتكابها من بين فئات متعددة من المجتمع، ونظرا لحجم الخسائر والأضرار الناجمة عنها قياسا بالجرائم

[1]- ملياني عبدالوهاب، مرجع سابق، ص 56.

[2] -Myriam Quéméner, yves charpenal (cybercriminalité droit penal appliqué),2010, économica ,paris ,France , page 158.

[3]- ملياني عبدالوهاب، مرجع سابق ، ص 57.

[4]- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية-دراسة مقارنة، ماجستير في القانون وباحث دكتواره، دار الفكر والقانون، المنصورة، ط الأولى، سنة 2017، ص 21.

التقليدية، كونها أضرارا تمس بالكيانات المعنوية ذات القيم المعنوية أو القيم المادية أو كلاهما معا التي يصعب قياسها وإعطائها التقدير الصحيح([1])، ولهذه الجرائم خطورة كبيرة على كافة مجالات الحياة، وتبرز خصوصا في الجانب الإقتصادي والجانب الشخصي والجانب العسكري والأمني

ففي الجانب الإقتصادي لها عدة أخطار لوقوعها في معظم الأحيان على معلومات وبرامج ذات قيمة إقتصادية عالية، سواء في ذاتها إو لإرتباطها بأموال قيمة، مما يؤدي في الغالب الى خسائر مالية فادحة، إذ إن المجرم المعلوماتي وبمجرد حصوله على الوقت والوسيلة الكافيتين لتنفيذ جريمته فأنه قد لا يتردد في القضاء على أكبر المؤسسات الإقتصادية في العالم([2]) بأن يدمر كل البيانات السرية لتلك المؤسسات أو أن يفشي سر صناعتها بوضعه على شبكات المعلومات ليصبح في متناول كل من هب ودب([3]).

وفي هذا الجانب يؤكد علماء الإقتصاد أن الإستثمار في مجال نظم المعلومات والبرمجيات تعد إستثمار المستقبل إذ أن صناعة البرمجيات قد ساهمت بأكثر من ترليون دولار في حركة التجارة عام 1998، كما أن الإعتماد على أجهزة الإعلام الآلي في الأعمال يوفر الوقت من جهة ويقتصر المسافات، إلا أنه يضاعف خطر تعرض المعلومات المتعلقة بكل هذه المعاملات لإعتداءات خاصة وأن كل المؤسسات المالية الضخمة والبنوك والشركات تعتمد كليا على برامج وأنظمة متصلة بشبكات معلوماتية في تسيير معاملاتها.

وورد في تقرير للمركز الوطني للبيانات في الولايات المتحدة الامريكية في بحث نشر سنة 1999، أنجزه( برنالدوستاندير) أن الخسائر الناتجة عن الجرائم المعلوماتية بلغت 810000 دولار، وفي تقرير نشرته المجموعة الاقتصادية الأروبية أحصت الخسائر ب 5.64 مليون اورو.

[1]- مناصرة يوسف، مرجع سابق، ص43

[2]- ملياني عبدالوهاب، مرجع سابق، ص 74.

[3]- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، ط الأولى، سنة 2014، ص 156.

ونظرا لأهمية الجانب المعلوماتي في الجانب الاقتصادي لكل دولة والخسائر التي تلحقها جراء التعدي على أنظمتها وجب على كل دولة وضع خطة لإقرار حماية جزائية من هذه الجرائم التي أصبحت أضرارها جسيمة مقارنة بالأضرار التي تخلفها الجرائم التقليدية([1]).

أما على مستوى الجانب الشخصي فمن ضمن إضرارها الخطيرة المساس بأعز شيء يملكه الإنسان إلا وهو حرمة حياته الخاصة، لذلك سارعت العديد من الدول الى إصدار قوانين خاصة لحماية البيانات الشخصية، ومن الحالات الخطرة على مستوى الدول أيضا وقوع أضرار ماسة بالمصالح الكبرى للدولة أو المجتمع ناجمة مثلا من إستخدام فيروسات virus أو قنابل منطقية أو هجمات إنكار الخدمة تمس بالقطاعات والشركات الاستراتيجية للدولة قد ينجر عنها عواقب جد وخيمة على المستوى الأمني الاقتصادي([2]).

أما على مستوى الجانب العسكري والأمني فأن هذه الجرائم تعتبر كالشبح بالنسبة للدول وبالأخص الدول النامية التي لا تملك ما يكفي من التقنية لمواجهتها وإكتشافها، وأهم المخاطر نلخصها في ما يلي:

1-على صعيد المخاطر العسكرية، فأن الخطر الحقيقي لهذه الجرائم يتمثل في جرائم التجسس المعلوماتي، حيث أصبح بإمكان الكثير من الدول التي تملك التكنولوجيا أن تقوم بالتجسس على المواقع والمنشآت العسكرية (السرية وغير السرية) للدول الأخرى من خلال إقمار صناعية وأجهزة تقنية متطورة ومعدة خصيصا لذلك، وأضحى بإمكان هذه الدول الوصول الى معلومات ما كان ليصل إليها الجاسوس الإعتيادي إلا بطريقة متميزة.

2-على صعيد المخاطر الأمنية، فإن بعض من الجرائم المعلوماتية كالإرهاب الإلكتروني وجرائم غسيل الأموال عبر الأنترنت وغيرها من الجرائم المنظمة أصبحت تشكل تهديدا حقيقيا للأمن القومي للدول المعاصرة([3]).

---

[1]- جدي نسيمة، مرجع سابق، ص 42.

[2]- مناصرة يوسف، مرجع سابق، ص 43.

[3]- ملياني عبدالوهاب، مرجع سابق، ص 79.

**الفرع الثاني: تقنيات إرتكاب جرائم نظام المعالجة الآلية للمعطيات**

تتعدد التقنيات التي يستخدمها مجرموا نظام المعالجة الآلية للمعطيات في تنفيذ جرائمهم، ومن أهمها تقنيتي الإختراق والفيروس

**أولا: إرتكاب جرائم نظام المعالجة الآلية للمعطيات عن طريق الإختراق**

يتعرض نظام المعالجة الآلية للمعطيات إلى الإختراق من قبل أفراد غير مصرح لهم بالدخول إليه أو البقاء فيه، وقد ساهم في إنتشار هذه الظاهرة تطور الإتصالات وتنامي الشبكات المعلوماتية([1]).

والإختراق عرفته المادة الأولى من القانون النموذجي الموحد في شأن مكافحة جرائم إساءة إستعمال أنظمة تقنية المعلومات بأنه" الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق إنتهاك الإجراءات الأمنية([2])، أو هو بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف أو الوصول الى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة، وينقسم الإختراق الى ثلاثة أنواع:

1- إختراق الأجهزة الخادمة: ويتم عن طريق ما يسمى بالمحاكاة وهي القيام بإنتحال شخصية مسموح لها بالدخول الى هذه الأجهزة.

2- التعرض للبيانات أثناء إنتقالها: وتستخدم هذه الطريقة للتعرف على أرقام بطاقات الإئتمان أثناء إنتقالها من المشتري الى موقع التسوق.

3- إختراق الأجهزة الشخصية: وهي الطريقة الأكثر شيوعا نظرا لتوفر العديد من برامج الإختراق سهلة الإستخدام.

**ثانيا: إرتكاب جرائم نظام المعالجة الآلية للمعطيات عن طريق الفيروسات**

الفيروس هو عبارة عن برنامج يحتوي على مجموعة من الأوامر الخاصة بكيفية إنتشاره داخل الملفات، ويتم كتابة هذا البرنامج بإستخدام إحدى لغات البرمجة منخفضة

---

[1]- نهلا عبدالقادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط الأولى، سنة 2008، ص 156.

[2]- عبدالفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والأنترنت في القانون العربي النموذجي(دراسة متعمقة في القانون المعلوماتي)، دار الكتب القانونية، مصر، ب ط، سنة 2007، ص 325.

المستوى ويحدث آثار تخريبية، وللفيروسات عدة أنواع وأهمها فيروسات الثغرات وفيروسات الماكرو.

1-فيروسات الثغرات: أن ثغرات النظم التي تنشأ في مرحلة التصميم يمكن أن تؤدي بشكل مباشر إلى ثغرات خطيرة عند تشغيل النظام([1])، وبذلك يقوم هذا الفيروس بالإعتماد على هذه الثغرات الموجودة داخل نظم التشغيل كنظام window والتي تحتاج الى قدرة عالية من المبرمج على تحليل نظام التشغيل وإكتشاف الأخطاء الموجودة به ثم إستغلالها.

2-فيروسات الماكرو: وتصيب بشكل أساسي الملفات التي تعمل على مجموعة برامج offis والملفات الخاصة ببرنامج word microsoft فتجعل التعامل معها غير متاح ويسفر دائما عن ظهور رسائل الخطأ([2]).

**المطلب الثالث: قصور الحماية الفنية لنظام المعالجة الآلية للمعطيات**

أن قصور الحماية الفنية لنظام المعالجة الآلية للمعطيات جعلت المشرع الجنائي يتدخل ليوفر حماية جنائية خاصة لهذا النظام، وسنبرز ذلك من خلال عدم كفاية الحماية الفنية لنظام المعالجة الآلية للمعطيات والتطرق الى دور الحماية الجنائية في الوقاية من جرائم نظام المعالجة الآلية للمعطيات.

**الفرع الأول: عدم كفاية الحماية الفنية لنظام المعالجة الآلية للمعطيات**

تكفل بعض القواعد الأمنية الحماية للمعلومات ونظم معالجتها في مواجهة العديد من الأخطار والتهديدات المختلفة، في حين يتركها البعض الآخر بدون حماية، ومن تم يمكن تقسيم هذه النظم وفق هذه الزوية الى ثلاثة أنظمة:

-أنظمة مفتوحة للجمهور، وهذه لا إشكال يثار بصددها.

-أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية، وهنا يثار الإشكال بشأنها.

---

[1]- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض-السعودية، الطبعة الأولى، سنة 2000، ص 41.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص ص 40-53.

-أنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية.

وقد أدى هذا الوضع في الوسط القانوني الى طرح التساؤل التالي: هل الأنظمة المحمية بأجهزة أمان هي وحدها التي تحظى بحماية وتطبيق نصوص قانون العقوبات؟ أم أن كل الأنظمة تحظى بتلك الحماية؟([1])

تباينت آراء الفقهاء بخصوص هذه الحماية، بين من يرى بضرورة خضوع الأنظمة لحماية فنية كالفقه الفرنسي مثلا، الذي يعتبر أن وجود هذا الشرط لا يكون له سوى دور واحد وهو إثبات سوء نية من قام بإنتهاك النظام والدخول إليه بطريقة غير مشروعة، ويدخل ذلك في عبء إثبات القصد الجنائي، بينما يرى جانب آخر بوجوب خضوع كل الأنظمة للحماية الجزائية بغض النظر عن إحتوائها لنظام آمان، وهذا الرأي أخذت به محكمة الإستئناف بباريس في قرار لها صادر سنة 1994 أشارات في حيثياته أنه ليس من اللازم لقيام جريمة الدخول الغير شرعي أن يكون الفعل قد تم مخالفته لتدابير أمنية، بل يكفي لقيام الجريمة أن يتم ذلك ضد إرادة المسؤول عن النظام([2]).

وهذا الرأي الأخير هو الراجح، ونميل إليه لكون النصوص القانونية تؤيده، وكذلك تم رفض رأي الفقه الفرنسي في الأعمال التحضيرية لمشروع القانون الذي كان يرى من الضروري وضع تعريف لنظام المعالجة الآلية للمعطيات يشترط ضرورة وجود نظام آمان، فصدرت النصوص القانونية المتعلقة بجرائم نظم المعالجة الآلية للمعطيات دون أن تشترط خضوع هذه الإنظمة لأية حماية فنية، ذلك أن المشرع الجزائري والفرنسي وبعض التشريعات الأخرى لم تنص صراحة على وجوب حماية فنية لنظام المعالجة الآلية للمعطيات، ومن تم فإنها تكفل الحماية لكافة الأنظمة حتى ولو لم تكن خاضعة لنظام حماية.

لا سيما وأن هذه الجرائم ترتكب من مجرم ذكي له قدرة على التحكم في تقنيات الحاسوب وإستخدام أنظمته، ويواكب كل تطور يحدث في هذه الأنظمة، ويجد له الطريق

[1] - رشيدة بوكر، مرجع سابق، ص،165،164.

[2] - جدي نسيمة، مرجع سابق، ص 24.

لتجاوزه وخرقه، بحيث أنه كلما أستحدثت إنظمة جديدة فإنه يطور بالمقابل وسائل لإختراقها([1]).

كما أولى قانون العقوبات الجزائري أهمية بالغة لحماية أنظمة المعالجة الآلية للمعطيات، ورغم ذلك شكك البعض في جدوى هذه الحماية بل هناك من ذهب الى القول بإنها تؤدي الى نتائج عكسية كما هو الشأن في تجريم بيع المخدرات الذي قد يؤدي الى وجود شبكات كبيرة للإتجار بها، وأن الرد المناسب على هذا الإجرام هو من طبيعة فنية وذلك بإيجاد حماية فنية تمنع كل إعتداء على هذه الأنظمة فيؤدي ذلك الى تلافي هذه الظاهرة بالكامل، وتدخل المشرع الجنائي ليس بالضروري إذ يمكن الإستغناء عنه بوسائل إخرى، وعندما تفشل كل تلك الوسائل يمكن أن يتدخل قانون العقوبات.

لكن الواقع يكشف عدم صحة هذا الرأي، فالإجرام المعلوماتي سابق في وجوده على تدخل القانون الجنائي وليس العكس، والحماية الفنية لنظام المعالجة الآلية للمعطيات وأن كانت هامة في الحد من الجرائم الواقعة على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات إلا إنها غير كافية والتجربة كشفت أن مجرمي نظام المعالجة الآلية للمعطيات بصفة خاصة ومجرمي المعلوماتية بصفة عامة لهم قدرة فائقة على تجاوز أنظمة الأمان التي تزود بها الأنظمة المعلوماتية، مما جعل الحرب حامية الوطيس بين شركات تصنيع برامج الآمان والمجرمين المعلوماتين الذين يتمتعون بمعرفة واسعة بتلك الأنظمة وبخباياها ويطورون وسائل جرائمهم بما يخترق أنظمة الأمآن الموجودة بطرق مختلفة ولا يمكن حمايتها بطرق فنية على نحو مطلق، وقد كشف الواقع أن أكبر الأنظمة المعلوماتية وأكثرها توافرا على الحماية الفنية تم إختراقها تحديا للقائمين عليها وطرق الحماية التي إستعانوا به([2])، لذلك كان لازما أن تواكب التشريعات المقارنة هذا التطور الملحوظ من خلال إقرارها قواعد قانونية غير تقليدية تتعامل بشكل عصري متقدم مع الجرائم المعلوماتية المختلفة وفي مقدمتها جرائم نظام المعالجة الآلية للمعطيات([3]).

---

[1]- جدي نسيمة، مرجع سابق، ص 41.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 29،30.

[3]- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والأنترنت، مكتبة الوفاء القانونية، الأسكندرية-مصر، ط الأولى، سنة 2011، ص 156.

وعليه يمكن القول أن الحماية الفنية والتقنية لنظام المعالجة الآلية وأن كانت لازمة وهامة فإنها تظل قاصرة وغير كافية لمواجهة الإعتداءات التي يتعرض لها النظام مما أستدعى تدخل المشرع الجنائي لفرض حماية جنائية خاصة.

**الفرع الثاني: دور الحماية الجنائية في الوقاية من جرائم نظام المعالجة الآلية للمعطيات**

أن النظام القانوني من خلال تحديده للمصالح المشروعة المتعلقة بنظام المعالجة الآلية للمعطيات وقيامه بوضع نصوص جنائية تحميه يكون قد وفر حماية جنائية للنظام، وتتخذ هذه الحماية شكلين وقائي وعقابي

فمن الناحية الوقائية يكون لنصوص قانون العقوبات دور وقائي لمنع الجريمة قبل وقوعها، ذلك أن التطور المعلوماتي الكبير يجد صداه في نصوص قانون العقوبات، ولابدا أن يتم إقراره وحمايته بواسطة قاعدة قانونية جنائية نظرا للخسائر الكبيرة التي تهدد الأفراد جراء الجرائم التي تمس بالمعطيات المدرجة ضمن نظام المعالجة الآلية وكذا المخاطر الجمة التي تمس حياتهم الخاصة، لا سيما مع تفاقم الأخطار في المجتمع الدولي المعاصر الذي يتميز بالحرب الإقتصادية، مما يلزم الدولة معه أن تتدخل فتبسط الحماية الجنائية على مشروعاتها الوطنية ضد هذا النوع من الإجرام، ومن تم فإن الحماية الجنائية تقي المصالح المحمية من الكثير من الإعتداءات التي كانت ستحصل لولا هذه الحماية([1]).

وقام المشرع الجزائري بوضع بعض القواعد الوقائية في القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، والتي تسمح بالرصد المبكر للاعتداءات المحتملة بتحديد مصدرها والتعرف على مرتكبها، وكذا القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي يحوي مجموعة من الضمانات والقواعد الإجرائية التي تحمي البيانات الشخصية للشخص الطبيعي و تضمن عدم إنتهاك حرمة حياته الخاصة

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق ، ص 31.

أما من الناحية العقابية فقانون العقوبات يلعب دورا كبيرا من الناحية القانونية إذ تتميز إجراءات البحث عن الجرائم بسهولة نسبية بما يمكن أن يؤدي الى تطبيق القانون، فالعدالة الجنائية تتمتع بوسائل تحري وإستقصاء غير متوفرة في القضاء المدني على تلك الجرائم التي تردع كثيرا ممن تسول لهم أنفسهم القيام بها([1]).

ونص المشرع الجزائري على عقوبات خاصة لقمع الاعتداءات الواردة على أنظمة المعالجة الآلية للمعطيات بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004، المتضمن تعديل قانون العقوبات الصادر بموجب الأمر رقم 66-156 المؤرخ في 06 جوان 1966، المتضمن قانون العقوبات، بمقتضى المواد من 394 مكرر الى 394 مكرر 8 المعدل بالقانون 16-02 المؤرخ في 19 يونيو سنة 2016 ، مستحدثا فيه جملة من النصوص جرم من خلالها الإعتداءات الواردة على نظم المعالجة الآلية للمعطيات وحدد لكل فعل منها ما يقابله من الجزاء.

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 31،32.

# الباب الأول
# الحماية الموضوعية لنظام المعالجة الآلية للمعطيات

لقد تعاظمت المصالح المرتبطة بمعطيات النظام في وقتنا الحاضر، الى حد أصبح معه تدخل المشرع الجنائي أمر لا بدا منه لحمايتها، لتشمل حماية كل المعطيات مع تشديد الحماية على طوائف معينة منها تحظى بأهمية إستثنائية، وتطال مختلف صور المعالجة ومواضعها، وذلك بالنظر للخسائر الكبيرة التي باتت تهدد مصالح الأشخاص والدول من جراء هذه الجرائم.

الأمر الذي إدى بالمشرع الجزائري الى التدخل بوضع حماية جنائية موضوعية لهاته المعطيات من خلال عدة نصوص، بداية باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات المعدل بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 والقانون 16-02 المؤرخ في 19 يونيو سنة 2016، بمقتضى المواد من 394 مكرر الى 394 مكرر 8 جرم من خلالها الإعتداءات الواردة على نظام المعالجة الآلية للمعطيات وحدد لكل فعل منها ما يقابله من الجزاء.

وبالرغم من تداركه في هذا القانون(15-04) للفراغ القانوني في مجال الإجرام المعلوماتي، بتجريمه لكافة الإعتداءات التي تمس بنظم المعالجة الآلية للمعطيات من خلال هاته النصوص القانونية الخاصة، إلا أنه أغفل تجريم الإعتداءات الواردة على منتوجات الإعلام الآلي فلم يقم باستحداث نص خاص بالتزوير المعلوماتي ولم يتبنى الإتجاه الحديث الذي أخذت به التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث([1]).

وقام الى جانب ذلك بوضع إطار قانوني أكثر ملائمة وإنسجاما مع خصوصية الجريمة الإفتراضية بسنه القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، كونه يجمع بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية وبين

[1]- مزياني عبدالغني، مداخلة بعنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعلومات، محكمة المسيلة، مجلس قضاء المسيلة، وزارة العدل، ص 49.

القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة بتحديد مصدرها والتعرف على مرتكبها.

فضلا عن ذلك، فإن المخاطر التي تحيط بالمعطيات الشخصية قد تفاقمت في العصر الحديث، فأوجبت على المشرع الجزائري التدخل مرة إخرى، بإصداره القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي يحوي مجموعة من الإجراءات التي تهدف الى حماية المعطيات ذات الطابع الشخصي للشخص الطبيعي وتضمن عدم المساس بحياته الخاصة، وكذا إنشائه للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي التي تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون.

لذلك سنقوم بتخصيص فصلا كاملا لحماية المعطيات الشخصية التي أقر لها المشرع الجزائري لأول مرة حماية خاصة، بموجب القانون 18-07 المشار إليه سالفا، لا سيما وأنها ترتبط بخصوصيات الأشخاص وتمس بحرمة حياتهم الخاصة، إضافة الى إن الحماية التي تتمتع بها المعطيات الشخصية تكون من جانب معين وهو الجانب المتعلق بإجراءات المعالجة الآلية لهذه المعطيات في الأصل، على عكس جرائم نظام المعالجة الآلية التي تكفل حماية عامة لكل المعطيات ومن كافة جوانبها الموضوعية،

وبناء على ما سبق، فإننا سنقوم بتقسيم هذا الباب الى فصلين:

الفصل الأول نتناول فيه الحماية الجنائية للمعطيات الشخصية وقسمته الى مبحثين المبحث الأول خصصته لتحديد الإطار القانوني للحماية الجنائية للمعطيات الشخصية من خلال تحديد مفهومها وتحديد القواعد القانونية للحماية الجنائية لهذه المعطيات، والمبحث الثاني خصصته للجرائم المرتبطة بالمعطيات ذات الطابع الشخصي من خلال إبراز صور هذه الجرائم وآليات الحماية الجنائية للمعطيات ذات الطابع الشخصي.

اما الفصل الثاني نتطرق فيه الى أركان جرائم نظام المعالجة الآلية للمعطيات وقسمته الى مبحثين، في المبحث الأول تناولت فيه أركان جرائم المساس بنظام

المعالجة الآلية في حد ذاته، وفي المبحث الثاني تطرقت فيه الى إركان جرائم المساس بمعطيات نظام المعالجة الآلية.

# الفصل الأول

# الحماية الجنائية للمعطيات ذات الطابع الشخصي

## الفصل الأول: الحماية الجنائية للمعطيات ذات الطابع الشخصي

إن حماية الحق في الحياة الخاصة تعني إيجاد توازن بين حاجيات المجتمع لجمع وتخزين ومعالجة البيانات الشخصية وضمان حماية فعلية لهذه البيانات من مخاطر الإستخذام غير المشروع لتقنيات معالجتها، وبذلك إرتبط مفهوم الخصوصية في العديد من الكتابات والبحوث بمصطلح حماية البيانات ومعالجتها، مما جعلها تضبط في إطار حماية البيانات الخاصة([1])، لذا فإن البحث في حماية المعطيات الشخصية يكتسي أهمية خاصة لكونه مرتبط بالتطور التكنولوجي الهائل والثورة المعلوماتية التي لعبت دورا بارزا في تأثيراتها على الحق في الخصوصية، وما نتج عنها من تطورات جعلتها عرضة للكثير من الإنتهاكات والإعتداءات.

وقد أشارت الدراسة الصادرة عن مجلس الدولة الفرنسي حول الأنترنت والشبكات الرقمية في 2 يوليو 1998 الى الموضوعات الهامة والرئيسية الواجبة الحماية، وكان في مقدمتها ضرورة حماية المعلومات الشخصية والحياة الخاصة على الشبكات، والتي تعد إحدى المسائل الأكثر حساسية في نظر المستخدمين، فأدرجتها الدراسة في مقدمة توصياتها التي خلصت إليها، إذ أشارت الى أن حماية المعلومات الشخصية أصبحت مهددة إزاء مخاطر جديدة في بيئة الشبكات الرقمية([2]).

ومن تم فإن المعطيات الشخصية أصبحت ذات أهمية كبيرة على المستوى الدولي، وهذا ما كرسته المادة 12 من الإعلان العالمي لحقوق الإنسان([3])، الذي أنضم إليه الجزائر سنة 1989، وذلك إلى جانب الإتفاقية الدولية للحقوق المدنية والسياسية، وكذا المادة 17 من العهد الدولي المتعلق بالحقوق المدنية والسياسية التي نصت على أنه " لا يجوز تعريض أي شخص على نحو تعسفي أو غير

---

[1]- حسين نوارة، مداخلة بعنوان آليات تنظيم المشرع الجزائري لجريمة الإعتداء على الحق في الحياة الخاصة إلكترونيا، مركز جيل البحث العلمي، أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة 29 مارس 2017، ص 109.

[2]- بوكر رشيدة، مرجع سايق، ص 78.

[3]- نصت المادة الثانية عشر (12) من الإعلان العالمي لحقوق الإنسان على أنه" لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته.." مقتبس عن: طارق صديق رشيد كه ردى، حماية الحرية الشخصية في القانون الجنائي (دراسة تحليلية مقارنة)، منشورات الحلبي الحقوقية، بيروت، لبنان، ط الأولى، سنة 2011، ص 209.

قانوني لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته ولا لأي حملات غير قانونية تمس شرفه أو سمعته، وأنه من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس"، إضافة الى تبني الأمم المتحدة سنة 1989 دليلا يتعلق بإستخدام الحوسبة في عملية تدفق البيانات الشخصية، وبتاريخ 14 ديسمبر 1990 تبنت الهيئة العامة دليل تنظيم إستخدام المعالجة الآلية للبيانات الشخصية([1])، هذا الى جانب تقديم الإتحاد الأروبي لأدلة توجيهية حول حماية البيانات وأبرزها دليل عام 1995 بشأن حماية الأفراد فيما يتصل بمعالجة البيانات الشخصية وحرية نقلها، وكذا دليل 1997 المتعلق بحماية معطيات الإتصالات، كما أكد على مبدأ حماية المعطيات الشخصية عبر الأنترنت وحماية الحياة الخاصة بموجب التوجيه الحالي رقم 58 لسنة 2002 الصادر في 12 يوليو 2002 المتعلق بمعالجة المعطيات ذات الطابع الشخصي وحماية الحياة الخاصة في إطار الإتصالات الإلكترونية([2]).

ونتيجة لذلك أهتمت القوانين المقارنة بمعالجة مسألة حماية البيانات الشخصية في برامج المعلوماتية، ووضعت قيودا على الحكومات والأجهزة الإدارية للدولة والخاصة والأفراد عندما تفكر في إنشاء أنظمة معلوماتية تتضمن بيانات شخصية، وذلك لحماية حق الإنسان في عدم الإفصاح عن معطياته الشخصية أو السرية المتعلقة به، في مواجهة الحكومة وأجهزتها وكذا النظم المعلوماتية للقطاع الخاص([3])، وحرصت على توفير أكبر قدرا من الحماية الجنائية للمعطيات الشخصية في تشريعاتها الوطنية، ومن بينها دولة السويد التي تعتبر السباقة في تبني إطار حماية لهاته المعطيات من خلال قانون حماية المعطيات بتاريخ 11 ماي 1973، وإطار قانوني جديد سنة 1998.

---

[1]-حمادي كردلاس، مقال بعنوان حماية المعطييات الشخصية، مجلة قانونك، المغرب، ص 1، على الموقع www.ganonak.com

[2]- محمد علي سويلم، الحماية الجنائية للمعاملات الإلكترونية الجرائم المعلوماتية والإلكترونية، دار المطبوعات الجامعية، الأسكندرية، مصر، ط الأولى، 2018، ص 173.

[3]- عبدالفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموجي لمكافحة جرائم الكومبيوتر والأنترنت، دار الفكر الجامعي، الأسكندرية، مصر، ط الأولى، 2006، ص 86،87.

أما بالنسبة للولايات المتحدة الأمريكية فقد تبنت الكثير من القوانين، ومن بينها قانون الخصوصية الفيدرالي سنة 1974 وقانون حرية المعلومات 1970، وكذلك قانون المقاضاة للكومبيتر وحماية الخصوصية سنة 1980.

في حين وضع المشرع الفرنسي حماية خاصة للمعلومات الشخصية والإسمية بموجب القانون رقم 78-17 المؤرخ في 06 يناير 1978، الخاص بالمعالجة الإلكترونية للمعلومات الإسمية الذي إشتهر باسم قانون المعلوماتية والملفات والحريات، وعدل سنة 2004، بحيث إستهل نصوص قانونه بمبدأ أساسي، وهو إن المعالجة الإلكترونية للبيانات يجب أن لا تحمل تعديا على حصانة الفرد ولا على حقوق الإنسان ولا على حياته الخاصة أو حرياته الفردية والعامة([1]).

أما على مستوى التشريعات العربية سارع المشرع المغربي بوضع قانون يواكب التوجهات الدولية، حيث أصدر القانون رقم 08-09 المؤرخ في 18 فبراير 2009، المتعلق بحماية الأشخاص الذاتيين إتجاه معالجة المعطيات ذات الطابع الشخصي، والذي يهدف الى حماية الأفراد إزاء الإستعمال المفرط واللامسؤول من طرف المؤسسات الخاصة والعمومية لمعطياتهم الشخصية كرقم الهاتف أو رقم البطاقة الوطنية أو المعطيات الجينية...الخ.

والى جانب ذلك قام المشرع التونسي بوضع نظام حماية ملائم لقواعد التوجيه الأروبي بواسطة القانون رقم 63-2004، المتعلق بحماية المعطيات ذات الطابع الشخصي بتاريخ 27 يوليو 2004([2])، وتجسيد ذلك من خلال إصداره قانون أساسي عدد 42 لسنة 2017 مؤرخ في 30 ماي 2017، يتعلق بالموافقة على إنضمام الجمهورية التونسية إلى الإتفاقية رقم 108 لمجلس أروبا المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي وبروتوكولها الإضافي رقم 181 الخاص بسلطات المراقبة وأنسياب وتدفق المعطيات عبر الحدود([3]).

---

1- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط الأولى، 2009، ص 84.

2- حمادي كردلاس، مرجع سابق، ص 200.

3- قانون أساسي عدد 42 لسنة 2017 مؤرخ في 30 ماي 2017، يتعلق بالموافقة على إنضمام الجمهورية التونسية إلى الإتفاقية رقم 108...، الرائد للجمهورية التونسية، عدد45 المؤرخ في 6 جوان 2017، ص 1853.

كما أصدر المشرع القطري القانون رقم 13 لسنة 2016، بشأن حماية خصوصيات البيانات الشخصية([1]).

أما المشرع الجزائري فلم يشر الى المعطيات ذات الطابع الشخصي كحق يستوجب حماية خاصة في بداية الأمر، إلا أنه فيما بعد كرسه كمرحلة أولى في المادة 47 من التعديل الدستوري لسنة 2020([2])، والتي تنص على أن حماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، هي حق أساسي يضمنه القانون ويعاقب على إنتهاكه، وكمرحلة ثانية قام مؤخرا بسن القانون رقم 18-07 المؤرخ في 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، والمصادق عليه في مجلس الوزراء في 8 مارس 2018 وفي المجلس الشعبي الوطني بتاريخ 28 مارس 2018 ومجلس الأمة بتاريخ 13 ماي 2018([3])، والذي يهدف الى تحديد قواعد لحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، وذلك تبعا للأسباب التي وردت في مسودة مشروع هذا القانون، والمتمثلة في وضع إطار قانوني يحدد نظام معالجة المعطيات ذات الطابع الشخصي في بلادنا والتصدي للآثار المترتبة على التطور السريع لتكنولوجيات الإعلام على الحياة الخاصة وحريات الأشخاص، بتحديد المبادئ الواجب إحترامها إثناء جمع ومعالجة وحفظ البيانات الشخصية وقواعد إستعمال هذه البيانات، وكذا حقوق الأشخاص

[1]- قانون رقم 13 لسنة 2016، بشأن حماية خصوصية البيانات الشخصية، الجريدة الرسمية القطرية، المؤرخة في 2006/12/29، العدد 15.

[2]- المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 ديسمبر سنة 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في إستفتاء أول توفمبر سنة 2020، في ج ر ج ج، ع 82 المؤرخ في 30 ديسمبر 2020..

[3]- مريم لوكال، مقال بعنوان الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 18-07، مجلة العلوم القانونية والسياسية ، جامعة الوادي، المجلد 10، العدد 01، أفريل 2019، ص 1315.

الذين تم جمع بياناتهم، من خلال تبني القواعد العالمية المعمول بها في هذا المجال([1]).

إضافة إلى أن المعطيات الشخصية للجزائريين كانت وإلى وقت قريب في متناول شركات أجنبية ناشطة في الجزائر في مجالات حساسة جدا على غرار شركات الهاتف النقال والهاتف الأرضي ومزودي خدمات الأنترنت وغيرها، والتي لا يعرف طبيعة معالجتها لهذه المعطيات ولا الغرض من تلك المعالجة([2]).

ونظرا لخطورة ما يترتب على معالجة البيانات الشخصية من تهديد لخصوصيات الأفراد فقد تضمن القانون رقم 18-07 السالف الذكر، عدة مخالفات تشكل جرائم ماسة بتلك المعطيات التي ترتكب إما أثناء عملية جمعها أو أثناء معالجتها أو أثناء إستعمالها أو التصرف فيها، والى جانب ذلك قام بتوفير حماية جنائية لهذه المعطيات.

الأمر الذي يستوجب منا التوقف لدراسة هذه الحماية الجنائية التي أوجبها المشرع الجزائري لهذه المعطيات ومقارنتها بالتشريعات الأخرى، لا سيما وإنها تعتبر من المستجدات المستحدثة لدى المشرع الجزائري في هذا المجال، وذلك من خلال التطرق الى الإطار القانوني للحماية الجنائية للمعطيات ذات الطابع الشخصي ( المبحث الأول )، والجرائم المرتبطة بالمعطيات ذات الطابع الشخصي ( المبحث الثاني ).

---

[1]- مسودة مشروع قانون يتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، وزارة العدل الجزائرية، 2018.

[2]- العيداني محمد، يوسف زروق، مقال بعنوان حماية المعطيات الشخصية في الجزائر على ضوء القانون 18-07 (المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي)، مجلة معالم للدراسات القانونية والسياسية ، لبنان، العدد 5، ديسمبر 2018، ص 115.

## المبحث الأول: الإطار القانوني للحماية الجنائية للمعطيات ذات الطابع الشخصي

أن تحديد الإطار القانوني لحماية المعطيات ذات الطابع الشخصي يقتضي منا تحديد مفهوم المعطيات ذات الطابع الشخص (المطلب الأول) والتطرق الى القواعد القانونية لحماية هذه المعطيات (المطلب الثاني).

### المطلب الأول: مفهوم المعطيات ذات الطابع الشخصي

تختلف المعطيات أو البيانات الشخصية أو المعطيات ذات الطابع الشخصي عن المعطيات بصفة عامة، لذلك سنقوم بتعريف المعطيات ذات الطابع الشخصي (الفرع الأول) وتحديد المصادر التي تهدد خصوصية البيانات الشخصية (الفرع الثاني).

#### الفرع الأول: تعريف المعطيات ذات الطابع الشخصي

تطورت البيانات الشخصية مع تطور الأنترنت، فلم تعد تقتصر على الأسم واللقب والعنوان البريدي، بل أزدادت وتنوعت لتشمل صورة الشخص وصوته، إضافة الى طائفة أخرى من البيانات التي تتعلق بقدراته(المالية) سلوكياته، عادته، ميوله وأذواقه، والأشد من ذلك كلها البيانات التي تتعلق بجسم الإنسان البيانات البيومترية([1]).

وتضمن القانون الفرنسي رقم 801 لسنة 2004، الخاص بحماية البيانات الشخصية تعريف للبيانات الشخصية، وذلك في المادة الثانية منه، حيث عرفها بأنه" يعتبر بيانا شخصيا أي معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة سواء تم تحديد هويته بالرجوع الى رقمه الشخصي أو بالرجوع الى أي شيء يخصه"([2]).

---

[1]- عثمان بكر عثمان، المسؤولية عن الإعتداءات على البيانات الشخصية لمستخدمي شبكات التواصل الإجتماعي، كلية الحقوق، جامعة طنطا، مصر، بدون سنة، ص 8.

[2]-Art 2 :.. -Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.. , modifiè par Loi N° 2004-801 du 6 août 2004-ART.1, JORF 7 août 2004.

وبالتالي فوفقا لهذا التعريف الذي أخذ به المشرع الفرنسي يمكن الوصول لهوية شخص عن طريق بيانات شخصية مثل اللقب، تاريخ الميلاد، محل الإقامة، الصورة أو رقم الهاتف، أو لوحة بيانات أو أي رقم هوية، كما يمكن التوصل لهوية الشخص عن طريق الإميل إذا كان يظهر به الإسم أواللقب، أو من خلال الغير مثل مورد خدمة الوصول، إذا كان يسمح بالكشف عن هوية الشخص الذي يستتر وراء إسم مستعار، فيفصح عن ملفات الصوت، البصمات الوراثية أو الحركية أو أي بيان بيومتري آخر.

وحسنا ما فعله المشرع الفرنسي لما توسع في مفهوم البيان الشخصي ليشمل أي معلومة من الممكن أن تحدد هوية أي شخص بطريقة مباشرة أو غير مباشرة، بحيث إن التضييق في مفهوم البيانات الشخصية قد يسمح للعديد من الجهات بالتعدي عليها خاصة مع تقدم تقنيات جمع البيانات ومشاركتها، فالبيانات الموزعة بقواعد بيانات مختلفة قد لا يدل على هوية الشخص بحد ذاتها، لكن إذا تم ربطها قد تفصح عن هوية الشخص، علاوة على ذلك فأن هذا التعريف الواسع المرن يسمح بتطبيق هذا القانون على أية صورة حديثة للبيانات الشخصية يمكن ظهورها في المستقبل([1]).

كما أن المشرع الفرنسي تخلى عن مصطلح المعلومات الإسمية الذي أستعمله عند صدور قانون المعلوماتية سنة 1978، وذلك عندما تم نقل النصوص العقابية إلى قانون العقوبات في المواد من 226-16 إلى 226-30 ليتبنى مصطلح المعطيات الشخصية متأثرا بموقف الفقه الذي أعتبر أن المعطيات إسمية أو شخصية فهي تحمل نفس المفهوم، بحيث تشمل كل المعلومات المتعلقة بالفرد سواء كانت مرتبطة بحياته الخاصة أو المهنية أو توجهاته الفكرية والثقافية والسياسية([2]).

أما المشرع الكويتي فلم يضع تعريفا مباشرا للبيانات الشخصية في القانون رقم 20 لسنة 2004، الخاص بالمعاملات الإلكترونية، ولكن من الممكن القول أنه قد عرفها تعريفا غير مباشرا بأنها: "المعلومات التي تتعلق بالشخص" ويمكن إستنتاج

---

[1]- عثمان بكر عثمان، مرجع سابق، ص 9.

[2]- طباش عزالدين، مقال بعنوان الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري-دراسة في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، لبنان، العدد 2، سنة 2018، ص 50.

ذلك من المواد 32 و33 من هذا القانون، حيث نصت على عدم جواز أفشاء الجهات العامة والخاصة للمعلومات الموجودة عندها والمتعلقة بالشخص، ويجوز لهذا الشخص أن يطلع على هذه المعلومات، ومن تم يمكن القول أن تعريف البيانات الشخصية في القانون الكويتي هو تعريف واسع مشابه للتعريف الوارد لتلك البيانات في القانون الفرنسي([1]).

وعرف المشرع المغربي مصطلح معطيات ذات طابع شخصي في المادة الأولى من القانون 09-08 المؤرخ في 18 فبراير 2009، المتعلق بحماية الأشخاص الذاتيين إتجاه معالجة المعطيات ذات الطابع الشخصي([2]) بإنه" كل معلومة كيفما كان نوعها بغض النظر عن دعامتها بما في ذلك الصوت والصورة، والمتعلقة بشخص معروف أو قابل للتعرف عليه بصفة مباشرة أو غير مباشرة، ولا سيما من خلال الرجوع الى رقم تعريف أو عنصر أو عدة عناصر مميزة لهويته البدنية أو الفيزيولوجية أو الجنسية أو النفسية أو الإقتصادية أو الثقافية أو الإجتماعية([3]).

كما عرف المشرع التونسي المعطيات الشخصية في الفصل الرابع من قانون أساسي عدد 63 لسنة 2004، المؤرخ في 27 جويلية 2004،المتعلق بحماية المعطيات الشخصية، بأنها" تعتبر معطيات شخصية على معنى هذا القانون كل البيانات مهما كان مصدرها أو شكلها، والتي تجعل شخصا طبيعيا معرفا أو قابل للتعريف بطريقة مباشرة أو غير مباشرة، بإستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانونا. وأتم تعريفها في الفصل الخامس الذي ينص على أنه" يعد قابلا للتعريف الشخص الطبيعي الذي يمكن التعرف عليه بصورة مباشرة أو غير مباشرة من خلال المعطيات أو الرموز المتعلقة خاصة بهويته أو بخصائصه

[1]- سامح عبدالواحد التهامي، ضوابط معالجة البيانات الشخصية"دراسة مقارنة بين القانون الفرنسي والقانون الكويتي"، مجاة كلية القانون الكويتية العالمية، الكويت، بدون سنة ، ص 402.

[2]- قانون رقم 08-09 المؤرخ في 10 يونيو 2009، المتعلق بحماية الأشخاص الذاتيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية المغربية، المؤرخة في 2009/02/23، العدد 5711.

[3]- المادة 1 من القانون المغربي رقم 09-08.

الجسمية أو الفيزيولوجية أو الجينية أو النفسية أو الإجتماعية أو الإقتصادية أو الثقافية([1]).

بالإضافة إلى المشرع القطري الذي عرف البيانات الشخصية في المادة الأولى من القانون رقم 13 لسنة 2016، بشأن حماية خصوصية البيانات الشخصية بأنها" بيانات عن الفرد الذي تكون هويته محدودة أو يمكن تحديدها بصورة معقولة، سواء من خلال البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى([2]).

أما بالنسبة للمشرع الجزائري فقد عرف المعطيات ذات الطابع الشخصي في المادة الثالثة من القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعين في مجال المعطيات ذات الطابع الشخصي بأنها" كل معلومة بغض النظر عن دعامتها متعلقة بشخص معروف أو قابل للتعرف عليه والمشار إليه أدناه"الشخص المعني" بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع الى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الإقتصادية أو الثقافية أو الإجتماعية"، كما عرف في نفس المادة الشخص المعني بأنه" كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع المعالجة"([3])

ويلاحظ أن المشرع الجزائري توسع في مفهوم المعطيات ذات الطابع الشخصي لتشمل أي معلومة وبغض النظر عن دعامتها يمكن أن تحدد هوية أي شخص معروف أو يمكن التعرف عليه سواء بصفة مباشرة أو غير مباشرة، إضافة الى ذلك، فإن هذه المعطيات تقتصر على الأشخاص الطبيعين فقط دون الأشخاص المعنويين كما يتضح من تعريف الشخص المعني المشار إليه أعلاه.

كما أن المشرع الجزائري لم يحدد العناصر التي تدخل ضمن المعطيات الشخصية، والتي هي عديدة أهمها: الأسم واللقب، الصوت والصورة، الأحوال العرقية

---

1- قانون أساسي عدد 63 لسنة 2004، المؤرخ في 2004/07/27، المتعلق بحماية المعطيات الشخصية، الرائد الرسمي للجمهورية التونسية، الصادرة بتاريخ 2004/07/30، عدد 61، ص 2084.

2- المادة 1 من القانون القطري رقم 13 لسنة 2016.

3- المادة 3 من القانون رقم 18-07 المؤرخ في 10 يونيو 2018.

والجنسية والآراء السياسية والمعتقدات الدينية والحالة الصحية، الرقم الشخصي، العنوان الشخصي وعنوان البريد الإلكتروني، رقم الهاتف ورقم السيارة، الرقم الخاص بالجهاز مهما كان نوعه، الحالة الإجتماعية، الخصائص الجسمانية، تاريخ ميلاد الشخص، الوظيفة أو المهنة، أرقام البطاقات المغناطيسية، هوايات الشخص...الخ، ومن تم يمكن القول أن أي معلومة مهما كانت دعامتها مرتبطة بشخص معروف أو قابل للتعرف عليه بصفة مباشرة أو غير مباشرة هي عبارة عن معطيات ذات طابع شخصي خاضعة للحماية الجنائية في إطار هذا القانون.

وتجدر الإشارة الى أن هذه المعطيات ذات الطابع الشخصي يجب أن تخضع لإجراءات المعالجة، لذلك تطرق المشرع الفرنسي الى تعريف معالجة البيانات الشخصية في المادة 2/3 من قانون رقم 801 لسنة 2004، المتعلق بحماية البيانات الشخصية، بأنها " أي إجراء يتعلق بالبيانات الشخصية أيا كانت الطريقة المستخدمة في هذا الإجراء، وخاصة التجميع، التسجيل، التنظيم، الحفظ، التعديل، الإستخلاص، الإطلاع، الإستخدام، الإبلاغ عن طريق النقل، النشر، الربط، المنع، المحو والتدمير"([1])

وهذا التعريف لفكرة المعالجة يعتبر تعريفا واسعا جدا، يؤدي الى القول بأنه لا يمكن تخيل أي أجراء يتعلق بالبيانات الشخصية لا يكون ضمن معالجة هذه البيانات.

أما المشرع الجزائري فقد عرف إجراءات المعالجة في المادة 3 من القانون 18-07 المذكور آنفا، بأنها" المشار إليها أدناه "معالجة" كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل الجمع والتسجيل والتنظيم أو الخطط أو الملائمة أو التغيير أو الإستخراج أو الإطلاع أو الإستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو

[1] - **Art 3/2 : II. - Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires**, modifiè par Loi N° 2004-801 du 6 août 2004-ART.1, JORF 7 août 2004.

الإتلاف"، كما عرف المعالجة الآلية في نفس المادة بأنها" العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو إستخراجها أو نشرها"([1]).

كما يلاحظ من خلال هذين التعريفين أن الإجراءات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي لا يمكن حصرها، وتم الإشارة الى أشهرها، لذلك قام المشرع الجزائري بترك الباب مفتوحا لإضافة إجراءات أخرى كما يتضح ذلك من قوله " أو بأي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني([2]) وكذا الإغلاق أو التشفير أو المسح أو الإتلاف".

**الفرع الثاني: المصادر التي تهدد خصوصية المعطيات ذات الطابع الشخصي**

إستتبع التحول إلى الرقمنة، إنتاج كميات هائلة من البيانات الشخصية للأفراد، مما أدى إلى تعاظم المخاطر التي تترتب عن إدارتها واستغلالها([3])، وتعددت بذلك المصادر التي تهدد خصوصية المعطيات ذات الطابع الشخصي، ولعل أهمها هي شبكة الأنترنت، نظم المعالجة الآلية وبنوك المعلومات.

**أولا: شبكات الإتصال كمصدر من مصادر تهديد خصوصية المعطيات ذات الطابع الشخصي**

تعتبر شبكة الأنترنت أهم شبكات الإتصال التي تشكل تطبيقا جديدا في مجال البيانات الشخصية، بحيث قد تكون هذه البيانات محل معالجة آلية عبر الأنترنت إما بالجمع أو الحفظ أو التسجيل أو النشر أو التحليل أو النقل، وكل معالجة آلية للبيانات([4])، وأن إستخدام هذه الشبكة يجعل حياة الفرد ككتاب مفتوح يمكن من خلالها متابعة ومراقبة المواقع التي يزورها الشخص على هذه الشبكة.

---

[1]- المادة 3 من القانون رقم 18-07.

[2]- عرف المشرع الجزائري الربط البيني للمعطيات في المادة الثالثة من القانون 18-07، السالف الذكر، بأنه" أي شكل من أشكال المعالجة التي تتمثل في إقامة ترابط بين معطيات معالجة لغاية محدودة مع معطيات أخرى يمسكها مسؤول أو مسؤولون آخرون عن المعالجة أو يمسكها نفس المسؤول لنفس الغرض أو لأغراض أحرى".

[3]- غزال نسرين، مرجع سابق، ص 121.

[4]- طارق عثمان، الحماية الجنائية للحياة الخاصة -دراسة مقارنة-، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة، 2007/2006، ص 94 .

والبيانات الشخصية قد تجمع من الشخص نفسه عبر شبكة الأنترنت، بتصفحه لبعض المواقع الإلكترونية التي تطلب بيانات من المستخدم قبل إستخدام الموقع، فمواقع العلاقات الإجتماعية ومواقع البريد الإلكتروني ومواقع التسوق وغيرها تطلب من المستخدم على سبيل المثال ذكر إسمه ولقبه والسن والمستوى التعليمي وعنوانه وحالته الإجتماعية وغيرها، وكذلك رقم بطاقته الإئتمانية كما في حالة التسوق، وقد تجمع هذه البيانات أيضا بشكل تلقائي عند تصفح الأنترنت مثل عنوان الكومبيتر(IP) الخاص بالمستخدم، لأن كل كومبيتر متصل بشبكة الأنترنت يتم منحه عنوانا من 32 رقما، وكذلك المعلومات الخاصة بالمتصفح المستخدم ووقت وتاريخ زيارة المواقع وغيرها، وسواء أكانت تلك المعلومات أو البيانات مأخوذة من قبل المستخدم أو بشكل تلقائي عند دخوله على المواقع المختلفة، فإن الإحتفاظ بها داخل السيرفرات الخاصة بالمواقع يمثل تهديدا لخصوصية الأفراد في العالم الإفتراضي([1]).

كما أن شيوع النقل الرقمي للبيانات خلق مشكلة أمنية وطنية، إذ سهل إستراق السمع أو التجسس الإلكتروني، ففي مجال نقل البيانات تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الإتصال على توفير الآمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات، وإمكانية إستخدام الشبكات في الحصول بصورة غير مشروعة عن بعد عن المعلومات([2]).

وقد أكدت اللجنة الوطنية للمعلوماتية والحريات المنبثقة عن القانون الفرنسي رقم 17-78، الصادر في 06 جانفي 1978، المتعلق بالمعلوماتية والملفات والحريات- المعروف لدى الفقه الفرنسي بقانون المعلومات والحريات-، على أن القواعد الواردة في قانون المعلوماتية والحريات تنطبق على الأنترنت، مما يسمح بإعداد مجموعة من القواعد الخاصة بمعالجة البيانات الشخصية عبر الأنترنت، كالبيانات التي يتعين على المتصفح لمواقع الأنترنت إستكمالها للإنتقال من مكان لآخر على الموقع من خلال الإستبيان الإختياري أو الإجباري، وكذلك الحال بالنسبة لملفات الكوكيز،

---

[1]- - عثمان بكر عثمان، مرجع سابق، ص 13،14.

[2]- بولين أنطونيوس، الحماية القانونية للحياة الخاصة في مجال المعلوماتية -دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى، 2009، ص 114.

وإعتبارا من سنة 1998 أكدت لجنة المعلوماتية والحريات على ضرورة إخطار اللجنة عن الرغبة في إستخدام نظام الكوكيز([1])، وإخطار المستخدمين بوجود ملفات الكوكيز على أجهزتهم، مما يسمح لهم بالإعتراض على ذلك.

كما أن من بين التوصيات التي خلصت إليها اللجنة الوطنية للمعلوماتية والحريات، والتي تعد كإلتزامات تقع على مقدمي الخدمات(مزودي خدمات الأنترنت، مسؤولي المواقع، متعهدي الإيواء) بشأن معالجة البيانات الشخصية:

1-على مقدمي الخدمات إعلام كل مستخدم للأنترنت بالمخاطر التي تهدد حياته الخاصة من خلال وضع بياناته الشخصية، وعلى حقه في الإعتراض على نشر بياناته الشخصية، وفي الإطلاع عليها في أي وقت، وكذلك حقه في تصحيحها أو محوها وفقا لأسباب مشروعة.

2-السماح لمستخدمي الأنترنت بالولوج الى خدماتها من دون الكشف عن بياناتهم الشخصية إلا في الحالات التي يكون فيها من الضروري الكشف عن شخصية المستخدم وبياناته لتقديم الخدمة المطلوبة([2]).

**ثانيا: نظام المعالجة الآلية كمصدر من مصادر تهديد خصوصية المعطيات ذات الطابع الشخصي**

أن بدأ مشكلات الكومبيتر في الستينيات ترافق مع مخاطر جمع وتخزين وتبادل ونقل البيانات الشخصية ومخاطر تكنولوجيا المعلومات في ميدان المساس بالخصوصية والحريات العامة، فأنتشر الحديث عن الخطر الكبير الذي يتهدد الحرية الشخصية القدرة المتقدمة لنظم المعالجة الإلكترونية على الوصول الى المعلومات المتعلقة بالأفراد وإستغلالها في غير الأغراض التي تجمع من أجلها، وخلال الثمانينات تغير الواقع التكنولوجي فيما يتعلق بالجهات التي تملك وتسيطر على نظم الكومبيتر، وكان ذلك سبب إطلاق الكومبيترات الشخصية وإنتشارها، وأصبح من الواضح أن حماية الخصوصية يتعين أن تمتد الى الكومبيترات الخاصة، وأن يتم

[1]- الكوكيز عبارة عن ملفات صغيرة تعرف بملفات تعريف الإرتباط على الأنترنت، ويتم تخزينها على القرص الصلب بواسطة متصفحك تحتوي على معلومات حول زيارتك لموقع ويب معين، مثل حالة تسجيل الدخول والتخصيص وتفضيلات الإعلانات، أنظر: موقع https: akhbarak.net.news

[2]-طارق عثمان، مرجع سابق، ص 95 .

ذلك في إطار إحداث توازن ما بين الحق في الخصوصية والحق في الوصول الى المعلومات.

هذا التغيير في الواقع التكنولوجي عكس نفسه على فصل الحماية القانونية في الخصوصية بأبعادها التنظيمية والمدنة والجزائية، وبدأت تكثر الأحاديث بشأن دعاوى الإستخدام غير المشروع للبيانات وللوثائق الشخصية، وظهرت أحداث شهيرة في حقل الإعتداءات على البيانات الشخصية والخاصة([1]).

والواقع أن هناك عدة مخاطر تهدد الحياة الخاصة للفرد أثناء قيام نظام المعلومات بجمع البيانات الإسمية، خاصة في الدول التي لم تنظم بعد عمل نظم المعلومات، بالرغم من الميزة التي تحسب للكومبيوتر في القدرة الفائقة على تجميع أكبر قدر من البيانات الإسمية، ومن مصادر مختلفة في سرعة زمنية لم يسبقه أحد إليها، إلا أن هذه القدرة الفائقة في جمع المعلومات قد أتاحت الفرصة لزيادة المخاطر على الحياة الخاصة للإنسان، ولا سيما إذا تم جمع هذه البيانات بطريق غير مشروع([2])، لذلك وجب حماية الأفراد من مظاهر الإعتداء المادي على حياتهم وممتلكاتهم وحماية القيم والعناصر المعنوية الخاصة بهم([3]).

وأن هذه المخاطر دفعت نحو وجوب توفير حماية تشريعية وسن قوانين في هذا الحقل، إذ أنه وقبل إختراع الكومبيتر فإن حماية هؤلاء الأشخاص كانت تتم بواسطة النصوص الجنائية التقليدية، ولا تغطي الى جانبا من الحقوق الشخصية وبعيدة عن حمايته من مخاطر جمع وتخزين والوصول الى المعلومات في بيئة الوسائل التقنية الجديدة([4]).

وبالتالي فأن الأمر الذي لا يسعنا إلا أن نؤكده هو أن هناك خطر لم يكن موجود من قبل، قد أصبح يتهدد الحياة الخاصة للأفراد نتيجة إستعمال نظام معالجة المعلومات آليا في حفظ المعلومات الشخصية المتعلقة بالإنسان، ولا يشترط أن يكون هذا الخطر متصلا بالمبدأ، وهو تسجيل هذه المعلومات في حد ذاته، بل يكفي أن

---

[1]- بولين أنطونيوس، مرجع سابق، ص 291،292.

[2]- المرجع نفسه، ص 113.

[3]- غزال نسرين ، مرجع سابق، ص 120.

[4]- بولين أنطونيوس ، مرجع سابق، ص 292.

يتعلق بطريقة أو أسلوب هذا التسجيل إذا كان من شأن هذه الوسيلة إنتهاك السرية التي يجب أن تحاط بها هذه المعلومات، ومن تم إنتهاك حرمة الحياة الخاصة للأفراد([1]).

**ثالثا: بنوك المعلومات كمصدر من مصادر تهديد خصوصية المعطيات ذات الطابع الشخصي**

أن جمع المعلومات في مركز واحد قد يكون بلا شك مصدر ضرر أكيد للأفراد، ومن المستحسن عدم الإقدام على مثل هذه الخطورة لتساعد برفع الأضرار الحاصلة قدر الإمكان عن كاهل المواطنين المعرضين قسرا لجمع المعلومات عنهم في الكومبيتر([2])، ويتم ذلك في إطار ما يعرف ببنوك المعلومات، والتي هي عبارة عن جهات تقوم بتجميع المعلومات المتصلة بموضوع معين قصد معالجتها آليا تمهيدا لإستغلالها، الأمر الذي أدى بأصوات حماية حق الخصوصية تتعالى لحماية حقوق الإنسان من أخطار التطور التكنولوجي المتسارع، ولعل أبرزها تلك الإعتداءات التي تتم بواسطة الحاسب الآلي على الحياة الخاصة.

وإذا كان الحاسب الآلي يحتوي على كم هائل من المعلومات المخزنة فأن مكمن الخطورة لدى هذا الحاسب تتمثل في أوجه الخطورة التي قد تنجم من الإستخدام الخاطئ أو غير المشروع لهذه المعلومات، وبذلك فأن خصوصية المعلومات هي المحور الذي ترتكز عليه حماية الحياة الخاصة في مواجهة الحاسب الآلي، وهذ ما دفع الأستاذ (frosini) الى القول بأن "الخصوصية وعلاقتها بالحاسب الآلي تعني أنه لا وجود اليوم لحرية رفض إعطاء المعلومات ذات المصلحة العامة والمتصلة بالبيانات الشخصية، ولكن بدلا من ذلك فأن الحرية أستقرت في القدرة على السيطرة على المعلومات الشخصية التي أدخلت في برنامج الحاسب الآلي، وترتيبا على ذلك يجب التأكيد على وجوب سلامة أمن الوصول الى بنوك المعلومات

---

[1]- عفيفي كامل، حماية أنظمة المعلومات ، دار الحامد للنشر والتوزيع، الأردن عمان، ط الأولى، سنة 2007، ص 255 .

[2]- بولين أنطونيوس ، مرجع سابق، ص 112.

وسلامتها وسريتها ومراقبة حق السماح بنشرها،فكل هذه الحقوق تشكل اليوم ما يسمى بالخصوصية في المفهوم الحديث"([1]).

وأن المعلومات الشخصية التي كانت فيما قبل منعزلة ومتفرقة، والوصول إليها صعب متعذر، تصبح في بنوك المعلومات مجمعة متوافرة متكاملة سهلة المنال، متاح أكثر من ذي قبل إستخدامها في أغراض الرقابة على الأفراد وهكذا تبدو صائبة مقولة ارثر ميلر" أن الحاسب الآلي بشراهته التي لا تشبع للمعلومات، والسمعة التي ذاعت حول عدم وقوعه في الخطأ وذاكرته التي لا يمكن لما تختزن فيها أن ينمحى أو ينسى، قد تصبح المركز العصبي لنظام رقابي يحول المجتمع الى عالم شفاف ترقد فيه عارية بيوتنا ومعاملاتنا المالية وإجتماعتنا وحالتنا العقلية والجسمانية لأي مشاهد عابر"

كما أنه من أخطر معالم خطر بنوك المعلومات على الحياة الخاصة بصفة عامة وعلى المعطيات الشخصية بصفة خاصة ما يمكن أن تحويه من بيانات غير دقيقة أو معلومات غير كاملة لم يجرى تعديلها بما يكفل إكمالها وتصويبها([2]).

**المطلب الثاني: القواعد القانونية للحماية الجنائية للمعطيات ذات الطابع الشخصي**

لقد منح القانون 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال الحماية الجنائية للمعطيات ذات الطابع الشخصي، بعض الضمانات في مواجهة الإعتداءات التي تمس بالمعطيات ذات الطابع الشخصي، بحيث أقر مجموعة من الحقوق( الفرع الأول) وفي مقابل ذلك ألزم المسؤولين عن المعالجة ببعض الإلتزامات( الفرع الثاني).

**الفرع الأول: حقوق الشخص المعني بالمعطيات المزمع معالجتها**

أن المشرع الجزائري عرف الشخص المعني في المادة الثانية من القانون 18-07، السالف الذكر، بأنه" كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع المعالجة"، وقام بوضع ضوابط معينة يجب إحترامها ومراعاتها عند القيام بمعالجة المعطيات ذات الطابع الشخصي، يهدف من خلالها

---

[1]- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع، عمان الأردن، ط الأولى، 2009، ص 70،71 .

[2]- بولين أنطونيوس ، مرجع سابق، ص 114،115.

الى حماية الشخص المعني بالمعطيات المزمع معالجتها، ولم يكتف بذلك، بل منح لكل شخص تتم معالجة معطياته مجموعة من الحقوق، وهي الحق في الإطلاع على البيانات، الحق في التصحيح، الحق في الإعتراض، الحق في نقل المعطيات نحو دولة أجنبية.

**أولا: الحق في الإعلام كحق من حقوق الشخص المعني بالمعطيات المزمع معالجتها**

أعطى المشرع الفرنسي لمن يتم معالجة بياناته الحق في الإطلاع على هذه البيانات حتى يتعرف على ما يحدث من إجراءات معالجة لها، ويعتبر الحق في الإطلاع على البيانات هو الإمتداد الطبيعي للإلتزام بالإعلام الذي يقع على عاتق القائم بمعالجة البيانات، حيث يسمح هذا الحق لمن تخصه هذه البيانات أن يراقب مدى إحترام قواعد معالجة البيانات التي نص عليها القانون من قبل معالج البيانات.

ويعهد هذا الحق تكملة للمنظومة التي وضعها المشرع الفرنسي في تأسيس مبدأ الشفافية الذي يسمح بالتعرف على كل ما يحدث للبيانات الشخصية من إجراءات المعالجة([1])، بحيث يحق له طلب نسخة من المسؤول عن معالجتها والحصول على جواب حول ما إذا كانت بياناته داخلة في عملية المعالجة وأهداف هذه العملية، وفئات البيانات المعالجة والجهات التي تسلم إليها أو تنقل إليها، لا سيما في حال إنتقال هذه البيانات الى دولة أخرى أو الى شركات في هذه الدول.

كما يتخذ الرد على هذا الطلب الشكل الخطي، وتقر بعض القوانيين كالقانون الفرنسي مثلا حق صاحب البيانات في الإطلاع على ما تجمعه الإدارات الرسمية عنه كأجهزة الأمن أو الدفاع أو غيرها، وذلك عبر طلب يتقدم به الى الهيئة الوطنية لحماية البيانات التي تقوم بالرد على صاحب هذه البيانات([2]).

---

1- سامح عبدالواحد التهامي، مرجع سابق، ص 430.

2- منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت لبنان، ط الأولى، 2018، ص 150 .

فوفقا للمادة (1-9/1) من قانون حماية البيانات الشخصية الفرنسي فإن كل شخص طبيعي له الحق في أن يوجه تساؤلات للقائم بمعالجة البيانات بهدف الحصول على المعلومات الآتية:

1- التأكيد على ما إذا كانت هناك بيانات شخصية خاصة به تخضع للمعالجة من عدمها.

2- الغاية من المعالجة التي تتم لبياناته الشخصية وأنواع البيانات التي تتم معالجتها.

3- ما إذا كان يتم نقل البيانات الشخصية الخاصة به لدولة ليست عضوا في الإتحاد الأروبي ومن هي هذه الدولة.

4- ما إذا كان يتم عمل إتصال بين بياناته لدى معالج البيانات، وبيانات خاصة به لدى معالج بيانات آخر، وما هو مصدر تلك البيانات الأخرى.

5- المعلومات التي تتعلق بدوافع المعالجة الأوتوماتكية للبيانات أن وجدت.

ومن تم فإن الحق في الإطلاع على البيانات هو إمتداد لإلتزام معالج البيانات بإعلام من تتم معالجة بياناته، وقد أكدت اللجنة القومية للحريات على أهمية الحق في الإطلاع، وكان ذلك بالنسبة لطلاب المدارس بمناسبة إنشاء نظام المعالجة البيومترية لتنظيم الدخول لمطعم المدرسة، حيث ذكرت أن لكل طالب له الحق في الإطلاع على بياناته التي تتم معالجتها، وأنه يجب أن يتم إعلام كل طالب بوجود هذا الحق، وذلك في الإستمارة الخاصة بالإشتراك في هذا النظام([1]).

كما ينحصر الحق في الوصول الى البيانات الشخصية في حق الشخص المعني بالوصول الى معلوماته، ولا يشمل حق الإطلاع على بيانات أشخاص آخرين ولا أي تعليقات أو تحليلات قانونية لها([2]).

ولكن إذا كانت المعلومات تتصل بقضية الأمن القومي للبلد فمن البديهي حجب هذا الحق، وضمانة لعدم إستخدام هذه المعلومات بطريقة سيئة فرضت بعض الدول

---

[1]- سامح عبدالواحد التهامي، مرجع سابق، ص 430،431.

[2] - منى الأشقر جبور، محمود جبور، مرجع سابق، ص 150.

وجود هيئة رقابة لحماية المعلومات كما هي عليه الحال في قانون حماية المعلومات الأنجليزي الصادر عام 1984([1]).

أما على مستوى التشريعات العربية، فأكد المشرع الكويتي على تقرير الحق في الإطلاع لمن تتم معالجة بياناته الشخصية، وذلك في نص المادة 33 من قانون المعاملات الإلكترونية، حيث نصت هذه المادة على أنه" يجوز للشخص أن يطلب من الجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية إطلاعه على البيانات الشخصية المسجلة لديها والمتعلقة به أو بأحد الأفراد الذين ينوب عنهم قانونا، وبذلك يكون القانون الكويتي قد أقر صراحة حق الشخص في الإطلاع على بياناته الشخصية لدى أي جهة حكومية أو غير حكومية-ما عدا الجهات الأمنية- والحصول على مستخرج رسمي لها، متوافقا بذلك مع القانون الفرنسي([2])، كما أكد المشرع التونسي على هذا الحق في الفصل 32 ضمن الفرع الثاني بعنوان حق النفاذ، من قانون أساسي عدد 63 لسنة 2004، السالف الذكر، والذي نص فيه على أنه" يقصد بحق النفاذ، على معنى هذا القانون، حق المعني بالأمر أو ورثته أو وليه في الإطلاع على جميع المعطيات الشخصية الخاصة به وطلب إصلاحها أو إتمامها أو تعديلها أو تحيينها أو تغييرها أو توضيحها أو التشطيب عليها إذا كانت غير صحيحة أو غامضة أو كانت معالجتها ممنوعة

كما يشمل حق النفاذ الحق في الحصول على نسخة من المعطيات بلغة واضحة ومطابقة لمضمون التسجيلات وبطريقة مبسطة إذا تمت معالجتها آليا"([3]).

وكذلك المشرع المغربي نص على حق الإعلام بمصطلح الحق في الإخبار أثناء تجميع المعطيات، في المادة الخامسة (5) النقطة الأولى من القانون 08-09، السالف الذكر، بأنه" يجب على المسؤول عن المعالجة أو من يمثله أخبار كل شخص تم الإتصال به مباشرة قصد تجميع معطياته الشخصية إخبارا مسبقا وصريحا ولا يحتمل اللبس بالعناصر التالية، ما عدا إذا كان على علم مسبق بها:

---

[1]- نعيم مغبغب، مخاطر المعلوماتية والأنترنت، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الثانية، 2008، ص 203 .

[2]- سامح عبدالواحد التهامي، مرجع سابق، ص431.

[3]- الفصل 32 من القانون الأساسي التونسي عدد 63 لسنة 2004 .

أ- هوية المسؤول عن المعالجة وعند الإقتضاء هوية ممثله.

ب- غايات المعالجة المعدة لها المعطيات.

ج- كل المعلومات الإضافية ....

د- خاصيات وصل التصريح لدى اللجنة الوطنية أو خاصيات الإذن المسلم من لدى اللجنة المذكورة([1]).

أما المشرع الجزائري فقد نص على حق الإعلام في المادة 32 من الفصل الأول ضمن الباب الرابع( حقوق الشخص المعني) من القانون 18-07، السالف الذكر، والتي تنص على أنه" ما لم يكن على علم مسبق بها، يجب على المسؤول عن المعالجة أو من يمثله إعلام مسبقا وبصفة صريحة ودون لبس، كل شخص يتم الإتصال به قصد تجميع معطياته ذات الطابع الشخصي بالعناصر الآتية:

- هوية المسؤول عن المعالجة وعند الإقتضاء هوية ممثله.
- أغراض المعالجة.
- كل معلومة إضافية مفيدة لا سيما المرسل إليه ومدى إلزامية الرد والآثار المترتبة عن ذلك، وحقوقه ونقل المعطيات الى بلد أجنبي.

إذا لم يتم جمع المعطيات ذات الطابع الشخصي لدى الشخص المعني، يجب على المسؤول عن المعالجة أو من يمثله، قبل تسجيل المعطيات أو إرسالها للغير، أن يزوده بالمعلومات المشار إليها أعلاه، ما لم يكن قد علم بها مسبقا.

في حالة جمع المعلومات في شبكة مفتوحة يجب إعلام الشخص المعني، ما لم يكن على علم مسبق، بأن المعطيات ذات الطابع الشخصي المتعلقة به يمكن أن تتداول في الشبكات دون ضمانات السلامة وأنها قد تتعرض للقراءة والإستعمال غير المرخص من طرف الغير.

[1]- المادة 5 من القانون المغربي رقم 08-09 .

وأورد المشرع الجزائري إستثناء على حق الشخص المعني في الإعلام في المادة 33 من نفس القانون، والتي تنص على أنه" لا تطبق إلزامية الإعلام المنصوص عليها في المادة 32 من هذا القانون:

**أ-** إذا تعذر إعلام الشخص المعني، ولا سيما في حالة معالجة المعطيات ذات الطابع الشخصي لأغراض إحصائية أو تاريخية أو علمية، يلزم المسؤول عن المعالجة في هذه الحالة بإشعار السلطة الوطنية باستحالة إعلام الشخص المعني وتقديم لها سبب الإستحالة.

ب- إذا تمت المعالجة تطبيقا لنص قانوني.

ج- إذا تمت المعالجة حصريا لأغراض صحفية أو فنية أو أدبية([1]).

**ثانيا: الحق في الولوج كحق من حقوق الشخص المعني بالمعطيات المزمع معالجتها**

نص المشرع المغربي على الحق في الولوج في المادة 7 من القانون 08-09، السالف الذكر، والتي تنص على أنه" يحق للشخص المعني بعد الإدلاء بما يثبت هويته أن يحصل من المسؤول عن المعالجة في فترات معقولة وعلى الفور ودون عوض على ما يأتي:

أ- تأكيد على أن المعطيات ذات الطابع الشخصي المتعلقة به تعالج أو لا تعالج، وكذا على معلومات مرتبطة على الأقل بغايات المعالجة وفئات المعطيات التي تنصب عليها والمرسل إليهم، أو فئات المرسل إليهم الذين أوصلت إليهم المعطيات ذات الطابع الشخصي.

ب- إحاطة وفق شكل مفهوم، بالمعطيات التي تخضع للمعالجة وكذا بكل معلومة متاحة حول مصدر المعطيات...

ج- معرفة المنطلق الذي يحكم كل معالجة آلية للمعطيات ذات الطابع الشخصي المتعلقة به"([2]).

---

[1]- المادتين 32 و33 من القانون رقم 18-07.

[2]- المادة 7 من القانون رقم 08-09.

وكذلك نص المشرع الجزائري على الحق في الولوج في المادة 34 من القانون 18-07، السالف الذكر، والتي تنص على أنه" يحق للشخص المعني أن يحصل من المسؤول عن المعالجة على:

- التأكيد على أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لا، وإعتراض المعالجة وفئات المعطيات التي تنصب عليها والمرسل إليهم.
- إفادته وفق شكل مفهوم، بالمعطيات الخاصة به التي تخضع للمعالجة وكذا بكل معلومة متاحة حول مصدر المعطيات.

يحق للمسؤول عن المعالجة أن يطلب من السلطة الوطنية تحديد آجال عن الإجابة على طلبات الولوج المشروعة، ويمكنه الإعتراض على الطلبات التعسفية لا سيما من حيث عددها وطابعها المتكرر، وتقع على عاتقه إثبات الطابع التعسفي لهذا الطلب"([1]).

ويلاحظ أن المشرع الجزائري الذي لم يكن دقيقا في تحديد هذا الحق باستعماله بعض العبارات الغامضة كوفق شكل مفهوم، من حيث عددها، دون أن يوضح ما معنى الشكل المفهوم وعدد الطلبات المسموح بها، ومن تم فإنه يجب على المشرع الجزائري ضرورة إعادة النظر في صياغة هذه المادة بصورة أكثر وضوحا بما يتلائم مع حق الولوج الى المعطيات ذات الطابع الشخصي.

**ثالثا: الحق في التصحيح كحق من حقوق الشخص المعني بالمعطيات المزمع معالجتها**

من الضمانات الأساسية والهامة لحماية الحياة الخاصة في مواجهة نظم المعلومات الشخصية بإعطاء الشخص الحق في تصحيح البيانات الخاطئة وغير الدقيقة، حيث يعد هذا الحق من أهم موضوعات قانون المعلومات، ويقصد به أن يكون للشخص من جهة أولى الإمكانية في تصويب الأخطاء في البيانات الشخصية والمعلومات المعالجة آليا والمختزنة في نظام المعلومات التي من

[1]- المادة 34 من القانون رقم 18-07.

شأنها أن تولد لدى الغير فكرة مختلفة عن حقيقة الشخص، ومن جهة أخرى محو البيانات التي تم تخزينها بطرق غير مشروعة([1]).

فتطرقت المادة 12 من الإرشادات الأروبية على حق الشخص المعني بطلب التصحيح([2])، بينما منح المشرع الفرنسي في المادة 20 من قانون المعلوماتية والحريات الفردية لكل شخص الحق في تصحيح وتكملة وإيضاح وتنقيح أو محو المعلومات الخاصة به إذا كانت قد تغيرت، وكذلك محو المعلومات التي يكون الحصول عليها أو إستخدامها أو الإحتفاظ بها غير مشروع قانونا([3]).

كما أقر المشرع التونسي أيضا هذا الحق في مواجهة السلطات العامة في الفصل 40 من القانون الأساسي عدد 63 لسنة 2004، السالف الذكر، والذي ينص على أنه" يمكن للمعني بالأمر أو ورثته أو وليه المطالبة بإصلاح المعطيات الشخصية الخاصة به أو إتمامها أو تعديلها أو توضيحها أو تحيينها أو التشطيب عليها إذا كانت غير صحيحة أو ناقصة أو غامضة أو إعدامها إذا كان جمعها أو إستعمالها مخالف لأحكام هذا القانون..."([4])، إضافة الى المشرع الكويتي الذي أعطى للفرد حق الحصول على بيان رسمي بالمعلومات المدنية المتعلقة به أو بأصوله أو بفروعه أو بأزواجه، بعد دفع الرسوم المتوجبة عليه، وذلك بموجب المادة 17 من قانون المعلومات([5])، وكذلك المشرع المغربي أيضا، قد نص على هذا الحق في المادة 8 من القانون 08-09، السالف الذكر، والتي تنص على أنه"يحق للشخص المعني بعد الإدلاء بما يثبت هويته أن يحصل من لدن المسؤول عن المعالجة على ما يأتي:

أ) تحيين أو تصحيح أو مسح أو إغلاق الولوج الى المعطيات ذات الطابع الشخصي التي تكون معالجتها غير مطابقة بهذا القانون ولا سيما بسبب الطابع غير المكتمل

---

[1]- بولين أنطونيوس ، مرجع سابق، ص 476،477.

[2]- منى الأشقر جبور، محمود جبور، مرجع سابق، ص 149.

[3]- بولين أنطونيوس ، مرجع سابق، ص 477.

[4]- الفصل 40 من القانون الأساسي التونسي عدد 63 لسنة 2004.

[5]- نعيم مغبغب، مرجع سابق، ص 202.

أو غير الصحيح لتلك المعطيات، ويلزم المسؤول عن المعالجة بالقيام بالتصحيحات اللازمة دون عوض لفائدة الطالب داخل أجل عشرة(10) أيام كاملة...

ب) تبليغ الأغيار الذين وصلت إليهم المعطيات ذات الطابع الشخصي بكل تحيين أو تصحيح أو مسح أو إغلاق للولوج إليهم بناء على البند أ) أعلاه ما لم يتعذر ذلك([1]).

أما المشرع الجزائري فقد نص على الحق في التصحيح في المادة 35 من القانون 18-07، السالف الذكر، والتي تنص على أنه" يحق للشخص المعني أن يحصل مجانا من المسؤول عن المعالجة على:

أ- تحيين أو تصحيح أو مسح أو إغلاق المعطيات الشخصية التي تكون معالجتها غير مطابقة لهذا القانون بسبب الطابع غير المكتمل أو غير الصحيح لتلك المعطيات على الخصوص أو لكون معالجتها ممنوعة قانونا، ويلزم المسؤول عن المعالجة بالقيام بالتصحيحات اللازمة مجانا لفائدة الطالب في أجل عشرة(10) أيام من إخطاره.

في حالة الرفض أو عدم الرد على الطلب خلال الأجل المذكور أعلاه، يحق للشخص المعني إيداع طلب التصحيح لدى السلطة الوطنية التي تكلف أحد أعضائها للقيام بكل التحقيقات الضرورية والعمل على أجراء التصحيحات اللازمة في أقرب الآجال وإخبار الشخص المعني بمآل طلبه.

ب- تبليغ الغير الذي أوصلت إليه المعطيات الشخصية بكل تحيين أو تصحيح أو مسح أو إغلاق للمعطيات ذات الطابع الشخصي، يتم طبقا للمطة (أ) أعلاه، ما لم يكن ذلك مستحيلا.

يمكن إستعمال الحق المنصوص عليه في هذه المادة من قبل ورثة الشخص المعني"([2]).

[1]- المادة 8 من القانون المغربي رقم 08-09.

[2]- المادة 35 من القانون رقم 18-07.

والملاحظ أن المشرع الجزائري قد أقر حق التصحيح للشخص المعني، والذي يجب إبلاغه الى الغير الذين سبق تزويدهم بالمعطيات ذات الطابع الشخصي الخاطئة وغير الدقيقة من أجل القيام بالإجراءات اللازمة على مستوى أجهزتهم.

**رابعا: الحق في الإعتراض كحق من حقوق الشخص المعني بالمعطيات المزمع معالجتها**

الحق في الإعتراض على معالجة البيانات الشخصية هو تكريس لحق الشخص في إحترام حرياته الأساسية، بحيث يمكن لصاحب هذه البيانات الإعتراض على معالجة بياناته الشخصية لأسباب مشروعة، كما يمكنه رفض إستخدام هذه البيانات في دراسات وأبحاث تجارية، وذلك دون أن يكون مجبرا على تقديم أي تبرير أو سبب، كما يمكنه كذلك ممارسة هذا الحق سواء في مرحلة جمع البيانات أو في مرحلة لاحقة، فلكل شخص من حيث المبدأ حق تقرير طريقة إستخدام بياناته بأن يرفض إدراجها ضمن ملفات الكترونية أو نقلها الى جهات أخرى([1]).

وقد نصت المادة (38/1) من قانون حماية البيانات الشخصية الفرنسي على حق الشخص في الإعتراض على معالجة بياناته الشخصية، والتي تنص على أن" كل شخص طبيعي له الحق في الإعتراض على معالجة بياناته الشخصية، وذلك إذا كانت هناك مبررات مشروعة لهذا الإعتراض".

ولم يشترط المشرع الفرنسي شكلا معينا لممارسة الحق في الإعتراض، فيجوز أن يتخذ أي شكل، ولكن من المهم أن يكون هناك تصرف إيجابي من قبل من تتم معالجة بياناته يفيد إعتراضه على معالجة البيانات بشكل معين، حتى يعتبر حق الإعتراض قد تم التعبير عنه، فمجرد السكوت لا يفيد الإعتراض على معالجة البيانات([2]).

كما أن المشرع التونسي أقر هذا الحق في الفصل 42 من الفرع الثالث ضمن القسم الثالث بعنوان "في حقوق المعني بالأمر"، من القانون الأساسي عدد 63 لسنة 2004، السالف الذكر، والذي نص فيه على أنه" فيما عدا حالات المعالجة التي

---

1- منى الأشقر جبور، محمود جبور، مرجع سابق، ص 148.

2- سامح عبدالواحد التهامي، مرجع سابق، ص 428،427.

يقضيها القانون أو طبيعة الإلتزام، يحق للمعني بالأمر أو ورثته أو وليه الإعتراض على معالجة معطياته الشخصية في كل وقت ولأسباب وجيهة ومشروعة وجدية تتعلق به.

كما للمعني بالأمر أو ورثته أو وليه الإعتراض على إحالة معطياته الشخصية الى الغير لاستعمالها في أغراض الدعاية.

ويوقف الإعتراض المعالجة فورا([1]).

وكذلك المشرع المغربي الذي تطرق الى هذا الحق بمسمى الحق في التعرض في الفقرة الأخيرة من المادة 9 من القانون 08-09، السالف الذكر، والتي تنص على أنه" يحق للشخص المعني، بعد تقديم ما يثبت هويته، أن يتعرض لأسباب مشروعة على القيام بمعالجة معطيات تخصه.

وله الحق في التعرض دون مصاريف على إستعمال المعطيات المتعلقة به لاغراض الإستقراءات ولا سيما التجارية منها من لدن المسؤول الحالي عن المعالجة أو مسؤول عن معالجة لاحقة.

لا تطبق أحكام الفقرة الأولى إذا كانت المعالجة تستجيب لإلتزام قانوني أو إذا كان تطبيق هذه الأحكام قد صرف عنه النظر بموجب مقتضى صريح في المحرر الذي يأذن بالمعالجة([2]).

كما نص المشرع القطري على هذا الحق في المادة 5([3]) من قانون رقم 13 لسنة 2016، بشأن حماية خصوصية البيانات الشخصية، إلا أنه قيده بقيدين ذكرهما في هذه المادة.

أما المشرع الجزائري نص على آليات ممارسة الحق في الإعتراض أو طرق ممارسته قانونا في المادة 36 من القانون 18-07، السالف الذكر، والتي تنص على أنه" يحق للشخص المعني أن يعترض لأسباب مشروعة على معالجة معطياته ذات الطابع الشخصي.

---

[1]- الفصل 42 من القانون الأساسي التونسي عدد 63 لسنة 2004.

[2]- المادة 9 من القانون المغربي رقم 08-09.

[3]- أنظر المادة 5 من القانون القطري رقم 13 لسنة 2016.

وله الحق في الإعتراض على إستعمال المعطيات المتعلقة به لأغراض دعائية، ولا سيما التجارية منها، من طرف المسؤول الحالي عن المعالجة أو مسؤول عن معالجة لاحقة.

لا تطبق أحكام الفقرة الأولى من هذه المادة إذا كانت المعالجة تستجيب لإلتزام قانوني، وإذا كان تطبيق هذه الأحكام قد أستبعد بموجب إجراء صريح في المحرر الذي يرخص بالمعالجة([1]).

ومن بين التطبيقات القضائية لهذا الحق، اعتبرت المحكمة الإبتدائية لكبرى بباريس أن إرسال رسائل إلكترونية دعائية لشخص على الرغم من إعتراضه على ذلك يعتبر إنتهاكا لحقه في الإعتراض على معالجة بياناته الشخصية.

وقد أكدت محكمة النقض الفرنسية على أن معالجة البيانات الشخصية على الرغم من الإعتراض على ذلك هو أمر غير مشروع، لذلك فقد اعتبرت المحكمة أن تجميع عناوين البريد الإلكتروني للأفراد على الرغم من إعتراضهم يعتبر أمر غير مشروع.

كما قد أيدت محكمة النقض الحكم بالغرامة على إحدى مستشفيات الأمراض النفسية لقيامها بمعالجة البيانات الصحية لبعض المرضى على الرغم من إعتراضهم على ذلك([2]).

وتجدر الإشارة الى أن المشرع الجزائري تطرق في المادة 37 من القانون 18-07، السالف الذكر، الى حق آخر للشخص المعني تمثل في منع إستخدام بياناته بأي شكل من الأشكال في الإستكشاف المباشر بأي وسيلة تستخدم التكنولوجيا ودون موافقته، وهذا الحق سماه المشرع المغربي الإستقراء المباشر ونص عليه في المادة 10 من القانون 08-09، السالف الذكر.

كما أن بعض التشريعات المقارنة أضافت حقوق أخرى للشخص الذي تتم معالجة بياناته حتى يتمتع بأكبر قدرا من الحماية في مواجهة كل الإعتداءات التي تطال بياناته الشخصية.

---

[1]- المادة 36 من القانون رقم 18-07.

[2]- نقلا عن: سامح عبدالواحد التهامي، مرجع سابق، ص 429.

ومن تم يمكن القول أنه في أي مجتمع لا تحمى فيه البيانات الشخصية من مخاطر الوصول إليها وإساءة إستخدامها فأن الحق في المعلومات سيكون محل إهدار حتى لو بدا أن حق الوصول يتعزز، لأن قيد الخصوصية لا يرد عليه وما سيتحقق واقعيا هو وصول الجهات التي تسيطر على المعلومات الى البيانات الشخصية وليس الجهات التي تسعى لالتماسها([1]).

**الفرع الثاني: الإلتزامات الملقاة على عاتق المسؤولين عن المعالجة**

لم يكتف المشرع الجزائري بإقرار حقوقا للشخص الذي تتم معالجة بياناته، بل وضع إلتزامات على عاتق المسؤول عن المعالجة([2]) حتى تكتمل منظومة الضوابط التي تحاط بها معالجة البيانات ذات الطابع الشخصي، وهذه الإلتزامات هي: سلامة المعالجة، سرية المعالجة، معالجة المعطيات ذات الطابع الشخصي في مجال التصديق والتوقيع الإلكتروني وفي مجال الإتصالات الإلكترونية، نقل المعطيات نحو دولة أجنبية.

**أولا: سلامة المعالجة كإلتزام على عاتق المسؤولين عن المعالجة**

نص المشرع الفرنسي على سلامة تأمين البيانات الشخصية في المادة 34 من قانون حماية البيانات الشخصية الفرنسي، والتي نصت على" إلتزام المسؤول عن معالجة البيانات الشخصية باتخاذ كل الإحتياطات اللازمة للحفاظ على أمن البيانات الشخصية، وخاصة منع أي تغيير أو إتلاف لهذه البيانات يمكن أن يحدثه أحد الأشخاص غير المأذون لهم بالإطلاع عليها"([3]).

وأشار المشرع التونسي في هذا السياق الى أن كل شخص يقوم بنفسه أو بواسطة الغير بمعالجة المعطيات الشخصية يكون ملزما أزاء الأطراف المعنية بأن

---

1- بولين أنطونيوس ، مرجع سابق، ص 83.

2- عرف المشرع الجزائري المسؤول عن المعالجة في المادة الثالثة من القانون 18-07، السالف الذكر، بأنه" كل شخص طبيعي أو معنوي عمومي أو خاص أو كيان آخر يقوم بمفرده أو بالإشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها".

3- Art 34 : Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.
Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8, modifiè par Loi N° 2004-801 du 6 août 2004-ART.5, JORF 7 août 2004.

يتخذ جميع الإحتياطات اللازمة المنصوص عليها في الفصل 19 للمحافظة على أمان المعطيات ومنع الغير من تعديلها أو الإضرار بها أو الإطلاع عليها دون إذن صاحبها، وذلك طبقا لأحكام الفصل 18 من القانون الأساسي عدد 63 لسنة 2004، السالف الذكر([1]).

كما نص المشرع القطري على الإلتزام بسلامة المعالجة، في المادة 13 من القانون رقم 13 لسنة 2016، السالف الذكر، والتي تنص على أنه" يجب على كل من المراقب والمصالح إتخاذ الإحتياطات اللازمة لحماية البيانات الشخصية من الضياع أو التلف أو التعديل أو الإفشاء أو الوصول إليها أو إستخدامها بشكل عارض أو غير مشروع..."([2])، إضافة الى المشرع الكويتي الذي نص في المادة 35 من قانون المعاملات الإلكتروني الكويتي على إلتزام الجهات الحكومية والهيئات والمؤسسات العامة أو الشركات أو الجهات غير الحكومية باتخاذ التدابير المناسبة لحماية البيانات الشخصية -الموجودة في أنظمة المعالجة الإلكترونية الخاصة بها- من كل ما يعرضها للفقد أو التلف أو الإفشاء أو إستبدالها ببيانات غير صحيحة أو إدخال معلومات عليها على خلاف الحقيقة.

هذا الإلتزام يلقى على عاتق من يقوم بمعالجة البيانات الشخصية أن يتخذ كل الإجراءات التقنية لإيجاد مستوى ملائم من الحماية للبيانات الشخصية، وهذا المستوى يعتمد على طبيعة البيانات الشخصية والأخطار التي من المحتمل أن تتعرض لها، والتقنيات المتاحة في مجال حماية البيانات الشخصية([3]).

وكذلك المشرع المغربي هو الآخر نص على سلامة المعالجات في المادة 1/23 من القانون 08-09، السالف الذكر، والتي تنص على أنه" يجب على المسؤول عن المعالجة القيام بالإجراءات التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو الإذاعة أو الولوج غير المرخص، خصوصا عندما تستوجب المعالجة إرسال معطيات عبر شبكة معينة، وكذا حمايتها من أي شكل من أشكال

[1]- الفصل 18 من القانون الأساسي التونسي عدد 63 لسنة 2004.

[2]- المادة 13 من القانون رقم 13 لسنة 2016.

[3]- سامح عبدالواحد التهامي، مرجع سابق، ص 418.

المعالجة غير المشروعة، ويجب أن تضمن هذه الإجراءات مستوى ملائما من السلامة بالنظر الى المخاطر التي تمثلها المعالجة وطبيعة المعطيات الواجب حمايتها، وذلك مع الأخذ بعين الإعتبار التقنيات المستعملة في هذا المجال والتكاليف المترتبة عن القيام بها"([1]).

أما المشرع الجزائري فنص على إلتزام سلامة المعالجة أو ما يطلق عليه البعض تأمين المعالجة الذي يقع على عاتق المسؤول عن المعالجة في المادتين 38 و39 من القانون 18-07، السالف الذكر، حيث نصت المادة 38 منه، على أنه" يجب على المسؤول عن المعالجة وضع التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين، خصوصا عندما تستوجب المعالجة إرسال معطيات عبر شبكة معينة وكذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة.

ويجب أن تضمن هذه التدابير مستوى ملائما من السلامة بالنظر الى المخاطر التي تمثلها المعالجة وطبيعة المعطيات الواجب حمايتها"([2]).

كما أنه عند إجراء المعالجة لحساب المسؤول عنها يجب عليه أختيار معالج من الباطن([3]) بموجب عقد أو سند قانوني يكون بغرض حفظ الأدلة، تقيد عناصره أو متطلباته المتعلقة بالتدابير المنصوص عليها في الفقرة الأولى من المادة 38 كتابة أو في أي شكل آخر معادل، طبقا لأحكام المادة 39 من نفس القانون.

ومن تم فيجب أن تضمن هذه التدابير مستوى ملائما من السلامة بالنظر إلى المخاطر التي تمثلها المعالجة وطبيعة المعطيات الواجب حمايتها([4]).

---

[1]- المادة 1/23 من القانون المغربي رقم 08-09.

[2]- المادتين 38 و39 من القانون رقم 18-07.

[3]- عرف المشرع الجزائري المعالج من الباطن في المادة الثالثة من القانون 18-07، السالف الذكر، بأنه" كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة ".

[4]- حزام فتيحة، مقال بعنوان الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي دراسة على ضوء القانون 18-07، مجلة الإجتهاد للدراسات القانونية والإقتصادية، المركز الجامعي تمنراست، المجلد 08، العدد 04، جوان 2019، ص 290.

**ثانيا: سرية المعالجة كإلتزام على عاتق المسؤولين عن المعالجة**

نص المشرع الفرنسي على سرية المعالجة في قانون العقوبات كإلتزام يقع على عاتق من يقوم بمعالجة البيانات بعدم إفشاء البيانات الشخصية للغير، إذا كان إفشاء هذه البيانات من شأنه أن يهدد أعتبار من تخصه هذه البيانات أو حياته الخاصة.

ويجوز لمعالج البيانات أن يفشي هذه البيانات للغير إذا حصل على أذن خاص بذلك ممن تخصه هذه البيانات.

والملاحظ من هذا النص أن معالج البيانات ملزم بالسرية، ومسموح له فقط بإفشاء البيانات الشخصية التي لا يكون في إفشائها أي تهديد لكرامة وإعتبار من تخصه هذه البيانات أو تهديد لحياته الخاصة، وهو أمر يحدده القاضي في كل حالة على حدى ولا يوجد معيار ثابت للقول بأن إفشاء هذه البيانات يمثل تهديدا للحياة الخاصة أو الكرامة من عدمه، وإنما هي أمور تختلف من شخص لآخر([1]).

وأن المشرع التونسي نص على واجب المحافظة على سرية المعطيات الشخصية في الفصل 23 من القانون الأساسي عدد 63 لسنة 2004، السالف الذكر، والتي تنص على أنه" يجب على المسؤول عن معالجة المعطيات الشخصية والمناول وأعوانهما ولو بعد إنتهاء المعالجة أو زوال صفتهم تلك المحافظة على سرية المعطيات الشخصية والمعلومات التي تمت معالجتها بإستثناء تلك التي وافق المعني بالأمر كتابيا على نشرها أو في الحالات المنصوص عليها بالتشريع الجاري به العمل"([2]).

وكذلك المشرع الكويتي نص هو الآخر على هذا الإلتزام في المادة 32 من قانون المعاملات الإلكترونية الكويتي، على أنه" لا يجوز للجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين أفشاء أو نشر بيانات شخصية مسجلة لديها أو موجودة بأنظمة المعالجة الإلكترونية الخاصة بها ما لم يتم ذلك بموافقة الشخص المتعلقة به هذه البيانات أو من ينوب عنه قانونا أو بقرار قضائي مسبب"([3]).

---

[1]- سامح عبدالواحد التهامي، مرجع سابق، ص 422.

[2]- الفصل 23 من لقانون الأساسي التونسي عدد 63 لسنة 2004.

[3]- مقتبس عن: سامح عبدالواحد التهامي، مرجع سابق، ص 422.

أما بالنسبة للمشرع الجزائري فنص على سرية المعالجة كإلتزام يقع على عاتق المسؤولين عن المعالجة من خلال إلزام المسؤول عن هذه المعالجة والأشخاص الذين أطلعوا أثناء ممارسة مهامهم على معطيات ذات طابع شخصي بالسر المهني حتى بعد إنتهاء مهامهم، وإلا يكونون تحت طائلة العقوبات المنصوص عليها في المادة 40 من القانون 18-07، السالف الذكر.

وكذلك لا يجوز لأي شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن الذي يلج الى معطيات ذات طابع شخصي أن يعالج هذه المعطيات دون تعليمات المسؤول عن المعالجة إلا في حالة تنفيذ إلتزام قانوني، طبقا لأحكام المادة 41([1]) من نفس القانون ، وهو ما تطرق إليه المشرع المغربي أيضا، بموجب المادة 26([2]) من القانون 08-09، السالف الذكر، والتي تلزم المسؤول عن معالجة المعطيات ذات طابع شخصي باحترام السر المهني حتى بعد توقفهم عن ممارسة مهامهم.

**ثالثا: معالجة المعطيات ذات الطابع الشخصي في مجال التصديق والتوقيع الإلكترونيين وفي مجال الإتصالات الإلكترونية كإلتزام على عاتق المسؤولين عن المعالجة**

أن مقدم الخذمات يقوم بمعالجة المعطيات ذات الطابع الشخصي في مجال التصديق والتوقيع الإلكترونيين وفي مجال الإتصالات الإلكترونية، وعرف المشرع الجزائري مقدم الخدمات في المادة 3 الفقرة 19 منها من القانون 18-07، السالف الذكر، بأنه"

1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات.

2- أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكور أو للمستعملين"([3]).

---

[1]- المادة 41 من القانون رقم 18-07.

[2]- أنظر المادة 26 من القانون المغربي رقم 08-09.

[3]- المادة 3 الفقرة 19 من القانون رقم 18-07.

ويلتزم مؤدي خدمات التصديق الإلكتروني([1]) في الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها من قبلهم لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني من الأشخاص المعنيين بها مباشرة والتي لا يجوز معالجتها لأغراض غير تلك التي جمعت من أجلها طبقا لأحكام المادة 42 من نفس القانون.

أما الإتصال الإلكتروني يعني كل المراسلات والإرسالات التي تقع سواء في شكل علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها يتم تناولها أو إرسالها بطريق الكتروني عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية([2])، وقد ورد تعريف الإتصال الإلكتروني في المادة 3 فقرة 11([3]) من قانون 07/18 المشار إليه أعلاه، ونفس النعريف تضمنه القانون 04/18 المتعلق بالبريد والإتصالات الإلكترونية في المادة 10 الفقرة الأولى منه([4])، وكذلك أيضا في القانون 04/09 السالف الذكر في المادة الثانية البند و([5]) منه.

ويلتزم مقدموا الخدمات في مجال الإتصالات الإلكترونية، وبعد إتخاذهم جميع الضمانات الضرورية لحماية المعطيات ذات الطابع الشخصي بإبلاغهم فورا السلطة الوطنية والشخص المعني أن كان هناك مساس بحياته الخاصة في حالة ما إذا أدت

---

[1]-عرفت المادة 2 في النقطة 12من القانون 15-04، المؤرخ في أول فبراير سنة 2015، الذي يحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، مؤدي خدمات التصديق الإلكتروني بأنه" شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني"، ج ر ج ج، ع 06، المؤرخ في 10 فبراير سنة 2015، ص 7.

[2]- طباش عزالدين، مرجع سابق، ص 50.

[3]- عرفت المادة 3 الفقرة 11 من قانون 07/18 الإتصال الإلكتروني بأنه" كل إرسال أو تراسل أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية"

[4]- عرفت المادة 10 الفقرة الأولى من قانون 04/18، المؤرخ في 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، الإتصال الإلكتروني بأنه"كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية"، ج ر ج ج، ع 27، المؤرخ في 13 مايو سنة 2018، ص 6 .

[5]- عرفت المادة 2 البند و من القانون 04/09 الإتصال الإلكتروني بأنه" أي تـراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صـور أو أصوات أو مـعلومـات مـختـلفـة بواسـطـة أي وسيلة إلكترونية"

معالجة هذه المعطيات في شبكات الإتصالات الإلكترونية المفتوحة للجمهور الى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، كما يلتزم مقدم الخدمات أيضا بمسك جرد محينا حول كل الإنتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي والإجراءات التي إتخذها بشأنها، وذلك طبقا لأحكام الماة 43 من نفس القانون([1]).

**رابعا: نقل المعطيات نحو دولة أجنبية كإلتزام على عاتق المسؤولين عن المعالجة**

نص المشرع التونسي على إلتزام نقل المعطيات نحو دولة أجنبية كإلتزام على عاتق المسؤولين عن المعالجة في الفصل 51 من القانون الأساسي عدد 63 لسنة 2004، السالف الذكر، والذي ينص على أنه" لا يمكن نقل المعطيات الشخصية الواقع معالجتها أوالمخصصة للمعالجة الى بلاد أخرى إلا إذا وفرت مستوى ملائما من الحماية يقدر إعتمادا على العناصر المتعلقة بطبيعة المعطيات المطلوب نقلها والغرض من معالجتها ومدة المعالجة والبلاد التي ستحال إليها المعطيات وما توفره من الإحتياطات اللازمة للمحافظة على أمان المعطيات، وفي كل الحالات يجب أن يتم نقل المعطيات الشخصية وفقا للشروط الواردة بهذا القانون"([2]).

أما المشرع الجزائري فنص على إلتزام المسؤول عن المعالجة بنقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية بشروط أقرها في المادة 44 من القانون 18-07، السالف الذكر، والتي تنص على أنه" لا يجوز لمسؤول عن معالجة نقل المعطيات ذات الطابع الشخصي الى دولة أجنبية إلا بترخيص للسلطة الوطنية وفقا لأحكام هذا القانون، وإذا كانت الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص آزاء المعالجة التي تخضع لها هذه المعطيات أو التي قد تخضع لها.

تقدر السلطة الوطنية المستوى الكافي من الحماية الذي تضمنه دولة معينة، لا سيما وفقا للمقتضيات القانونية المعمول بها في هذه الدولة ولإجراءات الأمن المطبقة

[1]- أنظر المادة 43 من القانون رقم 18-07.

[2]- الفصل 51 من القانون الأساسي عدد 63 لسنة 2004.

فيها، وللخصائص المتعلقة بالمعالجة مثل غاياتها ومدتها وكذا طبيعة وأصل ووجهة المعطيات المعالجة.

وفي جميع الأحوال، يمنع أرسال وتحويل معطيات ذات الطابع الشخصي الى دولة أجنبية عندما قد يؤدي ذلك الى المساس بالأمن العمومي أو المصالح الحيوية للدولة"([1]).

كما أن المشرع الجزائري وضع لهذا الإلتزام إستثناءات أربعة ذكرها في المادة 45 من من القانون 18-07، والتي تنص على أنه" إستثناء على أحكام المادة 44 من هذا القانون يمكن المسؤول عن المعالجة نقل معطيات ذات طابع شخصي نحو دولة لا تتوفر فيها الشروط التي تنص عليها المادة المذكورة في الحالات الآتية:

1- الموافقة الصريحة للشخص المعني.

2- إذا كان النقل ضروريا:

أ- للمحافظة على حياة هذا الشخص.

ب- للمحافظة على المصلحة العامة.

ج- إحتراما لالتزامات تسمح بضمان إثبات أو ممارسة حق أو الدفاع عنه أمام القضاء.

د- تنفيذ العقد بين المسؤول عن المعالجة والشخص المعني أو تنفيذا لإجراءات سابقة للعقد والمتخذة بناء على طلب هذا الأخير.

هـ- لإبرام أو تنفيذ عقد مبرم أو سيبرم بين المسؤول عن المعالجة والغير، لمصلحة الشخص المعني.

و- تنفيذا لإجراء يتعلق بتعاون قضائي دولي.

ز- للوقاية من إصابات مرضية أو تشخيصها أو معالجتها.

3- إذا تم النقل تطبيقا لإتفاق ثنائي أو متعدد الأطراف تكون الجزائر طرفا فيه.

4- بناء على ترخيص السلطة الوطنية، إذا كانت المعالجة تتطابق مع أحكام المادة 2 من هذا القانون"([2]).

---

[1]- المادة 44 من القانون رقم 18-07.

[2]- المادة 45 من القانون رقم 18-07.

**المبحث الثاني: الجرائم المرتبطة بالمعطيات ذات الطابع الشخصي**

أن الخطر الأبرز لنظام المعالجة الآلية للمعطيات ينتج من إنشاء بنوك للمعلومات التي تحتوي على معطيات ذات طابع شخصي، والتي يترتب على معالجتها بطريقة غير مشروعة خطرا حقيقيا على هذه المعطيات، الأمر الذي يستدعي معه وضع نصوص قانونية خاصة لمواجهة تلك الأخطار المستحدثة.

وقد شهدت الحماية الجزائية للحياة الشخصية تطورا في نطاقها ومشتملاتها، وجرى الوقوف أمام هول عالم الكومبيتر وقدراته المذهلة على حفظ وتخزين وأسترجاع وتحليل ومعالجة البيانات الشخصية، وذلك ما تطلب وجوب حماية الأفراد من صور الإعتداء التي تطال الحياة الشخصية عبر المساس بالبيانات الشخصية الخاصة بهم.

في هذا النطاق ولدت فكرة حماية البيانات الشخصية إبتداء من مخاطر المعالجة الآلية، وكان لا بدا من تحديد قواعد ومبادئ للحماية وفرض آليات تكفل سلامتها من خلال وضع القواعد الشكلية والإجرائية لعمليات المعالجة وتنظيم رسائل الرقابة عليها والوقوف على صور الإعتداء والإنتهاك في هذه البيئة وتجريمها، وبالتالي إسباغ حماية جنائية فاعلة على الحق في حماية البيانات الشخصية([1]).

وعلى المستوى الدولي صدر قرار الجمعية العمومية للأمم المتحدة لتنظيم البيانات الشخصية المعالجة إلكترونيا رقم 95/45 بتاريخ 1990/12/14، الذي تم فيه تكريس مجموعة من المبادئ المعتمدة حاليا في غالبية الدول حفاظا منها على البيانات الشخصية التي تتم معالجتها بالوسيلة الإلكترونية، كما تم توقيع العديد من الإتفاقيات الأروبية حول حماية الحياة الخاصة والبيانات الشخصية التي جاءت متوافقة والمقررات الصادرة عن الجمعية العمومية للأمم المتحدة كإتفاقية ستراسبورغ الموقعة بتاريخ 1981/01/28 والمعروفة بالإتفاقية 108 الخاصة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات الشخصية، والبرتوكول الإضافي المعدل لها والموقع في 2001/11/08، الذي عمدا على توفير حماية أقوى للبيانات الشخصية ، كما صدرت أيضا بعض الإرشادات الأروبية حول حماية الحياة الخاصة

---

1- بولين أنطونيوس ، مرجع سابق، ص 382،381.

والبيانات الشخصية وهذه الإرشادات والإتفاقيات كانت الأساس في وضع الشرعية الدولية على صعيد حماية البيانات الشخصية في إطار المعلوماتية([1]).

أما على المستوى الداخلي فقد بادرت العديد من الدول الغربية الى وضع نصوص قانونية خاصة تعاقب صراحة على الجرائم الواقعة على البيانات الشخصية، وتعتبر فرنسا من الدول الاوائل التي أصدرت تشريعا خاصا في هذا المجال بموجب القانون الفرنسي رقم 17/78 لسنة 1978، المتعلق بالمعالجة الالكترونية للبيانات الرسمية الذي تضمن بعض الجرائم الخاصة بحماية البيانات الشخصية المرتبطة بالحياة الخاصة للأشخاص.

ونظرا لخطورة ما يترتب على معالجة البيانات الأسمية من تهديد لخصوصية الأفراد فقد أحالت المواد من (41 إلى 44) والمادة 46 من القانون 17 لسنة 1978 معدلة بالقانون 1336 لسنة 1992 من قانون العقوبات الفرنسي الجديد إلى المواد 226-16 إلى 226-24 من ذلك القانون الأخير في شأن الجرائم التي تقع بالمخالفة لأحكام القانون الأول مع إجراء تعديلات في بعض الجرائم([2]).

كما قامت بعض الدول العربية بوضع قوانين خاصة للحماية الجنائية للمعطيات ذات الطابع الشخصي كالمشرع المغربي بموجب القانون 09-08 السالف الذكر، والتونسي بموجب القانون الأساسي عدد 63 لسنة 2004 السالف الذكر، والقطري بموجب القانون رقم 13 لسنة 2016 السالف الذكر.

إضافة الى المشرع الجزائري الذي قام مؤخرا بإصداره القانون 07/18، السالف الذكر، ومن خلاله تم تكريس حماية جنائية خاصة لهذه الفئة من المعطيات، وهو الأمر الذي سيجعلنا نركز كثيرا على المشرع الجزائري مع الإشارة أحيانا إلى بعض التشريعات المقارنة.

وسنتناول الجرائم المرتبطة بالمعطيات ذات الطابع الشخصي، من خلال تحديد صور هذه الجرائم(المطلب الأول) وآليات الحماية الجنائية المقررة لها( المطلب الثاني).

---

[1]- بولين أنطونيوس ، مرجع سابق، ص 384،385.

[2]- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، مرجع سابق، ص 86.

**المطلب الأول: صور جرائم المعطيات ذات الطابع الشخصي**

أن ردع الإعتداءات التي تطال المعطيات ذات الطابع الشخصي يتطلب وجود نصوص قانونية خاصة تجرم تلك الأفعال التي تمس بهذه المعطيات وتعاقب مرتكبها، وهو ما قام به المشرع الجزائري بتجريم مجموعة من الأفعال التي تشكل خرقا للقواعد الموضوعية أو الشكلية التي يجب مراعاتها عند القيام بكل معالجة للمعطيات ذات الطابع الشخصي.

وتتضمن هذه الجرائم عدة صور تشكل إعتداء عل المعطيات ذات الطابع الشخصي أشارت لها العديد من التشريعات المقارنة وأشار لها كذلك المشرع الجزائري في القانون 18-07، المذكور آنفا، فقد تتعلق بكيفية جمعها وإستغلالها على نحو غير مشروع (الفرع الأول) وقد تتعلق بالمخالفات المرتكبة أثناء إنشاء المعالجة (الفرع الثاني).

**الفرع الأول: تجريم الجمع والإستغلال غير المشروع للمعطيات ذات الطابع الشخصي**

أن المعطيات ذات الطابع الشخصي تتعرض لعدة إعتداءات، فقد يتم جمعها بطريقة غير مشروعة أو إستغلالها على نحو غير مشروع.

**أولا: تجريم الجمع غير المشروع للمعطيات ذات الطابع الشخصي**

أن هذه الجريمة تتضمن عدة صور مخالفة لأحكام جمع المعطيات ذات الطابع الشخصي فقد ترتكب بإستعمال أساليب غير مشروعة في عملية جمعها أو ترتكب بجمع نوع معين من المعطيات ألا وهي المعطيات المتعلقة بالماضي الجزائي للشخص المعني.

**1- إستعمال أساليب غير مشروعة في جمع المعطيات ذات الطابع الشخصي**

أن هذه الجريمة تقع في المراحل الأولى من المعالجة تتكون عناصرها من سلوك إجرامي يتضمن فعل الجمع للمعطيات ذات الطابع الشخصي الذي يعتبر إحدى مراحل المعالجة لتلك المعطيات، وأن تستعمل طرق غير مشروعة في عملية جمع هذه المعطيات سواء تم ذلك يدويا في ملفات أو سجلات ورقية أو آليا باستعمال الإجهزة المعلوماتية، وذلك تطبيقا لنص المادة الرابعة من القانون 18-

07، السالف الذكر، كما أن هذه الطرق غير المشروعة تكفي وحدها لتتضمن الوسائل التدليسية وغير النزيهة لجمع المعلومة يضاف إليها كل أشكال الإختلاس من الوثائق أو السجلات الرقمية أو الحصول عليها عن طريق الدخول غير المشروع.

وتتحقق هذه الجريمة بجمع بيانات شخصية تخص أشخاصا على أن يتم هذا الجمع بصورة غير قانونية من قبل أشخاص أو جهات ليس لهم الحق في القيام بجمع هذه المعلومات([1]).

وأن جمع المعطيات ذات الطابع الشخصي باستعمال أساليب غير مشروعة هو فعل منصوص عليه في المادة 226 الفقرة 18 من قانون العقوبات الفرنسي، والتي تنص على ما يلي:" الحبس خمس سنوات وغرامة 300.00 أورو كعقوبة لجمع معلومات إسمية بطريقة التدليس أو الخديعة أو أي طريق غير مشروع أو إجراء معالجة لمعلومات أسمية تتعلق بشخص طبيعي رغم معارضة هذا الشخص متى كانت المعارضة تقوم على أسباب مشروعة"([2]).

كما نص عليه المشرع الجزائري في المادة 59 من قانون 18-07، السالف الذكر، والتي تنص على أنه" يعاقب ....كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة"([3]) .

وطريقة التدليس تعني إستعمال كل وسائل الخداع والإحتيال بما فيها الكذب على الشخص المعني بالتأثير على إرادته إلى درجة أن يقتنع بصحة ما يدعيه الجاني، أما الطريقة غير النزيهة تعني مخالفة الجاني لواجباته الأخلاقية سواء أثناء ممارسته مهنته أو وظيفته أو في تعامله مع الجمهور أثناء جمع المعطيات ذات الطابع الشخصي كإستغلال النفوذ أو تقديم رشوة من أجل الحصول على تلك

---

[1]- حمي أحمد، كيسي زهيرة، مقال بعنوان صور جرائم تقنية المعلومات وفقا للإتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 10، العدد 1، أفريل 2019، ص 787.

[2]-Art 226-18 :Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, modifiè par Loi N° 2004-801 du 6 août 2004-ART 4, JORF 7 août 2004.

[3]-أنظر المادة 59 من القانون 18-07.

المعطيات([1])، إضافة إلى ذلك فأن المشرع الجزائري أشار إلى كافة الطرق الأخرى غير المشروعة في عملية جمع هذه المعطيات ليترك بذلك مجالا واسعا للقاضي الجزائي في تفسيرها.

كما أن هذه الجريمة لا تقوم إلا بتحقق القصد الجنائي العام بعنصريه العلم والإرادة، بأن يكون على علم بأن هذه المعطيات تم جمعها بطريقة غير مشروعة، وأن تتجه إرادته إلى القيام بذلك الفعل أيضا.

**2- جمع المعطيات ذات الطابع الشخصي المتعلقة بالماضي الجزائي للشخص المعني**

أن عملية الجمع في هذه الجريمة تتعلق بنوع خاص من المعطيات الشخصية وهي تلك المعطيات المتعلقة بالماضي الجزائي للشخص المعني، وهو الفعل المنصوص عليه ضمن أحكام المادة 226-19 من قانون العقوبات الفرنسي والتي تنص على أنه" يعاقب بالحبس لمدة خمس سنوات وبغرامة 200.000 فرنك، كل من قام...، كما يعاقب بذات العقوبات من يقوم في غير الحالات التي يقررها القانون بوضع أو حفظ بيانات أسمية في ذاكرة إلكترونية تتعلق بالجرائم أو أحكام الإدانة أو التدابير"([2])

ونص عليه المشرع الجزائري في المادة 68 من القانون 18-07، السالف الذكر، والتي تنص على أنه" يعاقب ...كل من قام في غير الحالات المنصوص عليها قانونا بوضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن"([3]).

---

[1]- طباش عزالدين، مرجع سابق، ص 32.

[2]- Art 226-19 : Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement,
font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle ou àl'identité de genre de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoireinformatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté, modifiè par Ordonnance N° 2018-1125 du 12 dècember 2018-ART 13.

[3]-أنظر المادة 68 من القانون 18-07.

والسلوك الإجرامي في هذه الجريمة عبر عنه المشرع الجزائري بعبارة"وضع أو حفظ" وحصر ذلك في الذاكرة الآلية فقط.

ويقصد بالوضع في هذه المادة إدراج المعطيات ذات الطابع الشخصي والمتعلقة بالماضي الجزائي للشخص المعني في سجلات معلوماتية مهما كانت طبيعتها، بحيث لا يشترط القانون أن تكون معدة خصيصا لذلك، بل قد يكون له غرض آخر وتم إدراج تلك السوابق فيه، كما لو كان هذا السجل متعلقا بتسيير هيئة المستخدمين.

أما الحفظ فيعني الإبقاء على هذا النوع من المعطيات داخل الذاكرة الآلية عن طريق تسجيلها بحيث يمكن العودة إليها في أي وقت.

وهذه الجريمة تم إستحداثها أساسا من أجل منع الخواص من إنشاء صحيفة سوابق قضائية خاصة، إذ أنها تقع بالمخالفة لأحكام المادة 10 من نفس القانون التي ذكرت على سبيل الحصر من هم المسؤولون عن المعالجة الذين يحق لهم معالجة أو جمع المعطيات الشخصية المتعلقة بالماضي الجزائي للشخص المعني تتصدرهم أساسا السلطة القضائية التي يناط بها لوحدها أنشاء صحيفة السوابق القضائية([1]).

وعليه، فإنه يحظر على الجهات الغير مخولة لها جمع هذه المعطيات معالجتها في حاسب آلي خاص مثلا، كما يجب على المشرع الجزائري أن يوسع الحظر ليشمل حتى المعلومات التي تقادمت والمتعلقة بالشخص المعني، حماية لسمعته وأعتبارا لشخصه.

**ثانيا: تجريم الإستغلال غير المشروع للمعطيات**

أن الإستغلال غير المشروع للمعطيات ذات الطابع الشخصي يتم بإرتكاب مخالفات من طرف المسؤول عن المعالجة أو غيره في مرحلة إستعمال المعالجة تؤدي إلى إحداث أضرارا بالمعطيات ذات الطابع الشخصي، وهو ما يجعلها تشكل جرائم يعاقب عليها القانون، وتتمثل في مخالفة بعض بنود التصريح بالمعالجة وإفشاء المعطيات الشخصية إلى غير المؤهلين بذلك.

[1]- طباش عزالدين، مرجع سابق، ص 33.

**1- تجريم إنتهاك بنود التصريح أو الترخيص**

أن تلقي التصريحات ومنح التراخيص المتعلقة بمعالجة المعطيات ذات الطابع الشخصي تعتبر من ضمن المهام الملقاة على عاتق السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ، لذلك فقد قام المشرع الجزائري بتجريم كل سلوك يؤذي إلى خرقهما سواء في المادة 58 من القانون 18-07، التي نصت على جريمة إستعمال المعالجة لأغراض غير تلك المصرح بها أو المرخص لها، أو في المادة 2/65 من نفس القانون، التي جرمت الإحتفاظ بالمعطيات ذات الطابع الشخصي بعد إنتهاء المدة القررة لذلك .

**أ- جريمة إستعمال المعالجة لأغراض غير تلك المصرح بها أو المرخص لها**

نص المشرع الفرنسي على جريمة إستعمال المعالجة لأغراض غير تلك المصرح بها أو المرخص لها في المادة 226-21 من قانون العقوبات الفرنسي المعدل والتي ورد فيها أنه"يعاقب بالحبس خمس سنوات وغرامة 300.000 فرنك كل من حاز بيانات أسمية بمناسبة قيامه بتسجيلها أو تصنيفها أو نقلها أو أي إجراء آخر من أوجه المعالجة إذا غير من الوجهة النهائية المقررة لهذه البيانات وفقا للقانون أ للقرار الصادر في شأنها أو في الإخطار المسبق على القيام بالمعالجة([1]).

وما يلاحظ أن المشرع الفرنسي قد رفع مدة الحبس إلى خمس سنوات ورفع قيمة الغرامة، مما يعكس إهتمامه بالحفاظ على البيانات الأسمية للأشخاص من أي إعتداء يؤدي إلى المساس بحرمة الحياة الخاصة للأفراد في حالة الإنحراف عن الغاية من المعالجة الإلكترونية لهذه البيانات([2]).

[1]-Art 226-21 :Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, modifiè par Loi N° 2004-801 du 6 août 2004-ART 4, JORF 7 août 2004.

[2] - محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، مصر، سنة 2005، ص299.

أما بالنسبة للمشرع الجزائري فنص على هذه الجريمة في المادة 58 من القانون 18-07، السالف الذكر، بقولها" يعاقب...كل من قام بإنجاز أو بإستعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص لها"([1]).

ومن تم فإنه يقتضي لقيام هذه الجريمة أن يكون المسؤول عن المعالجة قد صرح بالأغراض التي أنجزت من أجلها تلك المعالجة وصدر قبول بذلك من طرف السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو قدمت له ترخيص بذلك، ثم يقوم بتغيير في تلك الأغراض، ويوسع من نطاق تلك الأغراض لتشمل أهداف أخرى.

ويقصد بالأغراض في هذه الجريمة تلك الأهداف التي سطرها المسؤول عن المعالجة لتحقيقها عن طريق تلك المعالجة أو تحقيق الغاية من إنجازها، وهو ما يقتضي ضرورة الإلتزام بالدقة والوضوح أثناء تحديدها في التصريح خاصة إذا تعلق الأمر بنص قانوني أو تنظيمي، وفي كل الحالات يعود للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي تقدير ما إذا كان الغرض المحقق هو مجرد توسيع للأغراض المصرح بها فقط، أم أنه يشكل تحولا أو خروجا عن تلك الأغراض، في حين يقصد بإنجاز المعالجة واستعمالها لأغراض أخرى القيام بتغيير هدف وغاية المعالجة، ويكون ذلك بمثابة إنجاز معالجة جديدة تستعمل لأغراض أخرى([2]).

ب- **جريمة الإحتفاظ بالمعطيات خارج المدة المحدودة**

**نص** المشرع الفرنسي على جريمة الإحتفاظ بالمعطيات خارج المدة المحدودة في المادة 226-20 من قانون العقوبات الفرنسي المعدل والتي تعاقب عليها بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من إحتفظ بغير موافقة اللجنة المشار إليها بمعلومات على نحو أسمي مدة أكثر من المدة التي سبق طلبها أو التي تضمنها الإخطار المسبق([3]).

---

[1]-أنظر المادة 58 من القانون 18-07.

[2] - طباش عزالدين، مرجع سابق، ص 53.

[3]-Art 226-20 :Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

أما بالنسبة للمشرع الجزائري فنص على هذه الجريمة في المادة 65 الفقرة الثانية من القانون 18-07، السالف الذكر، بقولها" يعاقب بنفس العقوبة كل من قام بالإحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص"، ويتضح من خلال هذه المادة أن المشرع الجزائري جرم سلوك الإحتفاظ أو الإبقاء على المعطيات المعالجة رغم إنتهاء المدة المقررة للمعالجة وذلك تطبيقا للبند السادس من المادة 14 الذي أوجب أن يرد في التصريح مدة حفظ المعطيات، والتي تحدد من قبل المسؤول عن المعالجة نفسه، إلا أنه يمكن للسلطة الوطنية في حالة وجود مصلحة مشروعة بناء على طلب المسؤول عن المعالجة أن تأذن بحفظ المعطيات ذات الطابع الشخصي لغايات تاريخية أو إحصائية أو علمية بعد المدة المشار إليها في الفقرة هـ([1]) من نفس المادة.

ويمكن أن ترد مدة حفظ بعض المعطيات الشخصية في نص قانوني مثلما هو عليه الحال في المادة 14 من القانون 16-03 المتعلق بالبصمة الوراثية([2])، والتي أشارت إلى أن مدة حفظ المعطيات الجينية المتعلقة بالبصمة الوراثية في القاعدة الوطنية للبصمات الوراثية هي 25 سنة بالنسبة لأصول وفروع الأشخاص المفقودين، وكذا المشتبه فيهم المتابعين المستفيدين من أمر بإنتفاء وجه الدعوى أو الحكم بالبراءة نهائي، ومدة 40 سنة بالنسبة الأشخاص المحكوم عليهم والمفقودين والمتوفين مجهولي الهوية.

---

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa, modifiè par Loi N° 2004-801 du 6 août 2004-ART 4, JORF 7 août 2004.

[1]- نصت المادة 14 الفقرة هـ من القانون 18-07، السالف الذكر، على ما يلي" هـ- محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من إجلها تم جمعها ومعالجتها"

[2]- قانون رقم 16-03 مؤرخ في 19 يونيو 2016، يتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرق على الأشخاص، ج ر ج ج، ع رقم 37، صادر في 19 يونيو 2016.

**2- تجريم إفشاء المعطيات الشخصية لغير المؤهلين بذلك**

نصت المادتين 26 و40 من القانون 18-07، السالف الذكر، على ضرورة الحفاظ على الطابع السري للمعطيات ذات الطابع الشخصي من قبل رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وكذا المسؤول عن المعالجة وكافة الأشخاص الذين أطلعوا أثناء ممارسة مهامهم على هذه المعطيات حتى بعد إنتهاء مهامهم.

وإن إفشاء المعطيات ذات الطابع الشخصي يعتبر سلوك مجرم يعاقب عليه القانون، ويكون ذلك من خلال السماح للأشخاص غير المؤهلين بالولوج لهذه المعطيات، أو بإيصالها إلى غير المؤهلين لهم الإطلاع عليها.

**أ- جريمة السماح بالولوج إلى المعطيات ذات الطابع الشخصي لغير المؤهلين**

نصت المادة 60 من القانون 18-07، على جريمة السماح لغير المؤهلين بالولوج إلى المعطيات ذات الطابع الشخصي بقولها" يعاقب... كل من سمح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي" وعليه فأن هذه الجريمة تقوم من خلال سماح الأشخاص المسموح لهم الدخول إلى هذه المعطيات ذات الطابع الشخصي لأشخاص آخرين غير مؤهلين بالولوج إليها من خلال إتخاذهم أية سلوكات تعبر عن قبولهم للغير بالإطلاع على هاته المعطيات، ويتم ذلك بعدة أساليب إما بمنح كلمة المرور للدخول للنظام المعلوماتي الذي يحتوي المعالجة وإما بترك النظام مفتوحا لتسهيل الإطلاع، كما قد يتم بمنح مفتاح خزانة ملفات المعالجة غير الآلية للمعطيات، أو بعدم الإعتراض على الدخول إلى المعطيات رغم العلم بذلك، كما قد يقع أيضا بكشف التدبير التقني الذي يؤمن المعطيات من الولوج إليها([1]).

**ب- جريمة إيصال المعطيات المعالجة أو المستلمة لغير المؤهلين**

نص المشرع الفرنسي على جريمة إيصال المعطيات المعالجة أو المستلمة إلى غير المؤهلين بذلك في المادة 226-22 من قانون العقوبات الفرنسي المعدل والتي

[1]- طباش عزالدين، مرجع سابق، ص 56.

ورد فيها أنه" يعاقب بالحبس خمس سنوات وغرامة 300.00 أورو كل شخص كان قد أستقبل أو تلقى بمناسبة التسجيل أو التنصت أو النقل أو أي أجراء آخر من إجراءات المعالجة الإلكترونية بيانات أسمية من شأن إفشائها الإضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة وقام بنقلها إلى من لا حق له في العلم بها، وإذا وقع هذا الإفشاء للبيانات الأسمية بطريقة الإهمال تكون العقوبة هي الغرامة 100.000 أورو، ولا تقام الدعوى العمومية وفقا للفقرتين السابق الإشارة إليهما إلا من خلال شكوى المجني عليه أو ممثله القانوني أو من له صفة في ذلك"([1]).

أما بالنسبة للمشرع الجزائري فنص على هذه الجريمة في المادة 69 من القانون 18-07، بقولها" يعاقب...كل مسؤول عن معالجة وكل معالج من الباطن وكل شخص مكلف بالنظر إلى مهامه بمعالجة معطيات ذات طابع شخصي يتسبب أو يسهل ولو عن إهمال الإستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين بذلك"([2]).

ويتضح من خلال نص هذه المادة أن المشرع الجزائري جرم إرتكاب هذا السلوك من قبل أشخاص ذكرهم على سبيل الحصر وهم المسؤول عن المعالجة والمعالج من الباطن وكل شخص مكلف بالنظر إلى مهامه بمعالجة المعطيات ذات الطابع الشخصي، والذين يقومون بإيصال هذه المعطيات المعالجة أو المستلمة إلى غير المؤهلين لهم الوصول إليها، وبالتالي فأن هذه الجريمة تقوم بمجرد إستلام المعطيات ذات الطابع الشخصي في مرحلة الجمع دون معالجتها أو إيصالها إلى غير المؤهلين لهم الوصول إليها.

**الفرع الثاني: تجريم المخالفات المرتكبة أثناء إنشاء المعالجة**

[1] -Art 226-22 Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence, modifiè par Loi N° 2004-801 du 6 août 2004-ART 4, JORF 7 août 2004.

[2]- المادة 69 من القانون 18-07.

تعتبر مرحلة المعالجة من المراحل الأكثر تعرضا لارتكاب مخالفات عديدة تشكل جرائم معاقب عليها بمقتضى القانون 18-07، السالف الذكر، ومن أهمها مخالفة الشروط المسبقة للمعالجة وخرق الإلتزامات الملقاة على عاتق المسؤول عن المعالجة أثناء القيام بعمليات المعالجة.

**أولا: جريمة عدم إستيفاء الشروط المسبقة للمعالجة**

نص المشرع الفرنسي على جريمة عدم إستيفاء الشروط المسبقة للمعالجة في المادة 226-16 من قانون العقوبات الفرنسي المعدل والتي ورد فيها أنه"يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف أورو كل من أجرى أو طلب إجراء معالجة إلكترونية للبيانات الإسمية الشخصية دون مراعاة الشروط الواردة في القانون المشار إليه"([1]).

وأن القيام بمعالجة المعطيات ذات الطابع الشخصي لا تتم إلا بعد إستيفاء بعض الشروط المسبقة التي تضمنها القانون 18-07، والمتمثلة أساسا في الحصول على الموافقة الصريحة من الشخص المعني بتلك المعطيات أو عدم صدور إعتراض منه، بالإضافة إلى القيام ببعض الإجراءات الشكلية أمام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي والمتمثلة في التصريح والترخيص، وإن مخالفة هذه الشروط سيؤدي لا محال إلى قيام الجريمتين المنصوص عليهما في المادة 55 و56 من هذا القانون([2]).

ومن أجل تفعيل الإلتزام بضرورة الحصول على رضا الشخص المعني فقد جرم المشرع الجزائري فعل القيام بالمعالجة دون الحصول على موافقته، وكذا في حالة ما إذا عبر عن رفضه بشكل صريح بأن يقدم إعتراضا على تلك المعالجة، شريطة أن يكون حق الإعتراض مبنيا على أسباب مشروعة، إلا أنه تم وضع إستثناءات لبعض الحالات الواردة في المادة 18 من نفس القانون، والتي يمكن بسببها معالجة معطيات

[1]- Art 226-16 : Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du III de l'article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiè par Ordonnance N° 2018-1125 du 12 dècember 2018-ART 13.

[2]- أنظر المادتين 55 و56 من القانون 18-07.

حساسة([1]) دون الحصول على الموافقة بشرط أن ترخص بذلك السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وذلك عندما يتعلق الأمر بالمصلحة العامة وتكون ضرورية لضمان ممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة، أو عندما تتم المعالجة بناء على الموافقة الصريحة للشخص المعني، وفي حالة وجود نص قانوني يقضي بذلك أو بترخيص من السلطة الوطنية، كما يمكن لهذه الأخيرة منح تراخيص أخرى في الحالات الآتية:

أ)- إذا كانت المعالجة ضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص آخر وفي حالة وجود الشخص المعني في حالة عجز بدني أو قانوني عن الإدلاء بموافقته.

ب)- تنفيذ المعالجة بناء على موافقة الشخص المعني....

ج)- إذا كانت المعالجة تخص معطيات صرح بها الشخص المعني علنا...

د)- أن المعالجة ضرورية للإعتراف بحق أو ممارسته أو الدفاع عنه أمام القضاء وأن تكون قد تمت حصريا لهذه الغاية.

هـ)- معالجة المعطيات الجينية، بإستثناء تلك التي يقوم بها أطباء أو بيولوجيون والتي تعد ضرورية لممارسة الطب الوقائي..."([2]).

وتجدر الإشارة إلى أن المشرع الجزائري أعتبر المعطيات الجينية هي كل المعطيات المتعلقة بالصفات الوراثية لشخص أو عدد من الأشخاص ذوي قرابة، بل وإعتبرها من المعطيات الشخصية الحساسة حسب المادة الثالثة من قانون حماية المعطيات ذات الطابع الشخصي نظرا لإمكانية الإستغلال العلمي والإقتصادي لها من دون رضا الفرد.

**ثانيا: تجريم خرق الإلتزامات الواقعة عن المسؤول عن المعالجة**

أن المشرع الجزائري وضع عدة إلتزامات على كل من أراد معالجة المعطيات الشخصية ورتب على مخالفتها قيام عدة جرائم معاقب عليها في القانون 18-07،

---

[1]- عرفت المادة 3 الفقرة 6 من القانون 18-07، السالف الذكر، المعطيات الحساسة بإنها" معطيات ذات طابع شخصي تبين الأصل العرفي أو الأثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الإنتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية"

[2]- المادة 18 من القانون 18-07.

سواء تعلق الأمر ببعض الحقوق الممنوحة للأشخاص المعنيين بالمعالجة أو بضمان سرية وأمن وسلامة المعالجة أو بضمان التواصل مع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

**أ- جريمة عدم الإعتراف بحقوق الشخص المعني بالمعالجة:** نصت المادة 64 من القانون 18-07 على هاته الحقوق التي يشكل رفض الإعتراف بها دون سبب مشروع من طرف المسؤول عن المعالجة وذلك بمخالفة الإلتزام بضمانها، جريمة يعاقب عليها القانون، وهذه الحقوق تتمثل في حقوق الإعلام أو الولوج أو التصحيح أو الإعتراض المنصوص عليها في المواد 32، و34 و35 و36 من هذا القانون.

والإعتراف بهذه الحقوق يمنح الشخص المعني حق الإطلاع المباشر على كل ما يجري بخصوص المعالجة المتعلقة بمعطياته الشخصية، لذلك فهي تعتبر وسيلة منحها له المشرع الجزائري لممارسة رقابة حقيقية إلى جانب السلطة الوطنية([1]).

**ب- جريمة عدم الإلتزام بسرية وسلامة المعالجة للمعطيات ذات الطابع الشخصي:** نصت المواد 38،39، و40،41 من القانون 18-07 على عدة إلتزامات تقع على عاتق المسؤول عن المعالجة تتعلق بسرية وسلامة المعالجة، وتتمثل فيما يلي:

- أن يقوم المسؤول عن المعالجة بوضع التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين.

- أن يقوم المسؤول عن المعالجة بإختيار معالج من الباطن ليقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها ويسهر على إحترامها، وذلك عندما تجرى المعالجة لحسابه.

- أن يلتزم المسؤول عن المعالجة رفقة الأشخاص الذين أطلعوا أثناء ممارسة مهامهم على معطيات ذات طابع شخصي بالسر المهني حتى بعد إنتهاء مهامهم.

- لا يجوز لأي شخص يعمل تحت سلطة المسؤول عن المعالجة أو تحت سلطة المعالج من الباطن، والذي يمكنه الولوج إلى هذه المعطيات، أن يعالج هذه المعطيات إلا بموجب تعليمات صادرة عنه، بإستثناء حالة تنفيذ إلتزام قانوني.

---

1- طباش عزالدين، مرجع سابق، ص 44.

وأن خرق الإلتزامات المنصوص عليها في المادتين 38 و39 من هذا القانون يشكل جريمة معاقب عليها بموجب المادة 65 من القانون 18-07.

**ج- جريمة عرقلة عمل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:**

يمكن للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي القيام بإجراء عملية التحقيق في عين المكان، والحصول على المعلومات الصحيحة والوثائق الضرورية المتعلقة بالمعطيات الشخصية ، وفي سبيل ذلك فقد نصت المادة 61 من القانون 18-07، السالف الذكر، على هذه الأفعال ، والتي تشكل مخالفتها عرقلة لعمل السلطة الوطنية، وتعد جريمة معاقب عليها، والمتمثلة فيما يلي:

1- الإعتراض على إجراء عملية التحقيق في عين المكان.

2- رفض تزويد أعضاء السلطة الوطنية أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف هذه السلطة أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة.

3- إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح.

كما أن إمتناع مقدم الخدمات عن إعلام السلطة الوطنية لحماية المعطيات الشخصية عن كل الإنتهاكات المتعلقة بالمعطيات الشخصية في مجال الإتصالات الإلكترونية خلافا لأحكام المادة 43 من هذا القانون([1])، يشكل خرقا لهذا الإلتزام، ويعد جريمة معاقب عليها بموجب المادة 66 من نفس القانون.

**المطلب الثاني: آليات الحماية الجنائية للمعطيات ذات الطابع الشخصي**

تضمن القانون 18-07، مجموعة من القواعد المتعلقة بحماية المعطيات ذات الطابع الشخصي، وذلك ضمانا لحق الأفراد في معالجة معطياتهم الشخصية دون وجود أية مخاطر تهدد حياتهم الخاصة من خلال وضع مجموعة من الآليات

[1]- نصت المادة 43 من القانون 18-07، السالف الذكر، على ما يلي" إذا أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الإتصالات الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، يعلم مقدم الخدمات فورا السلطة الوطنية والشخص المعني، إذا أدى ذلك إلى المساس بحياته الخاصة، مالم تقرر السلطة الوطنية أن الضمانات الضرورية لحماية المعطيات قد تم إتخاذها من قبل مقدم الخدمات..."

لحمايتها وصونها، الأمر الذي أستدعى من الدولة التدخل بداية بإقرارها لهذا الحق في المادة 47([1]) من الدستور الجزائري الحالي التي تنص على أن" ...حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يعاقب على إنتهاكه"، ثم قام بسن مجموعة من المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي(الفرع الأول) نص عليها في الباب الثاني من القانون 18-07، السالف الذكر، والتي تعنى بتوفير الحماية لهذه المعطيات ، وكذا إنشائه هيئة خاصة لحماية المعطيات الشخصية لتساهم إلى جانب السلطة القضائية في الحماية الجنائية للمعطيات الشخصية تمثلت في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (الفرع الثاني)، إضافة إلى إقراره في نفس القانون عقوبات زجرية لردع الإعتداءات التي تطال هذه المعطيات(الفرع الثالث) نص عليها في الفصل الثالث من الباب السادس بعنوان الأحكام الجزائية.

**الفرع الأول: المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي**

أن المشرع الجزائري نص على مجموعة من المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي في القانون 18-07، المذكور سالفا، وذلك قبل معالجتها من طرف الأشخاص المسؤولين عن عملية المعالجة، وتتمثل في الموافقة المسبقة للشخص المعني، بتفعيل حمايتها من طرف ذات الشخص التي تكون هذه المعطيات موضوع المعالجة متعلقة به، وكذلك الإجراءات المسبقة عن المعالجة وهي التصريح والترخيص، والتي تخضع لها كل عملية معالجة لهذه المعطيات،

**أولا: الموافقة المسبقة للشخص المعني**

يقصد بالشخص المعني في المادة الثالثة(3) من أحكام هذا القانون "كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع المعالجة"، وأشار المشرع الجزائري في المادة 7 من أحكام هذا القانون([2])، والتي تقابلها المادة 4([1])

[1]- المادة 47 من المرسوم الرئاسي رقم 20-442.

[2]- عبارة هذا القانون في صلب الدراسة تعني القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

من القانون المغربي والمادة 4([2]) من القانون القطري، إلى تجسيد حماية المعطيات ذات الطابع الشخصي من طرف الشخص المعني، باشتراطه لمبدأ أساسي تمثل في الموافقة المسبقة للشخص المعني على معالجة معطياته الشخصية، والتي لا تتم إلا بناء على موافقته الصريحة، ويمكنه التراجع عنها في أي وقت ما، أما إذا كان هذا الأخير عديم أو ناقص الأهلية فتخضع هذه الموافقة للقواعد العامة المنصوص عليها في القانون العام.

ولا يمكن للغير الإطلاع على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة إلا من أجل إنجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة والمرسل إليه وبعد الموافقة المسبقة للشخص المعني،

وقد لا تكون هذه الموافقة واجبة في بعض الحالات التي ذكرها المشرع على سبيل الحصر في هذه المادة، وتعتبر فيها المعالجة ضرورية متى تعلق الأمر ب:

- إحترام إلتزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة.
- حماية حياة الشخص المعني.
- تنفيذ عقد يكون فيه الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد إتخذت بناء على طلبه.
- الحفاظ على مصالح حيوية للشخص المعني إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه.
- تنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم إطلاعه على المعطيات.

---

[2]- تنص المادة 4 من القانون المغربي رقم 08-09، السالف الذكر، على أنه" لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا إذا كان الشخص المعني قد عبر عن رضاه عن العملية أو مجموع العمليات المجمع إنجازها..."

[2]- تنص المادة 4 من القانون القطري رقم 13 لسنة 2016، السالف الذكر، على أنه" لا يجوز للمراقب معالجة البيانات الشخصية ، إلا بعد الحصول على موافقة الفرد، ما لم تكن المعالجة ضرورية لتحقيق غرض مشروع للمراقب أو الغير الذي ترسل إليه البيانات"

- تحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و/أو حقوقه وحرياته الأساسية.

أما بالنسبة للمعطيات ذات الطابع الشخصي المتعلقة بالأطفال لا يمكن القيام بمعالجتها إلا بعد الحصول على على موافقة ممثله الشرعي أو عند الإقتضاء بترخيص من القاضي المختص الذي يمكنه معالجتها دون موافقة ممثله الشرعي إذا أستدعت المصلحة الفضلى للطفل ذلك، أو العدول عن ترخيصه في أي وقت، طبقا لأحكام المادة 8 من نفس القانون([1]).

وأشترط المشرع الجزائري في المادة 9 من هذا القانون أن تكون هذه المعطيات الشخصية معالجة بطريقة مشروعة ونزيهة ومجمعة لغايات واضحة ومحددة ومشروعة وملائمة ومناسبة وغير مبالغ فيها وكذلك تكون صحيحة وكاملة ومحينة إذا إقتضى الأمر إضافة إلى حفظها بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها.

غير أن هناك فئة من المعطيات ذات الطابع الشخصي المتعلقة بالجرائم والعقوبات وتدابير الأمن لا يمكن القيام بمعالجتها إلا من قبل السلطة القضائية والسلطات العمومية والأشخاص المعنويين الذين يسيرون مصلحة عمومية، ومساعدي العدالة([2]) في إطار إختصاصاتهم القانونية، وذلك طبقا لأحكام المادة 10 من هذا القانون.

**ثانيا: الإجراءات المسبقة عن المعالجة**

تخضع كل عملية معالجة لمعطيات ذات طابع شخصي لإجراءات مسبقة عن عملية المعالجة، وتتمثل في تقديم تصريح مسبق لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو الحصول على ترخيص منها، وهذه الأخيرة هي التي تقوم بتجسيد هذه الإجراءات لذلك سنقوم بمعالجتها بعد التطرق لإجرائي التصريح والترخيص.

---

[1] - المادة 8 من القانون رقم 18-07.

[2] - أضاف المشرع المغربي الهيئة المكلفة بحماية حقوق المؤلف والحقوق المجاورة بموجب المادة 49 من 08-09، السالف الذكر.

**1- التصريح:** يودع طلب التصريح المسبق([1]) الذي يتضمن الإلتزام بإجراء المعالجة وفقا لأحكام هذا القانون لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، ويمكن تقديمه بالطريق الإلكتروني، مقابل تسليم وصل الإيداع أو يرسل بالطريق الإلكتروني فورا أو في أجل أقصاه 48 ساعة، بحيث يمكن للمسؤول عن المعالجة وبمجرد إستلامه الوصل وتحت مسؤوليته مباشرة عملية المعالجة، طبقا لأحكام المادة 13 من هذا القانون.

ويتضمن هذا التصريح حسب نص المادة 14 من القانون نفسه أسم وعنوان المسؤول عن المعالجة وطبيعة المعالجة وخصائصها ووصف فئات الأشخاص المعنيين وفئات المعطيات ذات الطابع الشخصي وفئات المرسل إليهم الذين قد توصل إليهم المعطيات، وطبيعة هذه المعطيات المعتزم إرسالها إلى دولة أجنبية، ومدة حفظها، والمصلحة التي يمكن للشخص المعني عند الإقتضاء أن يمارس لديها الحقوق المخولة له بمقتضى أحكام هذا القانون، وكذا كل وصف عام يمكن من تقييم أولي لمدى ملائمة التدابير المتخذة من أجل ضمان سرية وأمن المعالجة، إضافة إلى الربط البيني أو جميع أشكال التقريب الأخرى بين المعطيات، والتنازل عنها للغير أو معالجتها من الباطن، تحت أي شكل من الأشكال سواء مجانا أو بمقابل.

ولا تطبق إلزامية التصريح على المعالجات التي يكون الغرض منها فقط مسك سجل مفتوح ليطلع عليه الجمهور أو كل شخص يثبت أن له مصلحة مشروعة في ذلك، إلا أنه في هذه الحالات يجب تعيين مسؤول عن معالجة المعطيات يكشف عن هويته للعموم وتبلغ إلى السلطة الوطنية، ويكون مسؤولا عن تطبيق الأحكام المتعلقة بحقوق الأشخاص المعنيين المنصوص عليها في هذا القانون، وهذا طبقا لأحكام للمادة 16 من نفس القانون.

**2- الترخيص:** تخضع المعالجة لنظام ترخيص مسبق([2])، عندما يتبين للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أثناء دراستها للتصريح المقدم لها، أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة على إحترام وحماية الحياة

[1]- أشار المشرع المغربي إلى التصريح المسبق في المادة 13 من 08-09، السالف الذكر.

[2]- أشار إليه المشرع المغربي بمصطلح الإذن المسبق في المادة 21 من القانون 08-09، السالف الذكر.

الخاصة والحريات والحقوق الأساسية للأشخاص، وذلك وفقا لأحكام المادة 17 من هذا القانون.

وفي الأصل تمنع معالجة المعطيات الحساسة([1]) التي تبين الأصل العرقي أو الأثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الإنتماء النقابي للشخص المعني أو المتعلقة بصحته، إلا أنه يمكن للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي الترخيص بمعالجة هذه المعطيات لأسباب تتعلق بالمصلحة العامة وتكون ضرورية لضمان ممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة، أو عندما تتم المعالجة بناء على الموافقة الصريحة للشخص المعني، وفي حالة وجود نص قانوني يقضي بذلك أو بترخيص من السلطة الوطنية، كما يمكن لهذه الأخيرة منح تراخيص أخرى وفقا لأحكام المادة 18 من نفس القانون، والمشار لها أعلاه في جريمة عدم إستيفاء الشروط المسبقة للمعالجة.

ويجب أن يتضمن طلب الترخيص نفس المعلومات التي يتضمنها التصريح والمذكورة في المادة 14 من هذا القانون، وعلى السلطة الوطنية لحماية ذات الطابع الشخصي أن تتخذ قرارها في أجل شهرين من تاريخ إخطارها، ويمكنها تمديد هذا الأجل لنفس المدة بقرار مسبب لرئيسها، وفي حالة عدم ردها على هذا الطلب خلال الأجل المذكور فأن ذلك يعتبر بمثابة رفضا له حسب نص المادة 20 من هذا القانون.

كما يمكن لهذه السلطة الوطنية أن ترخص بمعالجة المعطيات ذات الطابع الشخصي التي تهدف إلى تحقيق مصلحة عامة للبحث أو الدراسة أو التقييم في مجال الصحة، في إطار إحترام المبادئ المنصوص عليها في هذا القانون، وبالنظر للمصلحة العامة التي يهدف إلى تحقيقها البحث أو الدراسة أو التقييم، وذلك طبقا لأحكام الفقرة الأولى من المادة 21 من نفس القانون.

[1]- يطلق عليها المشرع القطري مصطلح البيانات الشخصية ذات الطبيعة الخاصة في المادة 16 من القانون القطري رقم 13 لسنة 2016، السالف الذكر، والتي أشارت إلى أنه يمكن للوزير إضافة أصنافا أخرى من البيانات الشخصية ذات الطبيعة الخاصة إذا كان من شأن سواء إستخدامها أو إفشائها إلحاق ضرر جسيم بالفرد.

**الفرع الثاني:السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**

أنشئت العديد من الدول هيئات مستقلة مهمتها مرقبة وحماية الأفراد وبياناتهم الشخصية إتجاه الإستعمال غير المشروع وغير القانوني كاللجنة القومية للمعلومات والحريات في فرنسا، ونظام المفوض في ألمانيا([1])، واللجنة الوطنية لحماية مراقبة المعطيات ذات الطابع الشخصي في المغرب([2])، بموجب المادة 27 من القانون الصادر في 18 فبراير 2009، المذكور سابقا، والهيئة الوطنية لحماية المعطيات الشخصية في التشريع التونسي بموجب الفصل 75 من الباب السادس من القانون الأساسي عدد 63 لسنة 2004، السالف الذكر التي أصدرت مؤخرا مجموعة من النصوص المتعلقة بحماية المعطيات الشخصية بتاريخ 28 جانفي 2019.

أما في الجزائر تم مؤخرا النص على إحداث هذه السلطة في القانون 18-07، السالف الذكر، تحت مسمى "السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي" كآلية مؤسساتية تكلف بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي، وتضمن عدم إنطواء إستعمال تكنولوجيات الإعلام والإتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة، وذلك طبقا لأحكام الفقرة الأولى من المادة 25 من هذا القانون.

وتنشأ هذه السلطة لدى رئيس الجمهورية باعتبارها سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي تتمتع بالشخصية المعنوية والإستقلال المالي والإداري، مقرها بالجزائر العاصمة، وهذا طبقا لأحكام المادة 22 من القانون 18-07، السالف الذكر، كما نصت المادة 23 من نفس القانون على تشكيلة هذه السلطة، والتي تتشكل من:

- ثلاث(3) شخصيات، من بينهم الرئيس، يختارهم رئيس الجمهورية من بين ذوي الإختصاص في مجال عمل السلطة الوطنية.

---

[1]- عائشة بن قارة مصطفى، مقال بعنوان ضرورة آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم(18-07)، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 10، العدد 01، أفريل 2019، ص 748.

[2]- بن زيطة عبد الهادي، مقال بعنوان ضرورة إنشاء سلطة إدارية مستقلة كآلية للحماية القانونية للبيانات الشخصية في مواجهة إستخدامات المعلوماتية، مجلة الحقيقة، العدد 39، سنة 2017، ص 71.

- ثلاثة(3) قضاة، يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.

- عضو من كل غرفة من البرلمان يتم إختياره من قبل رئيس كل غرفة، بعد التشاور مع رؤساء المجموعات البرلمانية.

- ممثل واحد(1) عن كل من: المجلس الوطني لحقوق الأنسان، وزير الدفاع الوطني، وزير الشؤون الخارجية، الوزير المكلف بالداخلية، وزير العدل، حافظ الأختام، الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة، الوزير المكلف بالصحة، وزير العمل والتشغيل والضمان الإجتماعي.

ويعين رئيس الجمهورية أعضاء هذه السلطة ورئيسها بموجب مرسوم رئاسي، لعهدة مدتها خمس(5) سنوات، قابلة للتجديد، والذين يتم أختيارهم حسب إختصاصهم القانوني و/أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي، ويلزمون بأداء اليمين القانونية قبل التنصيب في وظائفهم أمام مجلس قضاء الجزائر، طبقا لأحكام المادة 24 من نفس القانون، كما يمكن لهذه السلطة أيضا الإستعانة بأي شخص مؤهل من شأنه مساعدتها في أشغالها،

وحددت المادة 25 من القانون نفسه جملة من المهام التي تضطلع بها السلطة الوطنية في مجال حماية المعطيات ذات الطابع الشخصي، وتتمثل في ما يلي:

1- منح التراخيص وتلقي المتعلقة بمعالجة المعطيات ذات الطابع الشخصي، والتي تعد بمثابة إجراءات مسبقة عن المعالجة نص عليه المشرع الجزائري في المواد من 12 إلى 22 من هذا القانون.

2- إعلام الأشخاص المعنيين بحقوقهم المنصوص عليها في الباب الرابع من هذا القانون بموجب المواد من 32 إلى 37، والمسؤولين عن المعالجة بوواجباتهم المشار لها في الباب الخامس بموجب المواد من 38 إلى 45 من نفس القانون.

3- تقديم الإستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.

4- تلقي الإحتجاجات والطعون والشكاوي بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.

5- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في المادتين 44 و45 من هذا القانون.

6- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.

7- الأمر بإغلاق معطيات أو سحبها أو إتلافها.

8- تقديم أي أقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.

9- نشر التراخيص الممنوحة والآراء المدلي بها في السجل الوطني المشار إليه في المادة 28 من هذا القانون.

10- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مرعاة مبدأ المعاملة بالمثل.

11- إصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون.

12- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.

13- وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

وضمن إطار ممارسة هذه السلطة لمهامها فإنها تعلم النائب العام المختص فورا في حالة معاينتها لوقائع تحتمل الوصف الجزائي وتعد تقريرا سنويا حول نشاطها ترفعه إلى رئيس الجمهورية، وتلتزم بالمحافظة على الطابع السري([1]) للمعطيات ذات الطابع الشخصي والمعلومات التي يطلع عليها رئيس السلطة وأعضائها بموجب هذه الصفة الممنوحة لهم، حتى ولو بعد إنتهاء مهامهم، ما لم يوجد نص قانون يقضي بخلاف ذلك، والذين تم منعهم من طرف المشرع من إمتلاك أية مصالح سواء بصفة مباشرة أوغير مباشرة في المؤسسات التي تمارس نشاطاتها في مجال معالجة المعطيات ذات الطابع الشخصي، وفي مقابل ذلك فإنهم يستفيدون من حماية الدولة

[1]- تناول المشرع الجزائري الأحكام الخاصة بإفشاء السر المهني في المواد من 301 إلى 303 من الأمر رقم 66-156 المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات الجزائري المعدل والمتتم.

ضد أي تهديدات أو إهانات أو إعتداءات من أي طبيعة كانت، قد تعرضوا لها خلال تأدية مهامهم أو بمناسبتها أوبسببها، وذلك حسب نص المادة 26 من نفس القانون.

وفي الجانب التنظيمي للسلطة الوطنية نص المشرع في المادة 27 من القانون نفسه، على تزويدها بأمانة تنفيذية يسيرها أمين تنفيذي ويساعده في مهامه مستخدمون يؤدون اليمين القانونية أمام مجلس قضاء الجزائر ويلزمون بالحفاظ على سرية المعلومات التي يطلعون عليها أثناء أو بمناسبة ممارسة مهامهم، وإلى جانب ذلك نصت المادة 28 منه، على إنشاء سجل وطني لحماية المعطيات ذات الطابع الشخصي يمسك من طرف السلطة الوطنية، وتقيد فيه هوية الشخص المسؤول عن المعالجة والملفات التي تكون السلطات العمومية والخواص مسؤولين عن معالجتها ومراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة إحداث ملفات عمومية وكذا التصريحات المقدمة للسلطة الوطنية والتراخيص التي تسلمها والمعطيات المتعلقة بالملفات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم المنصوص عليها في هذا القانون.

ويمكن للسلطة الوطنية أن تحدد بموجب أنظمة الشروط والضمانات المرتبطة بحقوق الشخص المعني في المجالات المتعلقة بحرية التعبير والصحة والشغل والبحث التاريخي والإحصائي والعلمي والمراقبة عن بعد واستعمال تكنولوجيات الإعلام والإتصال بالتنسيق مع القطاعات المعنية، طبقا لأحكام المادة 29 من هذا القانون، كما يمكن لهذه السلطة حسب نص المادة 30 من القانون نفسه أن تقرر تأمين الإرسال، لاسيما عن طريق تشفيره، في حالة ما إذا كان سير المعطيات ذات الطابع الشخصي في الشبكة، ويمكن أن يحتوي على مخاطر على حقوق الأشخاص المعنيين وحرياتهم والضمانات الممنوحة لهم.

وعليه يمكن القول أن السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي تعد آلية فعالة في حماية المعطيات ذات الطابع الشخصي من خلال ضمانات معالجتها في الإطار القانوني، وتساهم إلى جانب السلطة القضائية في حماية هذا النوع من المعطيات.

كما تجدر الإشارة في الأخير إلى عدم صدور النص الخاص الذي يحدد القانون الأساسي لمستخدمي السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي لحد الآن.

**الفرع الثالث: العقوبات المقررة لجرائم المعطيات ذات الطابع الشخصي**

قرر المشرع الفرنسي في قانون العقوبات حماية لخمسة أنواع من الجرائم بشان المعالجة الإلكترونية للبيانات الإسمية والتي تتمثل في جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص المادة 226-19 وجريمة التسجيل غير المشروع للبيانات الإسمية المادتين 226-17 و226-19 وجريمة الحفظ غير المشروع للبيانات الإسمية 226-20 وجريمة الإنحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الإسمية 226-21 وجريمة الإفشاء غير المشروع للبيانات المادة 226-22.

أما بالنسبة للمشرع الجزائري فقد أقر في القانون 18-07، السالف الذكر، مجموعة من العقوبات نص عليها في الفصل الثالث من الباب السادس بعنوان أحكام جزائية، لردع تلك الإعتداءات التي تطال المعطيات ذات الطابع الشخصي، وتشكل جرائم تمس بها، والتي ترتكب إما أثناء عملية جمعها واستغلالها أو أثناء عملية إنشائها والتصرف فيها.

**أولا: العقوبات المقرر للجمع والإستغلال غير المشروع للمعطيات ذات الطابع الشخصي**

تتضمن عمليتي الجمع والإستغلال غير المشروعين للمعطيات ذات الطابع الشخصي عدة صور مخالفة لأحكامهما، المنصوص عليها في القانون 18-07، السالف الذكر، فتتم عملية جمع المعطيات ذات الطابع الشخصي بطريقة غير مشروعة باستعمال أساليب غير مشروعة في جمع هذه المعطيات أو بجمع معطيات شخصية متعلقة بالماضي الجزائي للشخص المعني، أما إستغلال هذه المعطيات بطريقة غير مشروعة فتكون بمخالفة بعض بنود التصريح بالمعالجة أو الترخيص أو إفشاء المعطيات ذات الطابع الشخصي إلى غير المؤهلين بذلك.

**1- العقوبات المقرر للجمع غير المشروع للمعطيات ذات الطابع الشخصي**

أن الجمع غير المشروع للمعطيات ذات الطابع الشخصي يعني مخالفة أحكام جمع هذه المعطيات بطرق أخرى غير منصوص عليها قانونا، والتي تكون باستعمال أساليب غير مشروعة في جمع هذه المعطيات أو بجمع معطيات شخصية متعلقة بالوضعية الجزائية للشخص المعني

**أ- عقوبة أستعمال أساليب غير مشروعة في جمع المعطيات ذات الطابع الشخصي**: وهي الفعل المعاقب عليها في المادة 226 الفقرة 18 من قانون العقوبات الفرنسي، والتي تنص على ما يلي:" الحبس خمس سنوات وغرامة 300.00 فرنك كعقوبة لجمع معلومات إسمية بطريقة التدليس أو الخديعة أو أي طريق غير مشروع أو إجراء معالجة لمعلومات أسمية تتعلق بشخص طبيعي رغم معارضة هذا الشخص متى كانت المعارضة تقوم على أسباب مشروعة"([1]).

ونص المشرع المغربي على عقوبة هذه الجريمة في المادة 54 من القانون08-09، السالف الذكر، والتي نصت على أنه" يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 20.000 درهم إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط، كل من قام بخرق أحكام أ) وب) وج) من المادة 3 من هذا القانون بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة، أو أنجز معالجة لأغراض أخرى غير تلك المصرح بها أو المرخص لها..." ([2]).

أما بالنسبة للمشرع الجزائري فنص على عقوبة هذه الجريمة في المادة 59 من قانون 18-07، التي تنص على أنه" يعاقب بالحبس من سنة(1) إلى ثلاث (3) سنوات وبغرامة من 10.000 دج ألى 300.000 دج، كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة"([3]).

وما يلاحظ على هذه المادة أن المشرع الجزائري إستعمل مصطلح "طريقة غير مشروعة" بالإضافة إلى مصطلح "طريقة تدليسية وغير نزيهة" ، بحيث أن هذا

---

[1]-Art 226-18 :Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, modifiè par Loi N° 2004-801 du 6 août 2004-ART 4, JORF 7 août 2004.

[2]- المادة 54 من قانون رقم 08-09.

[3]- المادة 59 من القانون رقم 18-07.

المصطلح "طريقة غير المشروعة" وحده كافي ليشمل الطريقتين التدليسية وغير نزيهة بالإضافة إلى طرق أخرى كالحصول عليها عن طريق الدخول غير المشروع لنظام المعالجة الآلية للمعطيات.

ب- **عقوبة جمع المعطيات الشخصية المتعلقة بالوضعية الجزائية للشخص المعني**: وهي الجريمة المعاقب عليها في المادة 226-19 من قانون العقوبات الفرنسي والتي تنص على أنه" يعاقب بالحبس لمدة خمس سنوات وبغرامة 300.000 أورو، كل من قام...، كما يعاقب بذات العقوبات من يقوم في غير الحالات التي يقررها القانون بوضع أو حفظ بيانات أسمية في ذاكرة إلكترونية تتعلق بالجرائم أو أحكام الإدانة أو التدابير"([1])

كما نص المشرع المغربي على عقوبة هذه الجريمة في المادة 57 الفقرة الثانية منها، من القانون 08-09، والتي تنص على أنه" ...يعاقب بنفس العقوبات كل من قام بمعالجة معطيات ذات طابع شخصي متعلقة بمخالفات أو إدانات أو تدابير وقائية"، والعقوبة المقررة لهذا الفعل هي العقوبة نفسها المقررة للمعطيات الحساسة، والمتمثلة في الحبس من 6 أشهر إلى سنتين وبغرامة من 50.000 درهم إلى 300.000 درهم أو بإحدى هاتين العقوبتين فقط([2])، إضافة إلى المشرع التونسي الذي نص على عقوبة هذه الجريمة في الفصل 87، بقوله" يعاقب بالسجن مدة عامين وبخطية قدرها عشرة الآف دينار كل من خالف أحكام الفصل 13..."([3]).

أما بالنسبة للمشرع الجزائري فقد نص على عقوبة هذه الجريمة في المادة 68 من قانون 18-07، والتي نصت على ما يلي" يعاقب بالحبس من ستة أشهر(6) إلى ثلاث (3) سنوات وبغرامة من 60.000 دج ألى 300.000 دج، كل من قام في

---

[1]- Art 226-19 : Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement,
font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle ou àl'identité de genre de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoireinformatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté, modifiè par Ordonnance N° 2018-1125 du 12 dècember 2018-ART 13.

[2]-المادة 2/57 من القانون رقم 08-09.

[3]-الفصل 13 من القانون الأساسي التونسي عدد 63 لسنة 2004.

غير الحالات المنصوص عليها قانونا بوضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن"([1]).

**2- العقوبات المقررة للإستغلال غير المشروع للمعطيات ذات الطابع الشخصي**

أن الإستغلال غير المشروع للمعطيات ذات الطابع الشخصي يكون من المسؤول عن المعالجة أو غيره بارتكابه مجموعة من المخالفات تؤدي إلى الإضرار بهذه المعطيات، الأمر الذي يجعلها ترتقي إلى جرائم معاقب عليها، وتتمثل إما في مخالفة بعض بنود التصريح بالمعالجة أو الترخيص أو إفشاء المعطيات ذات الطابع الشخصي إلى غير المؤهلين بذلك.

**أ- عقوبة إنتهاك بنود التصريح أو الترخيص**

جرم المشرع الجزائري كل سلوك يؤدي إلى خرقهما سواء باستعمال المعالجة لأغراض أخرى غير تلك المصرح بها أو المرخص لها في المادة 58 من القانون 18-07، أو بالإحتفاظ بالمعطيات ذات الطابع الشخصي بعد إنتهاء المدة المقررة لذلك في المادة 2/65 من نفس القانون.

**1- عقوبة إستعمال المعالجة لأغراض غير تلك المصرح بها أو المرخص لها:**

وهي الجريمة المعاقب عليها في المادة 226-21 من قانون العقوبات الفرنسي المعدل والتي ورد فيها أنه"يعاقب بالحبس خمس سنوات وغرامة 300.000 فرنك كل من حاز بيانات أسمية بمناسبة قيامه بتسجيلها أو تصنيفها أو نقلها أو أي إجراء آخر من أوجه المعالجة إذا غير من الوجهة النهائية المقررة لهذه البيانات وفقا للقانون أ للقرار الصادر في شأنها أو في الإخطار المسبق على القيام بالمعالجة([2]).

ونص المشرع المغربي على عقوبة هذا الجريمة في المادة 54 من القانون 08-09، والتي تنص على أنه" يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 20.000 درهم إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط، كل من قام

[1]- المادة 68 من القانون 18-07.

[2]-Art 226-21 :Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, modifiè par Loi N° 2004-801 du 6 août 2004-ART 4, JORF 7 août 2004.

... أو أخضع المعطيات المذكورة لمعالجة لاحقة متعارضة مع الأغراض المصرح بها أو المرخص لها"([1]).

أما بالنسبة للمشرع الجزائري فنص على عقوبة هذه الجريمة في المادة 58 من القانون 18-07، والتي نصت على أنه" يعاقب بالحبس من ستة أشهر(6) إلى سنة (1) سنوات وبغرامة من 60.000 دج ألى 100.000 دج أو بإحدى العقوبتين فقط، كل من قام بإنجاز أو باستعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص لها "([2]).

والملاحظ أن المشرع الفرنسي قد شدد عقوبة الحبس والغرامة لما تمثله هذه الجريمة من إعتداء جسيم على خصوصية المعطيات الشخصية للأفراد عكس المشرعين المغربي والجزائري.

**2- عقوبة الإحتفاظ بالمعطيات ذات الطابع الشخصي خارج المدة المحددة لها:**

وهي الجريمة المعاقب عليها في المادة 226-20 من قانون العقوبات الفرنسي المعدل والتي تعاقب عليها بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من إحتفظ بغير موافقة اللجنة المشار إليها بمعلومات على نحو أسمي مدة أكثر من المدة التي سبق طلبها أو التي تضمنها الإخطار المسبق([3]).

ونص المشرع المغربي على عقوبة هذا الجريمة في المادة 55 من القانون 08-09، والتي تنص على أنه" يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 20.000 درهم إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط، - كل من إحتفظ بمعطيات ذات طابع شخصي لمدة تزيد عن المدة المنصوص عليها في

---

1- المادة 54 من القانون رقم 08-09.

2- المادة 58 من القانون 18-07.

3-Art 226-20 :Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa, modifiè par Loi N° 2004-801 du 6 août 2004-ART 4, JORF 7 août 2004.

النصوص التشريعية الجاري بها العمل أو المنصوص عليها في التصريح أو الإذن.-...

- يعاقب بنفس العقوبات كل من قام للأغراض أخرى غير تاريخية أو إحصائية أو علمية بمعالجة معطيات ذات طابع شخصي يتم الإحتفاظ بها بعد المدة المنصوص عليها في الفقرة الأولى"([1]).

أما بالنسبة للمشرع الجزائري فقد نص على عقوبة هذه الجريمة في المادة 65 الفقرة الثانية منها من القانون 18-07، والتي نصت على ما يلي" ...يعاقب بنفس العقوبة كل من قام بالإحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص"([2])، والعقوبة هي نفس العقوبة المقرر للمسؤول عن المعالجة الذي يقوم بخرق الإلتزامات المنصوص عليها في المادتين 38 و39 من هذا القانون، وتتمثل في الغرامة من 200.000 دج إلى 500.000 دج.

والملاحظ أن المشرعين الفرنسي والمغربي قد أقرا عقوبة الحبس والغرامة لما تمثله هذه الجريمة من إنتهاك لحق الإنسان في الحصول على حق النسيان بعد إنتهاء الغرض من التحزين، عكس المشرع الجزائري الذي إكتفى بعقوبة الغرامة فقط.

ب- عقوبة **إفشاء المعطيات ذات الطابع الشخصي إلى غير المؤهلين بذلك**

جرم المشرع الجزائري كل سلوك يؤدي إلى إفشاء المعطيات ذات الطابع الشخصي إلى غير المؤهلين بذلك، والذي يكون إما عن طريق السماح لغير المؤهلين بالولوج إلى هذه المعطيات طبقا لأحكام المادة 60 من القانون 18-07، أو بإيصال هذه المعطيات المعالجة أو المستلمة إلى غير المؤهلين بذلك طبقا لأحكام المادة 69 من نفس القانون.

**1- عقوبة السماح بالولوج إلى المعطيات ذات الطابع الشخصي لغير المؤهلين:**

وهي الجريمة المعاقب عليها بنص المادة 60 من القانون 18-07، حيث جاء نصها كالآتي" يعاقب بالحبس من سنتين(2) إلى خمس(5) سنوات وبغرامة من

---

[1]- المادة 55 من القانون رقم 08-09.

[2]- المادة 2/65 من القانون 18-07.

200.000 دج إلى 500.000 دج، كل من سمح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي"([1]).

**2- عقوبة إيصال المعطيات ذات الطابع الشخصي المعالجة أو المستلمة لغير المؤهلين**: وهي الجريمة المعاقب عليها في المادة 226-22 من قانون العقوبات الفرنسي المعدل والتي ورد فيها أنه" يعاقب بالحبس خمس سنوات وغرامة 300.00 أورو كل شخص كان قد أستقبل أو تلقى بمناسبة التسجيل أو التنصت أو النقل أو أي أجراء آخر من إجراءات المعالجة الإلكترونية بيانات أسمية من شأن إفشائها الإضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة وقام بنقلها إلى من لا حق له في العلم بها، وإذا وقع هذا الإفشاء للبيانات الأسمية بطريقة الإهمال تكون العقوبة هي الغرامة 100.000 أورو، ولا تقام الدعوى العمومية وفقا للفقرتين السابق الإشارة إليهما إلا من خلال شكوى المجني عليه أو ممثله القانوني أو من له صفة في ذلك"([2]).

ونص المشرع المغربي على عقوبة هذه الجريمة في المادة 61 في الفقرة الأولى منها من القانون 08-09، والتي تنص على أنه" يعاقب بالحبس من 6 أشهر إلى سنة وبغرامة من 20.000 درهم إلى 300.000 درهم أو بإحدى هاتين العقوبتين فقط، كل مسؤول عن المعالجة وكل معالج من الباطن وكل شخص بالنظر إلى مهامه مكلف بمعالجة المعطيات ذات طابع شخصي يتسبب أو يسهل، ولو بفعل الإهمال، الإستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة، أو يوصلها لأغيار([3]) غير مؤهلين..." ([1]).

---

[1]- قانون رقم 18-07، مرجع سابق، ص 22.

[2] -Art 226-22 :Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence, modifiè par Loi N° 2004-801 du 6 août 2004-ART 4, JORF 7 août 2004.

[3]- عرفت المادة 1 النقطة 7 منها من القانون المغربي 08-09، السالف الذكر، الأغيار بإنه" الشخص الذاتي أو المعنوي أو السلطة العامة أو المصلحة أو أية هيئة أخرى، غير الشخص المعني، والمسؤول عن المعالجة

أما بالنسبة للمشرع الجزائري فقد نص على عقوبة هذه الجريمة في المادة 69 من للقانون 18-07، والتي نصت على أنه" يعاقب بالحبس من سنة(1) إلى خمس(5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل مسؤول عن معالجة وكل معالج من الباطن وكل شخص مكلف بالنظر إلى مهامه بمعالجة معطيات ذات طابع شخصي يتسبب أو يسهل، ولو عن إهمال، الإستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك"([2]).

والملاحظ أن المشرع الفرنسي على عكس المشرعين المغربي والجزائري فرق في العقاب على هذه الجريمة مستندا إلى صورة الركن المعنوي، ففي حالة إرتكاب الفعل عمدا شدد العقوبة على فعل الإفشاء غير المشرووع للبيانات الشخصية حيث نص على عقاب الجاني بالحبس خمس سنوات وغرامة 300.000 أورو.

أما في حالة إرتكاب فعل الإفشاء غير المشروع للبيانات الشخصية بصورة الخطأ نتيجة إهمال أو رعونة أو ترك لهذه البيانات فيعاقب الجاني بالحبس ثلاث سنوات وغرامة 100.000 أورو.

**ثانيا: العقوبات المقرر للمخالفات المرتكبة أثناء إنشاء المعالجة**

تعد مرحلة المعالجة من بين المراحل الأكثر تعرضا لإرتكاب مخالفات عديدة تشكل جرائم معاقب عليها بمقتضى القانون 18-07، السالف الذكر، والتي تقوم إما بسبب مخالفة الشروط المسبقة للمعالجة، وإما بسبب خرق الإلتزامات الملقاة على عاتق المسؤول عن المعالجة أثناء القيام بعمليات المعالجة.

**1- عقوبة مخالفة الشروط المسبقة للمعالجة**

أن معالجة المعطيات ذات الطابع الشخصي لا تتم إلا بعد إستيفاء بعض الشروط المسبقة التي تضمنها القانون 18-07، المذكور سالفا، والمتمثلة في الحصول على الموافقة الصريحة من الشخص المعني بتلك المعطيات أو عدم

---

والمعالج من الباطن والأشخاص المؤهلون لمعالجة المعطيات الخاضعين للسلطة المباشرة للمسؤول عن المعالجة أو للمعالج من الباطن"

[1]- المادة 1/61 من القانون رقم 08-09.

[2]- المادة 69 من القانون رقم 18-07.

صدور إعتراض منه، وضرورة خضوع المعالجة لتصريح أو ترخيص مسبق من السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وأن مخالفة هذه الشروط يشكل قيام جريمتين معاقب عليهما بموجب المادتين 55 و56 من هذا القانون.

**أ- عقوبة معالجة المعطيات ذات الطابع الشخصي دون موافقة أو ترخيص أو رغم إعتراض من المعني:** وهي الجريمة المعاقب عليها في المادة 226-16 من قانون العقوبات الفرنسي المعدل والتي ورد فيها أنه"يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف أورو كل من أجرى أو طلب إجراء معالجة إلكترونية للبيانات الإسمية الشخصية دون مراعاة الشروط الواردة في القانون المشار إليه"([1]).

ونص المشرع المغربي على عقوبة هذه الجريمة في المادة 56 من القانون 08-09، والتي تنص على أنه" يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 20.000 درهم إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط، كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 4 أعلاه"([2]) وخرق أحكام هذه المادة يتمثل في معالجة المعطيات ذات الطابع الشخصي دون رضا الشخص المعني.

أما بالنسبة للمشرع الجزائري فقد نص على عقوبة هذه الجريمة في المادة 55 من القانون 18-07، والتي نصت على أنه" يعاقب بالحبس من سنة(1) إلى ثلاث(3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج، كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7 من هذا القانون.

ويعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم إعتراض الشخص المعني عندما تستهدف هذه المعالجة لا سيما الأشهار التجاري أو عندما يكون الإعتراض مبنيا على أسباب شرعية"([3]).

---

[1]- Art 226-16 : Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du III de l'article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiè par Ordonnance N° 2018-1125 du 12 dècember 2018-ART 13.

[2]- المادة 56 من القانون رقم 08-09.

[3]- المادة 55 من القانون رقم 18-07.

والملاحظ أن المشرع الجزائري قد أورد في المادة 64 من القانون 18-07 عقوبة على رفض الإعتراف بحقوق الشخص المعني، والتي يعد من بينها الحق في الإعتراض، وهو ما نراه إضافة في غير محلها ويعد من قبيل التكرار لأن العقوبة على هذه الجريمة منصوص عليها اصلا ضمن أحكام المادة 55 من نفس القانون.

**ب- عقوبة إنجاز عملية معالجة هذه المعطيات دون تصريح أو ترخيص مسبق:**

وهي الجريمة المعاقب عليها في المادة 52 من القانون 08-09، والتي تنص على أنه" دون المساس بالمسؤولية المدنية تجاه الأشخاص الذين تعرضوا لأضرار نتيجة هذه المخالفة يعاقب بغرامة من 10.000 درهم إلى 100.000 درهم كل من أنجز ملف معطيات ذات طابع شخصي دون تصريح بذلك أو الحصول على الأذن المنصوص عليه في المادة 12 أعلاه، أو واصل نشاط معالجة المعطيات ذات الطابع الشخصي رغم سحب وصل التصريح أو الأذن"([1]).

أما بالنسبة للمشرع الجزائري فقد نص على عقوبة هذا الجريمة في المادة 56 من القانون 18-07، والتي نصت على أنه" يعاقب بالحبس من سنتين(2) إلى خمس(5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون إحترام الشروط المنصوص عليها في المادة 12 من هذا القانون.

ويعاقب بنفس العقوبة كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له"([2]).

**2- عقوبة خرق الإلتزامات الواقعة على المسؤول عن المعالجة**

رتب المشرع الجزائري في القانون 18-07، على المسؤول عن معالجة المعطيات ذات الطابع الشخصي القيام بعدة إلتزامات منها ما يتعلق ببعض الحقوق الممنوحة للأشخاص المعنيين ومنها ما يتعلق بسرية وسلامة المعالجة، ومنها ما يتعلق أيضا بضرورة التواصل مع السلطة الوطنية لحماية المعطيات ذات الطابع

---

1- المادة 52 من القانون رقم 08-09.

2- المادة 56 من القانون رقم 18-07.

الشخصي، وأن خرق هاته الإلتزامات يشكل جرائم يعاقب عليها القانون بموجب المواد 61،64،65،61 من هذا القانون.

**أ- عقوبة عدم الإعتراف بحقوق الشخص المعني**: وهي جريمة يعاقب عليها المشرع المغربي بموجب أحكام المادة 53 من القانون 08-09، والتي تنص على أنه" يعاقب بغرامة من 20.000 درهم إلى 200.000 درهم عن كل مخالفة كل مسؤول عن معالجة المعطيات ذات الطابع الشخصي يرفض حقوق الولوج أو التصحيح أو التعرض المنصوص عليها في المواذ 7 و8 و9 أعلاه"([1]).

أما بالنسبة للمشرع الجزائري فنص على عقوبة هذا الجريمة في المادة 64 من القانون 18-07، والتي نصت على أنه" يعاقب بالحبس من شهرين(2) إلى سنتين(2) وبغرامة من 20.000 دج إلى 20.000 دج أو بأحدى هاتين العقوبتين فقط كل مسؤول عن المعالجة يرفض دون سبب مشروع، حقوق الإعلام أو الولوج أو التصحيح أو الإعتراض المنصوص عليها في المواد 32 و34 و35 و36 من هذا القانون"([2]).

**ب- عقوبة عدم الإلتزام بسرية وسلامة المعالجة للمعطيات ذات الطابع الشخصي**: وهي الجريمة المعاقب عليها بموجب المادة 65 في الفقرة الأولى منها من القانون 18-07، والتي نصت على أنه" دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بغرامة من 200.000 دج إلى 50.000 دج المسؤول عن المعالجة الذي يخرق الإلتزامات المنصوص عليها في المادتين 38 و39 من هذا القانون..." ([3]).

**ج- عقوبة عرقلة عمل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**: وهي جريمة يعاقب عليها المشرع المغربي بموجب أحكام المادة 62 في النقطة الأولى منها، من القانون 08-09، والتي تنص على أنه" يعاقب بالحبس من 3 أشهر إلى 6 أشهر وبغرامة من 10.000 درهم إلى 50.000 درهم أو بإحدى هاتين العقوبتين فقط كل من:

---

1-المادة 53 من القانون رقم 08-09.

2-المادة 64 من القانون رقم 18-07.

3-المادة 65 من القانون رقم 18-07.

- عرقل ممارسة اللجنة الوطنية لمهامها في المراقبة..." ([1])،

ونص المشرع التونسي على عقوبة عرقلة عمل السلطة الوطنية لحماية المعطيات الشخصية في الفصل 96، بقوله" يعاقب بخطية قدرها خمسة الآف دينار كل من:

- يتعرض لأعمال الهيئة الوطنية لحماية المعطيات الشخصية بمنعها من إنجاز الأعمال الميدانية أو يرفض تسليم الوثائق المطلوبة.

- تولى عن سوء نية الإدلاء إلى الهيئة أو إعلام المعني بالأمر ببيانات مخالفة للحقيقة"([2]).

أما بالنسبة للمشرع الجزائري فنص على عقوبة هذه الجريمة في المادة 61 من القانون 18-07، بقولها" يعاقب بالحبس من ستة(6) أشهر إلى سنتين(2) وبغرامة من 60.000 دج إلى 200.000 دج إو بإحدى هاتين العقوبتين فقط، كل من عرقل عمل السلطة الوطنية:

1- بالإعتراض على إجراء عملية التحقق في عين المكان.

2- عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة.

3- عن إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح"([3]).

**د- عقوبة الإمتناع عن إعلام السلطة الوطنية عن الإنتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي في مجال الإتصالات الإلكترونية**: وهي الجريمة المعاقب عليها بنص المادة 66 من نفس القانون، والتي جاء فيها" يعاقب بالحبس من سنة(1) إلى ثلاث(3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج أو بإحدى هاتين العقوبتين فقط، مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية

---

[1]-المادة 62 من القانون رقم 08-09.

[2]- الفصل 96 من القانون الأساسي التونسي عدد 63 لسنة 2004.

[3]- المادة 61 من القانون رقم 18-07.

والشخص المعني عن كل إنتهاك للمعطيات الشخصية خلافا لأحكام المادة 43 من هذا القانون"([1]).

وبناء على ماسبق ذكره يتضح أن المشرع الجزائري أعتبر جرائم المعطيات ذات الطابع الشخصي ذو طبيعة جنحية، إلا أنه وبالنظر لحداثة القانون 18-07، وفي ظل غياب النص الخاص الذي يحدد القانون الأساسي لمستخدمي السلطة الوطنية فإن هذه العقوبات تبقى غير كافية لتحقيق الردع المطلوب نظرا لعدم تنصيب أهم هيئة لحماية المعطيات ذات الطابع الشخصي ألا وهي السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وتحتاج إلى إجراء تعديلات في بعض العقوبات الخاصة ببعض صور هذه الجرائم، لتواكب من خلالها التشريعات المقارنة التي حققت قفزة نوعية في قمع هذا النوع من الإجرام، ولا سيما منها التشريع الفرنسي.

كما أن المشرع الجزائري لم يقتصر على العقوبات المقررة لهاته الصور فقط من جرائم المعطيات ذات الطابع الشخصي، وإنما تم الإشارة إلى أبرزها، سيما وأن الجزائر تعتبر من الدول المتأخرة في إصدار تشريعات في هذا المجال مقارنة بالعديد من التشريعات الأخرى التي تطرقت إلى عدة أنواع أخرى من المعطيات ذات الطابع الشخصي، وعمدت إلى تعديل تشريعاتها من أجل مكافحة هذا النوع من الإجرام الذي يرتبط بالتطور التكنولوجي المتسارع.

فضلا عن ذلك، فإن المشرع الجزائري قد أقر بعض الأحكام العامة المتعلقة بالعقاب المنصوص عليها في قانون العقوبات تطبق على كافة الجرائم المنصوص عليها في القانون 18-07، السالف الذكر، والمتمثلة أساسا في قيام مسؤولية الشخص المعنوي عن إرتكابه لهذه الجرائم طبقا لأحكام المادة 70 من القانون 18-07، وإمكانية تطبيق العقوبات التكميلية على مرتكبي هذه الجرائم طبقا لأحكام المادة 71 من هذا القانون، ومصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره طبقا للمادة 72 من نفس القانون، والمعاقبة على الشروع بنفس العقوبات المقررة للجريمة التامة طبقا للمادة 73 من القانون نفسه، وكذلك مضاعفة العقوبات

[1]- المادة 66 من القانون رقم 18-07.

المنصوص عليها في هذا القانون في حالة العود طبقا لأحكام المادة 74 من نفس القانون.

# الفصل الثاني

# أركان جرائم نظام المعالجة الآلية للمعطيات

## الفصل الثاني: أركان جرائم نظام المعالجة الآلية للمعطيات

يعتبر نظام المعالجة الآلية للمعطيات الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الإعتداء على نظام المعالجة، فإذا تخلف هذا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة بنظام المعالجة الآلية للمعطيات([1]).

وإن الجرائم الماسة بالأنظمة المعلوماتية وإن كانت تختلف في أركانها وعقوباتها إلا أن ما يجمعها أنها تحقق حماية جزائية تنظم المعالجة الآلية للمعطيات، أي أن القاسم المشترك بينها هو نظام المعالجة الآلية([2]).

لذلك فإن التطرق إلى أركان جرائم نظام المعالجة الآلية للمعطيات يستوجب ضرورة إبراز صورها التي تتعدد وتختلف من تشريع لآخر، ومن أهمها جرائم الدخول أو البقاء في نظام المعالجة الآلية للمعطيات وجرائم التلاعب بالمعطيات وجرائم التعامل في معطيات غير مشروعة، والتي تؤدي إلى المساس بالنظام في حد ذاته أو إلى المساس بالمعطيات الموجودة داخل نظام المعالجة الآلية أو التي لها علاقة به.

وإن جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية تعد من الجرائم التي يكون فيها الإعتداء منصبا ومرتكزا على النظام في حد ذاته، سواء كان ذلك بصفة مباشرة أو غير مباشرة، وبصرف النظر عن كون هذا النظام مشمولا بالحماية أم لا، طالما أن الدخول إليه أو البقاء فيه تم بطريقة غير مشروعة، ذلك أن الهدف من التجريم في هذه الجريمة هو منع إقتحام النظام الآلي لمعالجة المعلومات بحد ذاته، وليس سرقة ساعات العمل([3]).

أما بالنسبة لجرائم التلاعب بالمعطيات والتعامل في معطيات غير مشروعة فإن الإعتداء فيها يكون منصبا على المعطيات الموجودة داخل النظام أو التي لها علاقة

---

[1]- رابح وهيبة، مقال بعنوان الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد الرابع، ديسمبر 2014، ص 321.

[2]- عطاء الله فشار، مقال بعنوان مواجهة الجريمة المعلوماتية في التشريع الجزائري، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد 1، سبتمبر 2009، ص 484.

[3]- محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، ط الأولى،سنة 2006، ص 187.

به، ويؤدي إلى المساس بهذه المعطيات التي يتضمنها سواء بصفة مباشرة أو غير مباشرة.

وهذا ما جعل الفقه يتجه إلى وضع معيارا للتفرقة بين الإعتداء على النظام والإعتداء على المعطيات التي يتضمنها، وذلك على أساس ما إذا كان الإعتداء يشكل وسيلة أم غاية، فإذا كان الإعتداء مجرد وسيلة فإن الفعل يشكل جريمة إعتدء على نظام المعالجة الآلية أما إذا كان الإعتداء غاية فهو يشكل جريمة إعتداء على المعطيات([1]).

لذلك سنقوم بتقسيم هذا الفصل إلى مبحثين يتناول المبحث الأول أركان جرائم المساس بنظام المعالجة الآلية نعالج فيه جريمة الدخول أو البقاء غير المصرح بهما في النظام بصورتيها البسيطة والمشددة، أما المبحث الثاني نتناول فيه أركان جرائم المساس بمعطيات النظام نعالج فيه جرائم التلاعب بالمعطيات والتعامل في معطيات غير مشروعة، على أن يتضمن كل مطلب لهذين المبحثين تفصيل الركن المادي في الفرع الأول والركن المعنوي في الفرع الثاني، إضافة إلى العقوبات المقررة لهذه الجرائم([2]) في الفرع الثالث.

[1]- دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية-دراسة مقارنة، دار الفكر الجامعي، الأسكندرية، ط الأولى،سنة 2016، ص250.

[2]- أوجبت إتفاقية بودابست على الدول المنضمة إليها إقرار العقوبات الملائمة والفعالة لهده الجرائم بما فيها العقوبات المانعة للحرية بالنسبة للأشخاص الطبيعية والغرامات المالية للأشخاص المعنوية، أنظر: عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والأنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، لبنان، ط الأولى، سنة 2007، ص 136.

## المبحث الأول: أركان جرائم المساس بنظام المعالجة الآلية

تتجلى جرائم المساس بنظام المعالجة الآلية بصورة واضحة في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتيها البسيطة والمشددة، ومن تم فإننا نقوم بتقسيم هذا المبحث إلى مطلبين يتناول المطلب الأول أركان جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة بينما يتناول المطلب الثاني أركان جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة.

### المطلب الأول: أركان جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة

تشمل جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة فعلين وهما الدخول أو البقاء، وهي الصورة المنصوص عليها في المادة 394 مكرر الفقرة الأولى من قانون العقوبات الجزائري وتقابلها المادة 323 فقرة 1 من قانون العقوبات الفرنسي والمادة 2 من الإتفاقية الدولية للإجرام المعلوماتي، والتي حرص من خلالها المشرع الجزائري على تجريم كل تواجد غير مشروع داخل نظام المعالجة الآلية بتجريمه الدخول غير المصرح به إليه باعتباره الخطوة الأولى في إرتكاب هذه الجريمة، كما جرم البقاء بغير تصريح وهو الذي قد يحصل بعد دخول مشروع، وبغض النظر عن صفة مرتكب الفعل الإجرامي سواء كان هذا الشخص مسؤول عن الجهاز وصيانته أو منبث الصلة عن النظام([1]).

وهذا التجريم يشمل الدخول وكذا البقاء في كل أو جزء من النظام وبصرف النظر عن الغاية التي يهدف الجاني من خلال إرتكابه لهذه الجريمة، وكذلك بصرف النظر أيضا عما إذا كان هذا النظام محميا بجهاز للآمان أم لا، فالمشرع من خلال ذلك أراد أن يقفل الباب أمام كل وجود غير مصرح به داخل النظام، دخولا أو بقاء، في كل أو جزء من النظام بقصد خاص أم بدونه، وسواء كان محميا فنيا أم غير محمي، فتتحقق الجريمة سواء أدى هذا التواجد غير المشروع داخل النظام إلى نتائج

[1]- محمد أمين الرومي، جرائم الكومبيوتر والأنترنت، دار المطبوعات الجامعية، الأسكندرية ، ب ط، سنة 2004، ص 106.

معينة أم لم يؤدي، لكن إذا نجم عنه تخريب لهذا النظام أو محو أو تعديل لمعطياته فأن العقوبة تشدد([1]).

ومما لاشك فيه أن مجرد الدخول إلى نظام المعالجة الآلية لا يشكل فعلا غير مشروع وإنما يستمد هذا الدخول عدم مشروعيته من كونه قد تم بغش، ويكون كذلك في حالة ما إذا كان ضد إرادة المسؤول عن النظام وبعبارة أخرى بدون تصريح منه([2])، لذلك فهو لا يتم وفق طريقة معينة وإنما يتحقق بكل وسيلة تقنية تصلح لذلك([3]).

ويعرف فعل الدخول في إطار المعلوماتية بأنه كافة الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والأحاطة أو السيطرة على المعطيات التي يتكون منها أو الخدمات التي يقدمها([4])، أو هو الولوج إلى المعلومات المخزنة داخل النظام المعلوماتي بدون رضاء المسؤول عن النظام، وقد عرف المشرع السعودي الدخول بدون تصريح في المادة الأولى من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية بأنه" دخول شخص بطريقة متعمدة ألى حاسب آلي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها([5])، بحيث يستلزم القيام بمثل هذا العمل الإجرامي الولوج إلى المعلومات التي تمت معالجتها بأي من الأنظمة المعلوماتية، والإطلاع غير المصرح به على تلك المعلومات المخزنة في ذاكرات النظم المعلوماتية([6]).

أما فعل البقاء بدون تصريح يقصد به التواجد من قبل الجاني داخل نظام المعالجة الآلية والتجول بين الملفات والمجلدات والبيانات والمعلومات الإنتقال من

---

1- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 131.

2 - cass. Crim 8 dècember 1999, cass crim 5 janvier 1994, cite par : Alain-ben soussan , fraude informatique, la protèction d'un sustème informatique par un dispositif de sècuritè n èst pas une condition dàpplication de la loi God frain, art, disponble en lingne à làdresse suivante http://www.alain-bensossan.com/page/2903.

3 -Michel veron, droit pènal spècial, 6ème èdition armand colin, paris, 1998, p258.

4- نائلة عادل محمد فريد قورة، مرجع سابق، ص 332.

5- دلخار صلاح بوتاني، مرجع سابق، ص 190.

6- أحمد خليفة الملط، الجرائم المعلوماتية ، دار الفكر الجامعي، الأسكندرية، ط الثانية، 2006، ص 190.

جزء إلى جزء داخل النظام وبصفة مستمرة([1])، وقد أدرك المشرع في العديد من الدول الحاجة الملحة إلى حماية هذا النظام وما يحويه من معطيات، وذلك بتجريم فعلي الدخول والبقاء فيه بغير تصريح نظرا لعجز النصوص التقليدية العقابية عن توفير الحماية الجنائية اللازمة لهذا النظام.

فضلا عن ذلك فأن المشرع الجزائري نص على فعل المحاولة في المادة 394 مكرر في آخر الفقرة الأولى التي نصت على هذه الجريمة بقولها" ...أو يحاول ذلك" بالرغم من أنه تم النص على تجريم فعل الشروع في المادة 394 مكرر 7 وهذا ما يعد من قبيل التكرار الذي كان يجب على المشرع تحاشيه، إضافة إلى أنه أخطأ كذلك باستعماله لمصطلح منظومة للدلالة على النظام لأن مجموعة نظام هي أنظمة وليس منظومة، وذلك تماشيا مع عنوان القسم السابع مكرر" المساس بأنظمة المعالجة الآلية للمعطيات".

لذلك سنقوم بدراسة هذه الجريمة بنوع من التفصيل ببيان ركنها المادي في الفرع الأول وركنها المعنوي في الفرع الثاني وكذا العقوبات المقررة لها في الفرع الثالث.

**الفرع الأول: الركن المادي**

يتمثل الركن المادي في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة إتيان السلوك الإجرامي دون إحداث أي إتلاف أو تخريب للنظام، وهو ما نصت عليه المادة 394 مكرر([2]) من قانون العقوبات الجزائري في فقرتها الأولى بقولها" يعاقب...كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" وهذه المادة أستوحاها المشرع الجزائري من القانون الفرنسي بنفس عنوان التجريم، المساس بأنظمة المعالجة الآلية للمعطيات والمطابقة للمادة 323-1 من قانون العقوبات الفرنسي المعدل التي تنص على أن" الدخول أو البقاء -بطريق الغش- داخل كل أو جزء من نظام المعالجة الآلية للمعطيات يعاقب عليه بالحبس لمدة سنتين وغرامة

[1]- بلال أمين زين الدين، مرجع سابق ، ص 272.

[2]- المادة 394 مكرر من القانون 04-15.

مقدارها 60000 ألف يورو.."([1])، إضافة إلى الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 التي نصت على هذه الجريمة في المادة 6 الفقرة الأولى بعنوان جريمة الدخول غير المشروع بقولها"1-الدخول أو البقاء وكل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار به"([2])، وكذلك المشرع المصري الذي نص مؤخرا على هذه الجريمة في المادة 14 الفقرة الأولى([3]) من القانون الجديد رقم 175 لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات، بعنوان جريمة الدخول غير المشروع في الفصل الأول تحت عنوان الإعتداء على سلامة الشبكات وأنظمة وتقنية المعلومات، والتي نصت على ما يلي" يعاقب... كل من دخل عمدا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه"، إضافة إلى نص المادة الثانية من إتفاقية بودابست الموقعة في دولة المجر عام 2001 بشأن حماية نظم المعالجة الآلية للبيانات تحت عنوان الدخول غير القانوني، والتي نصت على أنه" يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل إعتبارها جريمة جنائية وفقا لقانونه الداخلي، الولوج العمدي لكل أو لجزء من جهاز الحاسب بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال إنتهاك إجراءات الأمن بنية الحصول على بيانات الحاسب أو نية أخرى إجرامية أخرى أو أن ترتكب الجريمة في حاسب آلي متصلا عن بعد بحاسب آخر"([4]).

ويتبين من خلال ما سبق أن الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة يتمثل في فعلي الدخول والبقاء غير المشروعين.

[1] -Art 323-1: Le fait d'accèder ou de se maintenir. Frauduleusement. dans tout ou partie d'un système de traitement automatisè de donnèes est puni de deux ans d'emprisonnement et de 60 000 € d'amende, modifiè par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

[2] - المادة 1/2 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[3] - المادة 1/14 من القانون رقم 175 لسنة 2018.

[4] - بوكر رشيدة، مرجع سابق، ص 162.

**أولا: فعل الدخول غير المشروع**

يقصد بفعل الدخول غير المشروع كافة الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والإحاطة أو السيطرة على المعلومات التي يتكون منها أو الخدمات التي يقدمها أو هو الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن النظام([1]) بهدف حماية المنظومة المعلوماتية أو المعلومات التي تحتوي عليها من الوصول إليها أو العبث بها من طرف من ليس لهم الحق في الدخول إلى هذا النظام([2])، ذلك أن الدخول إليه لا يعتبر في حد ذاته سلوك غير مشروع وإنما يتخذ هذا الوصف إنطلاقا من كونه تم دون وجه حق([3])، ويتحقق هذا الفعل متى دخل الجاني إلى النظام كله أو جزء منه مخالفا بذلك إرادة صاحب النظام أو من له الحق في السيطرة عليه، سواء كانت الأنظمة التي تم الدخول إليها متعلقة بأسرار الدولة أو دفاعها، أو تتضمن معطيات شخصية تتعلق بحرمة الحياة الخاصة أو غير ذلك من المعطيات التي لا يجوز الإطلاع عليها، لذلك يخرج من نطاق الدخول غير المشروع الدخول إلى برنامج منعزل عن نظام المعلومات الذي حظر عليه الدخول فيه، كما لا تتوافر الجريمة إن إقتصر دور الجاني على مجرد قراءة الشاشة دون الولوج إلى داخل النظام([4]).

وأشارت المذكرة التفسيرية لإتفاقية بودابست المبرمة في عام 2001، والتي تتعلق بحماية المعلوماتية إن الولوج غير القانوني في نظم المعالجة الآلية للبيانات يعد الجريمة الرئيسية التي تنطوي على تهديد وتعد على أمن بمعنى السرية والسلامة والإتاحة والنظم والبيانات المعلوماتية، إذ أن هناك ضرورة لتوفير حماية ملائمة

---

1- دلخار صلاح بوتاني، مرجع سابق، ص 190.

2- معتوق عبداللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و القارن، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية- جامعة العقيد الحاج لخضر -باتنة، الموسم 2012/2011، ص 50.

3- أحمد بن مسعود، مقال بعنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، المجلد 10، العدد 1، مارس 2017، ص 484.

4- أمحمدي بوزينة أمنة، مقال بعنوان الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري(دراسة تحليلية لقانوني العقوبات وحقوق المؤلف)، مجلة القانون والمجتمع، جامعة أحمد دراية-أدرار، المجلد 3، العدد 2، ديسمبر 2015، ص 100.

لمصالح المنظمات، وبالأخص لرجال الإدارة حتى يكون بمقدورهم أن يديروا ويستثمروا ويتحكموا في نظمهم بدون تشويش أو عقبة من أي نوع([1])، لذا فإن مجرد الدخول بدون تصريح بمعنى القرصنة أو السطو أو الدخول غير المشروع في النظام المعلوماتي يجب أن يوصف بأنه سلوك غير قانوني في حد ذاته كمبدأ عام، وذلك على أساس أن هذه الأفعال يمكن أن تخلق عقبات أمام المستخدمين الشرعيين للنظم والبيانات، كما يمكن أن تؤدي إلى إتلاف أو تدمير باهض التكلفة في حالة إعادة بناء الأنظمة التالفة أو المدمرة، كما أن هذا التدخل يمكن أن يترتب عليه الوصول إلى بيانات سرية وخصوصية مثل كلمات المرور أو معلومات عن النظام الهدف وأسرار تسمح باستخدام النظام مجانا، بل وتشجع القراصنة على إرتكاب أنواع أكثر خطورة من الجرائم المتصلة بالحاسب مثل ذلك الغش المعلوماتي أو التزوير المعلوماتي([2]).

وتقوم جريمة الدخول بغش بفعل الدخول لنظام المعالجة الآلية للمعطيات الذي يطلق عليه الدخول المنطقي، ويرى البعض أن هذه الجريمة ليست بالجديدة بل هي تعد قياسا على أفعال مشابهة تناولتها الكثير من القوانين بالتجريم مثل الإعتداء على حرمة المساكن عند الدخول بغش في ظروف محددة، وتباينت التشريعات التي تجرم الدخول بغش إلى نظام المعالجة الآلية للمعطيات بين تجريم مجرد الدخول إلى هذا النظام وما بين تجريم هذا الدخول مع إستيفاء شروط معينة، في حين تبنت بعض التشريعات الأخرى موقفا وسطا.

ومن أولى التشريعات التي جرمت الدخول المجرد إلى نظام المعالجة الآلية للمعطيات هو القانون السويدي للمعلوماتية لسنة 1973 المعدل سنتي 1986 و1990 في المادة 21 منه وقانون العقوبات الفرنسي في المادة 323-1، والقانون البرتغالي لجرائم المعلوماتية لعام 1991 في المادتين 7 و8 منه، وقانون العقوبات الدنماركي في المادة 263، وقانون العقوبات الهولندي في المادة 138-1، وقانون العقوبات الكندي في المادة 342، وقانون العقوبات الفلندي في المادة 8 من الفصل

---

[1]- بلال أمين زين الدين، مرجع سابق، ص 261.

[2]- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست الموقعة 23 نوفمبر 2001، دار النهضة العربية، القاهرة، ط الأولى، 2003، ص 70.

38 منه، وكذا قانون العقوبات السويسري في المادة 143 منه، وقانون العقوبات النرويجي في المادة 145 منه.

بينما إشترطت بعض التشريعات الأخرى لتجريم الدخول بغش توفر بعض الشروط الموضوعية أو الشخصية، كالقانون الألماني مثلا الذي يشترط أن يحصل الفاعل على معلومات نتيجة لهذا الدخول، ومن تم فإنه لا يكفي لهذا التجريم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات بل لا بدا من الوصول إلى المعلومات التي يحتوي عليها، فضلا عن ذلك فإنه يجب أن تكون مشمولة بحماية نظم أمنية([1])، وكذلك القانون الأمريكي الذي يشترط أن يتم الدخول بسوء نية وبأغراض محددة قانونا حتى يعاقب مرتكب هذه الأفعال([2]).

أما بعض التشريعات الأخرى فاتجهت إلى تبني موقفا وسطا، فجرمت الدخول بغش إلى نظام المعالجة الآلية للمعطيات ثم شددت العقوبة في بعض حالات الدخول مثل القانون الإنجليزي([3]).

وتختلف وسائل الدخول بدون تصريح إلى نظام المعالجة الآلية، بحيث يوجد العديد من الوسائل التي يمكن للشخص اللجوء إليها من أجل الدخول إلى هذا النظام، ومن أهمها تشغيل حاسب آلي مغلق(مطفئ) أو إستعمال حاسب مفتوح، أو الدخول إلى حاسب آلي عن طريق إستعمال كارت تشغيل أو عن طريق خط تليفوني، أو الدخول إلى حاسب آلي من خلال حاسب آلي آخر، كما أن الدخول إلى هذا النظام يتحقق بطريقتين مختلفتين، طريقة إلكترونية وهي الأكثر شيوعا من خلال إستعمال كلمات السر أو غيرها من الآليات الأخرى، أو طريقة مادية(فيزيائية) من خلال إقتحام خزانة الملفات وسرقة رقم الهوية الشخصية([4]).

لذلك لم يحدد المشرع الجزائري وسيلة الدخول والطريقة التي يتم بها الدخول إلى النظام، والتي يمكن أن تقع بأي وسيلة بجهاز تنصت أو برنامج إلتقاط وتجسس

---

1- مناصرة يوسف، مرجع سابق، ص118.

2- محمود أحمد عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ب ط، سنة 2005، ص 87.

3- مناصرة يوسف، مرجع سابق، ص 119.

4- دلخار صلاح بوتاني، مرجع سابق، ص 196.

أو غيرها من الآلات التي تسهل إختراق نظام مغلق، وهو ما تم الإشارة إليه في قرار لمجلس إستئناف باريس الذي قرر أن الدخول غير المشروع يمكن أن ينتج من مجرد إلتقاط الإشارات المشوشة صادرة ومرسلة من أجهزة إلكترونية، ويتحقق ذلك في الإعتراض والإلتقاط([1]).

واستغنى المشرع الجزائري شأنه شأن المشرع الفرنسي عن تخصيص نص قانوني لفعل الإعتراض غير المشروع لعملية نقل المعلومات، وأعطى في المقابل مفهوما موسعا لفعل الدخول عن طريق الغش إلى نظام المعالجة الآلية ليمتد ويشمل الإلتقاط غير المشروع والإعتراض غير المشروع للمعلومات أثناء إنتقالها باعتبارها تمثل إنتهاكا لإتصال معلوماتي بين النظم المختلفة أثناء عملها، وهذا ما يبدو واضحا من خلال نص المادة 394 مكرر من قانون العقوبات الجزائري والمادة 323-1 من قانون العقوبات الفرنسي([2]).

كما أن القانون لم يحدد ما إذا كان الدخول غير المشروع يؤدي أو يستلزم عنه إنتهاك أجهزة وسائل الحماية، وترك للقاضي السلطة التقديرية في هذا الأمر، وفي قرار مبدئي صادر عن مجلس إستئناف باريس قرر أن جريمة الدخول غير المشروع تكون واقعة حتى في غياب وسائل الحماية، وبالنتيجة الجنحة تنتج من مجرد دخول بسيط بدون حق، وهو ما ذهب إليه أيضا القضاء الجزائري للفصل في مسألة مدى إشتراط تأمين النظام المعلوماتي لوقوع جريمة الدخول غير المشروع، حيث جاء في قرار الغرفة الجزائية الثالثة بمجلس قضاء الجزائر رقم الفهرس: 09247/16 الصادر بتاريخ 27 جوان 2016، أن نيابة محكمة الحراش تابعت المتهم(م،ل) لإرتكابه منذ زمن لم يمضى عليه التقادم بدائرة إختصاص محكمة الحراش مجلس قضاء الجزائر جنح الدخول والبقاء عن طريق الغش في منظومة المعالجة الآلية للمعطيات وحيازة وإفشاء ونشر معطيات متحصل عليها من تلك الأفعال المنصوص والمعاقب عليها بالمواد 394 مكرر و394 مكرر 2 فقرة 2.

---

[1]- مناصرة يوسف، مرجع سابق، ص ص 121-123.

[2]- بوكر رشيدة، مرجع سابق، ص 210.

وتتلخص وقائع هذه القضية في أن الممثل القانوني لشركة إتصالات الجزائر سجل شكوى لدى مصالح الأمن جاء فيها بأن زبون الشركة (م،ل) قام بتصفح مجموعة من فواتير الهاتف الثابت لزبائن إتصالات الجزائر بدون حذف أو تغيير في المعطيات الموجودة على تلك الفواتير بعد أن دخل بطريقة غير شرعية للموقع الرسمي لإتصالات الجزائر، فضاء الزبون، بتاريخ 08 مارس 2014.

وقد أنكر المتهم التهمة الموجهة إليه وصرح أنه حاول دفع فاتورة هاتفه عن طريق الأنترنت فدخل لإستخراج الفاتورة وعن طريق الخطأ إستخرج فاتورة أخرى.

أما بالنسبة لممثل الطرف المدني فقد صرح أن المتهم دخل شبكة إتصالات الجزائر وإطلع على الفواتير لمدة حوالي 10 ساعات وقد تبين أنه إطلع على حوالي 100 فاتورة، وتأسس كطرف مدني والتمس تعويض قدره 5 مليون سنتيم.

وركز دفاع المتهم، على أن مصلحة الفوترة لم تكن محمية مما سمحت للمتهم بتصفح الموقع، حينها أرسل المتهم رسالة إلى وزارة الإتصال من أجل تأمين الموقع وتم ذلك موضحا أن موكله لم يقم بتغيير أي شيء في المعلومات والتمس أصلا البراءة واحتياطيا البراءة لفائدة الشك.

وأجاب قضاة الغرفة الجزائية الثالثة بأن المتهم قد قام بالدخول إلى موقع الطرف المدني ( إتصالات الجزائر) وتصفح مجموعة من الفواتير الخاصة بزبائن الهاتف الثابت وقد إعترف المتهم بذلك، كما أنه إتضح لإدارة إتصالات الجزائر بعد التحريات أن المتهم قد تصفح العديد من فواتير الزبائن ولمدة تقارب حوالي 10 ساعات، وقد قام بهذا الفعل دون أي ترخيص من إدارة الطرف المدني، كما أنه ثابت أن المدة التي تصفح فيها المتهم المعلومات هي مدة طويلة مما يؤكد سوء نيته وأن الفعل لم يرتكب بصفة عرضية أو عن طريق الخطأ، وعليه فإن الجنحة المتابع بها المتهم ثابتة في حقه ويتعين إدانته بها.

وقد أيد المجلس حكم محكمة الحراش مبدئيا ورأى تعديله بجعل عقوبة الحبس المحكوم بها على المتهم موقوفة النفاذ وخفض الغرامة إلى 20.000 دج، خاصة أنه

غير مسبوق قضائيا مما تعين معه إفادته بظروف التخفيف طبقا للمواد 53 من قانون العقوبات و592 من قانون الإجراءات الجزائية([1]).

**ثانيا: فعل البقاء غير المشروع**

يقصد بالبقاء غير المشروع في نظام المعالجة الآلية للمعطيات التواجد داخل نظام المعالجة الآلية ضد إرادة من له الحق في السيطرة على هذا النظام([2])، وقد يقترن البقاء بالدخول غير المشروع منذ البداية كما يتحقق مع دخول مشروع مصرح به إذا إستمر البقاء لغير المدة المحددة، وهذا ما يعرف بتجاوز التصريح فتجريم كل منهما غير مرتبط بالآخر([3])، وهو ما أشار إليه المشرع المصري في جريمة تجاوز حدود الحق في الدخول التي كرسها في المادة 15([4]) من القانون 175 لسنة 2018، السالف الذكر، والتي نصت على أنه" يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أوحساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول"

هذا وتتحقق جريمة البقاء داخل النظام كله أو جزء منه ويكفي البقاء داخل النظام لتوافر الركن المادي لتلك الجريمة، فلا يشترط أن يضاف إليه ضرورة إلتقاط معلومات أو أي شكل من أشكال الضرر([5]).

كما يتضح أن الهدف من تجريم البقاء غير المشروع في نظام المعالجة الآلية هو تجريم البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات، فالجاني لم يقصد الدخول إلى النظام، ولكن حين تبين دخوله كان يمكن أن يغادر النظام، ومع ذلك يبقى داخل النظام وتنصرف إرادته إلى ذلك([6]).

---

[1]- مقتبس عن: مناصرة يوسف، مرجع سابق، ص ص 162-165.

[2]- سامي منصور، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، المنشورات الحقوقية صادر، بيروت-لبنان، د ط، د س ن، ص 52.

[3]- جدي نسيمة، مرجع سابق، ص 53.

[4]-المادة 15 من القانون رقم 175 لسنة 2018.

[5]- مزاولي محمد، مرجع سابق، ص 283.

[6]- عبدالفتاح بيومي حجازي، الجريمة في عصر العولمة، دار الفكر الجامعي،الأسكندرية-مصر، ب ط، سنة 2008، ص 83.

وقد قضت محكمة النقض الفرنسية الغرفة الجنائية في جلسة علنية منعقدة بتاريخ 10 ماي 2017 رقم الطعن 81822-16 في قرار لها غير منشور تؤكد فيه قيام جريمة البقاء بغش في نظام المعالجة الآلية للمعطيات بحيث أنه إذا كان للسيد(س) الصفة لتثبيت برنامج في إطار ممارسة نشاطه كمحامي ووظائفه كمدير شبكة rèseau، فإن إستغلاله هذه الأداة ( البرنامج ) لأغراض لا تمت بصلة بتسيير مكتبه وبدون علم السيدة ( ع ) التي تعمل معه يشكل جنحة البقاء بغش في جزء من نظام المعالجة الآلية للمعطيات.

وأمام هذه التصريحات التي تقع في نطاق السلطة التقديرية لوقائع القضية يكون المجلس قد برر قراره بإدانة المتهم بالجرم المنصوص عليها في المادة 323-1 من قانون العقوبات الشخص الذي يعلم أنه غير مرخص له ويبقى في نظام المعالجة الآلية للمعطيات([1]).

كما أن البقاء لا يعني لزوم أن يقوم المخترق بارتكاب جريمة أخرى، وإنما يكفي هنا أن يتحكم في نظام المعالجة الآلية، والتحكم هنا قد يكون بأية وسيلة بما في ذلك إمكانية مراقبة "wiretop" عمل المزود أو حركة أحد المشتركين لديه، وهو على مفهوم إدارة دقة الأمور من جانب السيطرة على الخادم، ذلك أنه إذا لم تكن هناك سيطرة فلن يكون هناك تحكم وبالتالي يصعب البقاء([2]).

وأن القرار الذي يسرح المتهم من روابط البقاء بغش في نظام المعالجة الآلية للمعطيات يجب أن يخضع لرقابة محكمة النقض، ذلك أن المتهم الذي كان يدخل بانتظام للنظام المعلوماتي طيلة سنتين بواسطة كلمة مرور لم تعطى له إلا لفترة تجريبية محددة، وهي قاعدة معطيات لا يمكن الدخول إليها إلا للأشخاص المرخص لهم بذلك، وهو ما قضت به محكمة النقض الغرفة الجنائية في جلسة علنية يوم الأربعاء 3 أكتوبر 2007 رقم الطعن 81045-07([3]).

كما أن البقاء غير المشروع قد يتحقق مستقلا عن الدخول غير المشروع وقد يجتمعا، ويكون البقاء معاقبا عليه إستقلالا حين يكون الدخول إلى النظام

---

[1]- مقتبس عن: مناصرة يوسف، مرجع سابق، ص 127.

[2]- بوكر رشيدة، مرجع سابق، ص 214 .

[3]- مقتبس عن: مناصرة يوسف، مرجع سابق، ص 127.

مشروعا([1])، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ ينبغي على المتدخل في هذه الحالة أن يقطع وجوده ويخرج من النظام فورا، فأن بقي رغم ذلك فإنه يعاقب على جريمة أو فعل البقاء غير المشروع إذا ما توافر لها الركن المعنوي([2]).

لذلك يذهب بعض الفقه إلى القول باختلاف طبيعة جريمة الدخول عن البقاء غير المصرح به، بحيث أن الأولى تكون إيجابية ووقتية بينما الثانية سلبية ومستمرة، ومن تم فإنه يجب أن يكون لكل منهما نص تجريمي مستقل([3]).

**الفرع الثاني: الركن المعنوي**

أن جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة تعتبر من الجرائم العمدية التي يتعمد الجاني إرتكابها بتوافر القصد الجنائي لديه([4])، وهي تقوم على القصد الجنائي العام ولا تتطلب قصد جنائيا خاص، وهذا ما يستشف من نص المادة 394 مكرر من قانون العقوبات التي نصت على أنه"...كل من يدخل أو يبقى عن طريق الغش..." ونفس المعنى أشار إليه المشرع الفرنسي بموجب المادة 323-1 من قانون العقوبات الفرنسي.

ويتوافر القصد الجنائي العام بعنصريه العلم والإرادة.

**أولا-العلم:** هو إنصراف علم الجاني إلى واقعة ذات أهمية قانونية تتمثل بعلمه بكافة العناصر التي تشكل الجريمة خاصة ما تعلق منها بأن ليس له الحق في الدخول أو البقاء في كل أو جزء من نظام المعالجة الآلية للمعطيات([5])، بما يحويه من

---

1- علي عبدالقادر القهواجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، ب ط، سنة 1999، ص 133.

2- طعباش أمين، الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الأسكندرية، ط الأولى، سنة 2015، ص 56،57.

3- حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الإعتداء على التوقيع الإلكتروني، دار الكتب القانونية-دار شتات للنشر والبرمجيات، مصر-الإمارات، 2013، ب ط، ص 161.

4- بلعيات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط الأولى، 2007، ص 9.

5-حديدان سفيان، مقال بعنوان الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، المجلد 2، العدد 4، ديسمبر 2017، ص 676.

معلومات وبرامج، وأن يكون كذلك على علم بخطورة الفعل الذي يقوم به على المصلحة التي يحميها القانون، فضلا على ذلك لا بدا أن يعلم أن دخوله أو بقاءه داخل النظام قد تحقق بدون تصريح من المسؤول عن النظام أو صاحب الحق في منح التصريح، فإذا كان يعتقد على أنه مصرح له بالدخول أو البقاء في النظام أو أنه نظام مفتوح للجمهور فلا تقوم الجريمة بحقه لإنعدام القصد الجنائي لديه، وكذلك الأمر بالنسبة للدخول بالصدفة أو السهو أو بالخطأ في النظام، لكن في هذه الحالة ينبغي عليه الخروج فورا من النظام فور علمه بأن دخوله إليه غير مصرح به، فإذا أمتنع عن ذلك توافر لديه القصد الجنائي منذ لحظة تحقق علمه([1]).

كما أن هناك بعض العناصر لا يتطلب القانون توقعها لقيام الجريمة، فالقانون مثلا لا يحدد في حمايته نظاما بعينه، فإذا قصد الجاني الدخول إلى نظاما معين ثم وجد نفسه داخل نظاما آخر فإن الجريمة تقوم والقصد يتحقق ولا يغير هذا من أمر القصد شيئا، وذلك لأن القانون الجزائري وكذا الفرنسي لا يفرق بين نظام معلوماتي وآخر، وقد قررت هذا الأمر صراحة المادة 17 من قانون إساءة إستخدام الحاسبات الآلية بالمملكة المتحدة عندما نصت بأن الدخول غير المصرح به لا يرتبط بنوعية المعلومات أو البرامج أو الأنظمة محل الجريمة([2]).

**ثانيا -الإرادة:** هي أن تتجه إرادة الجاني إلى إرتكاب الفعل وهو الدخول أو البقاء في نظام المعالجة الآلية بدون تصريح، وطالما أن جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات في صورتها البسيطة هي جريمة شكلية([3]) في كل من التشريع الجزائري والفرنسي ولا يتطلب لقيامها تحقق نتيجة معينة فإن الإرادة فيها تقتصر على إتيان السلوك الإجرامي وإستغراقه بكل مقوماته ولا تمتد إلى أي نتيجة لأن هذه الأخيرة لا يعتد بها القانون في قيام الجريمة([4]).

---

1- دلخار صلاح بوتاني، مرجع سابق، ص 211.

2- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 165،166،

3- الجريمة الشكلية هي التي يكتمل شكلها القانوني بمجرد تحقق السلوك الإجرامي دون تطلب عنصر آخر في الركن المادي للجريمة، أنظر: جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة الكتاب الأول الجرائم الناشئة عن إستخدام الحاسب الآلي، دار التهضة العربية، القاهرة، ط الثانية، سنة 2011،2012، ص 153.

4- بوكر رشيدة، مرجع سابق، ص 237.

كما أنه لاعبرة بالباعث في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة سواء تمثل في السعي إلى تحقيق الربح المادي أو الإنتقام من رب العمل أو الرغبة في قهر النظام والتفوق عليه أو إثبات ضعفه أو مجرد التعلم أو الإستكشاف، وتطبيقا لذلك في فرنسا قضي بقيام جريمة الدخول بدون تصريح إلى النظام المعلوماتي بحق مهندس كومبيتر أراد أن يثبت لأحد المصارف قدرته الفنية على الدخول لأنظمة المصرف المعلوماتية حتى يفوز بعقد تدريب موظفي المصرف([1]).

وعلى خلاف التشريعين الجزائري والفرنسي تطلبت بعض التشريعات ضرورة توفر قصد جنائي خاص إلى جانب القصد الجنائي العام لقيام جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة كما هو الحال في قانون إساءة إستخدام الحاسبات الآلية لعام 1990 في المملكة المتحدة الذي يتطلب لقيام جريمة الدخول أن ترتكب بنية إرتكاب جريمة أخرى كالسرقة أو التهديد أو النصب...إلا أن هذه الجريمة لم تتم، كما أنه لا يمكن العقاب عليها بوصف الشروع نظرا لعدم إتيان الفاعل عملا بعد بدءا في تنفيذها، ولا بدا من توافر نية الدخول ونية إرتكاب تلك الجريمة معا لدى الفاعل، وكذلك القانون البرتغالي عام 1991 في مادته السابعة(7) إشترط لقيام جريمة الدخول أن تكون لدى الفاعل نية للحصول لحسابه أو لغيره على ربح أو فائدة غير مشروعة([2])، إضافة إلى المشرع الإمارتي الذي يتطلب قصدا خاص لتحقق جريمة الدخول غير المشروع، وهو مانص عليه في المادة 04 من مرسوم بقانون إتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، والتي نصت على أنه" يعاقب ...كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلوماتي إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو إقتصادية..."([3]).

---

1- دلخار صلاح بوتاني، مرجع سابق، ص 212.

2- بوكر رشيدة، مرجع سابق، ص 240.

3- مرسوم بقانون إتحادي رقم (5) لسنة 2012، في شأن مكافحة جرائم تقنية المعلومات، سلسلة التشريعات الإتحادية، دائرة القضاء، أبوظبي، سنة 2013، ص 21.

وبناء على ما سبق يمكن القول الإكتفاء بتوافر القصد الجنائي العام دون اشتراط قصد خاص متمثلا في نية الإضرار أمر يتفق وقيام هذه الجريمة إبتداء، لأن تطلب قصد جنائي خاص إنما يتعارض مع الركن المادي لهذه الجريمة على اعتبارها تصنف ضمن الجرائم الشكلية التي لا تستلزم تحقق نتيجة إجرامية([1]).

**الفرع الثالث: العقوبات المقررة لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة**

نص المشرع الجزائري على العقوبات المقررة لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة في المادة 394 مكرر الفقرة الأولى من قانون العقوبات المعدل والمتمم، باعتبارها عقوبات أصلية، وعلى العقوبات التكميلية في المادة 394 مكر 6 من نفس القانون.

**أولا: العقوبات الأصلية**

نص المشرع الجزائري على العقوبات الأصلية لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة في الفقرة الأولى من المادة 394 مكرر من قانون العقوبات الجزائري، بقولها" يعاقب بالحبس من ثلاثة(3) أشهر إلى سنة(1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" ويتضح من خلال هذه المادة أن المشرع وضع حد أدنى وأقصى للعقوبة حتى تكون له سلطة تقديرية في تفريدها بحسب ما تتطلبه الحالة المعروضة أمامه، ذلك أن بواعث إرتكاب الجريمة كثيرة ومتعددة وليس هناك باعث واحد والتي قد تكون بدافع الإكتشاف والفضول أو بدافع التجسس والربح وغيرها، وهذا بالنسبة للصورة البسيطة لهذه الجريمة، وهي الحالة التي لم ينجم عنها حذف أو تغيير لمعطيات النظام أو تخريب نظام إشتغاله.

وإن هذه العقوبات التي أقرها المشرع الجزائري هي مستوحاة من قانون العقوبات الفرنسي لعام 1988 المعدل بقانون 1994، والذي عدل في المادة 323-1 من تلك العقوبات برفعه الحد الأقصى للعقوبة إلى سنة وغرامة مائة ألف فرنك في حالة

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 213.

الدخول والبقاء في صورته البسيطة، وجعل لها حدا واحد ليسلب بذلك السلطة التقديرية من القاضي من التحرك بالعقوبة.

ولعل السبب في ذلك هو مواجهة تفشي وانتشار ظاهرة الإجرام المعلوماتي وتعدد صور الإعتداء على نظام المعالجة الآلية للمعطيات، والتي إنعكست بدورها على أنشطة الهيئات والمؤسسات والإدارات الإقتصادية التي ترتبط إنشطتها إلى حد بعيد بالنظام المعلوماتي وبتقنية المعلومات وكذلك الرغبة في حماية الشبكات الدولية والمحلية وبخاصة البنكية منها([1]).

ونظرا لكون جرائم نظام المعالجة الآلية للمعطيات في إزدياد مستمر وخسائرها في نمو دائم فقد قام المشرع الفرنسي بتشديد العقوبة مرة أخرى لتصبح العقوبة سنتين والغرمة ستون ألف يورو (30.000 يورو)([2]) محتفظا بذلك بالحد الواحد للعقوبة سواء كانت للحبس أو للغرامة، ومبديا رغبة قوية في مواجهة هذه الجرائم([3]).

كما عاقب المشرع الإمارتي على هذه الجريمة في المادة 4([4]) الفقرة الأولى من مرسوم بقانون إتحادي رقم (5) لسنة 2012، السالف الذكر، والتي تنص على أنه" يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم كل من يدخل بدون تصريح إلى موقع إلكتروني، أو نظام معلوماتي إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو إقتصادية"، إضافة إلى المشرع المصري الذي عاقب على هذه الجريمة في المادة 14 الفقرة الأولى من قانون 175 لسنة 2018، السالف الذكر، بقولها" يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنيه، ولا تجاوز مائة ألف جنيه، أو بإحدى

---

[1]- بلال أمين زين الدين، مرجع سابق، ص 282.

[2] - Art 323-1: Le fait d'accèder ou de se maintenir. Frauduleusement. dans tout ou partie d'un système de traitement automatisè de donnèes est puni de deux ans d'emprisonnement et de 60 000 € d'amende, modifiè par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 172.

[4]-المادة 1/4 من المرسوم بقانون إتحادي رقم (5) لسنة 2012.

هاتين العقوبتين، كل من دخل عمدا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه"([1]).

أما بالنسبة لعقوبة الشخص المعنوي هي الغرامة المضاعفة إلى 5 مرات عما هو مقرر للشخص الطبيعي حسب ما أشارت إليه المادة 394 مكرر4 من قانون العقوبات الجزائري، وبالتالي تكون الغرامة المقررة عليه في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة تتروح بين مائتين وخمسون ألف(250000 دج) وخمسمائة ألف(500000 دج) دينار جزائري([2]).

**ثانيا: العقوبات التكميلية**

إن العقوبات التكميلية التي توقع بخصوص جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة هي عقوبة المصادرة التي نصت عليها المادة 394 مكرر6 من قانون العقوبات الجزائري بقولها" مع الإحتفاظ بحقوق الغير حسن النية، تحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أرتكبت بعلم مالكها"([3]).

ولا يقصد المشرع هنا بالمواقع التي تكون محلا للجريمة تلك المواقع التي تتضمن أنظمة المعالجة الآلية للمعطيات والتي تم الإعتداء عليها بالدخول غير المشروع إليها، لأن هذه المواقع هي الضحية ولا يتصور غلقها، وإنما يقصد المواقع التي أستعملت في إرتكاب الجريمة، لذلك كان يجب على المشرع الجزائري أن يستعمل عبارة" المواقع التي تستعمل في إرتكاب الجريمة" والتي تنصرف إلى المواقع

[1]- المادة 1/14 من القانون رقم 175 لسنة 2018.

[2]- محمد خليفة، مرجع سابق، ص 173.

[3]- المادة 394 مكرر 4 من القانون رقم 04-15.

التي تسببت في إرتكاب الجريمة، بدلا من عبارة" المواقع التي تكون محلا لجريمة من الجرائم" والتي تنصرف إلى المواقع التي وقعت عليها الجريمة([1]).

أما بالنسبة لقانون العقوبات الفرنسي فقد نص على عقوبة المصادرة، بينما قام في قانوني 1994 و2004 بتقديم قائمة من العقوبات التكميلية التي توقع على الشخص الطبيعي في المادة 323-5 ([2]) منه([3]).

كما نص القانون المصري رقم 175 لسنة 2018، السالف الذكر، على العقوبات التبعية في المادة 38 منه، بقولها" مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد أستخدم في إرتكاب الجريمة، أو سهل أو ساهم في إرتكابها.

وفي الحالات التي يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الإعتباري المدان بأي جريمة منصوص عليها في هذا القانون لم يحصل على الترخيص فيحكم فضلا عن العقوبات المقررة بالغلق"([4]).

---

[1]- محمد خليفة، مقال بعنوان دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية للقانون والعلوم السياسية(revue critique de drait et sciences politiques)، جامعة مولود معمري تيزي وزو، المجلد 13، العدد 1، جوان 2018، ص 78،79.

[2] -Art 323-5: Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-3, modifiè par LOI N° 2004-575 du 21 juin 2004.

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 175.

[4]- المادة 38 من القانون رقم 175 لسنة 2018.

**المطلب الثاني: أركان جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة**

أن المشرع الجزائري بتجريمه لفعل الدخول المجرد بدون تصريح إلى نظام المعالجة الآلية يكون قد أعتبر جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة جريمة شكلية، بحيث يعد هذا السلوك في حد ذاته جريمة ولا يتطلب حدوث أية نتيجة معينة، فمجرد الدخول إلى هذا النظام سواء كان ذلك بقصد الحصول على البيانات أو لغرض التسلية يعد إنتهاكا له وإن لم بترتب على ذلك أية أضرار بهذا النظام أو بالمعلومات الموجودة بداخله، كما جرم البقاء في النظام بدون تصريح لمواجهة حالات الدخول عن طريق الخطأ أو السهو أو تجاوز التصريح، وهذا حسب ما جاء في نص المادة 394 مكرر الفقرة الأولى منها.

إلا أنه إذا نجم عن هذا الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية نتائج معينة يترتب على ذلك تشديد العقوبة، وهذا ما يعرف بجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة، نص عليها المشرع الجزائري في المادة 394 مكرر الفقرة الثانية والثالثة، والتي أشار فيها إلى النتائج التي يترتب عليها تشديد العقوبة وحصرها في ثلاثة نتائج فقط وهي حذف أو تغيير في معطيات النظام وتخريب أشتغال نظام المعالجة الآلية للمعطيات، أما بالنسبة للمشرع الفرنسي فقد أشار إلى جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة في المادتين 323-1 الفقرة الثانية و323-2، في حين تطرقت إليها الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 6 الفقرة الثانية منها.

وللوقوف على ثنايا هذه الجريمة سوف نقوم بتقسيم هذا المطلب إلى ثلاثة فروع يتناول الفرع الأول الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشدة والفرع الثاني نكرسه للركن المعنوي لهذه الجريمة، أما الفرع الثالث والأخير نخصصه للعقوبات المقررة لهذه الجريمة.

**الفرع الأول: الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشدة**

أن المشرع الجزائري شدد العقوبة في حالة إذا ماترتب عن الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية نتائج معينة ينجم عنها إحداث أضرارا بالنظام في حد ذاته أو بالمعطيات التي يتضمنها، وذلك طبقا للمادة 394 مكرر الفقرة الثانية والثالثة منها، والتي تنص على ما يلي" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة(6) أشهر إلى سنتين(2) والغرامة من 50.000 دج إلى 150.000 دج"([1]).

وذهبت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في نفس الإتجاه في المادة 6 الفقرة الثانية منها بقولها"2-تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الإتصال أو الإستمرار بهذا الإتصال:

أ- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الإتصال وإلحاق الأضرار بالمستخدمين والمستفيدين.

ب- الحصول على معلومات حكومية سرية"([2]).

أما بالنسبة للمشرع الفرنسي نص على هذه الجريمة في المادة 323-1 الفقرة الثانية من قانون العقوبات الفرنسي، والمعدلة بموجب القانون رقم 912-2015 الصادر بتاريخ 2015/7/24، والتي نصت على ما يلي"..وإذا نجم عن هذا السلوك محو أو تعديل المعطيات المختزنة في النظام أو إتلاف تشغيل النظام تكون العقوبة الحبس ثلاث سنوات والغرامة مقدارها 100000 يورو"([3])، ونص كذلك على إفساد تشغيل نظام المعالجة الآلية للبيانات كجريمة مستقلة في المادة 323-2 من قانون

---

1- المادة 394 مكرر الفقرة الثانية والثالثة من القانون رقم 04-15.

2- المادة 2/6 من الإتفاقية العربية لمكافحة تقنية المعلومات لسنة 2010.

[1]—Article 323-1/2 :Lorsqu 'il en est rèsultè soit la suppression ou la modification de donnèes contenues dans le système, sait une altèration du fonctionnement de ce systèmè, la peine est de trois ans d' emprisonnement et de 100 000 € d'amende, modifiè par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

العقوبات الفرنسي المعدل، والتي نصت على ما يلي" تعطيل أو إفساد تشغيل نظام المعالجة الآلية للبيانات يعاقب عليه بالحبس لمدة خمس سنوات وبغرامة قدرها 150000 يورو"([1]).

وهو ما ذهبت إليه العديد من التشريعات بإفراد هذا السلوك كجريمة مستقلة كالمشرع السعودي في المادة الخامسة([2]) الفقرة الثانية والثالثة من نظام مكافحة جرائم المعلوماتية رقم 17 لسنة 2007، والمشرع الإمارتي في المادة 8([3]) من مرسوم بقانون إتحادي رقم(5) لسنة 2012، السالف الذكر، وكذلك القانون العربي الإسترشادي النموذجي لمكافحة جرائم تقنية المعلومات في المادة 7([4]) منه، بينما البعض الآخر من التشريعات نص عليها ضمن النصوص الخاصة بالإتلاف كالمشرع الأمريكي في المادة 1030) أ من القانون الفيدرالي إتلاف المعلومات الذي يترتب عليه تعطيل أنظمة الحاسبات الآلية التابعة إلى الحكومة، وإتجه كذلك القضاء

[1] -Article 323-3 ; Le fait d'introduire frauduleusement des données dans un système de traitement automatisè, d'extraire, de dètenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende, modifiè par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

[2] - تنص المادة 5 الفقرة الثانية والثالثة من نظام مكافحة جرائم المعلوماتية السعودي رقم 17 لسنة 2007 على أنه " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية: 1...2- إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها.

3- إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت" أنظر: نظام مكافحة الجرائم المعلوماتية رقم 17 الصادر بتاريخ 2007/03/26.

[3]- تنص المادة 8 من مرسوم بقانون إتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، على أنه " يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع إلكتروني أو نظام معلوماتي إلكتروني"، أنظر: مرسوم بقانون إتحادي رقم (5) لسنة 2012.

[4]- تنص المادة 7 من القانون العربي الإسترشادي النموذجي لمكافحة جرائم تقنية المعلومات، على أنه " كل من أعاق أو شوش أو عطل عمدا أو بأية وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب وما في حكمها الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات يعاقب بالحبس... "، أنظر: قرار رقم 417 بشأن مشروع قانون عربي إسترشادي لمكافحة جرائم المعلوماتية، جامعة الدول العربية، الدورة 21، لسنة 2004.

الإنجليزي إلى تطبيق نص المادة الثالثة من قانون إساءة إستخدام الحاسبات الآلية لسنة 1990- والذي جاء خاليا من نص خاص يجرم تعطيل أو إفساد النظام المعلوماتي- والخاصة بإتلاف المكونات المنطقية للحاسب الآلي على تعطيل(إعاقة) النظام المعلوماتي مستندين في ذلك على ما أشارت إليه الفقرة الثانية من هذه المادة التي تقضي أن إتجاه الجاني إلى تعطيل(إعاقة) نظام الحاسب الآلي تتوافر به نية إحداث تغيير في محتوى الحاسب الآلي مما يعد مكونا لجريمة الإتلاف([1])، وإلى جانب ذلك إتجه جانب آخر إلى إدراجها ضمن النصوص الخاصة بالدخول بدون تصريح إلى نظام المعالجة الآلية كما فعل المشرع الجزائري، والذي برر البعض موقفه بعدم النص على جريمة تعطيل أو إفساد النظام المعلوماتي للتشابه الكبير بينها وبين جريمة الإعتداء على المعطيات، والتي يصعب بحسب هذا الرأي التمييز بينهما، ذلك لإن الأفعال التي تتضمنها جريمة الإعتداء على المعطيات تؤدي هي الأخرى إلى تعطيل النظام أو فساده([2]).

وإن الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة يتكون من عناصره الثلاث، والمتمثلة في السلوك الإجرامي(الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية) والنتيجة الإجرامية(حذف أو تغيير في معطيات النظام أو تخريب نظام إشتغاله) والعلاقة السببية بين السلوك الإجرامي والنتيجة الإجرامية المحددة أفعالها على سبيل الحصر في المادة 394 مكرر في الفقرة الثانية والثالثة من قانون العقوبات الجزائري، وهي:

أ- **حذف المعطيات:** وهو الفعل الذي يشير إلى إزالة المعلومات الموجودة داخل نظام المعالجة الآلية، وهو أقصى أنواع الضرر.

ب- **تغيير المعطيات:** وهو الفعل الذي يشير إلى إحداث تعديلات في المعلومات فحسب دون أن يصل الأمر إلى إزالتها، بحيث تظل المعلومة موجودة ولكن بدون معنى ولا فائدة.

---

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 252،251.

[2] - المرجع نفسه، ص 249.

ج- **تخريب نظام إشتغاله:** وهو الفعل الذي يتم عن طريق ممارسة بعض الأفعال على النظام من شأنها جعله غير قابل للإستخدام أو للإستعمال([1]).

وإن حدثت إحدى هذه النتائج نتيجة فعل آخر فلا نكون أمام هذه الصورة المشددة من الجريمة بل البسيطة لتحقق فعل الدخول أو البقاء فقط، وعليه فإذا أثبت الجاني إنتفاء العلاقة السببية بين فعله والنتيجة التي تحققت لم تقم الجريمة، كتدخل عامل آخر حادث مفاجئ أو قوة قاهرة([2]).

كما أن نتيجة حذف أو تغيير معطيات النظام هي النتيجة ذاتها المتطلبة في جريمة التلاعب بالمعطيات، وتتمثل في تغيير حالة المعطيات غير إن الفرق بينهما في جريمة التلاعب تقع إرادية أي يريدها الفاعل أو يقبلها على الأقل، بينما في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة لا تقع كذلك، إذ لا يريدها الفاعل وهي تفرقة تتعلق بالركن المعنوي ولا شأن لها بالنتيجة التي هي من عناصر الركن المادي.

أما النتيجة الأخرى التي أعتد بها المشرع في تشديد عقوبة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة هي تخريب اشتغال نظام المعالجة الآلية للمعطيات، وهي النتيجة ذاتها التي تتطلبها جريمة إفساد نظام المعالجة الآلية للمعطيات المنصوص عليها في المادة 323-2 من قانون العقوبات الفرنسي، وما يفرق بين النتيجتين هو الإرادة، إرادة النتيجة في جريمة إفساد نظام المعالجة الآلية للمعطيات وعدم إرادتها في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة، وهي أيضا تفرقة لا علاقة بالنتيجة في حد ذاتها بل تتعلق بالركن المعنوي أي بالموقف النفسي للفاعل من هذه النتيجة([3]).

وفضلا عن ذلك، فإن حصر المشرع الجزائري لهذه النتائج الثلاثة لا يعني أنه لا توجد أضرار أخرى قد تترتب على فعل الدخول أو البقاء المشدد بل هناك العديد

---

[1]- بوكر رشيدة، مرجع سابق، ص 231،232.

[2]- جدي نسيمة، مرجع سابق، ص 59.

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 161.

من أشكال النتائج الضارة التي قد تصيب المعلومات في بيئتها التقنية، مما قد يصعب حصرها، إلا أن المشرع الجزائري قد تناول أخطرها جسامة وأغلبها وقوعا في هذه البيئة، وتبعا لذلك فإن حدثت نتائج أخرى غير هذه النتائج لا يبقى أمام المتضرر إلا أن يطالب بالتعويض وفق ما تقتضيه قواعد المسؤولية المدنية([1]).

**الفرع الثاني: الركن المعنوي**

إن النتيجة المشددة التي نصت عليها الفقرة الثانية من المادة 323-1 من قانون العقوبات الفرنسي والفقرة الثانية والثالثة من المادة 394 مكرر من قانون العقوبات الجزائري هي نتيجة غير عمدية، وأن أول ما يتبادر إلى الذهن من خلال نص هذه المادة الأخيرة بفقرتيها الأولى والثانية أن الظرف المشدد هو من الظروف المشددة المادية التي لا تغير من وصف الجريمة، والتي تقوم بمجرد قيام الركن المادي له وهو حدوث النتيجة المشددة وارتباطها بفعل الدخول أو البقاء برابطة سببية، أي أن المسؤولية عن هذا الظرف المشدد هي مسؤولية مادية"موضوعية" تقوم بمجرد توافر الركن المادي، وهي لاتقوم إلا إذا حصلت النتيجة المشددة عن طريق قوة قاهرة([2]).

وهو الأمر الذي وجد معه البعض من الفقه أن تلك الجريمة المنصوص عليها في المادة 323-1 الفقرة الثانية من قانون العقوبات الفرنسي، بقولها أنه"..وإذا نجم عن هذا السلوك محو أو تعديل المعطيات المختزنة في النظام أو إتلاف تشغيل النظام تكون العقوبة الحبس ثلاث سنوات والغرامة مقدارها 100000 يورو"([3])، تقع بطريق الخطأ في التشريع الفرنسي ولا يتطلب المشرع فيها تطلب القصد الجرمي، بحيث أن الخطأ يعد كافيا لقيام الجريمة، ومن تم فإن هذه الجريمة تعد من جرائم الإهمال، وبالتالي فمجرد إرتكاب الفعل المادي يعد كافيا لقيام الجريمة إلا إذا

---

[1]- بوكر رشيدة، مرجع سابق، ص 233.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 169.

[4]—Article 323-1/2 :Lorsqu 'il en est rèsultè soit la suppression ou la modification de donnèes contenues dans le système, sait une altèration du fonctionnement de ce systèmè, la peine est de trois ans d' emprisonnement et de 100 000 € d'amende, modifiè par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

إستطاع الجاني إثبات حدوث قوة قاهرة أدت إلى حدوثها، والأمر ذاته ينطبق على المادة 394 مكرر في فقرتها الثانية والثالثة من قانون العقوبات الجزائري.

وعليه فإنه لا يمكن تطبيق الظرف المشدد إذا قصد النتيجة المشددة لإن ذلك يقع مباشرة تحت طائلة المادة 394 مكرر1 من قانون العقوبات الجزائري والمادة 323-3 من قانون العقوبات الفرنسي والمتعلقتين بجريمة التلاعب بالمعطيات والتين تضمنتا فعلي التعديل والإزالة العمديين([1]).

أما بالنسبة لظرف التشديد المتعلق بتخريب نظام اشتغال نظام المعالجة الآلية للمعطيات المنصوص عليه في الفقرة الثالثة من المادة 394 مكرر من قانون العقوبات الجزائري، فهو يتعلق بنتيجة لا تقع في القانون الجزائري إلا غير عمدية أي كظرف تشديد فقط، ولا تقع عمدية على الإطلاق، أما في القانون الفرنسي فقد تقع هذه النتيجة كظرف تشديد غير عمدي (المادة 323-1 من قانون العقوبات الفرنسي) أو كجريمة خاصة عمدية وهي جريمة إعاقة أو إفساد نظام المعالجة الآلية، والتي نصت عليها المادة 323-2 من قانون العقوبات الفرنسي([2]).

وكموقف للقضاء الجزائري عن جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة تمكنت فرقة الجرائم المعلوماتية لأمن ولاية الجزائر من توقيف المشتبه فيه المقيم بولاية باتنة (شرق البلاد) المتورط في قضية الدخول عن طريق الغش لنظام المعالجة الآلية مع البقاء والتغيير وحذف معطيات مخزنة من أجل الإضرار وتعطيل منظومة الإعلام الآلي والموقع الإلكتروني لمؤسسات إتصالات الجزائر، وذلك فور تقديم شكوى من قبل الممثل القانوني لذات المؤسسة، حيث أسفرت التحريات عن تحديد هوية المشتبه فيه، الذي يقيم بولاية باتنة، وتم التوصل إليه بعد إذن تمديد الإختصاص، وبالتنسيق مع فرقة مكافحة الجرائم المعلوماتية لأمن ولاية باتنة، تم تفتيش مسكنه أين حجزت دعائم رقمية أستعملت في عملية القرصنة ممثلة في هاتفين نقالين وجهاز إعلام آلي محمول ووحدة مركزية بلواحقها وقرص صلب خارجي وقرصين داخليين، وقد تم تقديم

---

[1]- بوكر رشيدة، مرجع سابق، ص 241.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 170.

المشتبه فيه إلى وكيل الجمهورية المختص أقلميا الذي إتهمه وفقا للمادة 394 مكرر 1 فقرة 1 وفقرة 3([1]).

**الفرع الثالث: العقوبات المقررة لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة**

نص المشرع الجزائري على العقوبات الأصلية لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة في المادة 394 مكرر الفقرة 2 و3 من قانون العقوبات الجزائري، وعلى العقوبات التكميلية في المادة 394 مكرر 6 من نفس القانون.

**أولا: العقوبات الأصلية**

بالرجوع إلى الفقرة الثانية والثالثة من المادة 394 مكرر من قانون العقوبات الجزائري نلاحظ أنه تم تشديد العقوبة في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة، وتضاعف العقوبة إذا ترتب على الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية حذف أو تغيير لمعطيات النظام عن تلك المقررة للجريمة البسيطة سواء في حدها الأدنى من 3 أشهر إلى 6 أشهر أو في حدها الأقصى من سنة إلى سنتين، أما الغرامة فتضاعف في حدها الأدنى من 50.000دج إلى 100.000 دج أو في حدها الأقصى من 100.000 دج إلى 200.000 دج.

أما إذا أدى الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية إلى تخريب نظام اشتغاله تضاعف العقوبة أيضا سواء في حدها الأدنى من 3 أشهر إلى 6 أشهر أو في حدها الأقصى من سنة إلى سنتين، أما الغرامة فتم تثبيت حدها الأدنى عند خمسين ألف دينار جزائري (50.000 دج) ويرتفع حدها الأقصى إلى مائة وخمسين ألف دينار جزائري(150.000 دج).

كما نص المشرع المغربي على العقوبات الأصلية المقررة لهذه الصورة في الفقرة الأخيرة من الفصل 3-607 من القانون الجنائي، والتي تنص على أنه"

[1]- مقتبس عن: مناصرة يوسف، مرجع سابق، ص 143.

تضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو إضطراب في سيره"([1]).

ويتجسد ذلك من خلال مضاعفة العقوبة المنصوص عليها في هذه الجريمة في صورتها البسيطة المشار لها في الفقرة الأولى من نفس الفصل والمتمثلة بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2000 إلى 10.000 درهم إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو إضطراب في سيره، ومن تم فإن المشرع هنا يحمي النظام من خلال حمايته للمعطيات التي يحتويها.

أما المشرع الفرنسي فقد إتجه إلى تشديد العقاب على جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية في صورتها المشددة بمقتضى المادة 323-1 والتي تقابلها المادة 462 الفقرة2 بحيث جعل عقوبة الحبس سنتين وغرامة مائتي ألف قرنك فرنسي إذا نتج محو أو تعديل للمعطيات المختزنة بالنظام([2])، كما إحتفظ بنفس عقوبة الحبس ورفع عقوبة الغرامة إلى 30.000 يورو في قانون العقوبات لسنة 1994، أما في قانون العقوبات الفرنسي لسنة 2004 فقد رفع العقوبة إلى ثلاث سنوات ورفع الغرامة إلى خمسة وأربعين ألف يورو (45000 يورو)، كما أحتفظ أيضا بنفس عقوبة الحبس ورفع عقوبة الغرامة إلى 100.000 يورو في قانون العقوبات لسنة 2015([3])، ولم يرفع المشرع الفرنسي عقوبة الجريمة المشددة إلى ضعف عقوبة الجريمة البسيطة لسببين في تقديرنا، يتمثل السبب الأول في أن عقوبة الجريمة البسيطة تضاعفت ولا يمكن مضاعفتها مرة أخرى بالنسبة للجريمة المشددة، بينما يتمثل السبب الثاني في إن عدم مضاعفة العقوبة تم إستجابة لإنتقاد الفقه بوجود فارق كبير بين العقوبة البسيطة والمشددة([4]).

---

[1]- مصطفى الفوركي، مقال بعنوان الجرائم الماسة بالنظم المعلوماتية في القانون المغربي، مجلة البحوث القانونية والإقتصادية، المركز الجامعي لافلو، المجلد 2، العدد 1، جانفي 2020، ص 14.

[2]- بلال أمين زين الدين، مرجع سابق، ص 282.

[3] -modifiè par LOI N° 2015-912 DU 24 JUILLET 2015-ART 4, JORF N° 0171 du 26 JUILLET 2015.

[4]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 174.

أما بالنسبة لعقوبة الشخص المعنوي عن جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات في صورتها المشددة فهي كذلك الغرامة المضاعفة خمس مرات عما هو مقرر للشخص الطبيعي، بحسب ما أشارت إليه المادة 394 مكرر 4 من قانون العقوبات الجزائري، وبالتالي تكون قيمتها في هذا القانون بين مائتي وخمسون ألف دينار جزائري(250.000 دج) وسبعمائة وخمسون ألف دينار جزائري(750.000 دج)، في حين تكون قيمتها في قانون العقوبات الفرنسي الجديد لسنة 2004 هي مائتان وخمسة عشرون ألف يورو(225000 يورو).

**ثانيا: العقوبات التكميلية**

إن العقوبات التكميلية المقرر لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة هي نفسها العقوبات التكميلية المقررة لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة سواء في القانون الجزائري أو الفرنسي على النحو الذي سبق الإشارة إليه.

**المبحث الثاني: أركان جرائم المساس بمعطيات نظام المعالجة الآلية**

إن المعطيات كمجموعة من الحقائق أو البيانات التي تتخذ شكل أرقام أو حروف أو رموز أو أشكال خاصة وتصف فكرة أو موضوعا أو حدثا معينا هي عبارة عن مادة خام يستخرج منها بعد معالجتها معلومات معينة تمثل ثروة هامة يمكن أن تكون عرضة لعدة إعتداءات([1]) نص عليها المشرع الجزائري في المادة 394 مكرر1 و394 مكرر2 من القانون 04-15 السالف الذكر، ونظرا لأهميتها وخطورة المساس بها فقد جرم المشرع الجزائري كل سلوك يؤدي إلى المساس بسلامة معطيات النظام سواء كانت موجودة بداخله أو التي لها علاقة به، وذلك بالإدخال أو التعديل أو الإزالة المقصودة غير المصرح بها لمعطيات نظام المعالجة الآلية، كما أنه عزز من هذه الحماية عند إدراجه جريمة أخرى تهدف إلى منع وقوع الجرائم السابقة أو التخفيف من آثارها أن وقعت وهي جريمة التعامل في معطيات غير مشروعة.

لذلك فإن الجرائم التي تمس بمعطيات النظام تكون مرتكزة بحق على معطيات النظام أو على إستخدام هذه المعطيات لأغراض غير مشروعة، وتكون هذه الأخيرة هي المستهدفة بالدرجة الأولى من الإعتداء وليس النظام الذي يتضمنها.

ولدراسة أركان جرائم المساس بمعطيات النظام سنقوم بمعالجة صور هذه الجرائم بالتطرق إلى أركان كل جريمة على حدى من خلال تقسيم هذا المبحث إلى مطلبين يتناول المطلب الأول أركان جريمة التلاعب بالمعطيات أما المطلب نخصصه لأركان جريمة التعامل في معطيات غير مشروعة.

---

[1]- برادل سمير، مقال بعنوان الجريمة المعلوماتية في التشريع الجزائري، مجلة القانون، كلية الحقوق والعلوم السياسية، المركز الجامعي لغيلزان ، المجلد 1، العدد 2 ، جويلية 2010، ص 190.

**المطلب الأول: أركان جريمة التلاعب بالمعطيات**

إن جريمة التلاعب بالمعطيات تقع على بيانات نظم المعالجة الآلية للمعطيات أي البيانات المعالجة دون المعلومة ذاتها، ولذلك يخرج من نطاق هذه الجريمة المعلومات التي لم تعالج بعد([1]).

ونصت الإتفاقية الأروبية في شأن جرائم تقنية المعلومات على هذه الجريمة وذلك بموجب المادة 4([2]) منها تحت عنوان الإعتداء على سلامة المعلومات، كما أن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 هي الأخرى نصت عليها بنفس العنوان في المادة الثامنة([3]) منها.

ولم تكن جريمة التلاعب بالمعلومات في قانون العقوبات الفرنسي لسنة 1988 عما هي عليه الآن، فالفقرة الرابعة(4) من المادة 462 من ذلك القانون تناولت بالتجريم مختلف أنواع السلوك التي تمس بسلامة المعطيات فنصت على ما يلي" كل من يقوم عمدا وبدون مرعاة لحقوق الغير بطريق مباشر أو غير مباشر بإدخال معطيات ذاخل نظام المعالجة الآلية أو يمحو أو يعدل المعطيات التي يتضمنها أو طرق معالجتها ونقلها يعاقب بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 2000 فرنك فرنسي إلى خمسمائة ألف(500000) فرنك فرنسي أو بإحدى هاتين العقوبتين"([4]).

---

[1]- بومعيزة جابر، مقال بعنوان الإعتداء على المعطيات الآلية في الحكومة الإلكترونية، مجلة البحوث والدراسات القانونية والسياسية، جامعة لونيس علي البليدة 2، المجلد 6، العدد 2، جوان 2017، ص 135.

[2]- نصت المادة 4 من الإتفاقية الأروبية في شأن جرائم تقنيات المعلومات على ما يلي" 1-يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم تبعا لقانونه المحلي، ’ذا حدث ذلك عمدا، ودون حق أي ضرر أو محو أو تعطيل، إتلاف أو طمس لبيانات الحاسب.2- يمكن لأي طرف أن يحتفظ بحق اشتراط أن يكون السلوك المنصوص عليه في الفقرة الأولى يؤدي إلى أضرار جسيمة"، مقتبس عن: بوكر رشيدة، مرجع سابق، ص 249.

[3]- نصت المادة 8 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 على جريمة التلاعب بالمعطيات بعنوان الإعتداء على سلامة البيانات بقولها"

1- تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.

2- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تسبب بضرر جسيم".

[4]-Art 462-4 :Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 2 000 F à 500 000 F ou de l'une de ces

ويلاحظ أن عبارات هذه المادة تميزت بالكثير من الغموض وأثارت الكثير من الجدل، مما جعلها محلا لإنتقاد الفقه، فعبارة " بطريق مباشر أو غير مباشر" تميزت بصعوبة التفسير فيما يتعلق بإدخال البيانات وطرق معالجتها أو نقلها... ، وكذلك عبارة " بدون مرعاة حقوق الغير" فهي عبارة جديدة في مصطلح القانون الجنائي وتثير الجدل حول ماهية الحقوق المقصودة، مما جعل الكثير من الفقه ينادي باستبدالها بعبارة "إضرارا بالغير"، وهو ما أدى بالمشرع الفرنسي أن يقوم بتعديل المادتين 462-3 و 462-4 وأحل محلهما المادتين 323-2 و323-3، واستبعدت هذه المادة الأخيرة الخاصة بجريمة التلاعب بالمعطيات عبارة " بدون مرعاة لحقوق الغير" وأحلت محلها عبارة" عن طريق الغش" كما إقتصرت هذه المادة على إدخال أو محو أو تعديل المعطيات ولم تتطرق لطرق معالجتها أو نقلها ليتم بعد ذلك المساوة في العقوبة بين جريمتي التلاعب بالمعطيات وإعاقة وإفساد إنظمة الحاسبات ستة 1994([1]).

وفي عام 2004 أجرى المشرع الفرنسي تعديلا آخر مس به الفصل الثالث الخاص بالجرائم الماسة بنظم المعالجة الآلية، وقد تم تشديد عقوبة الحبس والغرامة المقررة لجريمة التلاعب بالمعلومات، فجاءت المادة 323-3 كما يلي" كل ن أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو محا أو عدل بطريق الغش المعطيات التي يتضمنها يعاقب بعقوبة الحبس حتى 5 سنوات وبغرامة تقدر ب 75000 يورو([2])"، كما إحتفظ أيضا بنفس عقوبة الحبس ورفع عقوبة الغرامة إلى 150000 يورو في قانون العقوبات لسنة 2015([3]).

---

deux peines, Abrogè par LOI N° 92-1336 du 16 dècember 1992-art. 372(v), JORF 23 dècember 1992 en Vigueure le 1er mars 19994 Crèation Loi 88-19 1988-01-05 art.1JORF 6 janvier 1988.

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 177،178.

[2]- بوكر رشيدة، مرجع سابق، ص 247.

[3] - Article 323-3 ; Le fait d'introduire frauduleusement des données dans un système de traitement automatisè, d'extraire, de dètenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende, modifiè par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

وتعتبر الجريمة الثانية التي نص عليها المشرع الجزائري في قانون العقوبات بعد جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية بصورتيها البسيطة والمشددة، ويطلق عليها في بعض التشريعات الأخرى جريمة الإتلاف المعلوماتي، أما قانون العقوبات الفرنسي فنص عليها بعد جريمة إعاقة وإفساد نظم المعالجة الآلية للمعلومات، هذه الأخيرة التي إستغنى المشرع الجزائري على وضع نص خاص لها، وإكتفى بالنص عليها ضمن جريمة الإعتداء على المعطيات (المعلومات) في المادة 394 مكرر1([1])، نظرا للتشابه الكبير بينها وبين جريمة التلاعب بالمعطيات بحيث يصعب في الكثير من الأحيان التمييز بينهما وذلك لأن الأفعال التي تتضمنها جريمة التلاعب تؤدي هي الأخرى إلى إعاقة النظام وإفساده، وقد أخذ المشرع الجزائري بنتيجة إفساد النظام كظرف مشدد فقط لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة، واستبعدها كجريمة قائمة بذاتها([2]).

ومن الواضح تأثر المشرع الجزائري بالمشرع الفرنسي الدي جاء مشابه للوضع في قانون العقوبات الفرنسي بعد تعديله، إذ نصت المادة 394 مكرر 1 والخاصة بجريمة التلاعب بالمعطيات على ما يلي" يعاقب بالحبس من ستة(6) أشهر إلى ثلاث(3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"([3])،

ويلاحظ من هذه المادة أنها جاءت شاملة لكافة أنواع المعطيات ولم تقتصر على وسيلة معينة للتلاعب بالمعطيات، وأنه لا يشترط لقيام جريمة التلاعب أن يكون التلاعب قد تم بعد عملية دخول غير مشروع إلى نظام الحاسب الآلي إذ يستوي أن يكون الدخول مشروعا أو غير مشروع، ومن تم فإن جريمة التلاعب

---

[1]- ختير مسعود، الحماية الجنائية لبرامج الكومبيوتر أساليب وثغرات، دار الهدى، عين مليلة-الجزائر، 2012، ص 120.

[2] - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 175.

[3]- المادة 394 مكرر 1 من القانون 04-15.

بالمعطيات تقوم متى قصدها الجاني، ولا يهم بعد ذلك أن يكون الدخول مشروعا أو غير مشروع، وإن كان يثير في الحالة الأخيرة مسألة التعدد المادي للجرائم بالنسبة لجريمتي الدخول غير المشروع وجريمة التلاعب بالمعطيات فتطبق العقوبة الأشد وفقا للمواد 33 -38 من قانون العقوبات الجزائري([1]).

وسار المشرع الجزائري على نهج المشرع الفرنسي بجعل صياغة المادة المجرمة للتلاعب داخل الأنظمة المعلوماتية تتسم بالمرونة بحيث تستوعب شتى أنواع التلاعب بالمعطيات وتساير التطور المتواصل في هذا المجال وإن كان قد خص بعض أنواع البطاقات بنصوص مستقلة، كالقانون 08-01 المتعلق بالتأمينات الإجتماعية الذي يجرم الإعتداء على بطاقة الشفاء الإلكترونية([2])، غير أن هذا القانون يبقى قاصرا عن حماية باقي أنواع البطاقات([3]).

وفي السنوات الأخيرة أدى التزايد الكبير في إستخدام نظم معالجة البيانات عن بعد إلى زيادة التلاعب في تلك البيانات التي يتم تحويلها عن بعد، والتأثير بشكل كبير في تطوير الوسائل المختلفة المستخدمة للإحتيال في مجال تكنولوجيا المعلومات([4]).

كما

وإن جريمة التلاعب بالمعطيات تقتضي دراسة إركانها والعقوبات المقررة لها، لذلك سنقوم بمعالجة هذه الجريمة بنوع من التفصيل ببيان ركنها المادي في الفرع الأول وركنها المعنوي في الفرع الثاني وكذا العقوبات المقررة لها في الفرع الثالث.

---

[1]- بوكر رشيدة، مرجع سابق، ص 248.

[2]- قانون 08-01 المؤرخ في 2008/01/23 المتمم لقانون رقم 83-11 المؤرخ في 1983/07/02، المتعلق بالتأمينات الإجتماعية، ج ر ج ج، ع 04 المؤرخة في 2008/01/27، ص 4.

[3]- عباوي نجاة، مقال بعنوان الإشكالات القانونية في تجريم الإعتداء على أنظمة المعلومات، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية جامعة ورقلة، المجلد9، العدد 16 ، جانفي 2017، ص 288.

[4]- سامر سلمان الجبوري، جريمة الإحتيال الإلكتروني، منشورات زين الحقوقية، بيروت-لبنان، ط الأولى، سنة 2018، ص 96.

**الفرع الأول: الركن المادي لجريمة التلاعب بالمعطيات**

من خلال الإطلاع على نصوص المواد 394 مكرر1 من قانون العقوبات الجزائري والمادة 323-3 من قانون العقوبات الفرنسي والمادة 4 من إتفاقية الأروبية في شأن جرائم تقنية المعلومات، نستشف أن الركن المادي لجريمة التلاعب بالمعطيات يتم بسلوك إجرامي يرتكبه الجاني، يتحقق بارتكاب فعل الإدخال أو المحو أو التعديل وينصب هذا السلوك على محل معين وهو المعطيات ويستهدف تحقيق نتيجة معينة تتمثل في تغيير الحالة التي تكون عليها المعطيات في بيئتها التقنية.

**أولا: السلوك الإجرامي**

إن المشرع الجزائري في جريمة التلاعب بالمعطيات لا يحمي نظام المعالجة الآلية للمعطيات من الناحية المادية بقدر ما يوفر الحماية للمعطيات الموجودة داخل النظام ذاته، وذلك ضد أي سلوك إجرامي، يتحقق بارتكاب واحد من الأفعال التي نصت عليها المادة 394 مكرر1من قانون العقوبات الجزائري، وهي الإدخال والتعديل والإزالة للمعطيات التي يتضمنها النظام، والتي لا يشترط فيها أن تقع مجتمعة بل يكفي أن يقع فعل واحد منها، والذي يكون كافيا لقيام الركن المادي لهذه الجريمة، وسنتناول فيما يلي كل فعل على حدى:

1- **فعل الإدخال:** يقصد به بإضافة معطيات جديدة لم تكن موجودة من قبل على الدعامة الخاصة سواء كانت خالية أم يوجد بها معطيات من قبل([1])، ويتم ذلك من خلال تغذية الحاسب الآلي ونظامه بالمعلومات والبيانات المراد معالجتها آليا، أو بتعليمات لازمة لعملية المعالجة"([2]).

وإن إدخال المعلومات بصورة غير مشروعة في نظام الحاسب الآلي قد ينتج عنه إضافة إلى تعديل ذاكرة الحاسب الآلي تعديل في المعلومات ذاتها أو تدميرها، وذلك بمحوها كما في حالة إدخال أحد البرامج الخبيثة إلى نظام الحاسب الآلي، والذي يؤدي إلى إلحاق تعديل أو محو بالمعلومات الموجودة داخله إذ يتحقق فعل

---

[1]- علي جعفر، جرائم تكنولوجيات المعلومات الحديثة الواقعة على الأشخاص والحكومة-دراسة مقارنة، مكتبة زين الحقوقية والأدبية، ط الأولى، سنة 2013، ص 535.

[2]- نائلة عادل محمد فريد قورة، مرجع سابق، ص 437.

الإدخال المكون لجريمة الإتلاف المعلوماتي في كل حالة يتم فيها إدخال برنامج خبيث إلى الحاسب الآلي أو يؤدي إلى إضافة معلومات جديدة إلى المعلومات القائمة أصلا والتي قد يلحقها تعديل أو محو في النهاية كنتيجة لهذه الإضافة([1]).

كما أن إدخال المعطيات المحرفة إلى نظام الحاسب الآلي أمر يسهل القيام به في أولى مراحل تشغيل نظام المعالجة الآلية وهي مرحلة إدخال المعطيات لمعالجتها، فهذه الأخيرة تجهز وتحول في هذه المرحلة إلى شكل أو لغة مقروءة من قبل الآلة المستخدمة في المعالجة، ويكون من السهل تغذية الحاسب بمعطيات مغلوطة أو زائفة فيها، وهذا يعد من أهم الأساليب المستعملة في إرتكاب الإحتيال المعلوماتي، ذلك أن جهاز الحاسب الآلي يقوم بتخزين أي معلومات تقدم إليه سواء كانت خاطئة أو صحيحة([2]).

ومن الصور العملية لإدخال معلومات مصطنعة نذكر قيام هذا المسؤول بإدخال أسماء وهمية ضمن كشوف المرتبات، مما ينجم عنه صرف مرتبات شهرية لموظفين وهميين إو تعديل في معدلات الفائدة لبعض العملاء، وقد يكون التلاعب في معلومات العمليات مثل إدخال فاتورة وهمية بإسم أحد الموردين وسائر حالات إدخال معلومات غير صحيحة([3])، كإدخال معلومات وهمية لبيانات شخصية غالبا ما تتعلق بعناصر الذمة المالية بغية تحقيق الأموال([4]).

كما تعرض القضاء الفرنسي لجريمة التلاعب بالمعطيات في العديد من أحكامه، منها ما ذهبت إليه محكمة إستئناف باريس التي آدانت سنة 1990 أحد الأشخاص بتهمة إتلاف المعلومات، وذلك لقيامه بإدخال بيانات غير صحيحة إلى نظام الحاسب الآلي، كما أيدت محكمة النقض الفرنسية سنة 1994 حكما بإدانة أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بتدوين بيانات غير صحيحة تتعلق

---

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 258.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 180.

[3]- بوكر رشيدة، مرجع سابق، ص 253.

[4]- محمد إبراهيم سعد النادي، جرائم الأنترنت بين الشريعة الإسلامية والقوانين الوضعية-دراسة مقارنة، مكتبة الوفاء القانونية، الأسكندرية، الطبعة الأولى، سنة 2017، ص 146.

بالنسب الخاصة بضريبة المبيعات وذلك في الإستثمارت الخاصة بذلك، ثم قام بإدخال بعض هذه البيانات إلى نظام الحاسب الآلي، وذهبت ذات المحكمة في حكم صادر عنها سنة 1999 إلى القول" إن إدخال بيانات يترتب عليها إتلاف لأي من المكونات المنطقية لنظام الحاسب الآلي يعد سلوكا معاقبا عليه ولو كانت للجاني سلطة الدخول إلى النظام"([1]).

وإلى جانب المشرعين الجزائري والفرنسي نصت كثير من القوانين والتي جرمت التلاعب بالمعطيات على الإدخال كصورة من صور الركن المادي لهذه الجريمة ومنها القانون العربي النموذجي الإسترشادي لمكافحة الجرائم المعلوماتية الذي نص على ذلك في الفقرة الثانية([2]) من المادة الثالثة منه، وكذلك فعلت السويد ولكسمبورج، في حين فضلت جهات أخرى تجريم الإضرار القصدي بصفة عامة، وهو ما يسمح باستيعاب كافة مظاهر العبث والإضرار بالمعطيات، وهذا ما هو عليه الحال في إتفاقية بودابست وكذا المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في ريودي جنيرو بالبرازيل في الفترة من 4 إلى 9 سبتمبر 1994، والذي أكدت توصياته على وجوب تضمين قائمة الحد الأدنى للأفعال المتعين تجريمها ومن ذلك جريمة الإضرار بالمعلومات والبرامج بصفة عامة، وكذلك فعل القرار رقم 2005/222 الصادر عن مجلس أروبا في 24 فيفري 2005، والمتعلق بالهجمات الموجهة للأنظمة المعلوماتية وذلك في المادة الرابعة(4) منه، حيث ألزمت الدول الأعضاء في المجلس باتخاذ التدابير اللازمة لتجريم المحو الإضرار والإتلاف وتعديل وإزالة أو رد المعلومات المعلوماتية الغير مفهومة في نظام المعالجة الآلية بطريقة مقصودة([3]).

2- **فعل التعديل**: نصت المادة 394 مكرر1 من قانون العقوبات الجزائري والمادة 323-3 من قانون العقوبات الفرنسي على تجريم فعل تعديل معطيات الحاسب

---

[1]- مقتبس عن: دلخار صلاح بوتاني، مرجع سابق، ص 259.

[2]- نصت الفقرة الثانية من المادة الثالثة من القانون العربي النموذجي على ما يلي" أما إذا دخل عمدا –بطريقة مباشرة أو غير مباشرة- بيانات لنظام المعالجة الآلية للبيانات أو عدل البيانات التي يحتويها أو طريق معالجتها أو نقلها فإنه يعاقب..." أنظر: قرار رقم 417 بشأن مشروع قانون عربي إسترشادي لمكافحة جرائم المعلوماتية.

[3] - بوكر رشيدة، مرجع سابق، ص 255

الآلي بطريق الغش، وكذلك نص عليه القرار رقم 2005/222/jdi الصادر عن مجلس أروبا في 24 فيفري 2005، والمتعلق بالهجمات الموجهة للأنظمة المعلوماتية، وذلك في المادة الرابعة (4) منه، والتي ألزمت الدول الأعضاء في المجلس بإتخاذ التدابير اللازمة لتجريم الأضرار والإتلاف وتعديل وإزالة المعطيات المعلوماتية في نظام المعلومات بطريقة عمدية، في حين لم تتناول المادة الرابعة من إتفاقية بودابست سلوك التعديل بالتجريم وإنما تناولت الإضرار بالمعطيات عموما، وهو ما يتضمن التعديل المؤدي إلى ضرر، إضرار إلى المحو والتعطيل والإتلاف وطمس المعلومات([1]).

ويشير مصطلح التعديل إلى تغيير المعلومات داخل نظام المعالجة الآلية واستبدالها بمعلومات أخرى، كما يشير إلى أي تغيير غير مشروع للمعلومات والبرامج والذي يتم عن طريق إستخدام وظائف وظائف نظام المعالجة الآلية([2]).

وضمن هذا السياق كانت هناك توصية رقم (89) 9 الصادرة عن المجلس الأروبي في سبتمبر 1989 والمتعلقة بالجرائم المعلوماتية قد فرقت بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعطيات والبرامج وبين التعديلات غير المصرح بها والتي لا تؤدي إلى إحداث مثل هذه النتائج بل قد تساعد على تحسين أي من المكونات غير المادية للحاسب الآلي ونظامه، وتضمنت هذه التوصية بندا يطالب بإدراج التعليمات الأولى ضمن القائمة الأساسية للجرائم المعلوماتية في حين يكتفي في الثانية بإدراجها ضمن القائمة الإختيارية، إلا أن غالبية هذه القوانين لم تأخذ هذه التفرقة بعين الإعتبار وجرمت التعديل مطلقا وأن إختلفت التشريعات فيما بينها حول العبارات التي تم إستخدامها في هذا المجال([3]).

وفي الوقت الذي إستخدم فيه المشرع الجزائري والفرنسي مصطلح تعديل المعلومات بشكل مباشر أستخدمت تشريعات أخرى تعبيرات مختلفة وأن كانت تدل

---

1- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 182،183.

2- بوكر رشيدة، مرجع سابق، ص 256.

3-محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 183.

على نفس المعنى مثل قوانين المانيا والبرتغال والنمسا وإسبانيا والتي جرمت الأفعال التي تؤدي إلى عدم قابلية المعلومات لإستعمالها على النحو المعدة له، وكذلك ما نصت عليه المادة الرابعة(4) من إتفاقية بودابست على تجريم الإضرار بالمعلومات مطلقا[1] وهو ما يتضمن التعديل المرتب للضرر فضلا عن المحو والتعطيل والإتلاف والطمس([2]).

كما أن هذه المصطلحات بالرغم من إختلاف مفاهيمها إلا أنها لم تكن محل اعتبار لدى أغلب المشرعين من ناحية العقوبة، حيث ساوت التشريعات بينها في العقوبة وهو ما نراه يتعارض مع مبدأ تفريد العقوبة، فليس من العدل معاقبة الجاني الذي ترتب على سلوكه الإجرامي محو المعلومات الموجودة داخل النظام بنفس العقوبة على من أدى سلوكه إلى تعديل بعض المعلومات دون محوها، لا سيما وأن فعل المحو أشد من فعل التعديل أو الإدخال، أضف إلى ذلك أن صور السلوك الإجرامي المكونة للركن المادي لهذه الجريمة ( الإدخال، المحو، التعديل) قد وردت في التشريعات التي جرمتها على سبيل الحصر، ومن تم فإنه لا يمكن التوسع في تفسيرها ولا القياس عليها بحسب قواعد القانون الجنائي، وبالتالي لا يقع تحت طائلة التجريم أي فعل غيرها ولو كان يمثل إعتداء على المعلومات المعالجة والموجودة في النظام([3]).

3- **فعل الإزالة:** إن فعل الأزالة ليس له مصطلح موحد ، نصت عليه المادة 394 مكرر1 من قانون العقوبات الجزائري([4]) والمادة 323-3 من قانون العقوبات

---

[1]- نصت المادة 4 من إتفاقية بودابست بعنوان التدخل في البيانات على ما يلي:

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما أرتكبت عمدا، وبغير حقك إتلاف، أو محو، أو إفساد، أو تعديل، أو تدمير بيانات موجودة على كومبيوتر.

2- يجوز لطرف أن يحتفظ بحقه في أن يستلزم أن تسبب الأفعال الموضحة بالفقرة 1 في ضرر جسيم، مقتبس عن: مناصرة يوسف، مرجع سابق، ص355.

[2]- بوكر رشيدة، مرجع سابق، ص 256، 257.

[3]- دلخار صلاح بوتاني، مرجع سابق، ص 263.

[4]- نصت المادة 394 مكرر 1 من قانون العقوبات الجزائري المعدل والمتمم بالقانون رقم 04-15، على ما يلي" يعاقب بالحبس من ستة(6) أشهر إلى ثلاث(3) سنوات وبغرامة من 500.000 دج إلى 2.000.000

الفرنسي([1])، وتضمنه قرار مجلس أروبا السالف الذكر، ويختلف التعبير الذي يستعمله كل تشريع في تجريمه لذا الفعل، فاتفاقية بودابست عند تجريمها لمختلف أشكال العدوان على سلامة المعطيات ضمنت المادة الرابعة(4) منها عدة مصطلحات تصب في سياق الإزالة وهي مصطلحات الأضرار، المحو، الإتلاف، الطمس([2])، بينما أستخدم القانون العربي النموذجي مصطلح التدمير والذي يعد أثره أبعد من مجرد الأزالة متناولا أياه بالتجريم في المادة الثالثة(3)([3]) منه ضمن جريمة الإتلاف بصفة عامة.

ويعرف فعل الإزالة بأنه إزالة جزء من المعلومات المسجلة على الدعامة الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعلومات إلى المنطقة الخاصة بالذاكرة، بينما يعرفه الأستاذ (J.P.Buffelan) أنه إقتطاع خصائص مسجلة على دعامة ممنغطة عن طريق محوها أو عن طريق طمسها - أي ضغط خصائص أخرى فوقها - خصائص جديدة تطمس الخصائص القديمة، وكذلك عن طريق تحويل ورص خصائص مزالة في منطقة محفوظة من الذاكرة، أي أن محو المعلومات هي مرحلة لاحقة على عملية إدخال المعلومات فالمحو(الإزالة) تفترض الوجود السابق لعملية الإدخال، بمعنى أن محو المعلومات يعني إزالتها أي تدميرها بصورة كلية أو جزئية([4]).

---

دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"

[1]- Article 323-3 ; Le fait d'introduire frauduleusement des données dans un système de traitement automatisè, d'extraire, de dètenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les donnèes qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende, modifiè par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 184.

[3]- نصت الفقرة الثانية من المادة الثالثة من القانون العربي النموذجي على ما يلي" فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصية يكون الحد ألدنى لعقوبة الحبس ..... ولعقوبة الغرامة..... " أنظر: قرار رقم 417 بشأن مشروع قانون عربي إسترشادي لمكافحة جرائم المعلوماتية.

[4]- دلخار صلاح بوتاني، مرجع سابق، ص 259.

ولقد ميزت التوصية الصادرة عن المجلس الأروبي بين شكلين من أشكال المحو الذي يلحق بالمعلومات، الأول يتعلق بمحو المعلومات تماما، والثاني بإخفاء المعلومات بحبث لا يمكن الوصول إليها دون أن يترتب على ذلك محوها تماما([1]).

ومن القضايا التي تتعلق بهذا الفعل قضية شركة TRW Company Credit data الأمريكية التي كانت تعمل على تزويد عملائها (بنوك، شركات، متاجر...) بمعلومات من خلال أنظمة حاسباتها الآلية تتعلق بالمركز الإئتماني لأفراد الجمهور نظير أشتراك يدفعه هؤلاء العملاء، وكانت هذه الشركة تضم في أنظمة حاسباتها معطيات تتعلق بحوالي خمسين مليون شخص عام 1976، وقد أشتغل موظف بالشركة يعمل كاتبا بقسم علاقات المستهلكين هذا النشاط وقام ببيع مراكز إئتمانية جيدة، قام باختلاقها لذي المراكز الإئتمانية الرديئة مقابل مبلغ معين من المال يدفعه هؤلاء، وذلك عن طريق محو المعطيات المتعلقة بالمراكز الإئتمانية الرديئة أو تعديلها أو إستبدالها بمعطيات يمليها أصحاب تلك المراكز لتحسن من مركزهم الإئتماني ليحصلوا على سجل إئتماني نظيف.

ويلاحظ أن هذه العملية كانت تتضمن مختلف أشكال التلاعب بالمعطيات وهي الإزالة والتعديل والإدخال، بحيث أن هذا الموظف كان يزيل بعض المعطيات ويدخل محلها أخرى ويعدل معطيات ثالثة.

و كنتيجة لهذه التلاعبات فقد تورط العديد من عملاء الشركة في معاملات مالية وتجارية مع أشخاص ذو سمعة إئتمانية سيئة، ولم يتم إكتشاف هذه الجريمة إلا بعد تبليغ يقدم به أحد الأشخاص إلى مكتب التحقيقات الفيدرالي FBI بعدما تلقى عرضا من ذلك الموظف بتحسين سجله الإئتماني مقابل مبلغ معين([2])

وفضلا عما سبق فإن الأفعال السابقة لا يتم المعاقبة عليها إلا إذا أرتكبت بدون تصريح، وبالتالي فلا جريمة ولا عقوبة إذا كان إتيان هاته السلوكات مصرح به من

---

[1]-علي جعفر، جرائم تكنولوجيات المعلومات الحديثة الواقعة على الأشخاص والحكومة-دراسة مقارنة، مرجع سابق، ص 536.

[2]- مقتبس عن: محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 184،185.

مالك النظام أو مالك جزء منه، كما في حالة الأنشطة العادية المتضمنة في تصميم الشبكات أو تطبيقات شائعة للتشغيل أو لممارسات تجارية([1]).

**ثانيا: محل النشاط الجرمي**

أن النشاط الجرمي في جريمة التلاعب بالمعطيات يرد على محل معين وهو المعطيات أي المعلومات التي تمت معالجتها آليا والموجودة داخل النظام، محلية كانت أو منبع مشرك Source Partagè التي تشكل جزء منه([2])، وبذلك يخرج من نطاق هذه الجريمة المعلومات التي لم تعالج بعد ولم تدخل إلى نظام المعالجة الآلية والمعلومات التي أدخلت نظام المعالجة ولكن تبدأ بعد أي خطوة في طريق معالجتها، وكذلك المعلومات التي إنفصلت عن النظام وسجلت على شريط ممنغط أو قرص مدمج، كونها أصبحت خارج النظام([3]).

وتأسيسا على ذلك فإن الحماية الجنائية في هذه الجريمة تكون قائمة ومستمرة طالما أن المعلومات المعالجة أو التي في طريقها إلى المعالجة بأن أتخذت خطوة أو أكثر من مراحل معالجتها موجودة داخل النظام أو المعلومات المعالجة التي خرجت عن النظام ثم أعيد أدخالها فيه([4])، أما بالنسبة للمعلومات غير المعالجة التي لم تدخل في النظام أو دخلت ولم تبدأ معالجتها أو تمت معالجتها وانفصلت عن النظام ولو بعد فترة قصيره فهي تعد خارج نطاق الحماية الجنائية، وأن كانت تجوز حمايتها وفق نصوص جنائية أخرى([5])، وهذا ما يستخلص بوضوح من نص المادة 394 مكرر1 من قانون العقوبات الجزائري بقولها" ...بطريق الغش المعطيات التي يتضمنها..."، وكذلك المادة 323-3 من قانون العقوبات الفرنسي بقولها" ...المعطيات التي يتضمنها..."، وذات المعنى أكدته الفقرة الثانية من المادة الثالثة من القانون العربي النموذجي الموحد بقولها" ...أو عدل البيانات التي يحتويها...".

---

[1]- بوكر رشيدة، مرجع سابق، ص 259.

[2]- مناصرة يوسف، مرجع سابق، ص 153.

[3]- دلخار صلاح بوتاني، مرجع سابق، ص 256.

[4]- بوكر رشيدة، مرجع سابق، ص 262.

[5]- دلخار صلاح بوتاني، مرجع سابق، ص 258.

**ثالثا: النتيجة الإجرامية**

يعتبر المشرع الجزائري أن معظم جرائم نظام المعالجة الآلية جرائم خطر، ذلك أن المشرع يستشعر خطورة الجاني من السلوك المجرد الذي يقوم به ولا يشترط أن يترتب على حصوله أثر مادي ضار حتى يتم العقاب عليه، وبمعنى آخر لم يشترط لوقوعها أن يترتب على السلوك الإجرامي نتيجة مادية محسوسة وضارة تمثل عدوانا فعليا على المعطيات، وإنما أكتفى فيها لقيام الجريمة بالعدوان المحتمل أو التهديد بالخطر أي بحظر العدوان الفعلي على المعطيات، وهذا الوضع مطابق لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية.

أما بالنسبة لجريمة التلاعب بالمعطيات فهي من الجرائم المادية التي لا يكفي فيها أن تهدد سلامة المعطيات بخطر الإزالة أو التعديل أو الإدخال وإنما لا بدا من وقوع ضرر فعلي على هذه المعطيات يؤدي إلى تغيير حالتها من خلال تلك الأفعال التي تمثل النشاط الجرمي لهذه الجريمة([1]).

ومن تم فإن المشرع يتطلب نتيجة معينة من خلال السلوك الإجرامي في جريمة التلاعب بالمعطيات تتمثل في تغيير حالة المعطيات بالتعديل والإزالة، وهي نفسها النتيجة التي يترتب عليها تشديد العقوبة في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة، وما يميزهما أن هذه النتيجة في الجريمة الأخيرة تتم دائما بعد دخول أو بقاء غير مصرح بهما وتكون غير عمدية، بينما تتم في جريمة التلاعب بالمعطيات بعد دخول أوبقاء مصرح بهما أو غير مصرح بهما وتكون دائما عمدية يقصد الجاني إحداثها([2]).

أما عن موقف القضاء الجزائري فقد تجاوب مع هذا النوع من الجرائم في السنوات الأخيرة، وكمثال عن ذلك نستعرض القرار الجزائي لمجلس قضاء الجزائر الصادر عن الغرفة الثامنة، رقم الفهرس 09870/14 الصادر بتاريخ 2014/06/29، غير منشور، الذي تمت فيه متابعة(ق.ل) لإرتكابها بتاريخ 2013/02/03 جنحة المساس بأنظمة المعالجة الآلية للمعطيات أضرارا بالطرف

---

[1]- بوكر رشيدة، مرجع سابق، ص 268.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 186.

المدني مدير ديوان رياض الفتح ، الفعل المنصوص والمعاقب عليه بالمادة 394 مكرر 1 من قانون العقوبات الجزائري

وتتلخص وقائع القضية أنه بتاريخ 2013/02/03 تقدم المدير العام لديوان رياض الفتح بواسطة محاميها بشكوى مصحوبة بإدعاء مدني ضد (ق ل) من أجل واقعة المساس بأنظمة المعالجة الآلية للمعطيات، وأفاد في شكواه أن المشتكى منها كانت تشغل منصب عالي في الإدارة العامة للديوان الى غاية 2012/11/14، أين قدمت إستقالتها، وبتاريخ 2012/12/04 تم تنحيتها من منصب الإدارة العامة وإعادة إدماجها في منصب عملها الأصلي، وتم بنفس التاريخ التوقيع على محضر تسليم المهام بينها وبين الموظف المعين في المنصب العالي الجديد(ك.ه) غير أنها لم تقدم له الملفات المتعلقة بالأشغال المنجزة من طرف مختلف المصالح التابعة لمديرية الإدارة العامة وأن المسؤول الجديد عند تصفحه للوحدة المركزية للحاسوب لإعداد ميزانية 2012 تفاجأ بحذف كل المعطيات وأن المشتكى منها قامت بنفس الأفعال في جهاز الإعلام الآلي التابع للإمانة العامة للمديرية وعند مراسلتها للمدير العام لتبرير حذف هذه المعطيات من الجهازين أعترفت بحيازتها للمعطيات المتحصل عليها عند حذفها من الجهازين وعند سماع المشتكى منها أمام السيد قاضي التحقيق أنكرت وأفادت بأن الشاكي طلب منها القيام بإجراءات غير قانونية فرفضت وقدمت إستقالتها فرفضها ثم قام بإبعادها من منصبها وبعد رجوعها من العطلة أبلغت كتابيا بحذف بعض المعطيات من جهاز الإعلام الآلي فسلمت لهم نسخا من الملفات التي كانت تحتفظ بها في الذاكرة وأنها تحصلت على البراءة عند مثولها أمام مجلس التأديب بتاريخ 2013/02/07 وأن المدير العام لم يقتنع بما توصل إليه مجلس التأديب فقام باستدعائها مرة أخرى بتاريخ 2013/02/18 بسبب ظهور معطيات جديدة لم يفصح عنها، الأمر الذي جعل البعض من أعضاء لجنة التأديب خصوصا ممثلي العمال يرفضون إعادة النظر في قضيتهاويتمسكون ببرائتها وتنفيذا لمنطوق لجنة التأديب تم إجراء محاولة الصلح مع مفتشية العمل إلا أن المديرية العامة رفضت إرجاعها إلى منصب عملها وتم تحرير محضر عدم المصالحة بتاريخ 2013/03/27 وأن القضية مازالت مطروحة أمام العدالة، وبعد

سماع الشاهد(ك.هـ) أصدر قاضي التحقيق أمر بأن لا وجه للمتابعة بتاريخ 2013/05/27، وفصلا في الأمر المذكور، أصدرت غرفة الإتهام بتاريخ 2013/07/03 قرار بإلغاء الأمر المذكور ومواصلة التحقيق بإجراء خبرة تقنية وهي الخبرة التي خلصت إلى أن جهاز الإعلام الآلي تعرض ألى عملية مسح آلية بتاريخ 2012/12/13 وتم حفظ الملفات المسترجعة على نفس القرص وأن عمليات الحذف تمت على عدة فترات متفرقة في أواخر سنة 2012، وأنه لا يمكن تحديد تواريخ الحذف بصورة دقيقة بحكم أن نظام الجهاز لا يحتفظ بمثل هذه المعطيات لعدم أهميتها وتم توجيه الإتهام للمشتكى منها ق ل وإستجوابها ثم إحالتها على محكمة الجنح بمحكمة سيدي أمحمد بالجزائر العاصمة وأصدرت حكم بتاريخ 2014/04/08، يقضي ببراءة المتهم على أساس نتائج الخبرة التقنية التي أمرت بها غرفة الإتهام وتم إستئناف الحكم الصادر عن محكمة سيدي أمحمد بالجزائر العاصمة أمام مجلس قضاء الجزائر

فقضى قضاة المجلس بتأييد الحكم المستأنف الصادر عن محكمة سيدي أمحمد بالجزائر الصادر بتاريخ 2014/04/08، القاضي ببراءة المتهم على أساس أن الخبرة التقنية التي أمرت بها خلصت إلى أن جهاز الإعلام الآلي تعرض إلى عملية مسح آلية بتاريخ 2012/12/13 وتم حفظ الملفات المسترجعة على نفس القرص وأن عمليات الحذف تمت على عدة فترات متفرقة في أواخر سنة 2012، وأنه لا يمكن تحديد تواريخ الحذف بصورة دقيقة بحكم أن نظام الجهاز لا يحتفظ بمثل هذه المعطيات لعدم أهميتها وينعدم الدليل في قضية الحال بناء لما توصلت إليه نتائج الخبرة التقنية التي لم تسند للمتهمة واقعة المحو والحذف للمعطيات ولم تحدد تاريخه بدقة([1]).

ونلاحظ من خلال إطلاعنا على هذا القرار أن له طرفين متنازعين وهما الطاعن (مدير ديوان رياض الفتح بالجزائر العاصمة) والمطعون ضده (ق ل موظفة بديوان رياض الفتح)، بحيث قام الطاعن عن طريق محاميه بتقديم شكوى مصحوبة بإدعاء مدني ض (ق ل) من أجل واقعة المساس بأنظمة المعالجة الآلية للمعطيات،

[1]- مقتبس عن: مناصرة يوسف، مرجع سابق، ص ص 154-156.

والتي أثير من خلالها الإشكال القانوني الآتي: الى أي مدى تتجه نية المشتكى منها بالحاق الضرر بسلامة معطيات ديوان رياض الفتح من عدمه؟

فكان الحل القانوني لهذا الإشكال بالرجوع إلى نص المادة 394 مكرر1 والتي نجم عن تطبيقها منطوق القرار القاضي برفض الطعن المقدم من المدعي والحكم عليه بأداء المصاريف.

وبالتالي فإننا نستشف من هذه القضية بإن المشتكى منها(ق.ل) لم تقم بأي عمل يمس بسلامة المعطيات الموجودة داخل منظومة ديوان رياض الفتح بالجزائر العاصمة، سواء بإدخال معلومات غير صحيحة أو تعديلها وتغييرها أو حذفها، ولعل براءتها أمام مجلس التأديب بتاريخ 2013/02/07 إضافة الى إجراء محاولة الصلح تنفيذا لمنطوق لجنة التأديب وسماع الشاهد ك هـ كلها أدلة على أنها لم ترتكب أي سلوك من السلوكات المنصوص عليها في المادة 394 مكرر1(الإدخال، التعديل، الإزالة).

**الفرع الثاني: الركن المعنوي لجريمة التلاعب بالمعطيات**

إن جريمة التلاعب بالمعطيات تعتبر من الجرائم العمدية، والتي لا بدا لقيامها من توافر قصد جنائي عام لدى مرتكبها، ومع ذلك ذهبت بعض التشريعات إلى طلب قصد جنائي خاص إضافة إلى القصد الجنائي العام.

**أولا: القصد الجنائي العام**

يتحقق القصد الجنائي العام وفق القواعد العامة بتوافر عنصريه العلم والإرادة وانصراف كليهما إلى كافة العناصر التي يتكون منها الركن المادي للجريمة، وفي جريمة الإتلاف المعلوماتي(جريمة التلاعب بالمعطيات) ينبغي أن ينصرف علم الجاني إلى أنه يقوم بإدخال أو تعديل أو محو(إزالة) المعلومات وأن يعلم بأن نشاطه غير مشروع، ويشكل إعتداء على صاحب الحق في المعلومات أو من له السيطرة عليها، وأن من شأن نشاطه هذا أن يؤدي إلى نتيجة هي تغيير حالة المعلومات، ومن تم تتجه إرادته إلى هذا النشاط وتلك النتيجة([1]).

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 264.

ولا يشترط أن يكون القصد الجنائي مباشرا، أي أن تكون إرادة الجاني قاطعة في إتجاهها لإحداث النتيجة المتحققة، بل يكفي لقيام العمد أن تتخذ الإرادة شكل القبول أي قبول النتيجة، وهذا ما يسمى بالقصد غير المباشر أو القصد الإحتمالي، وفيه يستوي لدى الجاني وقوع النتيجة من عدمها([1])، كما لا يشترط أن يكون القصد محددا، إذا تقوم الجريمة سواء حدد القصد بمعلومات معينة أو لم يحدد، فلا فرق في التشريع الجزائري والفرنسي بين اتجاه إرادة الجاني إلى معلومات دون أخرى ويعد مرتكبا للجريمة من سعى للتلاعب بمعلومات ما فاعتدى على أخرى([2]).

والمعلومات كلها سواء في الحماية الجنائية، فلا يقتضي توافر الركن المعنوي في هذه الجريمة أي قصد جنائي خاص كنية الإضرار أو قصد الأضرار بالغير، والجريمة تقوم بتحقق ركنها المادي بمجرد إتيان فعل الإدخال أو المحو أو التعديل المنصب على المعلومات مع ركنها المعنوي المتمثل بعلم الجاني بذلك وتوجه إرادته إليه وإن كان الضرر قد يتحقق في الواقع نتيجة لهذه الأفعال إلا أنه ليس عنصرا في الجريمة([3])، وإذا كان الأمر على هذا الحال في قانون العقوبات الجزائري والفرنسي فإن الأمر يختلف في قوانين أخرى حيث تفرق بين المعلومات في الحماية، فتقوم بحصرها في أنواع معينة من المعلومات دون أنواع أخرى، ومن أمثلة ذلك ما تنص عليه المادة 1030(أ) من التشريع الفيدرالي الأمريكي لسنة 1986، والتي تجرم الإتلاف المقصود وغير المصرح به لمعلومات يحتوي عليها حاسب آلي تابع لحكومة الولايات المتحدة الأمريكية أو إدارتها أو حاسب آلي غير تابع للحكومة إلا أنه يستخدم من قبلها أو لصالحها، ووسع قانون لحماية بنية المعلومات القومية لعام 1996 من نطاق المعلومات محل الحماية ليشمل فضلا عما سبق المعلومات التي تحتويها الحاسبات التي يتم إستخدامها من قبل المؤسسات الإقتصادية التابعة

---

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 187.

[2]- بوكر رشيدة، مرجع سابق، ص 270.

[3]- دلخار صلاح بوتاني، مرجع سابق، ص 264.

لحكومة الولايات المتحدة وكذلك تلك التي تستخدم في التجارة والإتصالات بين الولايات أو بين الولايات والدول الأخرى([1]).

**ثانيا: القصد الجنائي الخاص**

يستفاد من نص المادة 394 مكرر1 أن المشرع الجزائري لا يتطلب توافر قصد خاص لدى الجاني لقيام جريمة التلاعب بالمعطيات، ذلك أن القصد الخاص هو إنصراف العلم والإرادة إلى وقائع لا تدخل ضمن عناصر الجريمة وأركانها.

وهو ما ذهب إليه المشرع الفرنسي، حيث أنه وبالرجوع إلى المادة 323-3 لم نجد ما يشير إلى تطلبه القصد الخاص لدى الجاني لكي تقوم جريمة التلاعب غير المصرح به بالمعلومات وإنما إكتفى بتوافر القصد العام، ويستفاد هذا بوضوح من عدم نصه في هذه المادة على نية خاصة كنية إلحاق الأذى أو تسبيبه للآخرين، وهو ما إستقر عليه القضاء في فرنسا وأكده في عدة أحكام له([2]).

وأن لفظ الغش لا يدل على هذا المعنى وإنما يدل على ضرورة توافر العمد أي القصد الجنائي العام، وهو ما أخذ به المشرع الفرنسي في المادة 323-3 من قانون العقوبات الفرنسي الحالي وأن كانت المادة 462- 4 قد أثارت جدلا كبيرا عندما نصت على عبارة" دون مرعاة لحقوق الآخرين"، واختلف الفقه حول هذه العبارة وفسرها البعض بضرورة توافر قصد خاص لدى الجاني يتمثل في نية الإضرار بالمجني عليه، أما بالنسبة لمصطلح"الغش" في المادة 323-3 الذي حل محل العبارة السابقة فقد تساءل بشأنه عضو مجلس الشيوخ Thyraud قائلا" إذا لم نضف هذا المصطلح فإن النص سيفهم فهما سيئا لأن فعل الإدخال العمدي للمعطيات داخل الإنظمة هو صميم المعلوماتية"

في حين أن الحجة التي إستند إليها في الجمعية الوطنية الفرنسية لتبرير إضافة هذا المصطلح هو أن إدخال المعطيات في نظام المعالجة الآلية للمعطيات أو إزالتها أو تعديلها هي بالتحديد الوظيفة التي يقوم بها المعلوماتيون ومستخدموا المعلوماتية، وأن هذه الجريمة لا تتحقق إذا أرتكبت هذه العمليات بقصد الغش وخارج

---

[1]- بوكر رشيدة، مرجع سابق، ص 270.

[2]- بوكر رشيدة، مرجع سابق، ص 271.

الإستعمال المرخص به من طرف مقدمي الخدمات، إضافة إلى أن هناك من يرى بأن "الغش" في نص تلك المادة يعني وجود قصد خاص وهو إرادة تسبيب ضرر للغير في ماله أو في حقوقه على إختلاف طبيعتها([1]).

وفي الواقع أن أغلب التشريعات التي جرمت أفعال الإتلاف المعلوماتي (التلاعب بالمعطيات) لم تتطلب قصد خاص يقوم عليه الركن المعنوي لهذه الجريمة، إلا فئة قليلة من هذه التشريعات مثل قانون العقوبات الفلندي الذي تطلب إتجاه نية الفاعل إلى الإضرار بالغير وقانون العقوبات البرتغالي الذي تطلب مثل هذا الإضرار أو تحقيق ربح غير مشروع للفاعل أو لغيره وقانون العقوبات التركي الذي تطلب نية إيذاء الغير أو الحصول على ربح مادي([2]).

غير أن البعض أنتقد تطلب هذا القصد الخاص في جريمة الإتلاف المعلوماتي، وبخاصة قصد تحقيق ربح مادي غير مشروع، لأن ذلك سوف يستبعد من نطاق هذه الجريمة جميع الحالات التي لا تتجه فيها نية الجاني إلى تحقيق ربح مادي غير مشروع على الرغم من أهمية المعلومات التي قد يتم إتلافها كما في حالة إتلاف معلومات علمية أو طبية، أما فيما يتعلق بالقصد الخاص المتمثل في الإضرار بالغير فيجب بحسب هذا الرأي أن يفسر تفسيرا واسعا بحيث لا يقتصر على مجرد الخسائر أو الأضرار المادية التي قد تصيب المجني عليه([3]).

والحقيقة نرى إن إشتراط القصد الخاص يؤدي في الكثير من الأحيان إلى إفلات الجناة من العقاب، لذلك ذهب الأستاذ الفرنسي Vergutch إلى إنتقاد تطلب القصد الخاص في جريمتي الإتلاف المعلوماتي وإعاقة النظام المعلوماتي، لا سيما إذا تعلق هذا القصد بنية تحقيق ربح مادي غير مشروع لأن مفاد إشتراط هذا القصد سيؤدي إلى إستبعاد جميع الحالات التي لا يتحقق فيها هذا الربح المادي غير

---

1- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 188،189.

2- عمار عباس الحسيني، جريمة الإتلاف المعلوماتي-دراسة مقارنة، منشورات زين الحقوقية، بيروت-لبنان، ط الأولى، سنة 2019، ص 194.

3- دلخار صلاح بوتاني، مرجع سابق، ص 256.

المشروع من نطاق تجريم أفعال الإتلاف المعلوماتي وأن كانت المعلومات التي وقع غليها الأتلاف بالغة الأهمية([1]).

ومتى توافر القصد العام (في التشريع الجزائري والفرسي) والخاص ( في التشريعات التي تطلبت ذلك) على النحو السالف الذكر، فلا عبرة بعد ذلك بالباعث على إرتكاب الجريمة، أذ أن الباعث ليس من عناصر القصد، فإذا قام الفاعل بالتلاعب بالمعطيات المبرمجة لإظهار مهارته في مجال تكنولوجيا نظم المعالجة الآلية، فإن توافر مثل هذه البواعث لا ينفي قصد التلاعب([2]).

وبالرجوع الى القضية التي تم الإشارة لها سابقا، نجد أن المشتكى منها (ق.ل) لم تتجه إرادتها الى التلاعب بتلك المعطيات أو المساس بسلامتها، ولعل تسليم نسخ من تلك الملفات التي كانت تحتفظ بها في الذاكرة دليل على أن إرادتها لم تتجه إلى الإضرار بالطرف المدني ديوان رياض الفتح بالجزائر العاصمة، كما أنها لم تقم بأي عمل يدل على ذلك بل أحتفظت بهذه المعطيات بعد عملية الحذف وعندما طلبت منها قامت بتسليمها، لذلك فإن حذف أو محو تلك المعطيات لم يسند الى المتهمة ولم يحدد تاريخه بدقة، ولأن المسألة تقنية محضة فقد طلبت غرفة الإتهام إستئناف أمر قاضي التحقيق بأن لا وجه للمتابعة الصادر بتاريخ 2013/05/27 ومواصلة التحقيق بإجراء خبرة تقنية، وهي الخبرة التي خلصت الى أن جهاز الإعلام الآلي تعرض لعملية مسح آلية بتاريخ 2012/12/13 وتم حفظ الملفات المسترجعة على نفس القرص، وأن عمليات الحذف تمت على عدة فترات متفرقة في أواخر سنة 2012، وأنه لا يمكن تحديد تواريخ الحذف بصورة دقيقة بحكم أن نظام الجهاز لا يحتفظ بمثل هذه المعطيات لعدم أهميتها.

وبناء على هذه الخبرة ثبت أنه ليس للمعنية قصد عام أو خاص للإضرار بالطرف المدني ديوان رياض الفتح بالجزائر العاصمة، وعليه تمت تبرئتها بداية بموجب حكم، وفي الإستئناف بموجب قرار جزائي، والذين تمت الإشارة لهما سالفا.

---

[1]- عمار عباس الحسيني، مرجع سابق، ص 197،198.

[2]- بوكر رشيدة، مرجع سابق، ص 273.

**الفرع الثالث: العقوبات المقررة لجريمة التلاعب بالمعطيات**

نص المشرع الجزائري في المادة 394 مكرر1 من قانون العقوبات على العقوبات الأصلية لمرتكب جريمة التلاعب بالمعطيات والمتمثلة في الحبس والغرامة، وفي المادة 394 مكرر6 على العقوبات التكميلية التي تشترك فيها مع باقي الجرائم الأحرى لنظام المعالجة الآلية للمعطيات.

**أولا: العقوبات الأصلية**

نص المشرع الجزائري في المادة 394 مكرر1([1]) من قانون العقوبات الجزائري على العقوبة الأصلية لمرتكب جريمة التلاعب بالمعطيات، بعقوبة الحبس من ستة(6) أشهر إلى ثلاث(3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، على كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق المعطيات التي يتضمنها.

أما المشرع الفرنسي فقد ذهب في القانون الخاص بالجرائم المعلوماتية بالرقم (88-19) والصادر في 22 ديسمبر 1987 والنافذ في 5 يناير 1988 إلى العقاب على هذه الجريمة بالحبس لمدة تتروح بين ثلاثة شهور وثلاث سنوات وبغرامة تتروح بين 2000 و 500.000 الف فرنك فرنسي، أو بإحدى هاتين العقوبتين، كل من أدخل عمدا إلى نظام المعالجة الآلية للمعلومات بطريق مباشر أو غير مباشر وبدون مرعاة لحقوق الغير، بيانات أو محا أو عدل في البيانات التي يحتويها أو في طريق معالجتها أو نقلها، إلا إن الإنتقادات الفقهية التي وجهت إلى بعض نصوص هذا القانون، ومن ضمنها هذا النص المشار إليه أدت بالمشرع الفرنسي إلى تجنب هذه الإنتقادت في قانون العقوبات الجديد الصادر سنة 1994، الذي أدمج نصوص قانون 1988 بين طياته في المواد (1/323-7) والتي جاءت تحت عنوان" الإعتداءات على نظام المعالجة الآلية للمعطيات" المضافة إلى قانون العقوبات الجديد([2])، الذي جعل حدا واحد لهذه العقوبة إذ أزال الحد الأدنى لها وثبتها عند الحد الأقصى وهو 3 سنوات أما عقوبة الغرامة فجعلها خمسة وأربعين ألف

---

[1]- المادة 394 مكرر 1 من القانون رقم 04-15.

[2]- عمار عباس الحسيني، مرجع سابق، ص 208،209.

يورو(45000 يورو)، أما في قانون العقوبات الفرنسي لسنة 2004 قام بتشديد العقوبة أكثر إذ رفع عقوبة الحبس إلى خمس(5) سنوات وعقوبة الغرامة إلى خمسة وسبعين ألف يورو ( 75000 يورو)، كما إحتفظ أيضا بنفس عقوبة الحبس ورفع عقوبة الغرامة إلى 150000 يورو في قانون العقوبات لسنة 2015([1]).

وبذلك يكون قد إستجاب للنقد الموجه له من طرف الفقه بكون جريمتي التلاعب بالمعطيات وجريمة الدخول أو البقاء غير المصرح بهما في صورتها المشددة متقاربتين في العقوبة وهو تقارب بين جريمة عمدية وأخرى غير عمدية، برفعه لعقوبة جريمة التلاعب بالمعطيات إلى خمس(5) سنوات، بينما رفع عقوبة جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة إلى ثلاث (3) سنوات.

والملاحظ أن عقوبة جريمة التلاعب بالمعطيات تفوق عقوبة جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية سواء كانت في صورتها البسيطة أو المشددة لأنها في صورتها البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات وبنظام معالجتها، وحتى في صورتها المشددة وأن أدت إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي إزالة المعطيات أو تعديلها فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية بتوافر لدى مرتكبها القصد الجنائي للتلاعب بينما لا يتوافر هذا القصد لدى جريمة الدخول أو البقاء في صورتها المشددة، فالموقف النفسي لكل واحد منهما إتجاه التلاعب مختلف، حيث يريده الأول ولا يريده الثاني([2]).

أما في قانون العقوبات في لوكسمبورج فقد ذهب إلى تجريم أفعال الإتلاف الواقعة على المعلومات التي يحتوي عليها نظام المعالجة الآلية وطرق معالجتها ونقلها، وكذلك قانون العقوبات الإلماني الذي عاقب على تخريب وإتلاف بيانات

[1] - Article 323-3 ; Le fait d'introduire frauduleusement des données dans un système de traitement automatisè, d'extraire, de dètenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende, modifiè par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

[2] - محمد خليفة،الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص191.

الحاسوب، كما ذهبت في نفس الإتجاه كل من هولندا والسويد وسويسرا والنمسا وفلندا وإيطاليا واليابان([1]).

وبالنسبة لعقوبة الشخص المعنوي المرتكب لجريمة التلاعب بالمعطيات في القانون الجزائري هي الغرامة المضاعفة إلى خمس مرات عما هو مقرر للشخص الطبيعي، وبالتالي تكون قيمتها متراوحة مليونين وخمسمئة ألف وعشرة ملايين دينار جزائري( من 2.500.000 دج إلى 10.000.000 دج)، بينما تصل قيمتها في القانون الفرنسي إلى ثلاثمائة وخمسة وسبعون ألف يورو(375000 يورو).

**ثانيا: العقوبات التكميلية**

أن العقوبات التكميلية المقررة لجريمة التلاعب بالمعطيات هي نفسها العقوبات التكميلية المقررة لباقي جرائم نظام المعالجة للمعطيات سواء تلك المشار لها في المادة 394 مكرر6 من قانون العقوبات الجزائري، أو في المادة 323-5 من قانون العقوبات الفرنسي.

**المطلب الثاني: أركان جريمة التعامل في معطيات غير مشروعة**

إن الإعتداء على معطيات نظام المعالجة الآلية يعد من أخطر الجرائم التي تلحق أضرارا بالدول والأفراد خاصة إذا كانت تلك المعطيات التي يتضمنها النظام تتعلق بأمن الدولة أو تتعلق بالحياة الخاصة أو تمثل قيمة مالية مهمة، لذلك حرص المشرع الجزائري على تبني سياسية جزائية تكفل الوقاية من هذه الجرائم بالتصدي لها قبل وقوعها أو التخفيف من آثارها أن وقعت.

ونظرا لكون معطيات النظام على قدر كبير من الأهمية فقد أولى لها المشرع الجنائي حماية خاصة، فقام بتجريم مجموعة من الأفعال التي تتعلق بالتعامل في معطيات تصلح لأن ترتكب بها إحدى الجرائم التي تمس بسرية المعطيات أو سلامتها أو إتاحتها أو وفرتها، وقد أشارت المذكرة التفسيرية لإتفاقية بودابست لسنة 2001 إلى ضرورة الوقاية هذه الأفعال، فقالت: ومن أجل وقاية أكثر فعالية من هذه

[1]- عمار عباس الحسيني، مرجع سابق، ص 213.

المخاطر فأنه يجب على قانون العقوبات أن يحظر الأفعال الراجحة الخطورة من المنبع، قبل إرتكاب الجرائم المشار إليها في المواد (من 2 إلى 5)([1]).

وهو ما أتجه إليه كذلك المشرع الفرنسي فنص على تجريم مجموعة من الأفعال التي تتعلق بالتعامل في معطيات صالحة لإرتكاب جريمة في المادة 323-1/3، وهذا الأمر يبدو طبيعيا على اعتبار أن فرنسا قد صادقت على إتفاقية بودابست، والتي نصت على تجريم هذه الأفعال في المادة 6 منها تحت عنوان " إساءة إستخدام الأجهزة".

في حين لم يتناول القانون اليمني هذه الجرائم كغيرها من جرائم المعلوماتية بحيث لا زالت النصوص التقليدية في قانون العقوبات اليمني هي التي يتم محاولة تطبيقها على هذه الجرائم بالرغم من أنها تثير العديد من الإشكاليات التي قد تحول دون تطبيق هذه النصوص([2]).

أما المشرع الجزائري فقام بتجريم العديد من الأفعال من خلال جريمة التعامل في معطيات غير مشروعة المنصوص عليها في المادة 394 مكرر2 من قانون العقوبات الصادر بموجب الأمر 66-156 المؤرخ في8 يونيو 1966، المعدل والمتمم بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004، وجرم من خلال هذه المادة مجموعة من الأفعال تصب كلها في التعامل في معطيات صالحة لأن ترتكب بها الجريمة بهدف المنع من حدوثها، كما جرم التعامل في معطيات المتحصل عليها من إرتكاب الجريمة بهدف الحد قدر الإمكان من الآثار والنتائج المترتبة على الجريمة الأولى من إحدى الجرائم المنصوص عليها في هذا القسم.

وإن هذه الصورة الأخيرة التي إنفرد بها المشرع الجزائري والتي لا نجد لها ذكرا لا في القانون الفرنسي ولا في إتفاقية بودابست تلم عن رغبة المشرع الجزائري في

---

1- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 194.

2- فايز محمد راجح غلاب ، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق -جامعة الجزائر1، سنة 2010/2009، ص 223.

تضييق نطاق الأشخاص الذين يمكنوا أن يتعاملوا في هذه المعطيات التي تم الحصول عليها بطريقة غير مشروعة، سعيا منه للحفاظ على سريتها.

ولدراسة أركان جريمة التعامل في معطيات غير مشروعة بصورتيها السالفتي الذكر(معطيات صالحة لإرتكاب جريمة ومعطيات متحصلة من جريمة) وجب التطرق إلى الأركان العامة التي تقوم عليها كافة الجرائم، والمتمثلة في الركن المادي(الفرع الأول) والركن المعنوي(الفرع الثاني)، مع التطرق إلى العقوبات المقررة لهذه الجريمة(الفرع الثالث).

**الفرع الأول: الركن المادي لجريمة التعامل في معطيات غير مشروعة**

أن جريمة التعامل في معطيات غير مشروعة بصورتيها تعتبر جريمة شكلية، أي أنها تقع بمجرد وقوع أحد الأفعال المكونة لها، وهي الأفعال المنصوص عليها في المادة 394 مكرر2([1])، من قانون العقوبات الجزائري، والتي تنص على ما يلي:" يعاقب بالحبس من شهرين الى ثلاث سنوات وبغرامة من 1.000.000 دج الى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

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

ونصت على تجريم هذه الأفعال كذلك المادة 323-3 في الفقرة الأولى من قانون العقوبات الفرنسي، والتي جاء فيها" كل من يقوم بدون مبرر قانوني باستيراد أو حيازة أو توفير تجهيزات، أدوات، برنامج معلوماتي أو كل معطيات مصممة أو معدة لارتكاب واحدة أو أكثر من الجرائم المنصوص عليها في المواد 323-1 إلى 323-3 يعاقب ..."([2])، وهذا الأمر يبدو طبيعيا على اعتبار أن فرنسا قد

[1]- المادة 394 مكرر 2 من القانون رقم 04-15.

[2] -Art 323-3-1:Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues

صادقت على إتفاقية بودابست، والتي ذكرت هاته الأفعال في المادة 6 منها تحت عنوان " إساءة إستخدام الأجهزة "، بقولها" يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات يرى أنها ضرورية للتجريم تبعا لقانونه الداخلي القيام عمدا ودون حق بما يلي:

أ- إنتاج أو بيع، أو الحصول من أجل الإستخدام، أو إستيراد أو نشر أو أي أشكال أخرى للوضع تحت التصرف.

1-أي جهاز يحتوي على برنامج معلوماتي مصمم أو موفق بشكل أساسي لغرض إرتكاب إحدى الجرائم المنصوص عليها وفقا للمواد من2-5 السابق الإشارة إليها.

2-كلمة المرور، أو شفرة الدخول، أو أي بيانات مماثلة تسمح بالولوج إلى كل إو جزء من نظام الحاسب بنية إستخدامها لغرض إرتكاب جريمة من الجرائم المشار إليها في المواد من 2-5.

**ب**- حيازة عنصر من العناصر المشار إليه في البندين أ-(1)، أ-(2) بنية إستخدامها لغرض إرتكاب جريمة من الجرائم المشار إليها في المواد من 2-5..."([1]).

وما يلاحظ أن هذه الأفعال ليست مساهمة مباشرة في الجريمة، وإنما هي أعمال مساعدة ومعاونة، جعل منها المشرع جريمة كاملة وتامة بنص هذه المواد، وعليه أصبحت فعل مجرم مستقل عن الجريمة الأصلية، والفائدة تكمن في إمكانية عقاب أفعال المساعدة في غياب الجريمة الأصلية([2]).

لذلك سنقوم بدراسة هذه الأفعال من خلال التطرق إلى النشاط الجرمي ومحل هذه الجريمة.

**أولا: النشاط الإجرامي**

يستفاد من نص المادة 394 مكرر2 من قانون العقوبات الجزائري أن السلوكات الإجرامية في جريمة التعامل في معطيات غير مشروعة تتخذ صورتين وهما

---

respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, modifiè par LOI N° 2013-1168 du 18 dècembre 2013-art.25.

[1]-مقتبس عن: بوكر رشيدة، مرجع سابق، ص 274،275.

[2]- جدي نسيمة، مرجع سابق، ص 71.

التعامل في معطيات صالحة لإرتكاب جريمة والتعامل في معطيات متحصلة من جريمة، وهي نفس السلوكات التي تطرق لها المشرع الفرنسي في المادة 323-3 الفقرة الأولى من قانون العقوبات الفرنسي، وكذا المادة 6 من إتفاقية بودابست، والتي تم إقتصارها في الصورة الأولى فقط.

**الصورة الأولى:التعامل في معطيات صالحة لإرتكاب جريمة**

هي الجريمة المنصوص عليها في البند الأول من المادة 394 مكرر2 من القانون الجزائري رقم 04-15، والتي نصت على مجموعة من الأفعال الخطيرة التي لو تركت بدون تجريم لأدت الى حدوث جرائم أخرى، ووردت على سبيل الحصر وتشمل كافة أشكال التعامل الواقعة على المعطيات السابقة لعملية إستعمالها في إرتكاب جريمة، ولا يشترط أن تقع هذه الأفعال مجتمعة لتقوم الجريمة بل يكفي أن تقع أحداها فقط، والتعامل هنا يكون بمفهومه الواسع ويقصد به في الجريمة محل الدراسة كل سلوك له علاقة بإعداد وإنتاج المعطيات غير المشروعة، أو هو كل سلوك يكشف عن وجود صلة معينة بين شخص ومعطيات غير مشروعة([1])، وهذه الصلة تتمثل في القيام بستة(6) أفعال منصوص عليها في البند الأول من المادة 394 مكرر2 من قانون العقوبات المعدل والمتمم، وهي:

**1-التصميم**: هو أول عملية في سلسلة التعامل في المعطيات وهي تتمثل في إعداد معلومات صالحة لإرتكاب جريمة، وهذا العمل يقوم به المتختصون كالمبرمجين ومصممي البرامج مثل تصميم فيروس، برامج خبيثة، برامج إختراق وقرصنة، وفي الغالب يكون مرتكبي هذه الجرائم على كفاءة ودراية عالية بالبرمجة ومختصين بالأعلام الآلي([2])، ومن قبيل ذلك تصميم برنامج لأهداف تخريبية(البرامج الخبيثة) مثل البرامج الفيروسية التي تكون ذات غرض تعديلي للمعلومات ويترتب عليها تعديل البرامج والتنقل بواسطتها إلى برامج أخرى، ومن أخطر الفيروسات المنشرة

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 200.

[2]- بوكر رشيدة، مرجع سابق، ص 279،280.

عبر شبكات الأنترنت، فيروس"Nimada" وفيروس "W.32mytob.U@mm" أو"W.32mytob.x" وفيروس "RtA"([1]).

إلا أنه لا يمكن أن نتصور هذه الجريمة إذا كان الغرض منها علمي بحث يهدف إلى دراسة برامج الإختراق أو تطوير وسائل الحماية الأمنية للحواسيب والشبكات، وهو الذي عناه المشرع الفرنسي بعبارة "دون سبب شرعي"([2]) حتى تستثنى الأعمال العلمية والتقنية([3]).

**2-البحث**: ماذا يقصد بالبحث في نص المادة 394 مكرر2؟ هل هو البحث عن المعطيات التي يمكن أن ترتكب بها الجريمة أم هو البحث في كيفية تصميم هذه المعطيات، أي إجراء أبحاث فيما يتعلق بوجود هذا النوع من المعطيات؟

ومن هذا المنظور فهل يعتبر من يشغل أحد محركات البحث المشهورة الموجودة على شبكة الأنترنت(yahoo وgoogle) ليقوم بالبحث عن مواقع تبين له كيفية إختراق نظام المعالجة الآلية مرتكبا للسلوك الإجرامي؟

لذلك ينبغي عدم التوسع في تفسير هذه العبارة، فما من شك أن التفسير السابق من شأنه أن يوسع كثيرا من نطاق التجريم، لأن الأصل أن البحث عن الوسيلة التي يمكن أن ترتكب بها الجريمة لا يعد جريمة، فمن يبحث عن سكين لا يعد مرتكبا لجريمة ما، ومن شأن هذه العبارة إذا أسيئ تفسيرها أن تشكل تهديدا جديدا للحريات.

وعلى هذا نرجح أن المشرع يقصد بعبارة البحث في هذه المادة البحث في تصميم هذه المعطيات وإعدادها، وليس مجرد البحث عن هذه المعطيات، ولذلك جاءت عبارة البحث بعد عبارة التصميم مباشرة، وأن كانت صياغتها عامة([4]).

**3-التجميع**: هو القيام بجمع أقدر ممكن من المعطيات التي تشكل خطرا كبيرا، والتي من الممكن أن ترتكب بها أحد جرائم الإعتداء على نظام المعالجة الآلية،

---

1- هروال هبة نبيلة ، جرائم الأنترنت، رسالة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية-جامعة أبوبكر بلقايد، تلمسان، سنة 2014/2013، ص 352.

2 - Art 323-3-1:Le fait, sans motif légitime, ……., modifiè par LOI N° 2013-1168 du 18 dècembre 2013-art.25.

3- مناصرة يوسف، مرجع سابق، ص 162.

4- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 201.

واستخدام المشرع لهذا المصطلح بصيغة الجمع له ما يبرره، ذلك أن تعدد المعطيات من شأنه أن يرفع من درجة الخطورة التي يشكلها، فما من شك إن هناك فرق بين من يحوز معلومة وبين من يسعى إلى تجميعها، بحيث أن المجرم يكون أشد خطرا في الحالة الثانية من الحالة الأولى([1]).

ولم يستخدم قانون العقوبات الفرنسي الجديد لسنة 2004 في مادته 323-3-1([2]) مصطلح التجميع بل إستخدم مصطلح الحيازة، ولا شك أن التجميع يقتضي الحيازة وإن كان أيضا يقتضي وجود عدد من المعطيات لا معطى واحد بعكس لفظ الحيازة التي يمكن أن تشمل معطى واحد وقد تشمل أكثر من معطى واحد، وكذلك الشأن بالنسبة لإتفاقية بودابست لعام 2001 التي إستخدمت مصطلح"الحصول للإستخدام" وما يميز هذا المصطلح عن مصطلح التجميع أن الأول يقتضي وجود نية إستخدام المعطيات المتحصل عليها، ولا يشترط فيها عددا معينا، بينما الثاني لا يشترط توافر مثل تلك النية ويشترط تعدد المعطيات([3]).

**4-التوفير**: تناول المشرع الجزائري صراحة بالتجريم كذلك فعل توفير معلومات يمكن أن ترتكب بها جريمة دخول أو بقاء أو جريمة تلاعب في المادة 394 مكرر2 بقولها"...أو توفير..." وتناولته الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 9 الفقرة الأولى "1-...أو توفير:.." كما أشار قانون العقوبات الفرنسي إلى نفس المعنى بموجب المادة 323-1/3 بقولها"..توفير أو الوضع تحت تصرف..." وكذلك فعلت إتفاقية بودابست تحت عبارة "أي أشكال أخرى للوضع تحت التصرف"

ويشير مصطلح التوفير إلى عرض المعلومات وإتاحتها وجعلها في متناول الغير بل وتحت تصرفه وحيازته، ومن قبيل ذلك كلمة المرور، شفرة الولوج أو بيانات معلوماتية مشابهة تسمح بالولوج لكل أو جزء من نظام المعالجة، بل أن القضاء

---

[1]- بوكر رشيدة، مرجع سابق، ص 281.

[2] - Art 323-3-1:Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, modifiè par LOI N° 2013-1168 du 18 dècembre 2013-art.25.

[3]- فايز محمد راجح غلاب ، مرجع سابق، ص 228.

الفرنسي قد توسع في تفسير مدلول التوفير ليشمل الكشف أو الإفشاء العلني للثغرات الأمنية في النظام([1]).

والفرق بين التوفير والتجميع هو أن هذا الأخير تقتصر فيه حيازة المعطيات والتصرف فيها على الشخص الذي يقوم بعملية التجميع، بينما في التوفير فإن دائرة الأشخاص الذين سيحصلون على المعطيات ويتصرفون فيها تتعدى ذلك الشخص وتتسع بذلك وتزيد الخطورة بازدياد هؤلاء([2]).

**5-النشر**: نصت المادة 394 مكرر2 في البند الأول منها من قانون العقوبات الجزائري على فعل النشر، وهو الفعل الذي تم تجريمه في الصورة الثانية(المعطيات متحصلة من جريمة)، ونصت عليه أيضا الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 9 في الفقرة الأولى منها بمصطلح التوزيع "1- ...أو توزيع.."، وكذلك فعلت إتفاقية بودابست بموجب الفقرة 2 من المادة 6 والتي نصت على ما يلي" ...أو النشر..." وذلك على خلاف التشريع الفرنسي الذي جاء خاليا من الأشارة إلى هذا الفعل.

ويقصد بالنشر أذاعة المعلومات محل الجريمة وتمكين الغير من الإطلاع عليها وذلك مهما كانت الوسائل التي يتصور النشر بها ومهما كانت طبيعتها، هذا وقد أشارت المذكرة التفسيرية لاتفاقية بودابست إلى أن مصطلح النشر ينبغي أن يمتد ليشمل كل نشاط من شأنه نقل البيانات إلى الآخرين([3]).

ولعل النشر بهذا المعنى يعد من أخطر الأفعال التي يمكن أن ترد على المعطيات المجرمة إذ أن هذا السلوك كفيل بأن ينقل هذه الأخيرة إلى عدد كبير من الأشخاص مما يجعل إحتمال إستعمال هذه المعطيات في الجرائم أكبر، وهو الأمر الذي أدى بالمشرع إلى محاولة علاجه من خلال تجريمه لهذه التعاملات، في خطوة

---

[1]- بوكر رشيدة، مرجع سابق، ص 282.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 203.

[3]- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية قسم القانون الخاص -جامعة أبوبكر بلقايد-تلمسان، سنة 2018/2017، ص 172.

الهدف منها التضييق قدر المستطاع من دائرة الأشخاص الذين يحصلون على هذه المعطيات بمقابل([1]).

**6-الإتجار**: الإتجار بالمعطيات هو تقديمها للغير بمقابل ولا يهم هذا المقابل، إذ يستوي أن يكون نقديا أو عينيا أو يقتصر فقط على مجرد خدمات أو غير ذلك.

والإتجار بهذا المعنى يختلف عن التوفير وفقا لمعناه السابق من حيث كون هذا الأخير ينصرف مدلوله إلى تقديم المعطيات سواء كانت بمقابل أو غير ذلك، على خلاف الإتجار الذي يكون بتقديم مقابل دائما([2]).

ولم يتضمن قانون العقوبات الفرنسي مصطلح الإتجار وكذلك لم تتضمنه إتفاقية بودابست، بل تضمنت هذه الأخيرة مصطلحي البيع والشراء والإستيراد ونفس المصطلح تضمنته الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 9 البند الأول([3]) منها بخلاف قانون العقوبات الفرنسي الذي إقتصر على مصطلح الإستيراد([4])، بينما المشرع الجزائري نص على الإتجار، وبذلك يكون قد شمل البيع والإستيراد وغيرهما من التعاملات التي يتصور وقوعها في المعطيات.

وأن ما يميز مصطلحي التوفير أو العرض والوضع تحت التصرف الذي نص عليهما المشرع الفرنسي عن مصطلح الإتجار هو حصول هذا الأخير بمقابل بينما التصرفات الأخرى تتم بدون مقابل، والظاهر أن المشرع الفرنسي لا يقيم اعتبارا للمقابل فيعتبر تقديم المعطيات مجرما سواء تم بمقابل أو بغير مقابل، بينما أراد المشرع الجزائري أن يشمل بالنص الحالتين معا([5]).

---

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 203.

[2]- بوكر رشيدة، مرجع سابق، ص 283.

[3]- نصت المادة 9 البند الأول من الإتفاقية العرربية لمكافحة جرائم تقنية المعلومات بعنوان جريمة إساءة إستخدام وسائل تقنية المعلومات على ما يلي:

1-إنتاج أو بيع أو شراء أو إستيراد أو توزيع أو توفير:.....، أنظر: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، الأمانة العامة لجامعة الدول العربية.

[4] - رابحي عزيزة ، مرجع سابق، ص 172.

[5]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 204.

وتطبيقا لذلك قضي في الجزائر بقيام جنحة المتاجرة في نظام معلوماتي في حق متهم قام بإنشاء موقع مشبه للموقع الخاص بالبنك الكندي مع علمه بأن الموقع يخص طرفا لا صلة له به، وأن الأشخاص الذين أتصلو به عجزوا عن إنشاء الموقع، وبالرغم من ذلك قام بالإستجابة لطلبهم دون معرفته لهم شخصيا، فقام ببيع الموقع لهم بمبلغ 500 إلى 900 دولار كندي لإستعماله في الإحتيال على الأشخاص منأجل الحصول على هوياتهم وإستعمالها في أغراض تجارية غير قانونية([1]).

**الصورة الثانية: التعامل في معطيات متحصلة من جريمة**

وهي الجريمة التي تمثل الصورة الثانية من جريمة التعامل في معطيات غير مشروعة، ولم يتم التطرق لها في قانون العقوبات الفرنسي ولا في إتفاقية بودابست ، ونص عليها المشرع الجزائري في الفقرة الثانية من المادة 394 مكرر2 من قانون العقوبات المعدل والمتمم، المشار لها أعلاه، والتي نصت على تجريم أفعال الحيازة أو الإفشاء أو النشر أو الإستعمال لأي غرض كان، والتي 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([2]).

ونلاحظ من خلال هذه المادة أن المشرع الجزائري نص على إستخدام المعطيات كوسيلة في إرتكاب الجرائم الماسة بالأنظمة المعلوماتية، وذلك من خلال تلك الأفعال التي ذكرها وأن يكون هذا الإستخدام عمدا أو بطريق الغش.

كما أن التدخل في المعطيات المعالجة آليا أو المحفوظة في النظام الآلي بغرض معالجتها يؤدي الى المساس بها وذلك بغرض الإتلاف أو التغيير أو التزييف أو التزوير سواء تعلق الامر بإدخال معلومات لم تكن موجودة سابقا بغرض المعالجة

---

[1]- بوكر رشيدة ، الحماية الجزائية للتعاملات الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم تخصص قانون جزائي، كلية الحقوق والعلوم السياسية قسم الحقوق -جامعة الجيلالي اليابس-سيدي بلعباس، سنة 2017، ص 57.

[2]- امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، سنة 2007، ص 123.

لهدف يبغيه المجرم أو بغرض التلاعب بالبيانات، وفي مختلف هذا الصور فأن النتيجة مؤداها التدخل في نظام المعالجة الآلية وإرباكه والتشويش عليه أو التزوير في البيانات المخزنة.([1])

وتتحقق الجريمة في هذه الصورة بواحدة من أربعة أفعال ذكرها المشرع الجزائري على سبيل الحصر وهي:

**1-الحيازة**: هي نقل الشيء أو نزعه من حيازة المجني عليه وإدخاله في حيازة الجاني بشرط أن يكون على جهاز أو ورق أو أي شيء آخر مادي([2])، ويعرفها أيضا "غارسون" بأنها سيطرة واقعية وإرادية للحائز على المنقول تخوله مكنة الإنتفاع به أو تعديل كيانه أو تحطيمه أو نقله، فهي إذا سيطرة إرادية للشخص على الشيء.

والحيازة في نطاق القانون الجنائي رابطة واقعية بين شخص ومال منقول، تتيح للأول أن يسيطر على الثاني سيطرة مستقلة مقترنة بنية الإحتباس وتكون السيطرة على المال مستقلة إذا كان يمكن للشخص أن يمارس أي عمل مادي على الشيء بدون رقابة من شخص آخر له على المال سلطة قانونية أعلى بمقتضى حق من الحقوق([3]).

وعلى ذلك فإن الحيازة في قانون العقوبات ليست حقا عينيا كالقانون المدني فقد تكون حيازة الجاني مشروعة أو غير مشروعة، وفيما يتعلق بجريمة التعامل في المعطيات فيفترض في الحيازة أنها غير مشروعة يسيطر من خلالها الجاني على المعطيات بالشكل الذي يمكنه من خلاله تعديلها، إستعمالها، إزالتها، الإنتفاع بها، وإستغلالها ولو كانت هذه الإستفادة محدودة([4]).

كما أن الحيازة لا تقوم إلا بسيطرة الحائز على المعطيات، بحيث يكون باستطاعته التأثير عليها تأثيرا يتفاوت حجمه تبعا لنوع الحيازة، إذ قد تكون السيطرة

---

[1]- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، سنة 2011، ص60.

[2]- بخوش هشام، مقال بعنوان الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في ظل التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 4، العدد 1، جانفي 2017، ص 198،199.

[3]- بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 285،286.

[4]-جدي نسيمة، مرجع سابق، ص 74.

مطلقة يستطيع معها الحائز أن يفني المعطيات أو يعدل فيها أو يستعملها، كما قد تكون هذه السيطرة من الناحية الواقعية محدودة تمكنه فقط من الإنتفاع بالمعطيات أو إستغلالها في وجه معين.

ولا تكفي مجرد سيطرة الحائز على المعطيات لكي تقوم الحيازة، بل يلزم أن تكون هذه السيطرة إرادية، أي أنها مقترنة بنية إحتباس المعطيات والسيطرة عليها، وهذا لا يتحقق إذا كان تمتع الحائز بسلطاته على المعطيات لم يكن إلا أمرا عرضيا أوجدته المصادفة أو تم بنية عدم التكرار، لأنه يلزم أن تكون سيطرة الشخص على المعطيات مقترنة بنية إحتباسها على الدوام أو لمدة معينة، وما دامت نية الإحتباس ركنا أصليا من أركان الحيازة فإن العلم بمضمون المعطيات المتحصلة من جريمة وبدخولها في نطاق السيطرة شرط لازم لقيام الحيازة لأنه من لا يعلم لا يحوز([1]).

**2-الإفشاء:** يقصد بالإفشاء نقل المعطيات من حيازة الشخص التي تحصل عليها بطريقة غير مشروعة الى غيره ومن يقوم بذلك ليس مؤتمنا على المعطيات - لا يكون ملزما قانونيا بكتمانها- التي قام بإفشاءها، وإنما تحصل عليها بطريقة غير مشروعة ونشرها([2]).

وأن كانت الوسائل التقنية(الحاسبات وشبكات الإتصال) قد لعبت دورا مهما في تسهيل الحصول على المعلومات التي تحتويها، إلا إنها في المقابل قد ضاعفت من فرص إفشاء ما تحتويه بعد إختراقها لتحقيق مصالح مختلفة، وذلك بمجرد نقرات بسيطة على الجهاز.

وإدراكا لهذا الوضع الخطير قامت العديد من التشريعات بتجريم الإفشاء غير المشروع للمعطيات التي يتحصل عليها بطرق غير مشروعة، ومن ضمنها المشرع الجزائري بموجب المادة 394 مكرر2 من قانون العقوبات في بندها الثاني بتجريم إفشاء المعطيات المتحصلة من جريمة الدخول أو البقاء غير المصرح بهما أو جريمة التلاعب بالمعطيات، وذلك على خلاف المشرع الفرنسي الذي لم يخصص لهذا الفعل نصا خاص.

---

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 206.

[2]- جدي نسيمة، مرجع سابق، ص 74.

بينما يختلف الأمر بالنسبة لبعض التشريعات كما هو الحال في القانون الأمريكي، فالقانون الفيدرالي لجرائم الحاسبات الآلية لسنة 1984 يعاقب في مادته(1030()أ)(3) كل من يقوم بالدخول غير المصرح به إلى النظام، وعن طريق هذا الدخول يقوم بإفشاء معلومات توجد داخل النظام متى كان هذا الحاسب يستعمل من طرف الويات المتحدة الأمريكية أو لمصلحتها أو ترتب على هذا السلوك الإضرار بهذا الإستعمال لكن التعديلات اللاحقة للقانون تجاهلت هذا النص([1]).

وعلى مستوى الولايات التابعة للولايات المتحدة الأمريكية، فالعديد من القوانين جرمت إفشاء المعلومات المبرمجة آليا كقانون ولاية"ألاباما" لجرائم الحاسب الآلي لسنة 1985، الذي يجعل من الإفشاء جنحة ويرفعه إلى جناية إذا تم إستخدام هذه المعلومات في إرتكاب جريمة، وكذلك الأمر مع قوانين ولاية فلوريدا وكانساس وأوكلاهوما متى ترتب على الإفشاء إضرارا بالغير أو الحصول على ربح غير مشروع([2]).

وإلى جانب ذلك يعاقب قانون العقوبات الهولندي في مادته 139 على الإفشاء العمدي للمعلومات المتحصل عليها بطريقة غير مشروعة عن طريق تسجيلها أثناء نقلها بواسطة نظام الحاسب الآلي([3]).

ولم يتطلب قانون العقوبات الجزائري حدوث نتيجة معينة من وراء الإفشاء بل يجرم هذا الأخير في حد ذاته، والفرق بين الحيازة والإفشاء أو النشر أن الحيازة تقتصر على وجود المعطيات غير المشروعة لدى الحائز فحسب دون قيامه بتقديمها لغيره، أما الإفشاء والنشر فهما يفترضان إنتقال هذه المعطيات من حيازة هذا الشخص إلى غيره من الأشخاص([4]).

---

[1]- بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 287.

[2]- نعيم مغبغب، حماية برامج الكومبيوتر، الأساليب والثغرات، دراسة في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، ط الأولى، سنة 2006، ص 231.

[3]- نائلة عادل محمد فريد قورة، مرجع سابق، ص 84.

[4]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 208.

**3-النشر:** هو فعل مشترك بين صورتي التعامل في معطيات غير مشروعة (معطيات صالحة لإرتكاب جريمة ومعطيات متحصلة من جريمة)، وهو ذات المفهوم بإختلاف محل كل منهما، والمقصود منه إذاعة المعطيات والتمكين من الإطلاع عليها بأي وسيلة من وسائل النشر([1]).

وتناول المشرع الجزائري فعل النشر في جريمة التعامل في معطيات غير مشروعة بصورتيها السالفتي الذكر في المادة 394 مكرر2، والتي لم تشترط عددا معينا من المرات التي يتم فيه النشر، بل جاءت مطلقة، مما يفهم معه أن النشر يتم ولو لمرة واحدة فقط، كما لم تحدد هذه المادة أن يكون النشر بمقابل أو بغيره، وبالتالي يتحقق في كلتا الحالتين، ولم تذكر أي وسيلة معينة يتم بها النشر، وعليه فهو يتم بكل وسيلة يمكن تصورها سواء كانت وسيلة معلوماتية كالنشر عن طريق شبكة الأنترنت أو الأقراص المضغوطة أو بطريقة تقليدية كالنشر عن طريق الكتابة مثلا([2]).

ومن قبيل ذلك ما يقوم به عادة المخترقون-الهاكرز- من إختراقات متكررة لمواقع معينة وحصولهم على كلمات العبور فيها أو معلومات سرية والقيام بنشرها على الجميع نكاية بأصحابها وتحديا لهم، وهو ما حدث تماما في أول قضية عرضت على القضاء الجزائري(مجلس قضاء باتنة) في مجال الإجرام التقني، كقضية أولى من نوعها على المستوى الوطني تتلخص وقائعها في قيام أبن إطار كبير في الدولة والبالغ من العمر 21 سنة باختراق الموقع الأمريكي "سايف ناتوورك" التابع لشركة عالمية مختصة في حماية الشركات والمؤسسات الإمريكية وذلك إنطلاقا من جهاز الكومبيتر والأنترنت الموصول بمكتب والده، وهو ما مكنه من الحصول على أسرار المؤسسات الأمريكية بغرض إبتزازها وتمكينها من الحصول على معلوماتها مقابل مبالغ مالية بالعملة الصعبة كانت تحول إليه من طرف الشركات الضحية أو من طرف زبائن منافسين والذين يبيعهم تلك الأسرار المعلوماتية مقابل مبالغ مالية يحصل عليها بحولات بنكية يتلقاها من وكالات.

---

[1]- جدي نسيمة، مرجع سابق، ص 75.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 209.

وهذه العملية كانت تتضمن مختلف أشكال التعامل في معلومات غير مشروعة، وهي البحث والجمع والنشر والإتجار، ولم يتم إكتشافه وتوقيفه إلا بعد شكوى تقدمت بها مؤسسة سايف ناتوورك وذلك وسط إجراءات أمنية وسرية مشددة بالتنسيق مع مكتب التحقيقات الفيدرالي الأمريكي FBI يوم الأحد 04 جويلية عام 2010([1])، حيث إعترف بإختراقه لعدة مواقع إلكترونية عن طريق القرصنة باستعمال الخط الهاتفي لمنزله مستعينا بشبكة الأنترنت للمتعامل "فوزي" وكذا إستعمال عدة عناوين إلكترونية وهمية، كما صرح بحصوله على مبالغ مالية من هذه العمليات، وقد قضت عليه بالحبس عاما نافذا وبغرامة 20.000 دج([2]).

**4-الإستعمال:** نصت المادة 394 مكرر2 في بندها الثاني من قانون العقوبات الجزائري على تجريم الإستعمال في حد ذاته باعتباره أخطر سلوك يمكن أن يقع على المعطيات المتحصلة من جريمة.

ذلك أنه إذا كانت حيازة المعطيات غير المشروعة وإفشاؤها ونشرها تعد أمورا خطيرة فإن الأخطر من ذلك كله هو القيام باستعمال هذه المعطيات كأن تستعمل شركة ما معطيات متعلقة بشركات منافسة لها كانت قد تحصلت عليها بعد دخول غير مصرح به إلى نظامها المعلوماتي الخاص بها، ويشمل هذا التجريم كل إستعمال للمعطيات مهما كان الهدف منه ومهما كان نوعه، وهو ما يستفاد بوضوح من العبارة الواردة في هذه المادة "...أو إستعمال لأي غرض كان..." وربما الهدف من ذلك هو غلق الباب أمام كل من يريد أستعمال هذه المعطيات.

كما يتضح من نص هذه المادة المطلق أن الإستعمال ولو لمرة واحدة تقوم به الجريمة لأنه لم يرد تحديد لعدد المرات اللازمة لقيامها([3]).

---

[1]- بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 289.

[2]- مقتبس عن: الهادي خضراوي، عبدالحليم بوقرين، بحث بعنوان تجربة الجزائر في مكافحة الجريمة الإلكترونية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية-السعودية، نوفمبر 2015، ص 155.

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 210.

وعليه، فأن مجرد توافر إحدى هذه الأفعال على هاتين الصورتين تعد جريمة قائمة بحد ذاتها ودون إشتراط تحقق نتيجة معينة أو ترتب ضرر معين من إرتكابها.

**ثانيا: محل الجريمة**

محل جريمة التعامل في معطيات غير مشروعة أشارت اليه المادة 394 مكرر2 وهو المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية والمعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها بالمواد 394 مكرر و394 مكرر1، ويلاحظ أن هذه المادة تختلف عن المادتين السابقتين لهما، والمتعلقتين بجريمتي الدخول والبقاء غير المصرح بهما والتلاعب بالمعطيات، وذلك في نقطتين:

النقطة الأولى: تتعلق بالحالة التي توجد عليها المعطيات.

النقطة الثانية: تتعلق بالنظام الذي توجد به المعطيات.

وكما أسلفنا القول فإن المعطيات في جريمة الدخول والبقاء غير المصرح بهما وجريمة التلاعب هي المعطيات الموجودة داخل النظام، أما المعطيات في جريمة التعامل في معطيات صالحة لإرتكاب جريمة فهي المعطيات المخزنة أو المرسلة، وبالنسبة للنظام الذي توجد به المعطيات في جريمتي الدخول والتلاعب نظام المعالجة الآلية للمعطيات كما سبق بيانه، أما في جريمة التعامل في معطيات صالحة لإرتكاب جريمة فهو أي منظومة معلوماتية([1])، ولا شك أن هذه الأخيرة تختلف عن نظام المعالجة الآلية للمعطيات لأنها أضيق منه([2]).

لذا يتضح بأن محل جريمة التعامل في معطيات صالحة لإرتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات هي المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، بحيث لا يقتصر الأمر على المعطيات المخزنة في نظام المعالجة الآلية للمعطيات، بل أنه يشمل المعلومات المرسلة عبر

[1]- عرفت المادة 2 من قانون قانون 09-04 المؤرخ في 2009/08/05، السالف الذكر، المنظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،...."

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص196.

منظومة معلوماتية، وهو ما يجعل هذه الجريمة تختلف عن جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات أو التلاعب بالمعطيات.

وأن تعدد محل الجريمة هدف المشرع منه الى إلى حماية المعطيات في حد ذاتها وعدم حصر هذه الجريمة في أي نوع من المعطيات([1])، ليوسع بذلك من دائرة التجريم إذ شمل بالحماية المعطيات مهما كانت حالتها إذ لم تقتصر على تلك الموجودة بنظام المعالجة الآلية كالجرائم السابقة بل وسع المجال الى مختلف المعطيات مهما كانت حالتها مخزنة أو مرسلة ، معالجة على اعتبار إمكانية إرتكاب جرائم حتى باستعمال معطيات موجودة على وسائط تخزين خارجية.

كما أن المشرع الجزائري لم يخص بالتجريم المعطيات المعدة لإرتكاب جريمة بالتحديد بل يكفي أن تكون صالحة أو قابلة لأن ترتكب بها جريمة، وهذا ما نصت عليه المادة 394 مكرر2 بالفقرة الأولى بعبارة"..يمكن أن ترتكب بها الجرائم...."([2]).

وإذا كان قانون العقوبات الجزائري قد إقتصر على المعطيات كمحل للجريمة فإن قانون العقوبات الفرنسي كان أكثر توسعا في ذلك عندما نص في مادته 323-1/3 كما يلي" من قام بدون حق...على تجهيزات أو أدوات أو على برنامج معلوماتي أو على كل معطيات مصممة أو معدة لارتكاب واحدة أو أكثر من الجرائم المنصوص عليها في المواد من 323-1 إلى 323-3"([3])

وما يمكن ملاحظته من هذه المادة أن المشرع الفرنسي قد وسع من نطاق تطبيقها لتشمل بالتجريم كل الوسائل التي يمكن إستخدامها في إرتكاب الجريمة مهما كانت طبيعتها سواء كانت ذات طبيعة مادية(تجهيزات وأدوات) أو ذات طبيعة غير مادية(البرامج والمعطيات) بخلاف المشرع الجزائري الذي إكتفى بحظر نطاق هذه الجريمة بالمعطيات التي تكون صالحة أو قابلة لأن ترتكب بها جريمة.

---

[1]- فايز محمد راجح غلاب ، مرجع سابق، ص 224،225.

[2]- جدي نسيمة، مرجع سابق، ص 72.

[3] - Art 323-3-1:Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, modifiè par LOI N° 2013-1168 du 18 dècembre 2013-art.25.

والظاهر أن المشرع الفرنسي قد تأثر في ذلك بما جاءت به إتفاقية بودابست التي حددت في المادة السادسة (6) منها نطاق هذه الجريمة بالأجهزة التي يمكن القول معها أنها قابلة أو معدة خصيصا لغرض إرتكاب الجرائم، وذلك بقولها" أي جهاز يحتوي على برنامج معلوماتي مصمم أو موفق بشكل أساسي لغرض إرتكاب إحدى الجرائم المنصوص عليها وفقا.."([1]).

وهذا كان بالنسبة لمحل هي محل جريمة التعامل في صورتها الأولى المتمثلة في معطيات صالحة لارتكاب جريمة، أما بالنسبة لمحل جريمة التعامل في معطيات غير مشروعة في صورتها الثانية ألا وهي المعطيات المتحصلة من جريمة فإنه يتمثل في أي نوع من المعطيات سواء كانت تتعلق بالحياة الخاصة أو تتعلق بمسألة علمية...على أن تكون هذه المعطيات قد تم الحصول عليها من خلال جريمة الدخول أو البقاء غير المصرح بهما في صورتيها أو جريمة التلاعب بالمعطيات([2]).

**الفرع الثاني: الركن المعنوي لجريمة التعامل في معطيات غير مشروعة**

جريمة التعامل في معطيات غير مشروعة جريمة عمدية، ويستفاد ذلك من العبارة الواردة في المادة 394 مكرر2 من قانون العقوبات الجزائري "عمدا وعن طريق الغش"، ولكن هذه العبارة تثير اللبس لا سيما وأن المشرع إستخدم عبارة"عن طريق الغش" فقط في جريمة الدخول أو البقاء غير المصرح بهما وجريمة التلاعب بالمعطيات، في حين وظف المصطلحين معا في جريمة التعامل في معطيات غير مشروعة نفسها، إذن فماذا يقصد المشرع من خلال ذلك ؟

**أولا: القصد الجنائي العام**

يقوم القصد الجنائي العام على العلم والإرادة.

**1- العلم:** لا بدا أن يعلم الجاني بكل العناصر التي تدخل في بناء الجريمة، فيجب أن يكون على علم بأنه يقوم بالتعامل في معطيات غير مشروعة وما يحمله سلوكه من قدرة على تهديد المصلحة المحمية، وذلك بأن يعلم أن من شأن المعطيات التي

---

[1]- نقلا عن: بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 193،291.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 199.

يتعامل فيها أنها صالحة لأن تستعمل في إرتكاب الجرائم، أو يعلم أن من شأن تعامله في المعطيات المتحصلة من الجريمة أن يزيد من الضرر المترتب على تلك الجريمة.

ولا بدا أن يعلم الجاني بالصفة غير المشروعة للمعطيات بأن يعلم أنه يمكن أن ترتكب بها جريمة، أو أنها متحصلة من جريمة، فإذا أعتقد أنها معطيات عادية لا علاقة لها بالجريمة أنتفى عنه القصد الجنائي([1]).

وبالرجوع الى قضية المدير العام لديوان رياض الفتح بالجزائر العاصمة ضد ق ل المشتكى منها نجد أن هذه الأخيرة

**2- الإرادة:** هي أن تتجه إرادة الجاني إلى فعل تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق نظام معلوماتي، أو حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

لذلك لا يكفي أن يكون المتعامل عالما بما يفعله لقيام جريمة التعامل في معطيات غير مشروعة، بل يجب أن تتجه إرادته إلى تحقيق أو إتيان أحد الأفعال التي نص عليها المشرع، وذلك رغم علمه بصفتها غير المشروعة([2]).

والإرادة هنا تنصب على السلوك الإجرامي فحسب وهو مختلف عن أشكال التعامل السابق بيانها، ذلك لأنه لا توجد نتيجة يعتد بها في بناء الجريمة كي تطالها الإرادة، وبالتالي فهذه الأخيرة تقتصر على السلوك فحسب عكس الجرائم الأخرى التي تشترط حدوث نتيجة معينة([3]).

وفي هذا الصدد نستعرض قرار جزائي لمجلس قضاء الجزائر الغرفة الجزائية السادسة رقم الفهرس: 05554/16 الصادر بتاريخ 17 أفريل 2016، وتتلخص

---

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 212.

[2]- بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 296.

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 212.

الوقائع في أنه بتاريخ 2015/08/04، تقدمت المدعوة(ت.م) بشكوى مصحوبة بإدعاء مدني أمام عميد قضاة التحقيق ضد المدعوة (د.م) من أجل الإعتداء على شرف واعتبار الأشخاص وإفشاء الأسرار والمساس بنظام المعالجة الآلية للمعطيات والتهديد، جاء فيها أن المشتكى منها كانت تعمل كاتبة في عيادة الشاكية الكائنة بباب الوادي إلى غاية نوفمبر 2014 أين إكتشفت أنها كانت تقوم بفحص المرضى أثناء غيابها وإعطائهم نصائح طبية وإجراء لهم فحوصات أشعة مقابل مبالغ مالية بالرغم من عدم تخصصها في التمريض ولا في الطب فقامت بطردها، وإنتقاما منها قامت المشتكى منها بالإتصال بالمدعوة(ج.ص) وأخبرتها أنها تحوز على مفتاح USB وبه جميع المعلومات الشخصية الخاصة بالشاكية وأنها ستقوم بنشرها عبر الأنترنت، وأنه بتاريخ 2015/02/20 تلقت الشاكية رسالة باللغة الفرنسية عبر العنوان الألكتروني تحت عنوان SURPRISE محتواه المعلومات المتعلقة بالحسابات البنكية ل(ت.ع)،(ت.ف) و(ت.م) وكذا الأرقام السرية الخاصة بالحسابات البنكية ل(ت.مر) و(ت.م)، كما تلقت رسالة إلكترونية تحتوي على وثيقتي تأمين على حياة والدها المرحوم أمام شركتي التأمين ببلجيكا وفرنسا، وأنه بتاريخ 2015/04/20، تلقت قرصا مضغوط عبر الصيدلي (ق.ك) والذي تسلمه من إمرأة متجلببة مجهولة كتب عليه إلى الدكتوارة (ت.م)، وتضمن هذا القرص عقد التأمين على الحياة لوالد الشاكية بفرنسا وببلجيكا وعمارة الشاكية ببلجيكا وبباب الوادي وأسماء كل المستأجرين ومبالغ الإيجار في العمارتين، إضافة إلى فهرس بطاقتي يحتوي على كلمات السر للشاكية والمراسلات الإلكترونية للشاكية مع بنك ب.ن ب باريبا ببلجيكا، وتقرير خبرة لعمارة الشاكية ببلجيكا، وكذا الميزانية السنوية لعمارة الشاكية ببلجيكا، وعليه التمست فتح تحقيق في القضية.

وبتاريخ 2015/11/29 تم سماع الشاهد (ب.س) الذي صرح أنه كان يعمل عند الشاكية كمهندس في الإعلام الآلي منذ نوفمبر 2013 وكان يتكفل بتنظيم جميع المعطيات الخاصة بمرضى العيادة وكذا معلوماتها الشخصية في الحاسوب وذلك إلى غاية أواخر جانفي 2014 أين قام بتنظيم الميزانية السنوية للشاكية وكذا كافة المعلومات الشخصية المتعلقة بها وبوظيفتها، وحرصا منه على القيام بمهمته

على أحسن وجه قام بتخزين جميع المعلومات في مفتاح Flash Disk USB الذي ضاع منه على مستوى العيادة وعندما إستفسر مع المشتكى منها أخبرته أنها لم تجده وبعد طردها من العمل وطرح النزاع بينها وبين الشاكية بدأت تنشر المعلومات التي كانت داخل المفتاح وكانت تتصل به المشتكى منها من أجل الشهادة معها في المحاكمة حينها تيقن أنها هي من أستولت على المفتاح.

وقد إحيلت المتهمة للمحاكمة بموجب أمر الإحالة على محكمة الجنح الصادر عن السيد قاضي التحقيق في 2015/12/02 طبقا للمادة 164 من قانون الإجراءات الجزائية.

وبتاريخ 2016/02/18، صدر حكم عن محكمة باب الوادي قضى بإدانة المتهمة(د.م) بجنحتي الإعتداء على الحياة الخاصة للأشخاص بوضع وثائق في متناول الجمهور والمساس بنظام المعالجة الآلية للمعطيات بنشر معلومات مخزنة ومرسلة عن طريق منظومة معلوماتية طبقا للمواد 303 مكرر،303 مكرر1، 394 مكرر2/2 من قانون العقوبات وعقابا لها الحكم عليها بستة أشهر حبسا موقوف النفاذ و20.000 دج غرامة نافذة.

وقضت الغرفة الجزائية السادسة بتأييد الحكم المستأنف الصادر عن محكمة باب الوادي، التي ورد في تسبيبها أن المتهمة قامت باستغلال معلومات شخصية عن الضحية وعائلتها من حواسيب العيادة وكذا مفتاح USB الذي ضاع من العيادة وقامت بإرسال هذه المعلومات إلى الضحية في قرص مضغوط عن طريق الشاهد(ق.ك) كما أنها إتصلت بالشاهدة (ع.ي) التي تعمل لدى الضحية كسكرتيرة وبدأت تستفسر منها عن وصول القرص المضغوط لدى الضحية وعن ردة فعلها، وثابت أن المتهمة أرسلت معلومات خاصة بالضحية وعائلتها في البريد الإلكتروني للضحية وكذا شبكات التواصل الإجتماعي وهو ما يعد مساسا بالمعطيات المعالجة آليا الموجودة في حواسيب الضحية.

وبناء على ما سبق إعتبر قضاة المجلس بأن جنحة الإعتداء على الحياة الخاصة للأشخاص بوضع وثائق في متناول الجمهور وجنحة المساس بنظام المعالجة الآلية للمعطيات بنشر معلومات مخزنة ومرسلة عن طريق منظومة

معلوماتية طبقا للمواد 303 مكرر،303 مكرر1، 394 مكرر2/2 من قانون العقوبات ثابتة في حق المتهمة([1]).

وبالرجوع إلى هذه القضية نلاحظ أن المشتكى منها(د.م) كانت تتجه إرادتها الى التعامل في تلك المعطيات، ولعل نشر معلومات مخزنة ومرسلة عن طريق منظومة معلوماتية دليل على أن إرادتها كانت تتجه الى الإضرار بالشاكية(ت.م)، وأن أرسال المدعوة(د.م) معلومات خاصة بالضحية وعائلتها في البريد الإلكتروني للضحية وكذا شبكات التواصل الإجتماعي أكد على إتجاه إرادتها للقيام بتلك السلوكات المنصوص عليها في البند الثاني من المادة 394 مكرر2 والمذكورة سالفا.

**ثانيا: القصد الجنائي الخاص**

بالنسبة للركن المعنوي في جريمة التعامل في معطيات غير مشروعة فهي تقوم في صورتها الأولى (التعامل في معطيات صالحة لارتكاب جريمة) بتوافر القصد الجنائي العام وكذا القصد الجنائي الخاص، بينما يكفي لقيامها في صورتها الثانية (التعامل في معطيات متحصلة من جريمة) توافر القصد الجنائي العام.

**1- القصد الخاص في جريمة التعامل في معطيات صالحة لإرتكاب جريمة**

لا يكفي لقيام جريمة التعامل في معطيات صالحة لإرتكاب جريمة أن يتوافر لدى الفاعل القصد الجنائي العام وحده، بل يلزم فضلا عن ذلك توافر لدى الفاعل القصد الخاص المتمثل في إتجاه العلم والإرادة الى وقائع معينة لا تدخل في تكوين أركان الجريمة([2])،

وبالنسبة لتحديد ماهية القصد الخاص فنرى أن التعامل في المعطيات الصالحة لإرتكاب الجريمة لا بدا أن يكون بقصد الإعداد و التمهيد لإستعمالها في إرتكاب جريمة من جرائم نظام المعالجة الآلية للمعطيات.

ومع هذا فإستعمال هذه المعطيات في ارتكاب جريمة ليس ركنا في هذه جريمة التعامل هذه، فقد لا يقوم أحد بإستعمال هذه المعطيات ومع ذلك تقوم الجريمة إذا

---

[1]- مقتبس عن: مناصرة يوسف، مرجع سابق، ص ص: 163-166.

[2]- بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 297.

توافر قصد الإعداد والتمهيد لإستعمال هذه المعطيات في إرتكاب جريمة وهذه مسألة نفسية محضة([1]).

وصحيح أن المشرع لم يتطلب ضرورة توافر هذا القصد الخاص صراحة ولكن إستقر الفقه والقضاء-في الجزائر- على تطلب القصد الخاص في بعض الجرائم بالرغم من عدم ورود أي عبارات تدل عليه ضمن البناء المعنوي للنص الذي يجرمها، وتظهر هذه المسألة بصورة جلية في جريمة التزوير التي بالرغم من عدم نص المشرع صراحة على ضرورة توافر قصد خاص فقد إستقر كل من الفقه والقضاء على تطلب القصد الخاص في هذه الجريمة، يتمثل في قصد إستعمال المحرر المزور فيما زور من أجله، فاستعمال المحرر المزور ليس ركنا في جريمة التزوير، وقد لا يستخدم المحرر قط ومع ذلك تقوم الجريمة إذا توافرت لدى الجاني نية إستعمال المحرر كمسألة نفسية محضة([2]).

وهو ما حدث تماما مع جريمة التعامل في معطيات صالحة لإرتكاب جريمة، إذ لم تتضمن المادة 394 مكرر2 إشتراط ها القصد، ذلك أنه ليس من مقتضيات العدالة مساءلة أي شخص يقوم بالتعامل في هذه المعطيات إلا إذا كان له قصد سيء يتجه إلى إعدادها أو إستعمالها في جريمة ما، فهذه المعطيات غير معدة خصيصا لارتكاب جريمة كما أشارت إليه المادة السابقة، مما يعني أنها تكون ذات إستخدام مزدوج بأن يمكنها أن تستعمل لأغراض مشروعة كما يمكن أن تستعمل لأغراض غير مشروعة([3]).

وليس هناك أي ذنب لمن يقوم باستخدامها في أغراض مشروعة كأغراض الحماية من الجرائم إذا لم تكن له نية إعدادها للإستعمال غير المشروع، وهذا ما تنبهت له إتفاقية بودابست في المادة السادسة منها عندما أشترطت صراحة العقاب

---

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 213.

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاصن جرائم الفساد،المال،الأعمال والتزوير، ج2، دار هومة، الجزائر، سنة 2006، ص 346.

[3]- بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 298،297.

على التعامل في الوسائل الصالحة لارتكاب جريمة أن يكون هذا التعامل بنية إستخدامها لغرض إرتكاب جريمة من الجرائم المشار إليها في المواد من 02 إلى 05، وقد نصت الفقرة الثانية من المادة ذاتها على ما يلي:" يجب أن لا تفسر على أنها تفرض مسؤولية جنائية حينما يكون إنتاج أو بيع أو الحصول من أجل االإستخدام أو الإستيراد أو النشر والأشكال الأخرى للوضع تحت التصرف المشار إليها في الفقرة الأولى من هذه المادة، ليس بهدف إرتكاب جريمة وفقا للمواد 2،5 من هذه الإتفاقية ومثال على ذلك حالة الإختيار المصرح به أو حماية نظام الحاسب([1]).

وعليه، فإن جريمة التعامل في معطيات غير مشروعة في صورتها الأولى المتمثلة في التعامل في معطيات صالحة لارتكاب جريمة، لا يكفي لقيامها توافر القصد الجنائي العام وحده، بل تتطلب إلى جانب ذلك وجود قصد خاص يتمثل في إنصراف العلم والإرادة إلى وقائع معينة لا تدخل في تكوين أركان الجريمة، إلا وهي إعداد المعطيات والتمهيد لاستعمالها في إرتكاب جريمة.

**2- القصد الخاص في جريمة التعامل في معطيات متحصلة من جريمة**

توصلنا فيما سبق إلى أن جريمة التعامل في معطيات صالحة لارتكاب جريمة تتطلب قصدا خاص لأن المعطيات التي يتم بها التعامل قد تكون لأغراض غير مشروعة، كأغراض الحماية من الجرائم مثلا، مما يجعل توافر القصد الخاص ضروريا للتمييز المشروع عن غير المشروع من أشكال هذا التعامل.

وهذا بخلاف الصورة الثانية لجريمة التعامل في معطيات غير مشروعة وهي التعامل في معطيات متحصلة من جريمة التي يكفي لقيامها وجود قصد جنائي عام لأن المعطيات كلها متحصلة من جريمة وصفتها ثابتة، وهو ما أكد عليه المشرع الجزائري في البند الثاني من المادة 394 مكرر2 بعبارة"...لأي غرض كان..".

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 214.

ولكن هناك أمر آخر توجب مناقشته وهو نص المادة 394 مكرر2 على مصطلح عمدا إلى جانب عن طريق الغش، فهل هذا يعني أن المشرع تطلب قصدا خاصا في الصورتين؟

والملاحظ أن المواد التي تضمنت جريمتي الدخول والتلاعب قد إقتصرت في تدليلها على الركن المعنوي على عبارة الغش، في حين أن المادة 394 مكرر2 التي تناولت جريمة التعامل في معطيات غير مشروعة أضافت إلى عبارة "الغش" عبارة "عمدا" فجاء نصها كما يلي:"..عمدا وعن طريق الغش...".

وإن أول ما يتبادر إلى الذهن أن هناك إختلافا بين عبارة "عن طريق الغش" وعبارة"عمدا" وإلا لما أستعمل المشرع المصطلحين معا وإقتصر على إستعمال مصطلح واحد في العبارتين، وهو ما يدعو إلى القول بأن مصطلح"الغش" يدل على تطلب المشرع قصد خاص حتى تقوم الجريمة، لكن الحقيقة أن عبارة الغش لا تعد وظيفتها إلا تأكيد عبارة عمدا التي سبقتها أي تأكيد القصد الجنائي العام وذلك للأسباب التالية:

- أن مصطلح "الغش" لو كان عاجزا عن الدلالة على عمدية الجريمة لما إستعمله المشرع لوحده في جريمة الدخول وجريمة التلاعب بالمعطيات، إذ أن عبارة "الغش" جاءت لوحدها في هذه الجرائم لتدل على عمديتها، وهذا يعني أن عبارة "عمدا" جاء زيادة وكان يكفي إستعمال عبارة "عن طريق الغش" كما هو في النصوص السابقة.

- إن المادة 394 مكرر2 في بندها الثاني تعاقب على حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم، ولو كان المشرع يتطلب بقوله"عن طريق الغش" قصدا خاصا فلماذا يعود في نفس المادة ويقرر أن الجريمة تقوم "لأي غرض كان" أي مهما كان قصد الجاني والوقائع التي ينصرف إليها من خلال التعامل في هذه المعطيات فإن الجريمة تقوم.

- كان هناك وضع مشابه في مشروع تعديل قانون العقوبات الفرنسي أمام مجلس الشيوخ والذي تم فيه الإكتفاء بعبارة "عن طريق الغش" وحذفت عبارة عمدا، وهذا

الذي حدث مشابه تماما للوضع في المادة 394 مكرر2 من قانون العقوبات الجزائري إذ كان من الأحسن الإكتفاء بعبارة"عن طريق الغش"([1]).

وربما أن المشرع الجزائري في جمعه بين العبارتين إنما أراد التأكيد على الصفة العمدية لهذه الجريمة فحسب، على اعتبار أن الأصل في الأفعال التي نصت عليها المادة 394 مكرر2 أنها أفعال مشروعة لا سيما أنها وردت على معطيات وصفتها هذه المادة بأنها" يمكن أن ترتكب بها جرائم" أي أنها غير معدة خصيصا لارتكاب جرائم، ذلك أن هناك معطيات مزدوجة الإستخدام تصمم للأغراض العلمية أو لأغراض الحماية لكنها قد تستعمل لأغراض الجريمة، وما يجعل هذا التعامل يدخل في دائرة التجريم ليس لأنه مقصود فحسب، ولن لأنه تم عن طريق الغش، والغش هذا يكمن في العلم بطبيعة هذه المعطيات وصفتها غير المشروعة ومع ذلك يقوم الجاني بالتعامل فيها([2]).

هذا وتتطلب إتفاقية بودابست قصدا خاصا لقيام هذه الجريمة يتمثل في التعامل في الجهاز أو الوسائل محل الجريمة بنية إستخدامها في إرتكاب جريمة أي إنصراف القصد(العلم والإرادة) فضلا عن الواقعة المكونة للجريمة- وهي التعامل في هذه الوسائل غير المشروعة- إلى واقعة أخرى لا تدخل في تكوين هذه الجريمة وهي إستخدام هذه الوسائل في إرتكاب الجريمة([3]).

وتشير المذكرة التفسيرية لهذه الإتفاقية لأهمية تطلب القصد الخاص إذا كانت الإجهزة والوسائل محل الجريمة يمكن أن تستخدم لأغراض مشروعة، فتقول:" من أجل تجنب حظر العقاب المبالغ فيه، حيث يتم إنجاز هذه الأجهزة وعرضها في الأسواق لأغراض شرعية من أجل التصدي لاعتداءات على أجهزة الحاسب الآلي فأنه يجب إضافة عناصر أخرى من أجل تطبيق نطاق الجريمة، وبالإضافة إلى

---

[1]- محمد خليفة، مقال بعنوان دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، مرجع سابق، ص 78،79.

[2]- بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 300.

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 218.

إشتراط القصد العام فأنه يجب توفر نية خاصة أو قصد خاص لاستخدام الجهاز من أجل إرتكاب جريمة من الجرائم المشار إليها في المواد من 2 إلى 5 من الإتفاقية"([1]).

أما بالنسبة للوضع في قانون العقوبات الفرنسي فإن المادة 323-1/3 منه([2]) لا تتطلب قصدا خاصا لارتكاب الجريمة، والعبارة التي أضافتها المادة هي" بدون مبرر شرعي" ولم تستعمل لا عبارة عمدا ولا عن طريق الغش، على خلاف مادتي الدخول والتلاعب، وعليه نستنتج أن هذه المادة لا تتطلب قصدا خاصا([3]).

وفي رأينا أن المشرع الجزائري أستعمل عبارة "الغش وعمدا" في المادة 394 مكرر2 للتأكيد على صفة العمدية، وكان يجب عليه أن يقتدي بالمشرع الفرنسي الذي لا يتطلب وجود قصد خاص لقيام هذه الجريمة وأضاف عبارة "بدون مبرر شرعي" التي تقوم بحماية الشخص الذي يقوم بإستخدامها لأغراض مشروعة مثل الأعمال العلمية والتقنية.

إضافة إلى أنه أستعمل أسلوبا غامضا وغير واضح في هذه المادة للدلالة على عمدية الجريمة بإضافته لمصطلح عمدا، وذلك أن الصورة الثانية من هذه الجريمة لا تحتاج الى العمد لأن التعامل فيها يتم أصلا في معطيات متحصل عليها من جريمة، أما في الصورة الأولى فعبارة الغش وحدها تدل على عمدية الجريمة، إضافة الى أنها لم تستثني الذين يستخدمون هذه المعطيات في أبحاث علمية، وكان من الواجب على المشرع أن يضع عبارة واضحة ودقيقة كعبارة بدون مبرر شرعي أو بدون سبب شرعي.

---

[1]- هلالي عبد اللاه أحمد، مرجع سابق ، ص 103،104.

[2] - Art 323-3-1:Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, modifiè par LOI N° 2013-1168 du 18 dècembre 2013-art.25

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 219.

**الفرع الثالث: العقوبات المقررة لجريمة التعامل في معطيات غير مشروعة**

نص المشرع الجزائري في المادة 394 مكرر2 على عقوبات أصلية لجريمة التعامل في معطيات غير مشروعة بصورتيها وعلى عقوبات تكميلية تشترك فيها مع باقي جرائم نظام المعالجة الآلية للمعطيات.

**أولا: العقوبات الأصلية**

تعاقب المادة 394 مكرر2 من قانون العقوبات الجزائري([1]) على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من شهرين إلى ثلاث سنوات وبغرامة من مليون(1.000.000 دج) إلى خمسة ملايين(5.000.000 دج).

وبهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول والبقاء غير المصرح بهما في نظام المعالجة الآلية بصورتيها البسيطة والمشددة وبين جريمة التلاعب بالمعطيات، غير أن حدها الأدنى يقل عن كلتا الجريمتين(شهرين) لأنه في جريمة الدخول أو البقاء في صورتها البسيطة ثلاثة أشهر وفي صورتها المشددة وفي جريمة التلاعب بالمعطيات هو ستة أشهر، أما حدها الأقصى فيزيد عن الحد الأقصى لجريمة الدخول أوالبقاء في صورتيها(سنة أو سنتين) ويتساوى مع الحد الأقصى لجريمة التلاعب بالمعطيات(ثلاث سنوت).

إلا أن ترتيب هذه الجريمة من حيث عقوبة الغرامة هو الأول سواء في حدها الأدنى أو الأقصى (مليون إلى 5 ملايين)، والغرامة في هذه الجريمة تفوق كثيرا الغرامة في جريمة الدخول أو البقاء غير المصرح بهما في صورتيها والمقدرة ب (50 ألف إلى 100 ألف أو 150 ألف دج) ونفس الأمر بالنسبة لجريمة التلاعب بالمعطيات والمقدرة ب(500 ألف إلى 2 مليون دج).

أما بالنسبة لقانون العقوبات الفرنسي فنص على العقوبات المقررة لهذه الجريمة في المادة 323-1/3 ([2]) التي تعاقب عليها بالعقوبة المقررة للجريمة نفسها، أي

[1]- المادة 394 مكرر 2 من القانون 04-15.

[2] - Art 323-3-1:Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, modifiè par LOI N° 2013-1168 du 18 dècembre 2013-art.25

المقررة للجريمة التي يمكن أن تؤدي الوسائل المتعامل فيها إلى إرتكابها، وهي إما جريمة الدخول أو البقاء غير المصرح بهما أو جريمة التلاعب بالمعطيات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات، ونرى أن المسلك الذي سلكه المشرع الفرنسي هو الأسلم، ذلك أنه من غير المعقول المعاقبة على جريمة التعامل في معطيات غير مشروعة بصفتها أعمالا تحضيرية لجريمة دخول أو تلاعب بعقوبة أشد من عقوبة هذه الأخيرة.

وعلى هذا فيجب أن تكون أشد عقوبة يمكن توقيعها على مرتكب جريمة التعامل في معطيات غير مشروعة هي عقوبة الجريمة التي يخشى وقوعها، أي عقوبة الدخول أو التلاعب وهو الأمر الذي فعله المشرع الفرنسي([1]).

فضلا عن ذلك فإن عقوبة الشخص المعنوي تكون أشد بكثير، إذ أن الغرامة المضاعفة إلى خمس مرات تكون كبيرة جدا وثقيلة على الشخص المعنوي، ذلك أنها تتراح بين خمسة ملايين وخمسة وعشرين مليون دينار جزائري، ويلاحظ أن هذا المبلغ ضخم، وأن من شأنه أن يضع حدا لهذا الشخص المعنوي، حتى وإن نزل القاضي الجزائري إلى الحد الأدنى لهذه الغرامة وهو خمسة(5) ملايين دينار جزائري فهو بدوره كبير وقد لا يتناسب مع بعض الحالات([2]) عكس القاضي الفرنسي الذي يتمتع بسلطة أكبر في هذا المجال تسمح له بتفريد العقوبة حسب الحالة المعروضة أمامه، فله أن ينقص من مبلغ الغرامة أو يجزئه([3]).

**ثانيا: العقوبات التكميلية**

العقوبات التكميلية المقررة لجريمة التعامل في معطيات غير مشروعة هي العقوبات نفسها المنصوص عليها في المادة 394 مكرر6 والمقررة لكافة جرائم نظام المعالجة الآلية للمعطيات.

---

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 220.

[2]- بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، ج2، دار الخلدونية، الجزائر، الطبعة1438هـ-2017م، ص 210.

[3]- محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص 223.

ويلاحظ أن عقوبة مصادرة الإجهزة والبرامج وكافة الوسائل المستخدمة في إرتكاب الجريمة([1]) تجد محلا لها في هذه الجريمة أكثر مما تجده في الجرائم الأخرى، ذلك أن جريمة التعامل في معطيات غير مشروعة تفترض وجود معطيات في القانون الجزائري وأجهزة وبرامج ووسائل في القانون الفرنسي، مما يجعل عقوبة المصادرة أكثر تطبيقا عليها([2]).

كما تجدر الإشارة إلى أن المشرع الجزائري قد نص على جريمة أخرى في المادة 394 مكرر 8 بموجب القانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016، المعدل والمتمم لقانون العقوبات، والمتمثلة في مخالفة الإلتزامات الخاصة بمقدمي خدمات الأنترنت، والتي لم نتطرق لها في هذا الفصل لكونها تمثل الجانب الإجرائي لجرائم نظام المعالجة الآلية للمعطيات، باعتبارها آلية فعالة في البحث والتحري والكشف عن مرتكبي هذه الجرائم، وموضعها هو القانون 09-04 الذي ينص على إلتزامات مقدمي خدمات الأنترنت ويعاقب على مخالفة القواعد الإجرائية في عدة مواد، ولذلك كان من الأحسن النص على هذه الإلتزامات ضمن هذا القانون الذي يجمع بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة بتحديد مصدرها والتعرف على مرتكبها، وهو ما سنقوم به، بمعالجة هذه الإلتزامات الخاصة بمقدمي خدمات الأنترنت ضمن الباب الثاني من هذه الرسالة.

وإلى جانب ذلك قام المشرع الجزائري بتشديد العقوبة في المادة 394 مكرر3 بحيث تصبح مضاعفة في حال ما إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

كما أن المشرع ورغبة منه في التصدي بكل فعالية وحزم للإعتدءات الواردة على نظام المعالجة الآلية للمعطيات، فقد نص على كافة الأحكام المشتركة المتعلقة بالجرائم، والمتمثلة في تجريم الإتفاق الجنائي على الإعداد لهذه الجرائم بموجب المادة 394 مكرر5 من قانون العقوبات المعدل والمتمم، وتجريم الشروع فيها بموجب

---

[1]- رامي حليم، مرجع سابق، ص 353.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق ، ص 223.

المادة 394 مكرر 7 من نفس القانون، وكذا إقرار مسؤولية الشخص المعنوي عن إرتكاب إحدى هذه الجرائم بموجب المادة 394 مكرر 7 من القانون نفسه.

ونتوقع في الأخير أن يحمل المستقبل أنواعا جديدة غير متوقعة من جرائم نظم المعالجة الآلية للمعطيات تستخدم فيها تقنيات حديثة ومتقدمة، وسيحتاج خبراء أمن المعلومات إلى أن يظلوا في حالة إستنفار دائمة في مواجهة هذه الأنواع الجديدة، كما ستظل وسائل الإعلام حريصة على إبراز المثير والغريب من هذه الجرائم.

## خلاصة االباب الأول

إن الحماية الموضوعية لنظام المعالجة الآلية للمعطيات أقرها المشرع الجزائري من خلال عدة نصوص، بداية باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات المعدل بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 والقانون 16-02 المؤرخ في 19 يونيو سنة 2016، بمقتضى المواد من 394 مكرر الى 394 مكرر 8 جرم من خلالها الإعتداءات الواردة على نظام المعالجة الآلية للمعطيات والتي أصبحت تهدد مصالح الأفراد والدول فحدد لكل فعل منها ما يقابله من الجزاء، وقام إلى جانب ذلك بوضع إطار قانوني أكثر ملائمة وإنسجاما مع خصوصية هذه الجريمة التي تقع في بيئة إفتراضية بسنه القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، فضلا عن ذلك، فأن تفاقم المخاطر التي تحيط بالمعطيات الشخصية في العصر الحديث، أوجبت على المشرع الجزائري التدخل مرة إخرى، بإصداره القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ويعتبر نظام المعالجة الآلية للمعطيات الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الإعتداء على نظام المعالجة، فإذا تخلف هذا الشرط لا يكون هناك ضرورة للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة بنظام المعالجة الآلية للمعطيات، وهي التي تتعدد صورها وتختلف من تشريع لآخر، ومن أهمها جرائم الدخول أو البقاء في نظام المعالجة الآلية للمعطيات بصورتيها البسيطة والمشددة وجرائم التلاعب بالمعطيات وجرائم التعامل في معطيات غير مشروعة، بحيث تؤدي هذه الجرائم إما إلى المساس بالنظام في حد ذاته (الإعتداء مجرد وسيلة) أو إلى المساس بالمعطيات الموجودة داخل نظام المعالجة الآلية أو التي لها علاقة به (الإعتداء غاية).

# الباب الثاني

# الحماية الإجرائية لنظام المعالجة الآلية للمعطيات

إن الجانب المظلم للمعلوماتية أعطى مفهوما جديدا لجرائم نظام المعالجة الآلية للمعطيات من خلال تواجد المجرم في بيئة إفتراضية متاحة للجميع تتعدد فيها الوسائل وتختلف فيها الأهداف، وتحتوي على بيانات معالجة إلكترونيا وكيانات منطقية غير مادية والتي يصعب فيها كشف الجاني الذي لم يعد مقتصرا على الدراية والذكاء وإستغلال مسرح الجريمة لأنه في بعض الأحيان ترتكب هذه الجرائم دون مسرح أو تتعدد فيها المسارح.

وبات لزاما على رجال القانون سواء كانوا ضباط شرطة أو قضاة أثناء ممارستهم لحق المجتمع في الزود عن كيانه أن يكونوا على علم بأهم النقاط القانونية الواجب مرعاتها في هذا النوع من الإجرام قصد الوصول بأسرع وقت وبأنجع الطرق إلى الجاني، وقبل ذلك الحفاظ على حريات الأفراد وخصوصياتهم، لا سيما وأنها آثارت العديد من المشكلات العملية في مجال الإجراءات الجنائية المتعلقة بالبحث والتحري في الكشف عن هذه الجرائم، والمتعلقة كذلك بالتعاون الدولي لمكافحة هذا النوع من الجرائم سواء من حيث الجهة المختصة بالتحري أو التحقيق أو الإدعاء والمطالبة بالعقاب أو المحاكمة حينما يقع النشاط في دولة وتحدث النتيجة في دولة أخرى، وبذلك أصبحت النصوص الإجرائية القائمة غير كافية لمواجهة جرائم نظام بالرغم من العديد من التعديلات التي طرأت عليها، مما إستدعى وضع نصوص إجرائية جديدة تتجاوب مع الطبيعة الخاصة لهده الجرائم.

وهو ما أوصت به الجنة الأروبية الخاصة بالمشكلات الإجرائية الجزائية المرتبطة بتكنولوجيات الإعلام للدول الأعضاء في المجلس الأروبي من خلال توصياتها رقم(ر 89) الصادرة في عام 1990 وأكدته في توصياتها رقم (ر 95) 13 المؤرخة في 11 سبتمبر 1995 بتصريحاتها أنه" إلى حين وضع نصوص إجرائية جديدة تخص التفتيش والضبط وإعتراض المراسلات في البيئة الإلكترونية، يمكن للسلطة القضائية المختصة في الدول الأعضاء الإستعانة بالنصوص الإجرائية

القائمة في هذا الخصوص، حتى لا تبقى الجرائم المتصلة بتكنولوجيات الإعلام بلا متابعة أو عقاب"([1]).

وتأسيسا على ذلك فقد إتجهت غالبية الدول كمرحلة أولى إلى تعديل قوانينها الإجرائية بصفة دورية ومستمرة بما يضمن مواكبة متغيرات وتطورات جرائم النظام، وإلى إرساء قواعد قانونية جديدة تواجه المشكلات المعاصرة التي أسفرت عنها هذه الجرائم المستحدثة وتطوراتها اللامتناهية، ثم قامت كمرحلة ثانية باستحداث نصوص قانونية خاصة أكثر إنسجاما مع الطبيعة الخاصة لهذه الجرائم.

في حين إقتصرت بعض الدول على تعديل قوانينها الإجرائية بما يتماشى والتطورات الحاصلة في هذا النوع من الإجرام والإعتماد على بعض النصوص القانونية المتفرقة في بعض التشريعات الخاصة كقوانين حماية الملكية الفكرية وقوانين حماية حقوق المؤلف وقوانين التوقيع الإلكتروني.

وعلى المستوى الدولي عرض موضوع "جرائم الحاسب والجرائم الأخرى في مجال تكنولوجيات المعلومات" على بساط البحث في الحلقة التمهيدية التي عقدت فريبورج بألمانيا في الفترة من 5 إلى 8 أكتوبر 1992 للتحضير للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المقرر عقده في ريودي جانيرو بالبرازيل في الفترة من 4 إلى 9 سبتمبر 1994، وفي توصياتها المتعلقة بالتقنيين الإجرائي، لفتت الحلقة النظر وأكدت على ما يلي:

1- أن تحقيق جرائم الحاسب والجرائم الأخرى الأكثر تقليدية في بيئة تكنولوجيا المعلومات يتطلب توافر أساليب قسرية ملائمة لسلطات التحقيق والملاحقة تتوازن على قدم المساواة مع كفالة حماية ملائمة لحقوق الإنسان وإحترام الخصوصيات.

2- يجب بوضوح تحديد ما يلي:

أ- سلطات إجراء النفنيش والضبط في بيئة تكنولوجيا المعلومات.

ب- واجبات التعاون الفعال من جانب المجني عليهم والشهود المباشرين وغيرهم من مستخدمي تكنولوجيا المعلومات عدا المشتبه فيه.

---

[1]- براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة مولود معمري تيزي وزو، سنة 2018، ص 247،248.

ج- الأساليب التي تسمح بمراقبة الإتصالات أن في نظم الحاسبات أو فيما بينها.

3- نظرا لتعدد وتنوع البيانات التي قد تكون مخزنة في نظم معالجة البيانات، فإن تنفيذ الأساليب القسرية يجب أن ينم بطريقة تتناسب مع خطورة الإعتداء ولا تسبب سوى الحد الأدنى من إعاقة الأنشطة القانونية للفرد.

4- وجوب إدخال تعديلات تشريعية ملائمة، إذا ما دعت الضرورة لمواجهة المشاكل التي يمكن أن تسبب فيها القواعد القائمة الخاصة بقبول ومصداقية الأدلة عند تطبيقها إثناء الإجراءات القضائية"([1]).

ويعتبر المشرعين الفرنسي والأمريكي من الأوائل الذين تيقنوا بأن التصدي لهذا النوع من الإجرام لا يكون إلا من خلال العمل على ملائمة النصوص القانونية القائمة للإعتدات الحاصلة على النظم المعلوماتية.

أما بالنسبة للمشرع الجزائري فقد قام كمرحلة أولى بتعديل قانون الإجراءات الجزائية بصفة دورية ومستمرة لمكافحة جرائم ذات خطورة بالغة حددها على سبيل الحصر من بينها جرئم المساس بأنظمة المعالجة الآلية للمعطيات، ثم قام كمرحلة ثانية بسن القانون 09-04،السالف الذكر، والذي يمثل الجانب الإجرائي لكافة جرائم تكنولوجيات الإعلام والإتصال بما فيها جرائم نظام المعالجة الآلية للمعطيات، لكونه يجمع بين القواعد الوقائية التي تسمح بالرصد المبكر لهده الجرائم والتعرف على مرتكبها والقواعد الإجرائية المكملة لقانون الإجراءات الجزائية وكذا القواعد المتعلقة بالإختصاص القضائي والمساعدة القضائية الدولية.

إلا أنه كان جدير بالمشرع مثلا حسب رأينا إستعماله لمصطلح منظومة للدلالة على النظام لأن مجموعة نظام هي أنظمة وليس منظومة، وذلك تماشيا مع تعريف المنظومة الوارد في المادة 2 النقطة "ب" من القانون 09-04" أي نظام منفصل أو مجموعة من الأنظمة.."، وكذلك أيضا مع عنوان القسم السابع مكرر" المساس بأنظمة المعالجة الآلية للمعطيات".

---

[1]- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية-دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط-مصر، سنة 1994، ص ص 9-11.

وعليه، فإننا سنفرد البحث في هذا الباب على التدابير المستحدثة في هذا القانون والتي تقتصر على هذا النوع من الجرائم دون التطرق إلى كافة التدابير المستحدثة الإخرى الواردة في قانون الإجراءات الجزائية والتي تعنى بكافة الجرائم الخطيرة.

ومن تم فإننا سنقوم بتقسيم هذا الباب إلى فصلين يتناول الفصل الأول التدابير المستحدثة للوقاية وللبحث والتحري عن جرائم نظام المعالجة الآلية للمعطيات مبرزا من خلاله التدابير الوقائية والإجرائية المستحدثة للكشف عن هده الجرائم، بينما نتناول في الفصل الثاني آليات التعاون الدولي لمكافحة هذا النوع من الإجرام، وذلك بالتطرق إلى الهيئات المختصة بمكافحة هذه الجرائم ومسألة الإختصاص القضائي والمساعدة القضائية الدولية .

# الفصل الأول

# التدابير المستحدثة للوقاية وللبحث والتحري عن جرائم نظام المعالجة الآلية للمعطيات

## الفصل الأول: التدابير المستحدثة للوقاية وللبحث والتحري عن جرائم نظام المعالجة الآلية للمعطيات

إن خصوصية جرائم نظام المعالجة الآلية للمعطيات تستدعي بأن يتم تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلائم مع هذه الخصوصية وتمكن ضابط الشرطة وقاضي التحقيق من كشف الجريمة والتعرف على مرتكبها بالسرعة والدقة اللازمتين.

وأشارت إلى ذلك إتفاقية بودابست في المادة 14 النقطة الأولى منها إلى ضرورة أن تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقرار الصلاحيات والإجراءات الواردة في هذا القسم، وكذلك الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في النقطة الأولى من المادة 22 على أن تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والإجراءات الواردة في الفصل الثالث من هذه الإتفاقية.

وأدخل المشرع الفرنسي عدة تعديلات على إجراءات المتابعة والتحقيق تتناسب مع طبيعة هذه الجرائم، بإستحداثه لإجرءات خاصة لا سيما منها إعتراض المراسلات والمراقبة الإلكترونية والتحفظ العاجل على المعطيات، في حين لم يكتف المشرع الأمريكي بتكريسه لتشريعات جنائية خاصة لهذا النوع من الجرائم بل إهتم كذلك بتدريب رجال الضبطية القضائية والعاملين في إدارات العدالة على مكافحة هذا النوع من الإجرام.

أما المشرع الجزائري فقد قام بإرساء قوانين إجرائية جديدة، تتضمن جملة من التدابير المستحدثة غير المألوفة في القوانين السابقة والأكثر ملائمة مع خصوصيات جرائم نظام المعالجة الآلية للمعطيات، تتنوع بين تدابير وقائية تتمثل في مراقبة الإتصالات الإلكترونية والإلتزمات المترتبة على مقدمي الخدمة وأخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائية وتتمثل في تفتيش الإنظمة المعلوماتية وحجز المعطيات المعلوماتية.

وعليه، فإننا سنقوم بتقسيم هذا الفصل إلى مبحثين، يتناول المبحث الأول التدابير المستحدثة للوقاية من جرائم نظام المعالجة الآلية للمعطيات بينما نتناول في

المبحث الثاني التدابير الإجرائية للبحث والتحري في الكشف عن جرائم نظام المعالجة الآلية للمعطيات المكملة لتلك الإجراءات المنصوص عليها في قانون الإجراءات الجزائية المعدل والمتمم، بموجب التعديلين رقما 14-04 المؤرخ في 10 نوفمبر 2004 (تمديد الإختصاص القضائي) و 06-22 المؤرخ في 20 ديسمبر 2006 (إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب)، والخاصة بالتحري والتحقيق للكشف عن جرائم نظام المعالجة الآلية للمعطيات.

## المبحث الأول: التدابير المستحدثة للوقاية من جرائم نظام المعالجة الآلية للمعطيات

وهي عبارة عن تلك التدابير التي يتم إتخاذها مسبقا من طرف مصالح مختصة لتفادي وقوع جرائم نظام المعالجة الآلية للمعطيات والكشف عنها ورصد مرتكبها في وقت مبكر ومن أهمها مراقبة الإتصالات الإلكترونية سواء من طرف القضاء أو من طرف هيئات خاصة وبعض الإلتزامات المترتبة على مقدمي خدمات الأنترنت.

لذلك سنقوم بتقسيم هذا المبحث إلى مطلبين نعالج من خلالهما في المطلب الأول التدابير الوقائية المتعلقة بمراقبة الإتصالات الإلكترونية وفي المطلب الثاني التدابير الوقائية المتعلقة بإلتزامات مقدمي الخدمة بالنسبة للإتصالات الإلكترونية.

### المطلب الأول: التدابير الوقائية المتعلقة بمراقبة الإتصالات الإلكترونية

يقصد بمفهوم الإتصالات الإلكترونية حسب المادة 2 من القانون 09-04، السالف الذكر، بأنه" أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترزنية"، وقد تبنى الدستور الجزائري هذا المبدأ بكل وضوح في نص المادة 47 منه بقولها" ...لكل شخص الحق في سرية مراسلاته وإتصالاته الخاصة بأي شكل كانت.."([1]).

ويبدو كذلك أن المشرع الجزائري لم يستثن المراسلات العادية التي تتم عن طريق وسائل الإتصالات السلكية واللاسلكية كما ورد ذلك في المادة 65 مكرر 5 من قانون الإجراءات الجزائية أذ نصت على أنه في الجرائم المعلوماتية أي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية([2]).

وإن مراقبة الإتصالات الإلكترونية في الغالب قد تتم عن طريق القضاء(الفرع الأول) وقد تتم عن طريق هيئات خاصة (الفرع الثاني).

---

1- المادة 47 من المرسوم الرئاسي 20-442.

2- زبيحة زيدان، مرجع سابق، ص 124.

**الفرع الأول: مراقبة الإتصالات الإلكترونية عن طريق القضاء**

نصت المادة 35 من قرار السلطة الفلسطينية لقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية على أنه:

1- لقاضي الصلح أن يأذن للنيابة العامة بمراقبة الإتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها للبحث عن الدليل المتعلق بالجريمة.

2- للنيابة العامة أن تأمر بالجمع والتزويد الفوري لأي بيانات بما فيها حركة الإتصالات...([1])

وفي مصر نصت المادة 57 من دستور 2014 على أن للحياة الخاصة حرمة وهي مضمونة لا تمس وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الإتصال حرمة وسريتها مكفولة..، ونصت المادة 90 من قانون الإجراءات الجنائية المصري على أن " لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص.."([2]).

أما بالتسبة للمشرع الجزائري فرغم ضمانه لسرية المراسلات والإتصالات بكل إشكالها قد خول إستثناء للسلطة القضائية وفي إطار قرار معلل بأن تتبع إجراءات تمس البيانات الشخصية بالنظر لخطورة بعض الجرائم المعلوماتية المحددة حصرا في تسجيل الإتصالات الإلكترونية في حينها([3])، وهو ما نصت عليه المادة 3 من القانون 09-04، السالف الذكر، بقولها" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد القانونية المنصوص عليها في

---

[1] - المادة 35 من القرار الفلسطيني بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية.

[2]- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات -دراسة مقارنة، مرجع سابق، ص 815،816.

[3]- أمحمدي بوزينة أمنة، بحث بعنوان إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، أعمال الملتقى الوطني: مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل للبحث العلمي، الجزائر 29 مارس 2017، ص 73.

قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"

كما نصت المادة 4 من نفس القانون على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية إستثناء بالنسبة لسلطات الأمن والتحقيق التابعين للسلطة القضائية، وحصرتها في أربع حالات، وهي كالاتي:"

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة"([1]).

ولا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بأذن مكتوب من السلطة القضائية المختصة".

ويظهر من خلال إستقراء هذه المادة أن المشرع الجزائري يحاول الإستفادة بدوره من التطور التكنولوجي والميزات التي يخولها من خلال وضع المشتبهين فيهم تحت المراقبة الإلكترونية وهي على عكس المراقبة الشخصية الأقل تكلفة من حيث الوقت والمال والمخاطر الأمنية إضافة إلى فعاليتها([2])، إلا أنه يترتب على تطبيق هده التدابير ميدانيا المساس بحرمة الحياة الخاصة التي هي مقدسة ومحمية دستوريا، لذلك ربط القيام بها بشرط الحصول عل أذن مكتوب من السلطة القضائية([3]).

كما ينبغي الإشارة إلى أن المراقبة السرية الإلكترونية للإتصالات الإلكترونية ومن ضمنها المحادثات الهاتفية لا يمكن إعتبارها نوع من أنواع التفتيش، وذلك لأن

---

1- المادة 4 من القانون 09-04.

2- أمحمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مرجع سابق، ص74.

3- زبيحة زيدان، مرجع سابق، ص 128.

المراقبة الإلكترونية ترد على البيانات الإلكترونية المتحركة التي تتجسد هنا بالإتصالات الإلكترونية حال إجرائها، دون تلك التي إنتهت وخزنت، في حين التفتيش إنما يرد فقط على البيانات الإلكترونية الساكنة أو المخزنة التي تتجسد هنا بالإتصالات الإلكترونية التي تمت وخزنت([1]).

**الفرع الثاني: مراقبة الإتصالات الإلكترونية عن طريق هيئات خاصة**

تسند بعض التشريعات مهمة مراقبة الإتصالات الإلكترونية إلى هيئات أو وحدات خاصة مثل ما فعل المشرع الفلسطيني عندما نص في المادة 3 من القرار الفلسطيني قانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية([2]) على أنه:" تنشأ وحدة متخصصة في الجرائم الإلكترونية في الأجهزة الشرطية وقوات الأمن..."([3])، وكذلك مثل ما فعله المشرع الجزائري عندما أسندها إلى هيئة خاصة تسمى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته.

لذلك سوف نتطرق أولا إلى تعريف هذه الهيئة ومهامها بصفة عامة ثم نقوم بدراسة مهمتها في إطار مراقبة الإتصالات الإلكترونية بصفة خاصة.

**أولا: تعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته**

نص عليها المشرع الجزائري في الفصل الخامس من القانون 09-04، السالف الذكر، تحت عنوان الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، وأنشأها بموجب المادة 13 من نفس القانون التي تنص على أنه" تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"([4]).

---

[1]- بن مكي نجاة ، مرجع سابق، ص 231.

[2]- المادة 3 من القرار الفلسطيني بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية.

[3]- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق، ص605.

[4]- المادة 13 من القانون 09-04.

وأحال المشرع الجزائري فيما يخص تنظيم الهيئة إلى المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو سنة 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها([1])، والذي ألغى المرسوم الرئاسي رقم 19-172 المؤرخ في 6 يونيو 2019، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها([2])، والذي ألغى بدوره قبل ذلك أحكام المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها([3]).

وعرف الهيئة في المادة 2 من المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو سنة 2020، بقولها" الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلالية المالية توضع تحت سلطة رئيس الجمهورية"، وتم تحديد مقرها بمدينة الجزائر، والذي يمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي طبقا لأحكام المادة 3 من نفس المرسوم.

وتتشكل هذه الهيئة بحسب المادة 5 من المرسوم نفسه من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية، ويقدمان له عرضا عن نشاطاتهما.

أما عن مهام الهيئة فقد نصت عليها المادة 4 من المرسوم الرئاسي رقم 20-183 ، بقولها:" في إطار المهام المنوطة بها والمنصوص عليها في المادة 14 من

---

1- المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج ر ج ج، ع 40، مؤرخة في 18 يوليو 2020، ص 5.

2- المرسوم الرئاسي رقم 19-172 المؤرخ في 6 يونيو 2019، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر ج ج، ع 37، مؤرخة في 09 يونيو 2019، ص 5.

3- المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، ج ر ج ج، ع 53، مؤرخة في 8 أكتوبر 2015، ص 16.

القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه، وتحت رقابة السلطة القضائية طبقا لأحكام التشريع الساري المفعول تكلف الهيئة على الخصوص بما يأتي:

- إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

- مساعدة السلطات القضائية المختصة ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، لا سيما من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل إستعمالها في إطار الإجراءات القضائية.

- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال إختصاصها.

- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والإتصال.

- المساهمة في تحيين المعايير القانونية في مجال إختصاصها"([1]).

والملاحظ أن المرسوم الخاص بتنظيم هذه الهيئة شهد عدة تعديلات بوضعها أولا لدى الوزير المكلف بالعدل ثم وضعت تحت سلطة وزير الدفاع، وأخير تم وضعها تحت سلطة رئيس الجمهورية، ويمكن نقلها إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي، إضافة إلى غياب بعض القرارات الوزارية المنصوص

1- المادة 4 من المرسوم الرئاسي رقم 20-183.

عليها في المادتين 14 و15 من المرسوم الرئاسي رقم 20-183 ، والتي تحدد تنظيم وكيفيات سير مكونات المديرية العامة للهيئة، وكذا كيفيات تطبيق الأحكام المنصوص عليها في المادة 15 من نفس المرسوم.

كما أن هذه الهيئة تخضع لمختلف أنواع المراقبة المنصوص عليها في التشريع والتنظيم المعمول بهما، ويخضع مستخدموها لمجموع الأحكام التشريعية والتنظيمية المطبقة في وزارة الدفاع الوطني وكذا كل النصوص اللاحقة به، طبقا لأحكام المادتين 35 و36 من نفس المرسوم.

وإلى جانب ذلك صدر أيضا المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق ل 20 جانفي سنة 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية([1])، بحيث تعتبر هذه المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها، طبقا لأحكام المادة الأولى من هذا المرسوم.

كما تشمل هذه المنظومة التي توضع لدى وزارة الدفاع الوطني مجلسا وطنيا يكلف بإعداد الإستراتيجية المذكورة والموافقة عليها وتوجيهها ووكالة تضطلع بتنسيق تنفيذ هذه الإستراتيجية، طبقا لأحكام المادة الثالثة من ذات المرسوم.

وتلزم المؤسسات والإدارات والهيئات العمومية والمتعاملون الخواص بتعيين مسوؤلهم المكلف بأمن الأنظمة المعلوماتية في أجل أقصاه سنة، إبتداء من تاريخ نشر هذا المرسوم في الجريدة الرسمية، طبقا لأحكام المادة 41 من نفس المرسوم.

**ثانيا: مهمة الهيئة الوطنية في مجال مراقبة الإتصالات الإلكترونية**

لقد أوكل المشرع الجزائري بموجب المادة 4 الفقرة الثالثة من قانون 09-04 والمادة 15 من المرسوم رقم 20-183، المذكور سالفا، مهمة المراقبة الوقائية للإتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية أو التخريبية والإعتداء على أمن الدولة إلى مديرية المراقبة الوقائية واليقظة الإلكترونية

[1]- مرسوم رئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

التابعة للمديرية العامة للهيئة، التي تمارس مهامها المرتبطة بالشرطة القضائية وفقا لأحكام التشريع المعمول به، لا سيما الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، وذلك طبقا لأحكام المادة 16 من نفس المرسوم.

وفي هذا السياق نصت المادة 4 في الفقرتين الثالثة والرابعة منها من القانون 09-04، على أنه" عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة(6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والإعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير"([1]).

وحسنا ما فعل المشرع الجزائري عندما حصر وضع الترتيبات التقنية للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة أن تكون موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والإعتداءات على أمن الدولة ومكافحتهما، وأن كل من يخالفها يقع تحت طائلة العقوبات المقررة في قانون العقوبات لمساسه بحرمة الحياة الخاصة للغير.

والضرورة هنا تتعلق بمسألة حماية أمن البلاد والمواطن والإقتصاد الوطني من هذه الجرائم الخطيرة والتي تعلو على حق المشتبه فيهم في الحفاظ على حقهم في السرية أو حرمة حياتهم الخاصة المكفولة دستوريا خاصة عدم جواز إنتهاك سرية المراسلات والإتصالات بمختلف أشكالها، والتي تتوقف في النهاية على قدرة المشرع

1- المادة 4 من القانون 09-04.

على إقامة التوازن بين حق المجتمع في الأمن ومنع الجريمة وحق الأفراد في السرية([1]).

**المطلب الثاني: التدابير الوقائية المتعلقة بإلتزامات مقدمي الخدمة بالنسبة للإتصالات الإلكترونية**

ألزم المشرع الجزائري مقدمو الخدمات ببعض الإلتزامات في إطار مراقبة الإتصالات الإلكترونية كتدابير وقائية للكشف عن جرائم نظام المعالجة الآلية للمعطيات، وعرفهم بموجب المادة 2 الفقرة د من القانون 09-04 بأنهم:"

1- أي كيان عام أو خاص يقدم لمستعمليه خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات.

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها"([2]).

أو هو كل شخص يمد المستخدمين بالقدرة على الإتصال بواسطة أنظمة حاسب آلي أو تقوم بمعالجة البيانات وتخزينها بالنيابة عن هؤلاء المستخدمين، حسب ما نصت عليه المادة 2 الفقرة ج من إتفاقية بودابست، والذي يقتصر دوره على تمكين المشتركين من الوصول إلى شبكة الأنترنت عن طريق مدهم بالوسائل الفنية اللازمة للوصول إلى الشبكة بمقتضى عقد توصيل الخدمة([3]).

ونص المشرع الجزائري على هذه الإلتزامات في الفصل الرابع من القانون 09-04 تحت عنوان " إلتزامات مقدمي الخدمات" كتدابير وقائية لمراقبة الإتصالات الإلكترونية من خلال تكريسه لها بموجب إلتزامات عامة وخاصة لمقدمي خدمات الأنترنت.

لذلك سوف نقوم بدراسة هذه الإلتزمات في كل فرع على حدى، بحيث نتناول في الفرع الأول الإلتزامات العامة لمقدمي الخدمات بالنسبة للإتصالات الإلكترونية

---

1- بوكر رشيدة، مرجع سابق، ص 376.

2- المادة 2 من القانون 09-04.

3- محمد نصر محمد، المسؤولية الجنائية لإنتهاك الخصوصية المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، الطبعة الأولى، سنة 2016، ص 79.

(الأنترنت)، أما الفرع الثاني فنخصصه للإلتزمات الخاصة لمقدمي الخدمات بالنسبة للإتصالات الإلكترونية (الأنترنت).

**الفرع الأول: الإلتزامات العامة لمقدمي الخدمات بالنسبة للإتصالات الإلكترونية (الأنترنت)**

نص المشرع الجزائري على الإلتزامات العامة لمقدمي خدمات الأنترنت في المادتين 10 و11 من القانون 09-04، والمتمثلة في إلتزام مقدمي الخدمات بمساعدة السلطات المكلفة بالتحريات القضائية وإلتزام مقدمي الخدمات بحفظ المعطيات المتعلقة بحركة السير.

**أولا: إلتزام مقدمي الخدمات بمساعدة السلطات المكلفة بالتحريات القضائية**

نص القانون الفرنسي للإتصال عن بعد الصادر في 30 سبتمبر 1986 على أنه يقع على متعهد الخدمة الإلتزام بحسن تنفيذ الخدمة المعلوماتية بحيث يتم تنفيذها بما يتفق مع أعراف المهنة ويلتزم أيضا بالإعلام عن وسائل الدخول إلى الخدمة مثل شفرة تحقيق الهوية، ويقوم بمراقبة محتوى الرسائل التي تصل إليه ويقرر عدم نشر تلك التي يقدر إنها غير مشروعة([1]).

أما بالنسبة للمشرع الجزائري ألزمت المادة 10 من القانون 09-04 على مقدمي خدمات الأنترنت تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة، كما ألزمتهم أيضا بكتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات التي يقررها القانون في حالة إفشاء أسرار التحري أو التحقيق.

وهو الإجراء والإلتزام الذي نجد له أصلا قانونيا على المستوى الدولي حسب ما تقرره أحكام المادتين 16 و17 من إتفاقية بودابست لمكافحة الجرائم المعلوماتية،

---

[1]- مقتبس عن: محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت(دراسة مقارنة) ، دار النهضة العربية، القاهرة، سنة 2005، ص 164.

وتقابلها المواد 23،24 و25 من الإتفاقية العربية لمكافحة الجرائم المتصلة بالتقنية المعلوماتية([1]).

إلا أنه وبالرجوع لنص المادة 10 الفقرة الأولى من هذا القانون فإن المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتوى الإتصال ولكن بشرط أن يكون في حينه، وهو إجراء تسخير من طرف السلطات القضائية لمقدمي الخدمات المعنيين لجمع وتسجيل المعطيات المتعلقة بمحتوى إتصالات أيا كانت( مكالمات صوتية هاتفية أو مكالمات فيديو عبر مواقع الأنترنت (SMS-Email-MMS)([2]).

ولم يحدد المشرع الجزائري مدة تسجيل هذه الإتصالات وتركها مفتوحة ولم يحدد كذلك الأشخاص المكلفين بتسخير مقدمي الخدمات للقيام بهذا الإجراء الخطير، عكس المشرع الفرنسي الذي سمح لضباط الشرطة القضائية بتسخير من وكيل الجمهورية مع ترخيص مسبق من طرف قاضي الحريات والحبس بتسخير مقدمي الإتصالات للجمهور عبر الأنترنت للقيام بكل الإجراءات التي تؤمن الحفظ لمدة لا تزيد عن سنة واحدة لمحتويات المعلوماتية التي تتم من طرف أشخاص مستعملين للخدمات التي يؤمنها مقدمو الخدمات المعنيون، طبقا لأحكام المادة 60-2 فقرة 2 من قانون الإجراءات الجزائية الفرنسي([3])، وبذلك تعتبر هذه الإجراءات بمثابة ضمانات قانونية تكفل حماية الحياة الخاصة للأشخاص وتحد من التجاوزات التي

---

1- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة باتنة 1، الموسم الجامعي 2015،2016، ص 232.

2- عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة مقدمة لنيل شهادة دكتواره علوم في القانون الجنائي، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة العربي التبسي –تبسة، الموسم الجامعي 2017،2018،ص 144.

3 -Article 60-2/2 : L'officier de police judiciaire ou , sous le contrôle de ce dernier, de l'agent de police judiciaire, intervenat sur rèquisition du procureur de la Rèpublique prèalablement autorisè par ordonnance du juge des libertès et de la dètention, peut requèrir des opèrateurs de tèlècommunications…,Code de procèdure pènale france, modifiè par LOI N° 2019-222 du 23 mars 2019-art.47.

يمكن لأعوان الضبط القضائي ممارستها في حالة التحريات عن جرائم متصلة بتكنولوجيات الإعلام والإتصال([1]).

وأن مقدمي خدمات الأنترنت عديدون ويطلق عليهم أحيانا الوسطاء في خدمة الأنترنت ودور هؤلاء هو تمكين مستخدمي الأنترنت من الدخول إلى الشبكة والإطلاع عما يبحث عنه أو ما يريد معرفته، ومنهم مزود الخدمة وهو إما أن يكون شخصا طبيعيا أو معنويا يقوم بنقل الخدمة بتمكين أوتسهيل دخول المستخدم لشبكة الأنترنت من خلال ربط المستخدم بالمحتوى المنقول بواسطة الشبكة وذلك في مقابل تسديد قيمة الإشتراك([2])، لذا فهو يعد الوسيط بين مستخدمي الأنترنت وبين موردي الخدمات وعن طريقه يتم إتصال مستخدمي الأنترنت بالمواقع التي يرغبون في الدخول عليها([3])، وبهذا فإن مزود الخدمة بإمكانه مساعدة جهات التحقيق بتمكينها بكل المعلومات التي تساعدها أو التي تبحث عنها بل أنه ملزم بذلك وفقا لنص المادة 10 المشار لها سالفا، ويوجد أيضا متعهد توصيل المعلومات ودوره تقني يتجسد في إيصال المستخدم إلى شبكة الأنترنت وذلك بربطه بالمواقع التي يريدها وليس له علاقة بالمعلومات أو بمحتواها.

وهناك أيضا متعهد الإيواء وهو أما أن يكون شخصا طبيعيا أو معنويا يقوم بعمل محدود وهو عرض الأمكنة على الشبكة أو بمعنى آخر إيواء صفحات WEB على حاسوبه الخادم مقابل أجر لصالح المستخدم الذي يعمل على نشر ما يريده من صور أو معلومات أو يقوم بربط علاقات مع مواقع أخرى([4])، وطبيعة هذه الخدمة

---

[1]- مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم 09-04، مذكرة مقدمة لنيل شهادة الماجستير تخصص قانون جنائي، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة قاصدي مرباح –ورقلة، الموسم الجامعي 2012،2013،ص 101.

[2]- ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالأنترنت والمعلوماتية-دراسة تطبيقية مقارنة، مركز الدراسات العربية للنشر والتوزيع، جهورية مصر العربية، الطبعة الأولى، سنة 2017، ص 562.

[3]- شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت-دراسة مقارنة، دار النهضة العربية، القاهرة، سنة 2009، ص 134.

[4]- زبيحة زيدان، مرجع سابق، ص 154.

التي يقدمها تجعله الأقدر على تحديد هوية مرتكبي الجريمة المعلوماتية ومعرفة مضمون أي نشاط معلوماتي متداول عبر شبكة الأنترنت([1]).

كما أدخل المشرع الجزائري إستغلال شبكة الأنترنت في نظام الخوصصة بعد أن كانت محتكرة من طرف مركز الإعلام العلمي والتقني سريست بموجب المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998، المتعلق بضبط شروط وكيفيات إقامة خدمات أنترنات واستغلالها([2])، الذي رتب عدة إلتزامات على مقدمي الخدمات من خلال ممارستهم لنشاطهم كإجراءات وقائية وأهمها تسهيل النفاذ إلى خدمات أنترنت حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك، باستعمال أنجع الوسائل التقنية والمحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيها الخاصة، وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون، وكذا إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات أنترنت وصيغة مساعدتهم كلما طلبوا ذلك، إضافة إلى إعلامهم بالمسؤولية المترتبة عليهم فيما يتعلق بمحتوى الصفحات التي يستخرجونها وفقا للأحكام التشريعية المعمول بها([3]).

**ثانيا: إلتزام مقدمي الخدمات بحفظ المعطيات المتعلقة بحركة السير**

رتبت المادة 11 من القانون 09-04([4]) على مقدمي خدمات الأنترنت إلتزاما آخر يتمثل في حفظ المعطيات التي من شأنها تمكين جهات التحقيق من التعرف على مستعملي الخدمة، وحددت المدة اللازمة لحفظها وهي سنة واحدة إبتداء من تاريخ التسجيل، إذ يلتزم مقدمو الخدمات مع مراعاة طبيعة ونوعية الخدمات بحفظ ما يلي:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

---

1- فهد عبيد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ، دار الجامعة الجديدة، الأسكندرية، سنة 2016، ص 446.

2- مرسوم تنفيذي رقم 98-257 مؤرخ في 03 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998، يضبط شروط وكيفيات أقامة خدمات"أنترنات" واستغلالها، ج ر ج ج، ع 63، مؤرخة في 26 غشت 1998.

3- قادري أعمر، الجرائم الخطيرة بين القانون والشريعة على ضوء بنود الإتفاقيات والتشريعات الخاصة ذات الطابع الجزائي ، دار هومة، الجزائر، سنة 2017، ص 343.

4- المادة 11 من القانون 09-04.

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة لإتصال.

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال.

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة أو مقدميها.

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة إبتداء من تاريخ التسجيل.

والملاحظ أن المشرع الجزائري حدد المعطيات الواجب حفظها من طرف مقدمي خدمة الأنترنت وهي المعطيات المتعلقة بحركة المرور أو كما سماها بحركة السير، وحدد مدة حفظها بسنة واحدة إبتداء من تاريخ التسجيل، وعرفها في المادة الثانية (2) الفقرة هـ من القانون 09-04، بأنها" أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة إتصالات، توضح مصدر الإتصال والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة"([1]).

وبالرجوع إلى المذكرة التفسيرية لإتفاقية بودابست نجدها تشير هي الأخرى إلى شمول معطيات المرور المتعلقة باتصالات سابقة ضمن المعطيات المشمولة بإجراء التحفظ المنصوص عليه في المادة 16 من الإتفاقية، وأن كانت هذه الأخيرة لا تتضمن ما يوجب الإحتفاظ بالمعطيات وكذا الجمع والإحتفاظ بكل أو حتى بعض المعطيات المجمعة بواسطة مزود الخدمة([2]).

وهو ما تضمنه قرار الجمعية العامة للأمم المتحدة رقم (63/55) المؤرخ في 22 يناير 2001، والمتعلق بمكافحة إستعمال تكنولوجيا المعلومات لأغراض إجرامية

---

1- المادة 2 الفقرة هـ من القانون 09-04.

2- بوكر رشيدة، مرجع سابق، ص 449.

وذلك في الفقرة "و" من المادة 1 منه، والتي ألزمت الدول أن تسمح بحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الحصول عليها([1]).

كما أقر المشرع الجزائري قيام المسؤولية الجزائية في حالة عدم إحترام الإلتزامات المنصوص عليها في المادة 11 من القانون 09-04 بالنسبة للأشخاص الطبيعين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية بمعاقبة الشخص الطبيعي بالحبس من ستة(6) أشهر إلى خمس(5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج، وكذا معاقبة الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات([2]).

وإلى جانب ذلك أورد المشرع الفرنسي هو الآخر عقوبات على مزود الخدمة في حالة عدم حفظه للمعطيات التقنية المفروض عليه تخزينها والمتعلقة بهوية المتصلين وساعة الإتصال، بموجب الفقرة الثانية(2) من المادة (L3-39) من قانون البريد والإتصالات الإلكترونية([3]).

**الفرع الثاني: الإلتزامات الخاصة لمقدمي الخدمات بالنسبة للإتصالات الإلكترونية (الأنترنت)**

نص المشرع الجزائري في المادة 12 من القانون 09-04، السالف الذكر، على الإلتزامات الخاصة لمقدمي خدمة الأنترنت، والتي تكون زيادة على الإلتزامات العامة المنصوص عليها في المادة 11 من نفس القانون والمذكورة آنفا، وحصرها في إلتزامين وهما: الإلتزام بالتدخل الفوري والإلتزام بوضع ترتيبات تقنية.

**أولا: إلتزام مقدمي الخدمات بالتدخل الفوري**

نص المشرع الجزائري على هذا الإلتزام في المادة 12 النقطة الأولى منها بقولها" زيادة على الإلتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الأنترنت" ما يأتي:

---

[1]- مقتبس عن: بوكر رشيدة، مرجع سابق، ص 446.

[2]- المادة 11 من القانون 09-04.

[3]- بوكر رشيدة، مرجع سابق، ص 453.

أ- التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن"([1]).

وهذا الإلتزام يتضمن سحب المحتويات غير المشروعة بدون تمهل أو عن طريق منع الوصول إليها من طرف مقدمي خدمات الأنترنت بمجرد علمهم بصفة مباشرة أو غير مباشرة، وذلك بالتدخل من تلقاء أنفسهم أو بناء على طلب من مستخدم الأنترنت، بحيث يجب أن يكون هذا التدخل عاجلا وسريعا لسحب المحتوى غير المشرع أو بغلق الموقع كلية.

وقد تداركت إتفاقية بودابست القصور في تحديد مفهوم المحتوى غير المشروع كون الفكرة في حد ذاتها مطاطة، وتختلف من دولة لإخرى، وذلك عن طريق البرتوكول الإضافي المتعلق بتجريم أفعال التمييز والتحريض على الكراهية بواسطة منظومة معلوماتية([2]).

كما رتب المشرع الفرنسي مسؤولية مدنية وجزائية على مقدمي خدمة الإيواء الذين يرفضون أو يتقاعسون عن القيام بإلتزامهم المتمثل في سحب المحتويات المخالفة للقوانين أو جعل الدخول إليها غير ممكن، وهو ما نصت عليه المادة 6 الفقرة 1 و2 من القانون رقم 2004/575 الصادر في 21 جوان 2004 من أجل الثقة في الإقتصاد الرقمي (LCEN)([3]) حيث نصت على أن" المسؤولية المدنية أو

---

1- المادة 12 النقطة 1 من القانون 09-04.

2- مناصرة يوسف، مرجع سابق، ص 187،188.

3-Art 6/1/2 ;

2. Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère manifestement illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.

3. Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance du caractère manifestement illicite de l'activité ou de l'information ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible.

الجزائية لمقدم خدمة الإيواء لا يمكن أن تقوم إلا في حالة العلم الحقيقي بالوقائع أو الظروف التي بموجبها يكون النشاط أو المعلومة مجرمة، وفيما يتعلق بالمطالبة بالتعويضات فلا تقوم إلا مع وجود العلم بأن الوقائع أو الظروف بحسب النشاط أو المعلومة تكون مجرمة ولم ينصرف مقدم خدمة الإيواء فورا لسحب المعلومات أو يجعل الوصول إليها مستحيلا([1]).

بينما تدارك المشرع الجزائري الغموض الذي كان يشوب قيام المسؤولية الجزائية لمقدمي خدمات الأنترنت في حالة مخالفتهم لهذه الإلتزامات الخاصة المنصوص عليها في المادة 12 من القانون 09-04 التي وردت في شكل إلتزامات بدون جزاءات، وذلك بترتيب المسؤولية الجزائية لهم من خلال تعديل قانون العقوبات بموجب القانون 16-02 المؤرخ في 19 يونيو سنة 2016 باستحداثه للمادة 394 مكرر8 في القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات، والتي نصت على ما يلي" دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساريي المفعول، يعاقب بالحبس من سنة إلى ثلاث (3) سنوات وبغرامة من 2.000.000 دج إلى 10.000.000 دج، أو بإحدى هاتين العقوبتين فقط، مقدم خدمات "الأنترنت" بمفهوم المادة 2 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل05 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، والذي لا يقوم رغم إعذاره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك:

أ- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الإطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا.

---

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa, modifiè par LOI N° 2020-766 du 24 juin 2020-art.1.

[1] - عفاف خذيري، مرجع سابق، ص 146.

ب- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة (أ) من هذه المادة أو لجعل الدخول إليها غير ممكن"([1]).

وفي رأينا بأن هذه المادة وضعت في غير موضعها باعتبارها تعاقب على مخالفة الإلتزامات الخاصة بمقدمي خدمات الأنترنت المنصوص عليها في المادة 12 من القانون 09-04، لذا كان من الأولى أن توضع في هذا القانون الذي ينص على هذه الإلتزامات الخاصة بمقدي خدمات الأنترنت.

كما أن وجود هيئة خاصة لمراقبة المحتوى غير المشروع لا يمنع من تدخل مقدم خدمة الأنترنت أزاء المحتوى غير المشروع إما بالحذف أو السحب أو منع الوصول وغيرها من الإجراءات في ظل أحكام المادة 12 من القانو 09-04 ضمن الإلتزامات الواقعة على عاتقه ومسؤوليته الجزائية لا تقوم إلا في ظل المادة 394 مكرر8 التي كرست مبدأ مسؤوليتهم على غرار دول القانون المقارن، وذلك بموجب صدور أمر أو حكم قضائي أو إعذار من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في حالة مخالفتهم للإلتزامات الخاصة بمقدمي خدمة الأنترنت([2]).

**ثانيا: إلتزام مقدمي الخدمات بوضع ترتيبات تقنية**

فرض المشرع الفرنسي على مقدمي الخدمات أن يعلموا مستخدمي الأنترنت بوجود تقنيات تسمح بحصر الوصول إلى مواقع معينة أو بتحديدها مع وجوب أن يعرضوا على مستخدمي الأنترنت واحدة من هذه الأساليب التقنية وكذلك وجوب أن توضع مباشرة آليات المراقبة، وأضافت المادة 6 في فقرتها 1 و7 من القانون رقم 2004/575([3]) بوجوب التبليغ السريع للسلطات القصائية عن النشاطات المجرمة

---

[1]- المادة 394 مكرر 8 من القانون 16-02.

[2]- مناصرة يوسف، مرجع سابق، ص 184.

[3]- Art 6/1/7 ;

1.Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.

7…. Les personnes mentionnées aux 1 et 2 informent leurs abonnés de l'interdiction de procéder en France métropolitaine et dans les départements d'outre-mer à des opérations de vente à distance, d'acquisition, d'introduction en provenance d'un autre Etat membre de l'Union européenne ou d'importation en provenance de pays tiers de produits du tabac manufacturé dans le cadre d'une vente à

الموجودة في الأنترنت والتي أعلنت عنها لمستعمليها بأنها مواقع تحوي مضامين مخالفة للقانون.

كما يجب على مقدمي الخدمات أن يقدموا للجمهور(مستعملي الأنترنت) الوسائل المكرسة لمكافحة الإنحرافات التي تكون جرائم في القانون العام([1]).

أما بالنسبة للمشرع الجزائري فقد نص على هذا الإلتزام في المادة 12 النقطة الثانية منها من القانون 09-04، بقولها" زيادة على الإلتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الأنترنت" ما يأتي:

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها"([2]).

وهذا الإلتزام يتمثل في وضع مقدمي خدمات الأنترنت ترتيبات تقنية تسمح لمستعملي الأنترنت بالتعرف وبسهولة على نوع هذه المواقع، وبالطبع يجب أن تكون واضحة لمن أراد إن يدخل لمواقع معينة معرفة أنه موقع مخالف للنظام العام والآداب العامة قبل الدخول إليه.

كما يجب لهذه التقنيات أن تعلم لمن يستعملها بوجود وسائل تقنية تسمح بحصر الدخول إلى هذه المواقع كالمراقبة الأبوية التي تمنع القصر من دخول هذه المواقع باستعمال برامج وقائية تتطلب كلمة سر معينة([3]).

وإن مقدم خدمة الأنترنت ليس ملزما بمراقبة محتوى الإتصالات الإلكترونية([4])، وإنما هو ملزم بوضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإعلام المشتركين لديهم

---

distance, ainsi que des sanctions légalement encourues pour de tels actes…., modifiè par LOI N° 2020-766 du 24 juin 2020-art.1.

[1]- مسعود مريم، مرجع سابق، ص 104،105.

[2]- المادة 12 النقطة 2 من القانون 09-04.

[3]- عفاف خذيري، مرجع سابق، ص 146، 147.

[4]- مناصرة يوسف، مرجع سابق، ص 188.

بوجودها، وإلا وقع تحت طائلة العقوبات المنصوص عليها في المادة 394 مكرر8 من قانون العقوبات المعدل والمتمم، والمشار لها إعلاه.

ومن تم يمكن القول أن هذه الإلتزامات سواء كانت عامة أو خاصة بمقدمي خدمات الإنترنت تعتبر بمثابة تدابير وقائية للكشف عن جرائم نظام المعالجة الآلية للمعطيات قبل وقوعها، وآلية فعالة للحد من التجاوزات الناجمة عن مخالفة النظام العام والآداب العامة.

## المبحث الثاني: التدابير الإجرائية للبحث والتحري في الكشف عن جرائم نظام المعالجة الآلية للمعطيات

تبنى المشرع الجزائري في القانون 09-04 السالف الذكر، تدابير إجرائية جديدة مكملة لتلك الإجراءات المنصوص عليها في قانون الإجراءات الجزائية بموجب التعديلين رقما 14-04 المؤرخ في 10 نوفمبر 2004 (تمديد الإختصاص القضائي) و 06-22 المؤرخ في 20 ديسمبر 2006 (إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب)، تتلائم وخصوصية البحث والتحري في الكشف عن جرائم الإعلام والإتصال بصفة عامة وعن جرائم نظام المعالجة الآلية للمعطيات بصفة خاصة، وتتمثل في التفتيش في النظام المعلوماتي وحجز المعطيات المعلوماتية، باعتبارهما إجراءين حاسمين خلال التحقيق([1]) في هذه الجرائم، وملائمين كذلك لخصوصية الدليل الرقمي الذي يتم الحصول عليه من خلالهما، بحيث لا يكفي مجرد الإلمام بالجانب التقني لهذه الجرائم بل لا بدا من وجود تدابير إجرائية فعالة وملائمة للبحث والتحري في الكشف عن هذا النوع من الإجرام.

وهو ما يستوجب وجود نصوص إجرائية تكميلية تكون ضرورية من أجل ضمان أن يكون الحصول على هذه البيانات المعلوماتية يتم بطريقة فعالة مساوية لعملية تفتيش وضبط حاملات البيانات المادية أو دعامات المعلومات المادية([2]).

لذلك سنقوم بدراسة هذه التدابير المستحدثة للكشف عن جرائم نظام المعالجة الآلية للمعطيات، من خلال التطرق إلى التدابير الإجرائية المتعلقة بالتفتيش في النظام المعلوماتي في المطلب الأول، والتدابير الإجرائية المتعلقة بحجز المعطيات المعلوماتية في المطلب الثاني.

---

[1]- حددت إتفاقية بودابست أفضل الطرق الواجب إتباعها في التحقيق في جرائم الأنترنت والتي تعهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها، أنظر: جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، دار البداية، الأردن، الطبعة الأولى، سنة 2007، ص228.

[2]- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 231.

**المطلب الأول: التدابير الإجرائية المتعلقة بالتفتيش في النظام المعلوماتي**

إن التفتيش في نظام المعالجة الآلية للمعطيات يكتسي طابعا خاصا لكونه مرتبط بمسرح جريمة إفتراضي قد يمتد فيه التفتيش إلى عدة أنظمة أو شبكات، وهو ما يستدعي إتخاذ تدابير إحتياطية والإستعانة ببرامج تقنية وإتباع أساليب مستحدثة للبحث والتحري للكشف عن هذا النوع من الجرائم.

ولم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفنيش بقدر ما إعتبره إجراء من إجراءات التحقيق وأحاطته بضوابط صارمة نظرا لأهميته في كشف الأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم، ومما يؤكد ذلك إهتمام الدستور الجزائري بهذه النقطة إذ نص في المادة 48 منه على أنه" ...لا تفتيش إلا بمقتضى القانون، وفي إطار إحترامه.

ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"([1]).

ويعرف التفتيش في قانون الإجراءات بأنه بحث في مستودع السر عن أشياء تفيد في الكشف عن الجريمة المرتكبة ونسبتها إلى المتهم([2])، أما على الصعيد الفقهي فيعرف بأنه إجراء من إجراءات التحقيق الإبتدائي يقصد من ورائه الإطلاع على محل له حرمة خاصة للبحث عما يفيد التحقيق([3])، ولا يعد من إجراءات الإستدلال وهو ما أجمع عليه الفقه سواء في مصر أو فرنسا([4])، وبالتالي فإنه لا يجوز لسلطة التحقيق مباشرته أو الأذن به إلا بمناسبة جريمة وقعت بالفعل وقامت دلائل كافية على إتهام شخص معين بارتكابها([5]).

وإذا كان التفتيش المتعارف عليه في قانون الإجراءات الجزائية يتعلق بنوعين من التفتيش وهما تفتيش المساكن وتفتيش الأشخاص، فأن التفتيش المنصب على النظام

---

1- المادة 48 من المرسوم الرئاسي رقم 20-442.

2- هشام محمد فريد رستم، مرجع سابق ، ص 63.

3- عمار تركي السعدون الحسيني، الحماية الجنائية للحرية الشخصية في مواجهة السلطة العامة، منشورات الحلبي الحقوقية، بيروت-لبنان، ط الأولى، سنة 2012، ص 278.

4- محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الأسكندرية، ط الأولى، سنة 2014، ص 736.

5- عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والأنترنت، دار الكتب القانونية، مصر، سنة 2007، ب ط، ص 355.

المعالج آليا يختلف عنهما كلية سواء من حيث الشروط الموضوعية أو الشكلية وكذا موضوع ومحل التفتيش، بحيث أنه لا يشكل أي عائق عندما يستهدف المكونات المادية للنظام، إذ أنه من السهولة بمكان ضبط الأجهزة وحجزها أو إتلافها، وإنما يقوم الإشكال عندما ينصب التفتيش على مكونات النظام المعنوية أو المنطقية والمتمثلة في البرامج والمعطيات.

ونص المشرع الجزائري على القواعد الإجرائية لتفتيش النظام المعلوماتي في المادة 5 من القانون 09-04، بقولها" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى:

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

ب- منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك..."([1]).

والملاحظ أن المشرع الجزائري أشار من خلال هذه المادة إلى الكيفيات التي يتم بها إجراء التفيتش ولو عن بعد، وكذا إمكانية تمديد التفتيش في النظام المعلوماتي.

وهو ما سنقوم بدراسته من خلال التطرق إلى إجراءات التفتيش في النظام المعلوماتي في الفرع الأول، وتمديد التفتيش في النظام المعلوماتي في الفرع الثاني.

1- المادة 5 من القانون 09-04.

**الفرع الأول: إجراءات التفتيش في النظام المعلوماتي**

نصت إتفاقية بودابست في الفقرة الأولى من المادة 19 منها المتعلقة بتفتيش وضبط البيانات المعلوماتية المخزنة على أنه"

1- يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بطريقة مشابهة:

أ- لنظام معلوماتي أو لجزء وكذلك للبيانات المعلوماتية المخزنة فيه، وعلى أرضه.

ب- لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية.

وتلزم الفقرة الأولى من هذه المادة الأطراف بتخويل سلطاتها المكلفة بمكافحة الإجرام صلاحيات التفتيش والولوج للبيانات المعلوماتية التي تم إحتوائها سواء في داخل نظام معلوماتي، أو في جزء منه على دعامة تخزين مستقلة، أي القيام بتفتيش نظام معلوماتي ومكوناته المتصلة به، ويمكن إعتبارها كأنها تكون معا نظاما معلوماتيا منفصلا، كما في حالة على سبيل المثال: حاسب محمول، والطابعة وأجهزة التخزين المتصلة أو شبكة محلية، وفي بعض الأحيان قد تكون البيانات مخزنة ماديا في نظام آخر أو في جهاز تخزين آخر، لكن يمكن الوصول إليها بطريقة قانونية من خلال النظام المعلوماتي الذي يتم تفتيشه، وذلك بعمل إتصال مع النظم المعلوماتية المنفصلة الأخرى.

وإن عملية تفتيش وضبط دعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية وفقا لما هو منصوص عليه في الفقرة الأولى بند "ب" من هذه المادة، والتي يمكن إجراؤها بالإستفادة من سلطات التفتيش التقليدية، بحيث أن تطبيق إجراءات التفتيش المعلوماتي يستلزم غالبا ليس فقط تفتيش النظام، بل أيضا كل دعامة تخزين مشتركة كالأقراص التي تكون مجاورة مباشرة لهذا النظام المعلوماتي، ولذلك وبسبب العلاقة بين الإثنيين فإن الفقرة الأولى تقرر تأهيل سلطة كلية تغطي الموقفين([1]).

[1]- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص ص 225-234.

كما أنه في حالات محددة بمقتضى قوانين خاصة، يخول المقنن في بعض الدول، القائم بالتفتيش والضبط صلاحية إستخدام نظام الحاسب الذي يجري تفتيشه أو غيره مما يوجد بالمكان نفسه، في الإطلاع على البيانات التي يحويها أو يتيح الإطلاع عليها، وكذلك إستخراج ما قد يلزم منها في صورة مطبوعة أو مفهومة...ومن قبيل ذلك ما جاء بقانون المنافسة الكندي بخصوص تفتيش وضبط السجلات وغيرها مما يمكن أن يشكل دليلا على إنتهاك أحكامه([1]).

ولكن ماذا لو كان النظام المعلوماتي مزودا بنظام حماية يمنع من ولوجه دون تدخل القائم على النظام ومساعدته؟ فهل يجوز في هذه الحالة أجبار المتهم مثلا على تزويد السلطات المختصة بالتحقيق بمفاتيح المرور إلى النظام المعلوماتي؟

تباينت الآراء بصدد هذه المسألة بين من يرفض إجبار المتهم وبين من يرى عكس ذلك إلا أنه لا يكون على إطلاقه، بحيث يجوز إجبار غير المتهم على تقديم المعلومة التي من شأنها تسهيل الدخول إلى النظام كمقدم الخدمة مثلا، وذلك بحمله على الإفصاح عن كلمة السر التي بحوزته للوصول إلى المصدر أو شبكة الإتصالات، لأن الإكراه الواقع على غير المتهم لا يمس حقوق الدفاع خلافا للوضع بالنسبة للمتهم([2]).

وفي هذا الصدد صرحت الإتفاقية الأروبية في شأن جرائم تقنية المعلومات بحق الدول الأعضاء في تفتيش النظم في إطار الإجراءات الجزائية وذلك من خلال الفقرة الأولى من المادة 19 من القسم الرابع حيث نصت على" إن لكل طرف من حقها أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش أو الدخول إلى:

- نظام الكومبيوتر أو جزء منه أو المعلومات المخزنة فيه.
- الوسائط التي يتم تخزين معلومات الكومبيوتر بها ما دامت مخزنة في إقليمها([3]).

---

[1]- هشام محمد فريد رستم، مرجع سابق، ص 79.

[2]- موسى مسعود أرحومة، بحث بعنوان الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس خلال الفترة 28- 29 أكتوبر 2009، ص 8،9.

[3]- بوكر رشيدة، مرجع سابق، ص 399.

أما الإتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد نصت على إجراءات التفتيش في المادة 26 في النقطة الأولى منها بقولها" 1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:
أ) تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.
ب) بئة أو وسيط تخزين معلمات تقنية معلومات والتي قد تكون معلومات التقنية مخزنة فيه أو عليه"([1]).

وإلى جانب ذلك نجد كذلك المشرع الفرنسي الذي قام بتعديل بعض نصوصه، بحيث أضاف عبارة المعطيات المعلوماتية في المادة 94 من قانون الإجراءات الجزائية وذلك بموجب المادة 42 من القانون رقم (545-2004) المؤرخ في 21 جوان 2004، المتعلق بالثقة في الإقتصاد الرقمي لتصبح المادة على النحو التالي" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة"([2])، كما أقر ضوابط خاصة لتفتيش وضبط نظم الحاسب الآلي من حيث السلطة المختصة للقيام بهذا الإجراء نظرا لطبيعة النشاط الذي تقوم به وخصوصية المكان الذي توجد به هذه النظم مثل مكاتب المحامين وعيادات الأطباء ودور النشر ومؤسسات الإتصال السمعي بصري([3]).

وفي نفس السياق نصت المادة 12 من قانون جرام أنظمة المعلومات الأردني رقم 30 لسنة 2010 على أن" أ- مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية يجوز لموظفي الضبطية العدلية بعد الحصول على أذن من المدعي العام المختص أو من المحكمة المختصة الدخول إلى أي مكان تشير إليه الدلائل الى إستخدمه لإرتكاب أي من تلك الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج

---

1- المادة 26 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

2- Art 94 : Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité, modifiè par LOI N° 2004-575 du 21 juin 2004-art.42() JORF 22juin 2004.

3- هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، مرجع سابق، ص 179.

والأنظمة والوسائل التي تشير الدلائل في إستخدامها لإرتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذاك ويقدمه إلى المدعي العام المختص"، وكذلك نصت المادة 14 من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية على أن" للنيابة العامة أو من تندبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة، يجب أن يكون أمر التفتيش مسببا ومحددا، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة فإذا أسفر التفتيش عن ضبط أجهزة وأدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لإتخاذ ما يلزم بشأنها"([1]).

كما نصت المادة 6 من القانون المصري 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات أن" لجهة التحقيق المختصة بحسب الأحوال أن تصدر أمرا مسببا لمأموري الضبط القضائي المختصين، لمدة لا تزيد عن ثلاثين يوما قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على إرتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يأتي:...

2- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط"([2])، بالإضافة إلى نص المادة 33 من قرار للسلطة الفلسطينية بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية على أنه" للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيات المعلومات ذات الصلة بالجريمة"([3]).

أما بالنسبة للمشرع الجزائري فقد أجاز تفتيش النظام المعلوماتي عن بعد، بموجب المادة 5 الفقرة الأولى من القانون 09-04، المشار لها أعلاه، التي تجيز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في الحالات التي يسمح فيها باللجوء إلى المراقبة الإلكترونية الدخول بغرض التفتيش ولو عن بعد إلى

---

[1]- القانون القطري رقم (14) لسنة 2014 المؤرخ في 2014/09/15، المتعلق بإصدار قانون مكافحة الجرائم الإلكترونية، الجريدة الرسمية القطرية، المؤرخة في 2014/10/02، العدد 15، ص 18،17.

[2]- المادة 6 من القانون المصري 175 لسنة 2018.

[3]- المادة 3 من القرار الفلسطيني بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية.

منظومة معلوماتية(نظام معلوماتي) أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها أو إلى منظومة تخزين معلوماتية.

ويلاحظ أن المشرع الجزائري من خلال هذه المادة قد فصل في العديد من الإشكاليات الإجرائية بإضافته محلين للتفتيش وهما:

- المنظومة المعلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية([1]).

ولم يعرف المشرع الجزائري مفهوم التفتيش عن بعد، وقدم في هذه الحالة إمكانية تفتيش المنظومة المعلوماتية عن بعد على سبيل التفتيش الوقائي أو التفتيش الإفتراضي، وهو يختلف عن مراقبة الإتصالات الإلكترونية من حيث التقنية، فالمراقبة تعني إعتراض المراسلات(Email-SMS) وكشف محتواها بدون الدخول إلى النظام المعلوماتي للجهاز الذي يتم مراقبته، أما التفتيش عن بعد فهو يتم عن طريق برنامج تجسس (حصان طراوادة) يسمح بالولوج للنظام المعلوماتي([2]).

وهذا إجراء جديد، بحيث يمكن الدخول إلى النظام المعلوماتي بدون إذن صاحبه بالدخول في الكيان المنطقي للحاسوب للتفتيش عن أدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس([3]).

وإن التفتيش هنا وخلافا للتفتيش التقليدي عن الأدلة التي تثبت وقوع الجريمة ونسبتها إلى المتهم إنما هي حالة إجراء تفتيش وقائي قد تسفر عنه أدلة يمكن أن تكون إثبات لتخطيط مسبق يراد به إرتكاب جرائم ذات خطورة على الأمن الداخلي للدولة([4]).

كما إن سبب التفتيش في الحالات التقليدية بوصفه إجراء من إجراءات التحقيق هو وقوع جناية أو جنحة وإتهام شخص أو أشخاص معينين بإرتكابها أو المشاركة

---

[1]- ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيات المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان-الجزائر، سنة 2018، ص 107.

[2]- مسعود مريم، مرجع سابق، ص 91،92.

[3]- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية ، جامعة الجزائر1، الموسم الجامعي 2011،2012، ص 132،133.

[4]- مسعود مريم، مرجع سابق، ص 89.

فيها، وتوافر أمارات قوية وقرائن على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو غيره([1]).

وإن هذه القواعد لا يمكن أن تكون سببا لتفتيش النظم المعلوماتية لأنه طبقا لنص المادة 5 الفقرة 1 من القانون 09-04، أجازت التفتيش بقصد الوقاية من جرائم حددها المشرع لم ترتكب ولكن تعد أسلوبا وقائيا فقط، وهو ما يعد إعتداء فعلي على الحياة الخاصة للأشخاص لكون القانون لم يحدد صفات من يقع عليهم التفتيش، هل هم مجرمون سابقون أم أشخاص لهم علاقة بمجرمين إرتكبوا هذه الأفعال، وهو الأمر الذي أسال الكثير من الحبر خاصة في بعض الدول الأروبية كالمانيا وسويسرا مثلا، التي منعت اللجوء إلى أسلوب التفتيش الوقائي، لأنه يعد إعتداء فعليا على الحياة الخاصة للأفراد التي كفلها الدستور ولا يمكن اللجوء إليه إلا في حالة الوقوع الفعلي للجريمة([2]).

ولم ينص المشرع الجزائري في المادة 5 من القانون 09-04، صراحة على وجوب إستصدار إذن بتفتيش نظم معلوماتية من طرف ضابط الشرطة القضائية في حالة التحريات المتعلقة بالجرائم المتلبس بها أو في حالات التحريات الأولية كما هو الحال بالنسبة لمراقبة الإتصالات الإلكترونية، ولكن يستشف ذلك من خلال مضمون هذه المادة التي نصت على أنه" يجوز للسلطات القضائية وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية..." أي بتطبيق نفس الأحكام المتعلقة بالتفتيش المنصوص عليها في قانون الإجراءات الجزائية على التفتيش في الأنظمة المعلوماتية.

ويجب أن يتصف الأذن الصادر عن النيابة العامة بالمرونة من حيث إتاحة مساحة واسعة لمأموري الضبط في تنفيذ الأذن بالتفتيش ولكن بضوابط معينة بحيث

---

[1]- هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، مرجع سابق، ص 104.

[2]- مسعود مريم، مرجع سابق، ص 89.

لا يؤدي ذلك إلى البعد عن الهدف المقصود من صدور الأذن، وذلك عن طريق تحديد مجال التفتيش وما يستتبعه بالضرورة من تتبع في شبكات المعلومات([1]).

**الفرع الثاني: تمديد التفتيش في النظم المعلوماتية**

نصت المادة 19 المتعلقة بتفتيش وضبط البيانات المعلوماتية المخزنة في فقرتها الثانية من إتفاقية بودابست على أنه"

2- يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل التأكد مما إذا كانت سلطاته تقوم بالتفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي معين أو جزء منه وفقا للفقرة "1" بند "أ" وأنها تملك أسبابا تدعو للإعتقاد بأن البيانات التي تسعى إليها مخزنة في نظام معلوماتي آخر أو في جزء منه على أرضه، وأن هذه البيانات يمكن الوصول إليها بشكل قانوني سواء من خلال النظام الأولى أو من خلال كونها مهيأة من أجله، وأن هذه السلطات المذكورة ستكون قادرة على التوسع العاجل لنطاق التفتيش أو الولوج بطريقة مشابه لنظام آخر.

ويتضح أن هذه الفقرة تخول للسلطات المكلفة بالتنقيب والتحرى مكنة توسيع مشروع التفتيش أو الولوج بطريقة مشابهة ليشمل نظاما معلوماتيا آخر أو جزء منه إذا كانت هناك أسباب تدعو للإعتقاد بأن البيانات المطلوبة مخزنة في هذا النظام المعلوماتي أو في أجزاء منه، وفي كل الحالات يجب أن يكون هذا النظام المعلوماتي الآخر أو لذلك الجزء المتصل به يقع على أرضه.

كما أن هذه الأتفاقية لا تقرر نماذج معينة للإذن بالتفتيش ولا لكيفية تطبيق عملية توسيع نطاق التفتيش، وتعهد بذلك للقانون الداخلي لكل دولة لتحديده، والتي يجب عليها أن تراعي كذلك سهولة الدخول إلى هذه البيانات بطريقة قانونية([2]).

لذا فأنه بالنظر للطبيعة الخاصة لتفتيش أنظمة الكومبيوتر وتواجد بعضها في مكان والبعض الآخر في مكان مختلف وهي مرتبطة فيما بينها بشبكة وتنتمي إلى

---

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الأسكندرية، ط الأولى، سنة 2009، ص 232.

[2]- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص ص 227-236.

شركة واحدة أو شخص واحد فإن بعض القوانين المقارنة -كما في ألمانيا والنمسا وفلندا والنرويج- سمحت بامتداد التفتيش إلى هذه الأجهزة المرتبطة لمعرفة ما يفيد في كشف الحقيقة([1]).

وفي هذا الصدد سمحت الإتفاقية الأروبية لجرائم تقنية المعلومات لسنة 2001 للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به في حالة الإستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في الجهاز من خلال الجهاز محل التفتيش، فتنص الفقرة الثانية من المادة 19 من القسم الرابع على أنه" من حق السلطة القائمة بتفتيش الكومبيوتر المتواجد في دائرة إختصاصها أن تقوم في حالة الإستعجال بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الكومبيوتر الأصلي محل التفتيش([2]).

أما بالنسبة للإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، فقد نصت في النقطة الثانية من المادة 26 منها على أن" تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1-أ) إذا كان هناك إعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى"([3]).

وإلى جانب ذلك نجد المشرع الفرنسي قد حسم هذه المسألة أيضا وذلك بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانو (239-2003) بشأن الأمن الداخلي الصادر في 18 مارس 2003، حيث أضاف المادة (57-1) من قانون الإجراءات الجزائية وذلك بموجب المادة (17-1) والتي نصت على أنه" يجوز لضباط الشرطة القضائية أو تحت مسؤوليتهم أعوان الشرطة القضائية وفي إطار التفتيش المنصوص

---

1- شيماء عبدالغني محمد عطاالله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، مصر، سنة 2007، ص 298.

2- بوكر رشيدة، مرجع سابق، ص 402،403.

3- المادة 26 النقطة الثانية من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

عليه الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على المعطيات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر بما أن المعطيات يتم الدخول إليها أو تكون متاحة إنطلاقا من النظام الرئيسي"([1]).

وفي هذا السياق نصت كذلك المادة 88 من قانون الإجراءات البلجيكي لعام 2000 على أنه" إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي ويتم هذا الإمتداد وفقا لضابطين:

(أ) إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث.

(ب) إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظرا لسهولة عملية محو إو إتلاف أو نقل البيانات محل البحث"([2]).

والشيء نفسه بالنسبة لقانون الجرائم المعلوماتية الإسترالي لعام 2001 الذي سمح بعمليات التفتيش على وجه السرعة للبيانات خارج المواقع التي تم إختراقها عن بعد بواسطة الحواسيب الجاري تفتيشها، وذلك دون إشتراط الحصول على موافقة مسبقة من السلطات المختصة([3]).

كما نصت المادة 15 في فقرتها الثانية من القانون البحريني رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات([4]) على أنه"

2- إذا قامت لدى النيابة العامة أثناء تنفيذ الأمر المشار إليه في البند (أ) من الفقرة (1) من هذه المادة أمارت قوية بأن البيانات المتصلة بالجريمة مخزنة في نظام تقنية

---

[1] - Article 57-1 :les officiers de police judiciaire ou, sous leur responsabilitè, les agents de police judiciaire peuvent, au cours d'une perquisition effecuèe dans les conditions prèvues par le prèsent code, accèder par un système informatique implantè sur les lieux où se dèroule la perquisition à des donnèes intèressant l' enquête en cours et stockèes dans ledit système ou dans un autre système informatique, dès lors que ces donnèes sont accessibles à partir du système initial ou disponibles pour le système initial…, Code de procèdure pènale, modifiè par LOI N° 2016-731 du 3 juin 2016-art.58.

[2]- MEUNIER.C : ia loi du 28 novembre 2000 relative à la Criminalitè informatique, formation Permanent CUP, fevrier 2001, no 103.

[3]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 683.

[4]- القانون البحريني رقم (60) لسنة 2014، بشأن جرائم تقنية المعلومات، الجريدة الرسمية البحرينية، المؤرخة في 9 أكتوبر 2014، العدد 3178، ص11.

المعلومات آخر أو في جزء منه، وكانت هذه البيانات قابلة لأن يتم الدخول إليها من خلال نظام تقنية المعلومات الأول أو متاحة من خلاله على نحو مشروع، فإن للنيابة العامة أن تصدر أمرا مسببا بمد الدخول والتفتيش إلى النظام الآخر"([1]).

أما بالنسبة للمشرع الجزائري فقد أجاز تمديد التفتيش في النظام المعلوماتي فنص على ذلك في الفقرة الثانية من المادة 5 من نفس القانون بقولها" في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك".

ويتضح أن الولوج إلى منظومة المعلومات تتم هنا بمجرد الشك أو الإعتقاد بتواجد المعلومات محل البحث داخل هذه المنظومة أو تلك، ولكن لكي تكتسي هذه الإجراءات طابعها الرسمي وتقع تحت طائلة القانون، أوجب المشرع أن يكون الدخول إلى النظام المعلوماتي المقصود قانونيا ويندرج دون شك في إطار حماية الحياة الخاصة التي تفرض في كل مرة ضرورة إبلاغ الجهات القضائية المختصة مسبقا([2]).

وإن إمتداد نطاق التفتيش إلى نظام غير النظام محل الإشتباه يعتبر محل تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش([3])، لا سيما وإن هذه القواعد المقررة في نطاق التفتيش تناقض القواعد المقررة قانونا في جعل ضمانات المتهم المعلوماتي وضمانات إحترام حقوق الإنسان والحريات الفردية وفي مقدمتها الخصوصية، فمثل هذه الإجراءات قد تؤدي إلى كشف بيانات شخصية أو كشف أسرار العمل أو الوصول إلى ملفات يحرص أصحابها على سريتها أو يتيح لهم

---

1- المادة 15 الفقرة 2 من القانون البحريني رقم (60) لسنة 2014.

2- زبيحة زيدان، مرجع سابق، ص 140 .

3- عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية-دراسة مقارنة، مذكرة لنيل درجة الماجستير في القانون العام، جامعة الشرق الأوسط، سنة 2014، ص 81.

القانون ذلك، وتعدو المسألة أكثر خطورة عندما يمتد التفتيش إلى نظم مرتبطة بالنظام موضوع الإشتباه، فتطال ملفات وبيانات جهات لا علاقة لها بالجريمة قد تكون خاصعة لسرية مهنية أو قواعد حماية سرية بيانات العملاء كما في نظم الكومبيوتر الخاصة بمزودي الخدمات أو نظم كمبيوترات البنوك أو الجهات الصحية أو أعمال المحاماة أو غيرها([1]).

كما أن لإمتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي أهمية في إمكانية الحصول على دليل عن بعد وفي بضع ثوان، إلا أن بعض الفقه يتحفظ على القيام بذلك لأنه يعتبر أنتهاكا لسيادة الدولة الأجنبية، لذا فانه إذا ما إقتضت ضرورة التحقيق القيام بذلك فينبغي مراعاة العديد من الضمانات يكون متفقا عليها سلفا عن طريق إتفاقيات ومعاهدات في هذا المجال([2]).

وهو ماجعل المشرع الجزائري يقوم بحصر إمكانية تمديد التفتيش عن بعد في الشبكة في الحالة "أ" من المادة 4 من القانون 09-04، للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

وفي هذه الحالة يختص النائب العام لدى مجلس قضاء الجزائر بمنح الإذن لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال أثناء ممارستهم لوظيفتهم أو بمناسبتها طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول لا سيما في قانون الإجراءات الجزائية تفتيش أي مكان أو هيكل أوجهاز بلغ إلى علمها أنه يحوز و/أو يستعمل وسائل أو تجهيزات موجهة لمراقبة الإتصالات الإلكترونية([3])، على أن تكون مدته ستة (6) أشهر قابلة للتجديد.

---

[1]- عبدالفتاح مراد، شرح جرائم الكومبيوتر والأنترنت، شركة البهاء للبرمجيات والكومبيوتر والنشر الإلكتروني، الأسكندرية، ب ط، ص 499.

[2]-- ليندا بن طالب، مقال بعنوان التفتيش في الجريمة المعلوماتية، مجلة الحقوق والعلوم السياسية، جامعة الوادي، المجلد 8، العدد 2، جوان 2017، ص 491.

[3]- شرف الدين وردة، بلجراف سامية، مقال بعنوان الجوانب الموضوعية والإجرائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية، جامعة فارس يحي المدية، المجلد 1، العدد 3، ديسمبر 2017، ص 50.

ويتم ذلك بناء على تقرير يتضمن ويبين طبيعة الترتيبات التقنية الحصرية المشار إليها في الفقرة الإخيرة من المادة 4 من القانون 09-04، حتى لا يتم إستعمال تلك التقنيات في مجالات غير مسموح بها أو من شأنها المساس بحرمة الحياة الخاصة للأفراد أو الجماعات، أما فيما عدا هذه الحالة المنحصرة في الفقرة "أ" من هذه المادة فيتعين الرجوع إلى التدابير التي رسمها قانون الإجراءات الجزائية في مجال التحري والتفتيش بالنسبة للجرائم الإلكترونية بمنح الإذن بالتفتيش من وكيل الجمهورية وقاضي التحقيق([1]).

كما أنه في حالة وجود معطيات مبحوث عنها يمكن الدخول إليها إنطلاقا من المنظومة الأولى ولكن مخزنة في منظومة معلوماتية تقع خارج الأقليم الوطني فإن الحصول عليها بناءا على أحكام الفقرة 3 من المادة 5 من هذا القانون يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، وضمن هذا الإطار نصت المادة 32 من الإتفاقية الأروبية بشأن الجرائم المعلوماتية التي أعدها المجلس الأروبي وتم التوقيع عليها في بودابست في 2001/11/23 على إمكانية الدخول بغرض التفتيش والضبط في أجهزة وشبكات تابعة لدول أخرى بدون إذنها في حالتين:

الأولى: إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور.

الثانية: إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش([2]).

إضافة الى ذلك أنه يمكن للسلطات المكلفة بالتفتيش حسب نفس المادة المشار إليها آنفا في فقرتها الأخيرة تسخير كل شخص له دراية بعمل النظام المعلوماتي محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

وهذا الإجراء يساهم في تسهيل عملية التفتيش عن طريق اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المتخصصين في الإعلام الآلي وفن الحاسبات لإجراء

---

[1]- زبيحة زيدان، مرجع سابق، ص 141،142.

[2]- علي عدنان الفيل، مرجع سابق، ص 47.

عمليات التفتيش على النظام المعلوماتي وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات([1]).

**المطلب الثاني: التدابير الإجرائية المتعلقة بحجز المعطيات المعلوماتية**

يعتبر الضبط الأثر المباشر للتفتيش([2])، وحتى يحقق التفتيش غايته في جمع الأدلة لا بدا من وسيلة إلتقاط تلك الأدلة، وهذه الوسيلة هي الضبط([3])، بحيث تكون الغاية من التفتيش هو حجز أي شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها، سواء أكان هذا الشيء أدوات أستعملت في إرتكاب الجريمة أو شيئا نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة([4])، وبالتالي ينبغي القيام بضبط ما يترتب عليه التفتيش وتحريزه بطريقة علمية حتى لا يفقد قيمته القانونية حال تفقده أمام القضاء إذا تطلب الأمر ذلك([5]).

و يعرف الضبط بأنه العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والتحفظ على هذه الأدلة، فالضبط هو الغاية من التفتيش ونتيجته المباشرة المستهدفة ولذلك يتعين عند إجرائه أن تتوافر فيه نفس القواعد التي تطبق بشأن التفتيش([6]).

ويترتب على هذا الأرتباط بين التفتيش والضبط أن الضبط لا يجوز أن يقع على شيء إلا وصفه دليلا من أدلة الجريمة التي يجري التفتيش بشأنها، ولذلك فأنه يباشر من أجل الحقيقة المطلقة، بمعنى أنه ما دام التفتيش يستهدف ذات الحقيقة فيتعين أن يباشر ضبط ما يتعلق بها من أدلة سواء كانت للإدانة أم للبراءة، لأن ما

---

[1]- طرشي نورة، مرجع سابق، ص 133.

[2]-المعيني، سرحان حسن، مقال بعنوان التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، مركز بحوث الشرطة- القيادة العامة لشرطة الشارقة، الإمارات، المجلد 20، العدد 79، أكتوبر 2011، ص 46

[3]-صالح شنين، مقال بعنوان إجراءات التحري والتحقيق في جرائم تكنولوجيات الإعلام والإتصال في التشريع الجزائري(قانون 09-04)، مجلة الدراسات الحقوقية، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي سعيدة، العدد الأول، سنة 2014، ص 283.

[4]- علي عدنان الفيل، مرجع سابق، ص 54.

[5]- مروك نصر الدين، محاضرات الإثبات الجنائي، الجزء الأول( النظرية العامة للإثبات الجنائي)، دار هومة، الجزائر، سنة 2007، ص 337.

[6]-عبدالله سيف الكيتوب، الأحكام الإجرائية لجريمة الإحتيال المعلوماتي، دار النهضة العربية، القاهرة، سنة 2013، ص 142.

يضبط في الحالتين يحقق العدالة الجنائية([1])، لذلك يقول فوستان هيلي:" أنه لما كان التفتيش يباشر للكشف عن الحقيقة، سواء كانت في إدانة المتهم أو براءته، فإنه ينبغي ألا يقتصر الضبط على الأشياء التي تؤدي الى إدانة المتهم دون غيرها، بل إنه يتعين أن ينصب على الأشياء التي تفيد الحقيقة أيا كانت وأن أدت الى تبرئة المتهم"([2]).

ونظرا لكون محل الحجز في جرائم نظام المعالجة الآلية للمعطيات هو البيانات المعالجة إلكترونيا (المعطيات المعلوماتية)، فقد ثآر التساؤل حول قابلية حجز هذا النوع من البيانات.

وهذا الخلاف دعا المشرع الجنائي في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط ليشمل فضلا عن الأشياء المادية المحسوسة البيانات المعالجة إلكترونيا أو إصدار تشريعات تتعلق بجرائم الحاسبة الإلكترونية تتضمن القواعد الإجرائية المناسبة لهذه الصورة من البيانات، وهو ما نصت عليه المادة 39 من قانون تحقيق الجنايات البلجيكي، المدخلة في التقنيين بمقتضى القانون الصادر في 2001/11/23، حيث يشمل الحجز وفقا لهذا النص على الأشياء المادية وعلى البيانات المعالجة إلكترونيا([3]).

إضافة إلى ذلك نجد المادة 251 من قانون الإجراءات الجنائي اليوناني تعطي سلطات التحقيق إمكانية القيام (بأي شيء يكون ضروريا لجمع وحماية الدليل)، ويفسر الفقه اليوناني عبارة "أي شيء" بأنها تشمل بالضبط البيانات المخزنة أو المعالجة إلكترونيا، ومن تم فإن ضبط البيانات المخزنة في الذاكرة الداخلية لحاسب الآلي لا تشكل أي مشكلة في اليونان، إذ بمقدور المحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية([4])، وكذلك

---

[1]- مسعود مريم، مرجع سابق، ص 94.

[2]- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة للطباعة والنشر والتوزيع، ط الأولى، سنة 2009، ص 209.

[3]- علي عدنان الفيل، مرجع سابق، ص 58.

[4]- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، الأسكندرية، سنة 2009، ص 234.

فإن المادة 487 من القانون الكندي تمنح سلطة إصدار إذن بالضبط -لأي شيء- طالما توافرت أسس معقولة للإعتقاد بأن الجريمة المعلوماتية التي أرتكبت أو يشتبه في ارتكابها أو أن هناك نية في إرتكاب الجريمة بواسطته أو أنه سوف ينتج دليلا على وقوع الجريمة([1]).

في حين إعتبر المشرع الألماني في المادة 94 من قانون الإجراءات الجنائية أن البيانات المعالجة إلكترونيا لا يسوغ ضبطها إلا بعد تحويلها إلى كيان مادي كطباعتها على الأوراق أو بتصوير الشاشة أو نقلها على حافظة بيانات أو على دعامات مادية أخرى([2])، بينما في هولندا إتجه قانون الإجراءات إلى تقليص المجال النظري للضبط الذي يمكن أن يقع على نظام معلوماتي بأكمله عن طريق فرض واجب بالتعاون الإلزامي على مشغلي نظم المعلومات([3]).

وإن طريقة ضبط المعلومات المعالجة آليا تختلف عما هي عليه عند ضبط المكونات المحسوسة كالأقراص المرنة والمودم والخادم...ونتيجة لذلك يفضل البعض فضلا عن المصطلح التقليدي "الضبط" إستخدام مصطلح الحصول بطريقة مشابهة، وذلك من أجل الأخذ في الإعتبار الطرق الأخرى لرفع المعنويات غير المادية، وهو ما يظهر جليا من الفقرة 3 من المادة 19 من الإتفاقية الأروبية لجرائم تقنية المعلومات([4]).

أما المشرع الجزائري فكان قد أضفى بداية، حماية قانونية لقواعد البيانات بموجب المادة 5 الفقرة 2 من الأمر 03-05 المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، والتي إعتبرت قواعد البيانات من المصنفات المحمية سواء كانت مستنسخة على دعامة قابلة للإستغلال بواسطة آلة

---

[1]-خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، سنة 2011، ص 161،162، أنظر أيضا: عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والأنترنت، مرجع سابق، ص 149.

[2]- مقتبس عن: زبيحة زيدان، مرجع سابق، ص 149، أنظر أيضا: المعمري، عادل عبد الله خميس، مقال بعنوان التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مركز بحوث الشرطة- القيادة العامة لشرطة الشارقة، الإمارات، المجلد 22، العدد 86، يوليو 2013، ص 268.

[3]-هشام محمد فريد رستم، مرجع سابق، ص 100.

[4]- بوكر رشيدة، مرجع سابق، ص 421.

أو بأي شكل من الأشكال الأخرى، ثم قام بسن التدابير الإجرائية الخاصة بحجز المعطيات المعلوماتية في الفصل الثالث من القانون 09-04، السالف الذكر، بموجب المواد 6،7،8،9.

وإعتمد طريقتين في حجز هذه المعطيات المعلوماتية التي تستدعي المعرفة التقنية الدقيقة والإلمام بالمبادئ القانونية الضروية([1])، بحيث تتمثل الطريقة الأولى في الحجز عن طريق نسخ المعطيات المعلوماتية التي تفيد في الكشف عن الجرائم وعن مرتكبيها، لتقدم كأدلة إقناع، وهذا دون الحاجة إلى حجز كل النظام المعلوماتي الذي يحتوي على هذه المعطيات، أما الطريقة الثانية فتتمثل في الحجز عن طريق منع الوصول إليها وهذا تفاديا لإتلافها أو تغييرها([2])، لذلك سنقوم بدراسة الطريقة الأولى في الفرع الأول بينما نعالج الطريقة الثانية في الفرع الثاني.

**الفرع الأول: الحجز عن طريق نسخ المعطيات المعلوماتية**

إن المعطيات الرقمية المعلوماتية المجمعة يمكن نسخها على:"جميع دعائم التخزين" وهذا الذي يناسب تسمية الحجز المعلوماتي الذي هو غير متعارض مع الضبط المادي التقليدي لدعائم التخزين المعلوماتية المستخرجة من نفس مكان التفتيش، أي بدل حجز القطع الصلبة التي تتضمن المواد الممنوعة، فالنسخ يعد أحد أساليب الضبط المستخدمة في حالة عدم وجود إمكانية لضبط القطع الصلبة المتضمنة للمواد غير المشروعة([3])، ويمكن عن طريقه الإستيلاء على كافة أنواع المعطيات، والتي تشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها([4])، فيتم مثلا نسخ المواد التي تحتاج الى فك شفرتها لكي يتم التعرف على محتوياتها أو نسخ

---

[1]- ناني لحسن، مرجع سابق، ص 113.

[2]- درياد مليكة، مقال بعنوان المساس بأنظمة المعالجة الآلية للمعطيات، حوليات جامعة الجزائر 1، الجزء الأول، العدد 33، ، مارس 2019، ص 251.

[3]- محمد عبدالله إبراهيم، المواجهة الأمنية لجرائم شبكات المعلومات الدولية، مطابع الشرطة للطباعة والنشر والتوزيع، سنة 2016، ص 168.

[4]- سعيدي سليمة، أمن المعلومات وأنظمتها في العصر الرقمي، دار الفكر الجامعي، الأسكندرية، ط الأولى، سنة 2018، ص 76.

البيانات التي يتم وضعها في إطار برمجية تحوي قنبلة زمنية موقوتة"، وهنا نجد أسلوب النسخ يصلح تماما أن ينتج عنه دليل رقمي مقبول أمام القضاء"([1]).

ونصت المادة 19 المتعلقة بتفتيش وضبط البيانات المعلوماتية المخزنة في فقرتها 3 بند "ب" من إتفاقية بودابست على ما يلي:

3- يجب على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تحويل سلطاته المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين 1 و2، وهذه الإجراءات تشمل السلطات التالية:

ب- التحقق والتحفظ على نسخة من هذه البيانات المعلوماتية.

وتناقش الفقرة 3 من هذه المادة المسائل التي يتم حلها عن طريق تخويل السلطات المختصة صلاحيات الضبط أو الحصول بوسيلة مشابهة على البيانات المعلوماتية التي كونت موضوع التفتيش أو الولوج بطريقة مشابهة كالضبط عن طريق نسخ البيات المعلوماتية عملا بأحكام الفقرتين 1 و2 من نفس المادة، كما تشمل الإجراءات المقررة ضبط الأجزاء المادية للحاسب ودعامات التخزين المعلوماتية، ذلك أنه قد يحدث في بعض الحالات، عندما تكون البيانات المخزنة في نظام إستثماري خاصيته لا تسمح بالحصول على نسخة من البيانات ففي هذه الحالة لا توجد أية حلول أخرى سوى ضبط دعامة التخزين ذاتها، وهذا الحل ينبغي اللجوء إليه أيضا في حالة ما إذا كان يجب فحص الدعامة من أجل إستعادة بيانات قديمة كان قد تم الكتابة فوقها ولكنها قد تركت بعض الآثار على هذه الدعامة([2]).

أما بالنسبة للإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، فقد إعتمدت طريقة نسخ المعطيات بموجب المادة 27 في فقرتها الأولى بند "ب" ، وذلك في نطاق ضبط المعلومات المخزنة، والتي نصت على ما يلي"

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (1) من المادة السادسة والعشرين من هذه الإتفاقية.

---

[1]- مسعود مريم، مرجع سابق، ص 95.

[2]- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 228،238.

هذه الإجراءات تشمل صلاحيات:

ب) عمل نسخة من معلومات تقنية المعلومات والإحتفاظ بها"([1]).

كما نصت المادة 26 المتعلقة بالتقصي الإلكتروني والتفتيش والضبط في البند "هـ" من المرسوم التشريعي السوري رقم 17 لعام 2012 المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أنه"

هـ- على كل صاحب أو مدير أي منظومة معلوماتية ترتكب جريمة معلوماتية باستخدام منظومته أن يتيح للضابطة العدلية تفتيش وضبط البيانات والمعلومات والبرمجيات الحاسوبية والحصول على نسخة منها

ويمكن في حالات الضرورة ضبط الأجهزة والبرمجيات الحاسوبية المستخدمة أو جزء من مكوناتها" ([2]).

أما بالنسبة للمشرع الجزائري فقد أعتمد هذا الأسلوب في المادة 6 في فقرتها الأولى من القانون 04/09، السالف الذكر، بقولها:"عندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية"([3]).

ومن خلال نص هذه المادة يتضح أن المشرع الجزائري إعتمد طريقة نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية سواء بحجز النظام المعلوماتي برمته إذا كان ضروريا لمصلحة التحقيق أو القيام بحجز المعطيات المعنية بالذات وذلك بعد نسخها على دعامة مادية أو أي وعاء للبيانات كطبعها على الورق أو ضبطها على الشاشة قصد تسهيل قراءتها

---

[1]- المادة 27 الفقرة 1 البند ب من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]- المرسوم الشريعي السوري رقم 17 لعام 2012 المؤرخ في 2012/02/08، المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، مجلس الشعب السوري، ص7.

[3]- المادة 6 في فقرتها 1 من القانون 09-04.

والتعامل معها([1])، بحيث أنه في بعض الأحيان قد لا يكون بالإمكان فصل البيانات أو العناصر التي تفيد في كشف الحقيقة عن النظام الذي يحويها، بالرغم من أهمية ضبطها لإثبات الجريمة المعلوماتية الواقعة، مما يجبر معه سلطات التحقيق والإستدلال على ضبط النظام بأكمله([2])، وهذا بدوره يؤدي إلى عزل النظام المعلوماتي بالكامل عن دائرته المعلوماتية لمدة زمنية قد تطول أو تقصر، مما قد يتسبب عنه أضرار مادية فادحة بالجهة مستخدمة النظام([3]).

لذا وبغية معالجة هذه الإشكالية وإيجاد نوع من التوازن ما بين حق الدولة وضحايا الجريمة في الوصول إى الجناة ومعاقبتهم وبين حق الجهة صاحبة النظام أو الشبكة في عدم تعطيل عملها، فقد لجأ القضاء في معظم الدول الأروبية إلى تطبيق معيار أو مبدأ "التناسب" الذي يقضي بضرورة إقتصار الضبط المعلوماتي فقط على تلك البيانات والأنظمة التي تفيد في كشف الحقيقة وبما يحفظ النظام أو الشبكة المعلوماتية من التعطيل الكامل، وبناء على ذلك فقد قضت المحكمة الفيدرالية في ألمانيا، في حكم لها بهذا الصدد، بنقض وإلغاء قرار قضائي كان قد صدر بخصوص ضبط (220) قرص ليزري بالإضافة إلى الوحدة المركزية، لعدم وجود التناسب في قرار الضبط([4]).

كما إن حجز المعطيات المساعدة لفهم المعطيات المحجوزة الأساسية من شأنه إعطاء قوة إضافية للدليل المستقى منها، كما أنه يساعد جهات الحكم في فهم الأمور التقنية وبالتالي الوصول إلى حكم منصف وعادل([5]).

وقد إستعمل المشرع مصطلح "دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز" مثل القرص المرن والقرص الصلب والذاكرة الوسيطة والأشرطة المعناطيسية ...الخ، كما ترك المجال مفتوحا أمام ظهور تقنيات تخزين جديدة بناء

---

1- زبيحة زيدان، مرجع سابق، ص 150.

2- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، المكتب الجامعي الحديث ، ب ط، سنة 2013، ص 148.

3 - فتوح الشادلي، عفيفي كامل عفيفي، مرجع سابق، ص 354.

4 - رشاد خالد عمر، مرجع سابق، ص 148،149.

5- ناني لحسن، مرجع سابق، ص 123.

على التطورات التقنية المذهلة في مجال صناعة الحواسيب وملحقاتها([1])، وذلك لأنه لا يمكن أن يتم التعامل مع تلك المعطيات في شكلها الأولي المعنوي وهي عبارة عن نبضات أو ذبذبات إلكترونية أو إشارات ممنغطة، أما إذا كانت المعلومات على دعامة مادية فلا تطرح صعوبة في ضبطها أو حجزها([2]).

كما لم يحدد المشرع الجزائري محل الحجز بصفة دقيقة عكس ما قامت به جل التشريعات الحديثة، كالقانون البلجيكي لسنة 2000 الذي نص في المادة 39 مكرر على أنه" تتم سحب البيانات التي سبق أخذ نسخة منها من الجهاز في الحالات الآتية:

أ- إذا كانت محلا للجريمة أو ناتجة عنها.

ب- إذا كانت مخالفة للنظام العام أو حسن الآداب.

ج- إذا كانت تمثل خطرا علة الأنظمة الإلكترونية.

د- إذا كانت تمثل خطرا بالنسبة للمعلوومات المخزنة أو المعالجة أو المرسلة بهذه الأنظمة([3]).

وقد أجازت المادة 88 من هذا القانون لقاضي التحقيق في حالة إمتداد البحث الإلكتروني عن أدلة الجريمة خارج نطاق بلجيكا أن يحصل على نسخة من البيانات التي يحتاجها، وهذا دون الحصول على أذن تلك الدولة التي توجد في نطاق إقليمها البيانات المطلوبة، وهو ما يعد إعتداء صارخا على سيادتها([4]).

كما أن تفتيش نظم الحاسب الآلي يمكن أن يتم بعدة طرق تساهم في عملية الحجز عن طريق نسخ المعطيات المعلوماتية، فمثلا المرشد الأمريكي جاء بأربع طرق أساسية للتفتيش ممكنة التحقيق وهي:

1- تفتيش الحاسب الآلي وطبع نسخة ورقية من ملفات معينة في ذات الوقت.

---

[1]- يزيد بوخلط، مقال بعنوان تفتيش المنظومات المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل ET-Tawassal ، كلية الحقوق والعلوم السياسية، جامعة باجي مختار عنابة، المجلد 22، العدد 2، ديسمبر 2016، ص 90.

[2]- زبيحة زيدان، مرجع سابق، ص 150.

[3]- ناني لحسن، مرجع سابق، ص 121.

[4]- علي عدنان الفيل، مرجع سابق، ص 60.

2- تفتيش الحاسب الآلي وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت.
3- عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.
4- ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع([1]).

وإن عملية الحجز عن طريق نسخ المعطيات تتم وفق للقواعد المقررة في قانون الإجراءات الجزائية، ومثال ذلك ما ورود عبارة الأشياء في المادة 84 من هذا القانون التي تتصرف على المعطيات أو المعلومات المبحوث عنها أو المضبوطة والمراد حجزها، ليتنبه بذلك المشرع الجزائري إلى جانب مهم في هذا الموضوع وهو المتعلق بالجانب العلمي أو التقني في مجال ملاحقة الجريمة المعلوماتية والبحث عن مرتكبيها وجمع الأدلة التي من شأنها إدانتهم([2])، وكذلك إحترام إجراءات التحقيق وخاصة إحترام سر المهنة وحقوق الدفاع بما يكفل أمن وسرية وسلامة المعطيات في النظام المعلوماتي، إضافة إلى إجراء الحجز، نص قانون العقوبات في المادة 394 مكرر6 على تدابير أخرى كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع الإلكترونية التي تكون محلا للجريمة([3]).

كما أوجب المشرع الجزائري على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في النظام المعلوماتي الذي تجري به العملية، وفقا لأحكام المادة 6 الفقرة 2 منها من القانون 09-04، وذلك لصيانتها عن العبث منذ لحظة إكتشافها حتى لحظة عرضها على القضاء، لا سيما وأنه بحسب مصدر عليم لجريدة الفجر الجزائرية، فقد تم في الجزائر تسجيل 58 قضية في مجال جرائم الإعتداء على سلامة الأنظمة المعلوماتية خلال سنة 2016([4]).

---

[1]-حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت-دراسة مقارنة-، رسالة مقدمة لنيل درجة الدكتواره في القانون الجنائي، كلية الحقوق-جامعة عين الشمس، ص 387،388.

[2]- زبيحة زيدان، مرجع سابق، ص 152.

[3]-يزيد بوخلط، مرجع سابق، ص 91.

[4]- مقتبس عن: حفوظة الأمير عبد القادر، غرداين حسام، بحث بعنوان الجريمة الإلكترونية وآليات التصدي لها، مركز جيل البحث العلمي، أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة 29 مارس 2017، ص 98.

وحيال ذلك يمكن إتخاذ بعض الإجراءات الخاصة للحفاظ على سلامة المعطيات في النظام المعلوماتي وصيانتها من العبث أبرزها:

أ- ضبط الدعائم الأصلية للبيانات وعدم الإكتفاء بضبط النسخ.

ب- مراعاة ظروف الحرارة والرطوبة المناسبتين لتخزين الأحراز المعلوماتية، بحيث يراعى في أماكن تخزين الأقراص والأشرطة الممنغطة المحرزة أن تتروح درجة الحرارة داخلها بين 4 و32 درجة مئوية، وأن تكون نسبة الرطوبة فيها بين 20% و80% وفي ظل هذه الظروف يمكن أن تصل مدة التخزين إلى ثلاث سنوات.

ج- إلتزام القواعد الفنية المتعلقة بكيفية نقل الأحراز المعلوماتية كالتحرز من المرور بها أو تخزينها على مقربة من محطة إرسال لاسلكي وعدم وضعها في أماكن متربة أو قاعدة نافذة لتأثير الأتربة والغبار عليها.

د- تأمين البرامج المضبوطة قبل تشغيلها فنيا وعمل نسخ منها سليمة وكاملة([1]).

هـ- إحكام الحلقات الإجرائية للضبط من خلال الإهتمام ببيان التسلسل والترابط وإبراز الأحكام في الحلقات الإجرائية التي مرت بها المادة المعلوماتية تأمينا لسلامتها وصيانتها عن العبث من لحظة إكتشافها وحتى لحظة عرضها على القضاء.

و- تمييز المادة المضبوطة بوضع علامة مادية خاصة بها من قبل من كانت في حيازته على أن يتم بعد ذلك وضعها في علب مغلقة وتحريزها([2]).

وأجاز المشرع في نفس المادة في فقرتها الأخيرة لهاته السلطة إستعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للإستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

كما أنه حاليا يتم إستخدام برامج متخصصة في النسخ مثل برنامج lap link([1])، كما يوجد أسلوب تجميد التعامل بنظام المعالجة الآلية أو إحدى القطع المكونة له

---

[1]- يوصي الاستاذ Sieber بضرورة إستعانة الجهات القائمة بالضبط والتحقيق بخبراء فنيين للقيام بعملية الإستنساخ عامة، وأن تتم عملية إنتاج النسخ من قبل هؤلاء من خلال أنظمة الحاسبات التي يألفونها فقط، وأن يستخدموا -إذا كان ذلك ممكنا- نظام التشغيل(الآمن) الخاص بهم. أنظر: هشام محمد فريد رستم، مرجع سابق، ص 132.

[2]-حسين بن سعيد الغافري، مرجع سابق، ص 362،363.

التي أستخدمت في إرتكاب الجريمة، ويتخذ هذا الأسلوب عدة مظاهر، من أبرزها: نظام ضغط محتويات القرص الصلب، وكذلك نقل المحتويات إلى أقراص صلبة متعددة أو ممنغطة، ومثل هذا الإجراء يصلح أن يستخدم في مواجهة الحاسبات الخادمة التي تحتوي على مواقع الهكرة أو ملفات فيروسية، كما يصلح أيضا إذا كان القرص الصلب يحتوي مثلا على ملفات مشفرة وتتطلب فك شفرتها([2]).

**الفرع الثاني: الحجز عن طريق منع الوصول إلى المعطيات**

نصت المادة 19 المتعلقة بتفتيش وضبط البيانات المعلوماتية المخزنة في فقرتها 3 بند "د" من إتفاقية بودابست على ما يلي:

3- يجب على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تحويل سلطاته المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين 1 و2، وهذه الإجراءات تشمل السلطات التالية:

د- منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتي.

وقد تم إستخدام مصطلح الحصول بطريقة مشابهة وذلك من أجل الأخذ في الإعتبار الطرق الأخرى لرفع بيانات غير مادية والتي لا يسهل الوصول إليها أو أن فرص السيطرة عليها تتم بطريقة أخرى في البيئة المعلوماتية، وبما أن الإجراءات تتعلق ببيانات غير مادية مخزنة فإن السلطات المختصة يجب أن تتخذ إجراءات تكميلية من أجل الحصول عليها، كما أن وصف البيانات بصعوبة الوصول إليها يمكن أن يعني ترميزها أو تقييدها عن طريق أية وسيلة إلكترونية أخرى تمنع الدخول إلى هذه البيانات، وتطبيق هذا الإجراء يمكن أن يعود بالفائدة وذلك في الحالات التي تتضمن خطرا أو ضررا بالمجتمع، ويبدو ذلك في حالة البرامج التي تحتوي على

---

[1]- برنامج lap link : هو برنامج يمكن تشغيله من قرص مرن، ويسمح بنسخ البيانات من الحاسب الخاص بالمتهم ونقلها إلى قرص آخر من من خلال المنفذ المتتالي Serial port أو المنفذ المتوازي Parallel port، وهذا البرنامج مفيد جدا للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم. أنظر: حسن طاهر داود، مرجع سابق، ص 229.

[2]- بوكر رشيدة، مرجع سابق، ص 421،422.

فيروسات أو في الحالات التي تكون فيها هذه البيانات محتواها غير قانوني كما في حالة المواد الإباحية الطفولية.

أما بالنسبة لمصطلح رفع فأنه يقصد به التعبير عن فكرة أنه إذا كانت البيانات يتم رفعها أو جعلها غير قابلة للوصول إليها إلا أنه لا يتم تدميرها بل تستمر في الوجود، والشخص المشتبه فيه يتم حرمانه مؤقتا من الولوج إلى هذه البيانات، لكن يمكن إعادتها بعد إنتهاء التقيب والتحري أو بعد الإجراءات الجنائية، ويتجسد ذلك عند مصادرة البيانات، بحيث يتم العمل على نسخ البيانات، وبعد ذلك جعل النسخة الإصلية غير قابلة للوصول إليها أو رفعها دون القيام بالمحو النهائي للبيانات المضبوطة([1]).

كما نصت المادة 27 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، التي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، على طريقة الحجز عن طريق منع الوصول إلى المعطيات في فقرتها الأولى بند "د" ، وذلك في إطار ضبط المعلومات المخزنة، بقولها على أنه"

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (1) من المادة السادسة والعشرين من هذه الإتفاقية.

هذه الإجراءات تشمل صلاحيات:

د) إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها."([2]).

وإلى جانب ذلك نصت المادة 16 في فقرتها الأولى البند "د" من القانون البحريني رقم (60) لسنة 2014 بشأن جرائم تقنية المعلومات على أنه"

---

1- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 239-241.

2- المادة 27 الفقرة 1 البند د من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات..

1- للنيابة العامة سلطة الضبط والتحفظ على بيانات وسيلة تقنية المعلومات التي يتم الدخول إليها إستنادا إلى أحكام المادة (15) من هذا القانون، ويشمل ذلك ما يلي:

د- رفع بيانات وسيلة تقنية المعلومات من نظام تقنية المعلومات الذي تم الدخول إليه أو جعل الدخول إليها غير متاح"([1]).

أما بالنسبة للمشرع الجزائري فقد أشارت المادة 7([2]) من قانون 04/09، السالف الذكر، أنه في حالة إستحالة إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 من هذا القانون لأسباب تقنية يتعين على هذه السلطة التي تقوم بعملية التفتيش إستعمال تقنيات مناسبة لمنع الوصول الى المعطيات التي تحتويها المنظومة المعلوماتية أو الى نسخها والموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة.

ويلاحظ أن المشرع الجزائري حصر اللجوء إلى طريقة الحجز عن طريق منع الوصول إلى المعطيات في حالة واحدة وهي إستحالة إجراء الحجز عندما لا يمكن اللجوء إلى الطريقة الأولى والمتمثلة في نسخ المعطيات محل البحث والمعطيات اللازمة لفهمها، بأن يتم التحفظ على البيانات محل الجريمة وكذلك الأدوات التي أستخدمت في إرتكابها أو الآثار المتخلفة عنها والتي تفيد في كشف الحقيقة([3]).

ويتعين على السلطة التي تقوم بالتفتيش في هذه الحالة تكليف هؤلاء المختصين (مزودي الخدمة) بإستعمال الوسائل التقنية المناسبة والضرورية للحيلولة دون الوصول إلى المعطات التي يحتويها النظام المعلوماتي ومنع القيام بأي إستعمال لها أو نسخها أو الإطلاع عليها، والمقصود هنا تلك المعلوماتية التي تشكل محل الجريمة أو تحوي على أدلة لها، كل ذلك لمنع تهريبها أو تدمير تلك الأدلة المؤدية لها، وهو ما أشير إليه بنص المادتين 7 و8 من القانون 09-04([4]).

---

[1]- المادة 16 الفقرة 1 البند د من القانون البحريني رقم (60) لسنة 2014.

[2]- المادة 7 من القانون 09-04.

[3]- ناني لحسن، مرجع سابق، ص 124.

[4]- زبيحة زيدان، مرجع سابق، ص 153.

كما أن الهدف من هذا الإجراء الإحترازي هو الحفاظ على الأدلة في محيطها الإلكتروني ومنع أي محاولة لطمسها أو إخفاء معالمها، وهو ما سيكون له دون شك الأثر الإيجابي في نجاح إجراءات التفتيش والحجز([1]).

وبالنسبة لحالة حجز معطيات ذات محتوى مجرم أو يشكل محتواها جريمة منح المشرع الفرنسي لوكيل الجمهورية أو لقاضي التحقيق حسب الحالة بإعطاء أوامر لقيام بحذف جميع المعطيات نهائيا من الدعائم التي تم نسخها والتي – المعطيات المعلوماتية- في حالة إستعمالها أو حيازتها تكون مجرمة أو تشكل خطرا على أمن الأشخاص أو الممتلكات مثال ذلك الصور الخاصة بالإعتداءات الجنسية على القصر([2]).

وفي هذا الإطار نصت المادة 39 من المرسوم بقانون إتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات على أنه" يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين أي مالك أو مشغل لموقع إلكتروني أو شبكة معلوماتية خزن أو أتاح متعمدا أي محتوى غير قانوني، مع علمه بذلك، أو لم يبادر بإزالة أو منع الدخول إلى هذا المحتوى غير القانوني خلال المهلة المحددة في الإشعار الخطي الموجه له من الجهات المختصة والذي يفيد بعدم قانونية المحتوى وأنه متاح على الموقع الإلكتروني أو شبكة المعلوماتية" ([3]).

كما لجأت بعض التشريعات المقارنة إلى حجب المواقع التي تحوي معطيات ذات محتوى مجرم أو القيام بحذف جميع المعطيات نهائيا من الدعائم التي تم نسخها، ومثال ذلك ما نصت عليه المادة 8 من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات على أن" لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون ويشكل تهديدا للأمن القومي أو من يعرض أمن

---

[1]- رضا هميسي، مقال بعنوان تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة ورقلة، المجلد 3، العدد 2، جوان 2012، ص 177.

[2] -Myriam Quéméner, yves charpenal , op.cit,p179.

[3]- المادة 39 من مرسوم بقانون إتحادي رقم (5) لسنة 2012.

البلاد أو إقتصادها القومي للخطر، أن تأمر بحجب المواقع محل البث كلما أمكن تحقيق ذلك فنيا([1]).

أما بالنسبة للمشرع الجزائري فقد نصت المادة 8 من القانون 09-04، على أنه" إنه يمكن للسلطة التي تباشر التفتيش أن تأمر بإتخاذ الإجراءات اللازمة لمنع الإطلاع على هذه المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل بإستعمال الوسائل التقنية المناسبة لذلك"([2]).

وقد تم تكليف مقدمو خدمة الأنترنت في إطار إلتزاماتهم الخاصة التي تقع على عاتقهم بوضع ترتيبات تقنية تسمح لهم بالتدخل الفوري لسحب المحتويات أو جعل الدخول إيا غير ممكن أو حصر إمكانية الدخول الى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها، مع قيام مسؤوليهم الجنائية في حالة مخالفتهم وضع هذه الترتيبات بموجب العقوبات المقررة في المادة 394 مكرر 8 من القانون 16-02 المؤرخ في 19 يونيو سنة 2016، المعدل والمتمم لقانون العقوبات الجزائري، والمشار لها سالفا.

كما وضع المشرع الجزائري أيضا قيودا لإستعمال هذه المعطيات المتحصل عليها وذلك ضمن الحدود الضرورية للتحريات أو التحقيقات القضائية وإلا يتعرض مخالفها الى العقوبات المنصوص عليها في التشريع المعمول به طبقا لأحكام المادة 9 من القانون 09-04، السالف الذكر.

ويمكن القول في الأخير إلى أن مشاركة عدة أطراف في عمليتي التفتيش والحجز عن المعطيات المعلوماتية، سواء تمثلت في السلطات القضائية( النيابة، التحقيق، الضبطية القضائية) أو مقدمو الخدمات أو الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وكذا كافة الأشخاص الذين لهم دراية واسعة بعمل النظام المعلوماتي محل البحث والتحري، كل ذلك يعكس خطورة

---

1- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص426.

2- المادة 8 من القانون 09-04.

هذه الجرائم وجسامة المخاطر الناجمة عنها، لاسيما إذا كانت هذه المعطيات المعلوماتية المبحوث عنها تقع في نظام معلوماتي لدى دولة أجنبية أخرى .

# الفصل الثاني

# الآليات الإجرائية الدولية لمكافحة جرائم نظام المعالجة الآلية للمعطيات

## الفصل الثاني: الآليات الإجرائية الدولية لمكافحة جرائم نظام المعالجة الآلية للمعطيات

إن التطور المستمر للأنظمة المعلوماتية وما تتميز به من سرعة في إعداد ونقل وتخزين المعلومات وما تتوفر عليه من السرية التامة جعلها بيئة ملائمة للإجرام بعيدا عن أعين الجهات الأمنية.

ونتج عن ذلك ظهور ما يعرف بجرائم نظام المعالجة الآلية للمعطيات التي تعد من أهم الجرائم العابرة للحدود الإقليمية، باعتبارها تتميز بمجموعة من الخصوصيات وأهمها البعد الدولي الذي ينجم عنه تعدي النشاط الإجرامي لعدد من الدول، وهو الأمر الذي يثير العديد من الصعوبات في مجال تفعيل الآليات الإجرائية الدولية لمكافحة جرائم نظام المعالجة الآلية للمعطيات، وخصوصا مسألة الإختصاص القضائي الدولي من حيث الجهات المختصة وما يثور عنه من تنازع الإختصاص القضائي وذلك نتيجة لإختلاف التشريعات في المعايير والمبادئ المطبقة في تحديده، وكذا مسألة المساعدة القضائية الدولية المتبادلة بخصوص تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، وعدم كفاية مجالاتها التقليدية (تبادل المعلومات ونقل الإجراءات والإنابة القضائية) المخصصة لمجابهة كافة الجرائم الخطيرة بما فيها جرائم نظام المعالجة الآلية للمعطيات للتصدي لهذا النوع من الجرائم.

فالبعد الدولي لجرائم نظام المعالجة الآلية للمعطيات يفرض على المجتمع الدولي ضرورة البحث عن وسائل أكثر ملائمة لطبيعة هذه الجرائم، والعمل على تضييق الثغرات القانونية التي برع مرتكبوها في إستغلالها لتهرب من العقاب ونشر نشاطهم الإجرامي في مناطق مختلفة من أنحاء العالم([1])، لاسيما وإنها ترد إلى ثلاثة أسباب وهي: الأولى سياسية وتتجسد في سقوط الحواجز بين الدول واقعيا، والثانية إجتماعية وإقتصادية وترتبط بدور المعاهدات الدولية بصفة عامة وإتفاقيات الجات بصفة خاصة وما أسفرت عنه من قيام منظمة التجارة العالمية بكل آثارها المختلفة وأخصها عولمة النشاط المصرفي، أما الثالثة فهي عملية وتتجسد في تقدم المواصلات

[1]-خليفي محمد، مقال بعنوان إشكالية الإختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية، مجلة الميزان، المركز الجامعي بالنعامة، العدد1، ديسمبر 2016، ص 256.

والإتصالات السلكية واللاسلكية وبصفة خاصة شبكة الأنترنت، وبذلك تتوزع أركان هذه الجرائم أو تتغير أو قد تختفي نتيجة التقدم العلمي الهائل على أقاليم العديد من الدول، وتتلاشى أدلة إثباتها، ويسهل تنقل فاعليها من دولة إلى أخرى، ومن تم يصعب على القوانين الجنائية الوطنية ملاحقة مرتكبي جرائم نظام المعالجة الآلية للمعطيات([1]).

كما أن الإختلاف في التشريعات الداخلية بشأن قواعد الإختصاص وعدم وجود آليات إلزام الدول بتوحيد هذه التشريعات والسهر على تطبيقها يساهم في إنتشار هذه الجرائم وإفلات مرتكبيها من العقاب([2]).

وهو الأمر الذي يستحيل معه مكافحة هذا النوع من الإجرام بغير تفعيل الآليات الإجرائية الدولية سواء على صعيد الإختصاص القضائي الدولي أو المساعدة القضائية الدولية المتبادلة بالنسبة لتبادل المعلومات في هذه الجرائم والمساعدة على التحقيق فيها وتتبع مرتكبيها، وذلك كله وفقا للقواعد التي تقررها الإتفاقيات الثنائية أو المتعددة الأطراف أو وفقا لمبدأ المعاملة بالمثل.

وبناء على ما تقدم، فإننا سنقوم بتقسيم هذا الفصل إلى مبحثين يتناول المبحث الأول الإختصاص القضائي الدولي في جرائم نظام المعالجة الآلية للمعطيات، أما المبحث الثاني فنخصصه للمساعدة القضائية الدولية المتبادلة في جرائم نظام المعالجة الآلية للمعطيات.

---

[1]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 754.

[2]- خليفي محمد، مرجع سابق، ص 256.

## المبحث الأول: الإختصاص القضائي الدولي في جرائم نظام المعالجة الآلية للمعطيات

الإختصاص القضائي الدولي هو بيان القواعد التي تحدد ولاية محاكم الدولة في المنازعات التي تتضمن عنصرا أجنبيا إزاء غيرها من محاكم الدول الأخرى([1])، وتنظم هذه القواعد الحالات التي ينعقد فيها الإختصاص لمحاكم الدولة للفصل في منازعات تشمل على عنصر أجنبي([2])، لذا فإن القاضي الوطني يكون ملزما منذ البداية بالفصل في الإختصاص الدولي أي بيان ما إذا كان هو أصلا كقضاء وطني مختص بنظر الدعوى أم لا([3]).

والإختصاص القضائي الدولي يرتبط تماما مع سيادة الدولة، بحيث يتوقف تحديده على إرتباط عناصر العلاقة القانونية بتلك الدولة التي تحكم المحكمة بإسمها وسواء أكان هذا الإرتباط شخصيا أم إقليميا([4]).

فتتجه غالبية الدول لحل مشكلة الإختصاص القضائي في هذا العالم الإفتراضي إلى تطبيق المبادئ ذاتها المعمول بها لحل مشكلة الإختصاص الجزائي الدولي في الجرائم التقليدية وعلى رأسها مبدأ أقليمية القوانين([5]).

كما تثار مشكلة الإختصاص القضائي الدولي بالنسبة للجرائم المرتكبة في نطاق المعلوماتية عبر أنظمة المعلومات خارج حدود الدول بصورة أكبر مما هي عليه على مستوى أقليم الدولة الواحدة، حيث يكون بإمكان الدولة وضع حد للمشكلة على المستوى الوطني أو المحلي من خلال النصوص القانونية التي يمكن إقرارها بهذا البلد أو ذلك، لأن الجريمة محصورة في النطاق الأقليمي للدولة، ومعالجتها

---

1- هشام صادق، تنازع الإختصاص القضائي الدولي، دار المطبوعات الجامعية، الأسكندرية-مصر، سنة 2007، ص 5.

2- زياد خليف العنزي، مقال بعنوان إختصاص القضاء الإمارتي بنظر المنازعات الإلكترونية ذات العنصر الأجنبي، مجلة جامعة الشارقة، أبوظبي-الإمارت، المجلد 15، العدد 2، ديسمبر 2018، ص 424.

3- حسين بن سعيد الغافري، مرجع سابق، ص 452.

4- ممدوح عبد الكريم، القانون الدولي الخاص- تنازع القوانين، دار الثقافة للنشر والتوزيع، عمان، ط 1، سنة 2005، ص 248.

5- عراب مريم، مقال بعنوان الإختصاص القضائي في الجرائم المعلوماتية، مجلة annales de facute de droit، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد وهران، المجلد 7، العدد3، ديسمبر 2015، ص 276.

يرتبط بكل دولة على إنفراد بخلاف مشكلة الإختصاص القضائي على المستوى الدولي، لأن الجريمة في الأخير لا ترتبط بحدود إقليمية لدولة ما، بل هي على العكس من ذلك، فهي جريمة عابرة للحدود، بالإضافة إلى إختلاف التشريعات والنظم القانونية من دولة إلى أخرى([1]).

وقد يحدث أن ترتكب الجريمة في أقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للإختصاص الجنائي للدولة الأولى إستنادا لمبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الإختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في إختصاصها إستنادا لمبدأ العينية([2]).

وعلاوة على ذلك، من المتصور أن يحصل تنازع الإختصاص القضائي في حالة إرتكاب الجريمة من طرف أحد المواطنين على أقليم الدولة التي يتبعها وحصول الضرر على أقليم دولة أخرى، إذ وفقا لمبدأ الإختصاص الإقليمي يؤول إختصاص النظر في النزاع إلى قضاء الدولتين دون مفاضلة بينهما، ومثل هذا الوضع لا يستبعد أن يطبق على جرائم نظام المعالجة الآلية للمعطيات([3]).

ومع هذا فإن تطور الإجرام وتوسعه إلى دول العالم يتطلب وجود إتفاقيات دولية لتسليم المجرمين، غير أن أغلبية الدول لا تسلم رعاياها وفقا لمبدأ السيادة من جهة، ومن جهة أخرى التعارض مع مبدأ أساسي وهو عدم جواز محاكمة الشخص عن فعل واحد أكثر من مرة.

وعلى هذا الأساس فلا بدا من وضع نظام قانوني يسمح بمتابعة وملاحقة مرتكبي جرائم نظام المعالجة الآلية للمعطيات دون المساس بحقوق وحريات الأفراد التي تقرها المواثيق الدولية، ووجوب إحترام مبدأ الشرعية دون إعطاء فرصة للجناة

---

[1]- فايز محمد راجح غلاب ، مرجع سابق، ص 379.

[2]- محمد نصر محمد ، مرجع سابق، ص 113.

[3]- شوقي يعيش تمام، عزيزة شبري، مقال بعنوان تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الإجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 9، العدد15، جوان 2017، ص 100.

من الإفلات من المتابعة الجنائية وتوقيع العقاب عليهم مما يحقق الأمن والإستقرار للمجتمع، ومن تم الحصول على معيار يتلائم مع طبيعة هذه الجرائم([1]).

ويعتبر مبدأ الإقليمية([2]) من أهم المعايير المعتمدة في تحديد الإختصاص القضائي الدولى، بالإضافة إلى بعض المعايير الأخرى كمبدأ الشخصية([3]) ومبدأ العينية([4]) ومبدأ العالمية أو الصلاحية الشاملة([5]).

---

[1]- بن محمد محمد، مقال بعنوان تنازع الإختصاص في الجرائم الإلكترونية، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح ورقلة، العدد 2، ديسمبر 2009، ص 143.

[2]- يقصد بمبدأ الإقليمية أن قانون العقوبات يطبق على أي جريمة تقع داخل الأقليم الوطني بغض النظر عن جنسية مرتكبيها أو المجني عليه، وينعقد الإختصاص وفقا لهذا المبدأ بتحقق أحد العناصر المكونة للجريمة سلوكا أو نتيجة ولو كان الفعل غير معاقب عليه في البلد الأصلي، وهو المبدأ السائد في معظم الإتفاقيات الدولية والإقلمية وغالبية التشريعات المقارنة ، إلا أنه يواجه صعوبة كبيرة في تطبيقه بالنسبة لجرائم نظام المعالجة الآلية للمعطيات وهذا بالنظر لطبيعتها والخصائص التي تميزها عن الجرائم التقليدية وخصوص صعوبة تحديد مكان وقوعها وارتكابها بدقة وكذا زمان حدوثها. أنظر: آمال فكيري، مقال بعنوان إشكالات الإثبات والإختصاص في جرائم تكنولوجيا الإعلام والإتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية،جامعة الوادي، المجلد 9، العدد 1، جانفي 2018، ص 641.

[3]- يقصد بمبدأ الشخصية أن القانون الجنائي يطبق على كافة الأشخاص الذين يحملون جنسية الدولة أينما وجدو ليحكم أفعالهم الأجرامية المرتكبة بالخارج، ويأخذ هذا المبدأ وجهان: إيجابي ويعني تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو أرتكبت الجريمة خارج إقليمها، سلبي ويعني تطبيق القانون الجزائي على كل جريمة يكون المجني عليه حاملا لجنسية الدولة، ولو كان الجاني أجنبيا، إلا أن هذا المبدأ يتعارض مع مبدا عدم جواز محاكمة الشخص على نفس الفعل الواحد مرتين، كما أن محاكمة المجرم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات طويلة وشاقة ومعقدة ومكلفة، وهذا ما يصدق كذلك بالنسبة لتنفيذ الأحكام في الخارج، أنظر: لموسخ محمد، مرجع سابق، ص149.

[4]- يقصد بمبدأ العينية أن التشريع العقابي ينطبق على جرائم معينة تتميز بكونها تمس مصالح الدولة الأساسية والجوهرية حتى وأن وقعت خارج أقليم الدولة وبغض النظر عن جنسية مرتكبيها، ويوجد تطبيق لهذا المبدأ في بعض الإتفاقيات الدولية والإقليمية وبعض التشريعات المقارنة كالتشريع الجزائري في المادة 15 من القانون 09-04، السالف الذكر،إلا أن هذا المبدأ يصادف العديد من الصعوبات ترجع بالأساس إلى طبيعة جرائم نظام المعالجة الآلية للمعطيات، بالإضافة إلى أن تعدد وتنوع الأنظمة القانونية في العالم يترتب عليه البطء والتعقيد وطول مدة الإجراءات، أنظر: حسين بن سعيد بن سيف الغافرين مرجع سابق، ص 458.

[5]- يقصد بمبدأ العالمية أو الصلاحية الشاملة أن القانون الجنائي يطبق على كل جريمة يقبض على مرتكبها في أقليم الدولة أيا كان مكان إرتكابها وجنسية الفاعل أو الجاني وبغض النظر عن مساسها بالسيادة الوطنية أو المصالح الوطنية، وهذا المبدأ يتلائم كثيرا مع طبيعة جرائم النظام رغم ما يطرحه من تنازع حاد بين التشريعات الجنائية في الدول، كما أنه يبقى عاجزا عن معالجة العديد من القضايا ما لم يكن هنالك تعاون دولي جاد

لذلك وجب تنظيم الإختصاص القضائي الدولي بمعايير موحدة تفرض على التشريعات الوطنية إحترامها والعمل بها من أجل مكافحة جرائم نظام المعالجة الآلية للمعطيات، حتى لا يثور هناك تنازع في الإختصاص القضائي بين محاكم أكثر من دولة لملاحقة نفس النشاط، وبالتالي يؤدي ذلك إلى إفلات المجرمين من العقاب.

ومن تم فإننا سنقوم بتقسيم هذا المبحث إلى مطلبين يتناول المطلب الأول تنظيم الإختصاص القضائي الدولي، بينما نتاول في المطلب الثاني تنازع الإختصاص القضائي الدولي.

**المطلب الأول: تنظيم الإختصاص القضائي الدولي في جرائم نظام المعالجة الآلية للمعطيات**

إن تنظيم الإختصاص القضائي الدولي لمكافحة جرائم نظام المعالجة الآلية للمعطيات نصت عليه الإتفاقيات الدولية والإقليمية والقوانين الداخلية في التشريعات المقارنة ، لذلك سوف نقوم بدراسة تنظيم الإختصاص القضائي الدولي في الإتفاقيات الدولية والإقليمية في الفرع الأول، بينما نتطرق في الفرع الثاني إلى تنظيمه في القوانين الداخلية.

**الفرع الأول: تنظيم الإختصاص القضائي الدولي في الإتفاقيات الدولية**

نصت المادة 22 من إتفاقية بودابست لمكافحة الجرائم المعلوماتية المؤرخة في 22 نوفمبر 2001، على أن"

1- أن كل طرف سوف يتبنى تدابير تشريعية وتدابير أخرى كلما لزم الأمر لإنشاء جهات إختصاص فيما يتعلق بالجراتئم الموصوفة في المواد من 2 إلى 11 من هذه المعاهدة، وذلك إذا تم إقتراف الجريمة:

(أ) داخل إقليم الولة أو

(ب) على متن إحدى السفن التي ترفع علم تلك الدولة أو

(ج) على متن طائرة مسجلة في قوانين تللك الدولة أو

---

وسريع، وكذا وجوب إعداد تشريعات وطنية لمعاقبة كل من يتم القبض عليه على أقليم الدولة دون مراعاة لجنسيته أو مكان وقوع الفعل الإجرامي، أنظر: بن محمد محمد، مرجع سابق، ص 150.

(د) من قبل حاملي جنسية تلك الدولة، إذا كانت الفعلة معاقب عليها في ظل قانون العقوبات في المكان الذي تم إقتراف الفعلة فيه أو إذا تم إقترافها في خارج نطاق الإختصاص الإقليمي لأية دولة.

2- يجوز لأي من الأطراف أن يتحفظ في أن يطبق أو لا يطبق فقط قواعد الإختصاص الموضحة في الفقرات من (1) ب إلى (1) د من هذه المادة أو أي من أقسامها إلا في حالات محددة أو في ظل شروط محددة.

3- سوف يتبنى كل الأطراف كلما لزم الأمر التدابير المناسبة لإنشاء وإقامة جهات إختصاص في شأن الجرائم المشار إليها في المادة 24 فقرة (1) من هذه المعاهدة، وذلك في الحالات التي يتواجد فيها شخص مدعى بإقترافه لتلك الجرائم في إقليم الدولة الطرف وذلك حين ترفض الدولة تسليمه لطرف آخر، وذلك فقط على أساس من جنسيته وبعد تقدم الطرف الآخر بطلب التسليم.

4- لا تستبعد هذه المعاهدة أي جهة إختصاص جنائي قائم ونافذ طبقا للقانون الداخلي.

5- عندما يدعي أكثر من طرف من الأطراف إختصاصه بشأن جريمة قائمة طبقا لهذه المعاهدة فإن الأطراف التي يعنيها الأمر سوف تتشاور في المكان الملائم للتوصل إلى أنسب دائرة إختصاص فيما يتعلق بإقامة الدعوى العمومية.

والملاحظ أن الفقرة الأولى هذه المادة وضعت مجموعة من المعايير التي تستند لها الأطراف المعنية في تحديد نطاق إختصاصها القضائي بالنسبة للجرائم المعلوماتية، وهي مبدأ الإقليمية ومبدأ الشخصية، وتاركة المجال في نفس الوقت لهاته الأطراف أن تمارس أي أختصاص جنائي آخر وفقا لقوانينها الداخلية، طبقا لأحكام الفقرة الرابعة من نفس المادة

كما نصت المادة 18 من ذات الإتفاقية على أنه" عندما يحاط أحد الأطراف المعنية، علما بأن شخص موجود في إقليمها أن تصدر السلطات المختصة أمرا إليه لتسليم بيانات حاسب محددة موجودة في حيازة ذلك الشخص أو تحت سيطرته مخزنة في نظام حاسب أو في وسيط لتخزين بيانات الحاسب، وأن تصدر أمرا إلى مقدم

خدمة يقدم خدماته في أقليم ذلك الطرف لتسليم بيانات المشترك المتصلة بتلك الخدمات الموجودة في حيازة أو تحت سيطرة مقدم الخدمة"

والملاحظ أن لهذه الإتفاقيات الدولية تأثيرها على القوانين الداخلية للدول الأطراف باعتبار إنها تفرض على الشارع الوطني إلتزاما بإقرار ما ورد بها من نصوص دولية بتجريم أفعال معينة، حتى يتسنى للمحاكم الوطنية تطبيقها([1]).

وفي ذات السياق أشارت الإتفاقية الأروبية حول الجريمة الإفتراضية لعام 2001 في مادتها الثانية والعشرين (22) إلى المبادئ التي يجب على الدول الأطراف إعتمادها لتحديد الإختصاص القضائي فيما يخص الجرائم المنصوص عليها في هذه الإتفاقية، وهذه المبادئ هي:

- مبدأ الأقليمية في فقرتها (1) البند (a).
- مبدأ الإختصاص المكاني في فقرتها (1) البندين ( c وb).
- مبدأ الجنسية في فقرتها (1) البند (D).
- مبدأ التعاون الدولي في مكافحة الإجرام أو الصلاحية الشاملة أو العالمية في فقرتها (3) .

ولقد سمحت في فقرتها الثانية (2) للدول الأطراف التحفظ على هذه المعايير، ولكن لا يجوز التحفظ في نقطتين: الأولى مبدأ الأقليمية، والثانية عندما يكون هناك على الدولة إلتزام بالتسليم.

كما سمحت كذلك في فقرتها الرابعة للدول الأطراف أن تتخذ أشكالا أخرى من معايير الإختصاص على نحو يتناسب مع قانونها الوطني([2]).

ونصت المادة 30 في فقرتها الأولى والثانية من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، على أن"

---

[1]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص ص 554-556.

[2]- محمد طارق عبدالرؤف الحق، جريمة الإحتيال عبر الأنترنت، منشورات الحلبي الحقوقية، لبنان، ط الأولى، سنة 2011، ص 200،201.

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد إختصاصها على أي من الجرائم المنصوص عليها في هذا الفصل الثاني من الإتفاقية وذلك إذا أرتكبت الجريمة كليا أو جزئيا أو تحققت:

أ- في إقليم الدولة الطرف.

ب- على متن سفينة تحمل علم الدولة الطرف.

ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف.

د- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان إرتكابها أو إذا إرتكبت خارج منطقة الإختصاص القضائي لأي دولة.

هـ- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الإختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (1) من هذه الإتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم"([1]).

كما نصت المادة 22 من القانون العربي النموذجي في مكافحة جرائم الكومبيوتر والأنترنت، على أنه" تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا إرتكبت كلها أو جزء منها داخل حدودها وفقا لمبدأ الإقليمية، كما تختص المحاكم فيها بنظر الدعوى المترتبة على تلك الجرائم، وعلى الدول العربية عقد إتفاقات لتبني المعيار الأولى بالإتباع في حالة تنازع الإختصاص بين الدول.

كما يسري التشريع الجنائي للدولة على الجرائم المعلوماتية التي تقع خارج الحدود إذا كانت مخلة بأمنها وفقا للقواعد العامة المنصوص عليها في قانون العقوبات"([2]).

وبالمجمل يمكن القول أن مسألة الإختصاص القضائي الدولي في جرائم نظام المعالجة الآلية للمعطيات قد أضحت معقدة أكثر في ظل عدم وجود إتفاق دولى

---

[1]-المادة 30 الفقرة 1 و2 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[2]- مقتبس عن: عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والأنترنت، مرجع سابق، ص 49.

موحد ينظم هذه المسألة، وهذا بالنظر لما تتميز به النظم المعلوماتية من صعوبة الرقابة عليها، والسيطرة على المعلومات المتداولة عبرها، ذلك أن العديد من الدول المتقدمة في مجال التكنولوجيا الرقمية تقوم بالرقابة الإلكترونية والتحليل الآلي لكل معلومة أو رسالة شاردة أو واردة منها أو إليها، إلا أن ضخامة المعلومات الموجودة بها تعيق ذلك، وهو ما يؤكد لنا أنه في ظل عدم التعاون الدولي في متابعة وضبط مرتكبي جرائم نظام المعالجة الآلية للمعطيات، فستظل مسألة الإختصاص القضائي الدولي تثير العديد من الإشكاليات خاصة في الجوانب الإجرائية المتعلقة بالتفتيش والضبط([1]).

**الفرع الثاني: تنظيم الإختصاص القضائي الدولي في القوانين الداخلية**

نص المشرع الفرنسي على الضوابط التي تحكم الإختصاص القضائي الفرنسي فيما يتعلق بالجرائم المرتكبة في الخارج، وإذ أن الجريمة وقعت في الخارج وتحققت النتيجة الإجرامية في فرنسا فإن القضاء الفرنسي يختص بنظر الجريمة وفقا للمادة 113-2 من قانون العقوبات الفرنسي الجديد([2])، والتي تعتبر الجريمة وقعت على الأراضي الفرنسية متى وقعت أحد عناصرها المكونة لها داخل الأراضي الفرنسية([3]).

وفي بريطانيا يشترط لاختصاص القضاء البريطاني أن تكون الواقعة الإجرامية لها إرتباطا ببريطانيا يستوي في ذلك أن يكون مرتكب الواقعة قد إرتكبها في بريطانيا أو كانت نتيجتها قد أمتدت إلى بريطانيا يصرف النظر عن مكان إقامة الفاعل فيكفي أن يكون نشاط الفاعل قد تضمن تعديلات على حاسوب في بريطانيا([4]).

---

[1]- فايز محمد راجح غلاب ، مرجع سابق، ص 392.

[2] -Art 113-2: La loi pénale française est applicable aux infractions commises sur le territoire de la République.
L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire, code pènal France 1 mars1994.

[3]- معتز سيد محمد أحمد عفيفي، قواعد الإختصاص القضائي بالمسؤولية الإلكترونية عبر شبكة الأنترنت، دار المطبوعات الجامعية، الأسكندرية- مصر، ط الأولى، سنة 2013، ص 45.

[4]- فايز محمد راجح غلاب، مرجع سابق، ص 381.

كما إن مشكلة الإختصاص القضاء الدولي ترتبط بمشكلات إمتداد أنشطة الملاحقة والتحري، والضبط والتفتيش خارج الحدود وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية([1]).

لذلك إتجه القانون الأمريكي إلى توسيع نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الأمريكية وكرس هذا الإتجاه في العمل القضائي فيما إنتهت إليه الدائرة الخامسة الإستئنافية في قضية قمار ومراهنت عبر الأنترنت، وقد إعتبر القضاء المذكور مجرد وضع برمجية فك التشفير (PGP) على الأنترنت بمثابة تصدير لها، وهو ما يخول المحاكم الأمريكية التصدي لها باعتبارها صاحبة الإختصاص بصرف النظر عن مكان وضع البرمجية([2]).

ونصت كذلك العديد من الشريعات العربية على تنظيم الإختصاص القضائي الدولي، من بينها دولة الإمارت التي نصت في المادة 47 من المرسوم بقانون رقم 5 لسنة 2012، بشأن مكافحة جرائم تقنية المعلومات على أنه" مع عدم الإخلال بأحكام الفصل الثاني من الباب الثاني من الكتاب الأول من قانون العقوبات، تسري أحكام هذا المرسوم بقانو على كل من إرتكب إحدى الجرائم الواردة به خارج الدولة، إذا كان محلها نظام معلوماتي الكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية المعلومات خاصة بالحكومة الإتحادية أو إحدى الحكومات المحلية لامارت الدولة أو إحدى الهيئات أو المؤسسة العامة المملوكة لأي منهما"([3]).

وفي مصر نصت المادة 3 من القانون رقم 175 لسنة 2018، بشأن مكافحة جرائم تقنية المعلومات، على أنه" مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على كل من إرتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقبا عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وذلك في الأحوال الآتية:

---

1- عبدالله دغش العجمي، مرجع سابق، ص 86.

2- ناني لحسن، مرجع سابق، ص 60.

3- المادة 47 من المرسوم بقانون إتحادي رقم (5) لسنة 2012.

1- إذا أرتكبت الجريمة على متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها.

2- إذا كان المجني عليهم أو أحدهم مصريا.

3-ا إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في جمهورية مصر العربية.

4- إذا أرتكبت بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية.

5- إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها أو بأمنها أو بأي من مصالحها، في الداخل أو الخارج.

6- إذا وجد مرتكب الجريمة في جمهورية مصر العربية، بعد إتكابها ولم يتم تسليمه"([1]).

وفي السودان نصت المادة 2 من قانون جرائم المعلوماتية لسنة 2007، على أنه" تطبق أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه إذا أرتكبت كليا أو جزئيا داخل أو خارج السودان أو إمتد أثرها داخل السودان وسواء كان الفاعل أصليا أو شريكا أو محرضا على أن تكون تلك الجرائم معاقبا عليها خارج السودان مع مراعاة المبادئ العامة الواردة في القانون الجنائي لسنة 1991"([2]).

وفي سلطنة عمان نصت المادة 2 من المرسوم السلطاني رقم 12 لسنة 2011، بإصدار قانون مكافحة جرائم تقنية المعلومات، على أن" تسري أحكام هذا القانون على جرائم تقنية المعلومات ولو أرتكبت كليا أو جزئيا خارج السلطنة متى أضرت بأحد مصالحها، أو إذا تحققت النتيجة الإجرامية في إقليمها أو كان يراد لها أن تتحقق فيه ولو لم تتحقق"([3])

وفي الأردن نصت المادة 16 من قانون جرائم أنظمة المعلومات الأردني على أنه" يجوز إقامة حق دعوى الحق العام والحق الشخصي على المشتكى عليه أمام القضاء الأردني إذا أرتكبت أي من الجرائم المنصوص عليها في هذا القانون

---

[1]- المادة 3 من القانون رقم 175 لسنة 2018.

[2]-المادة 2 من قانون جرائم المعلوماتية السوداني لسنة 2007.

[3]- المادة 2 من المرسوم السلطاني العماني رقم 12 لسنة 2011.

باستخدام أنظمة معلومات داخل المملكة أو ألحقت أضرارا بأي من مصالحها أو بأحد المقيمين فيها أة ترتبت آثار الجريمة فيها، كليا أو جزئيا، أو أرتكبت من أحد الأشخاص المقيمين فيها"([1]).

أما بالنسبة للمشرع الجزائري فقد نص على تنظيم الإختصاص القضائي الدولي لمكافحة جرائم نظام المعالجة الآلية للمعطيات في المادة 15 من القانون 09-04، السالف الذكر، والتي تنص على أنه " زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال المرتكبة خارج الأقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني"([2]).

والملاحظ على هذه المادة أنه بإمكان العدالة الجزائرية مباشرة الدعوى الجزائية ضد أي شخص أجنبي مشتبه به أو قام بارتكاب جرينة من الجرائم التي لها صلة بتكنولوجيات الإعلام والإتصال، عندما يثبت بأن هذه الجريمة تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني، وتتم إحالته إلى المحاكم الجزائرية باعتبارها مختصة حسب نص المادة 15 من القانون 09-04، المشار لها أعلاه([3]).

وإلى جانب ذلك أسندت بعض التشريعات الإختصاص القضائي للفصل في قضايا الجرائم المعلوماتية بصفة عامة بما فيها جرائم نظام المعالجة الآلية للمعطيات إلى محاكم معينة ، كما هو الحال في المادة 2 البند "أ" من القانون السوري رقم 9 لعام 2018، القاضي بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والإتصالات، والتي نصت على أنه" تحدث محاكم جزائية بدائية وإستئنافية للنظر في قضايا جرائم المعلوماتية وجرائم الإتصالات..." ([4]).

---

[1]- المادة 16من قانون جرام أنظمة المعلومات الأردني رقم 30 لسنة 2010.

[2]- المادة 15 من القانون 09-04.

[3]- زبيحة زيدان، مرجع سابق، ص 175،176.

[4]- القانون السوري رقم 9 لعام 2018، القاضي بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والإتصالات ، مديرية المعلومات والتوثيق، رئاسة مجلس الوزراء، سنة 2020، ص2.

بينما لم ينص المشرع الجزائري على محاكم خاصة للنظر في قضايا هذا النوع من الجرائم، وإكتفى بإسنادها إلى أقطاب جزائية متخصصة للنطر في بعض الجرائم الخطيرة، والتي ذكرها على سبيل الحصر، من بينها جرائم المساس بأنظمة العالجة الآلية للمعطيات.

إلا أن تخصص أي جهة قضائية لا معنى له دون تخصص القضاة المشكلين لهذه الجهة، لأن الغرض من إنشاء الجهات القضائية المتخصصة هو إسناد الفصل في الجرائم ذات خصوصية إلى قضاة متخصصين مؤهلين للنظر في هذه القضايا بصفة سريعة وفعالة، فالقاضي المتخصص شرط ضروري لتجسيد فكرة إتشاء جهاز قضائي متخصص([1]).

**المطلب الثاني: تنازع الإختصاص القضائي الدولي في جرائم نظام المعالجة الآلية للمعطيات**

إن إختلاف التشريعات والنظم القانونية في مكافحة جرائم نظام المعالجة الآلية للمعطيات، ينجم عنها تنازع في الإختصاص القضائي الدولي، فيؤدي تارة إلى تنازع إيجابي في الإختصاص القضائي بين محاكم أكثر من دولة لملاحقة نفس النشاط، وتارة أخرى يؤدي إلى تنازع سلبي في الإختصاص القضائي بأن تمتنع أي دولة من الدول المعنية بملاحقة نشاط الجاني، وهذا النوع الأخير من التنازع نادر الوقوع.

وتعد مسألة تنازع الإختصاص القضائي من أكبر التحديات التي تواجهها عملية التحقيق في جرائم نظام المعالجة الآلية للمعطيات، إذ أن ما تتميز به هذه الجرائم من طابعها المتخطي لحدود الدولة الواحدة، وإتسامها بالطابع الدولي، بالإضافة إلى تجرد السلوك الإجرامي فيها من الطابع المادي لإرتباطه بالعالم الإفتراضي أو الرقمي يجعلها ترتبط بأكثر من ولاية قضائية ويجتمع فيها أكثر من معيار واحد من معايير إسناد الإختصاص، مما يؤدي إلى تنازع إيجابي في الإختصاص بين جهات قضائية عدة.

---

1- كريمة علة، مقال بعنوان الجهات القضائية الجزائية ذات الإختصاص الواسع، مجلة revue Academique de la Recherche jurdique، جامعة عبدالرحمان ميرة بجاية، المجلد 6، العدد1، سبتمبر 2015، ص 123.

وبالرغم من أن مبدأ الإقلمية هو المبدأ المهيمن عند تنازع الإختصاص القضائي الدولي، إلا أنه يثير عدة صعوبات تتعلق بتحديد معيار الإختصاص المكاني في جرائم نظام المعالجة الآلية للمعطيات، والتي لا يقتصر نطاقها على المستوى المحلي أو القومي، بل يمتد ليشمل المستوى الأقليمي والدولي، بحيث يقع بذلك جزء من النشاط أو الركن المادي في أقليم دولة معينة بينما تقع النتيجة في أقليم دولة أخرى، فتزعم كل من الدولتين إختصاصها إستنادا إلى المبرر القانوني الخاص بها.

وأصبح لمبدأ الإقليمية مفهوما واسعا فيما يتعلق بتحديد مكان وقوع هذه الجرائم ولم يعد يلازم وقوع الفعل المادي أو أحد العناصر المكونة له مثلما هو معروف في السابق، بل بلغ الأمر حد نزع الصفة اللمادية كلية من هذا الفعل، نظرا لارتباط هذه الجرائم بالعالم الإفتراضي وكون تقنيات إرتكابها لا تترك أية آثار محسوسة.

وتطبيقا لهذا المفهوم الجديد لمبدأ الأقليمية أقر القضاء الفرنسي إختصاصة بالنظر في قضية yahoo وفقا للقانون الفرنسي، حتى وإن كان المدعى عليها- yahoo فرنسا- فرعا لمركز رئيسي في الولايات المتحدة الأمريكية، طالما أن البث يصل إلى الجمهورية الفرنسية، وبالتالي فإنه يمكن الإطلاع على المعلومات المخزنة في الإقليم الوطني([1]).

ولقد ذهب القضاء الأمريكي إلى أبعد من ذلك حينما وسع إختصاصه ليشمل كل الجرائم التي يمتد آثارها إلى إقليمه، وقضى بأنه إذا تم إدخال بيانات من أقليم دولة معينة تتضمن جريمة معلوماتية وكانت هذه البيانات مقروءة في دولة أخرى وتمس بمصالحها أو تعرضها للخطر أو يمكن أن تمتد آثارها إلى إقليمها، فإن محاكم هذه الدولة تكون مختصة للتصدي لتلك البيانات الإجرامية ما دام يمكن الإطلاع عليها في إقليمها([2]).

---

[1]- مقتبس عن: حسين بن سعيد الغافري، مرجع سابق، ص 456.

[2]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 566.

غير أن تفاقم مسألة تنازع الإختصاص القضائي الدولي وتحولها إلى عائق حقيقي أمام مكافحة جرائم نظام المعالجة الآلية للمعطيات، جعلت الفقه الجنائي يتدخل ويقوم بعقد إتفاقيات دولية لإيجاد حلول لهذه المسألة.

كما أن الفقه الجنائي اليوم وإن كان قد قبل فكرة تطبيق القانون الأجنبي لمواجهة الجريمة عبر الوطنية، ما أظهر ضرورة تجاوز فكرة تلازم الإختصاص الجنائي القضائي والتشريعي، فيلزم من باب أولى قبول هذه الفكرة والتوسع فيها بالنسبة للجرائم التي ترتكب في الفضاء الإلكتروني الذي يتجاوز الحدود والقارات، ويصل بذلك إلى ضرورة التفكير في وضع ضوابط إسناد جنائية لتحديد الإختصاص القضائي الدولي لجرائم نظام المعالجة الآلية للمعطيات([1]).

ومن تم فإننا سنقوم بدراسة تنازع الإختصاص القضائي الدولي من خلال إبراز موقف الفقه الجنائي من هذه المسألة في الفرع الأول، وموقف الإتفاقيات الدولية من ذات المسألة في الفرع الثاني.

**الفرع الأول: موقف الفقه الجنائي من مسألة تنازع الإختصاص القضائي الدولي**

تدخل الفقه الجنائي وقدم حلا لمشكلة تنازع الإختصاص القضائي الدولي يتمثل في إعطاء الأولوية في النظر في الجرائم الإلكترونية للدولة التي تتوفر على أحد معايير تحديد الإختصاص الذي يكون الأكثر جدوى وفعالية لضمان سرعة ملاحقة للمجرم الإلكتروني، وثمة طريقتان للتغلب على التنازع بين دولتين أو أكثرفي جرائم تقنية المعلومات، وهما:

الطريقة الأولى: تتمثل في منح الأولوية لأي من الدول المتنازعة، ويكون ذلك وفقا لأحد معايير الإختصاص الأكثر جدوى وفعالية لضمان ملاحقة الجريمة([2]).

وأول هذه المعايير مبدأ الأقليمية، باعتبار أن الدولة التي تقع في أقليمها الجريمة كلها أو الجزء الأكبر من النشاط المكون لركنها المادي أو النشاط التبعي

---

[1]- محمد نصر محمد ، مرجع سابق، ص 106.

[2]- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق، ص 641.

كله أو بصفة عامة الدولة التي توجد في إقليمها متحصلات الجريمة تبدو أرجح الدول إختصاصا بملاحقة الجريمة ومحاكمة فاعليها([1]).

ويكون مبدأ الأقليمية الأكثر قبولا لأن الدولة التي ترتكب على إقليمها الجريمة أو أحد العناصر المكونة لركنها المادي تكون الأقرب إلى مسرح الجريمة وملابستها والأوفر حظا للوصول إلى أدلة الإثبات، وبالتالي فهي الأولى بالتحقيق في الجريمة وملاحقة فاعليها من غيرها من الدول([2]).

ولا يجد هذا الحل مبرره الحقيقي في اعتبارات السيادة الوطنية الصيقة بمبدأ الأقليمية وإنما أيضا في جدواه العملية، حيث أين تقع الجريمة كلها أو جلها تصبح أدلة الإثبات متوافرة ويصبح من السها إجراء التحقيقات الكفيلة لإظهار الحقيقة.

وثان هذه المعايير مبدأ العالمية حيث يكون هو الملائم لمعظم الجرائم الإلكترونية التي يتوزع النشاط المكون للركن المادي لها في أكثر من دولة([3])، فيبدأ الإعداد والتنفيذ لها في دولة ويستمر في دولة أخرى وينتهي التنفيذ في دولة ثالثة.

وثالث هذه المعايير مبدأ الشخصية في شقه الإيجابي، بحيث ينعقد الإختصاص للدولة التي يحمل جنسيتها مرتكب هذه الجريمة فإن تعددت جنسية المتهم أنعقد الإختصاص للدولة التي يحمل جنسيتها، حتى لا يأخذ بعض المتهمين إكتساب جنسية جديدة سببا للإفلات من الملاحقة القضائية([4]).

الطريقة الثانية: تدعيم الملاحقة القضائية في كل حالة يخشى فيها لسبب إجرائي أو لآخر إفلات المتهم مرتكب الجريمة المعلوماتية من المحاكمة ويقتضي هذا التدعيم بصفة أساسية الإعتراف بمبدأ إما المحاكمة أو التسليم، كما يقتضي الإعتراف بإمكانية إحالة الدعوى الجنائية عن الجريمة المعلوماتية من دولة إلى أخرى، وتفعيل قواعد المساعدة القضائية بين الدول، خاصة فيما يتعلق بالحصول على شهادة

---

[1]- عراب مريم، مرجع سابق، ص 280.

[2]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 567.

[3]- عراب مريم، مرجع سابق، ص 280.

[4]- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق، ص 642.

الأشخاص والإنابة القضائية وفحص الأشياء وتبادل الأدلة الإلكترونية أو الأدلة الرقمية([1]).

ويتحقق ذلك عندما تقع جريمة تقنية المعلومات في أقليم دولة معينة، ويتم القبض على الفاعل في دولة أخرى يحمل جنسيتها فيثور التنازع بين مبدأين متعارضين: الأول مبدأ الإقليمية الذي يخول الإختصاص لدولة وقوع الجريمة، والثاني مبدأ العالمية الذي يمنح الإختصاص لدولة مكان القبض على المتهم، ويعطيها الحق في الإمتناع عن تسليمه إذا لم يكن بينها وبين الدول الطالبة إتفاقية دولية([2]).

كما ينجم عن تنازع الإختصاص القضائي الدولي تنازع فيما يخص مسألة تخزين المعلومات أو البيانات المعالجة إلكترونيا في النظم المعلوماتية خارج إقليم الدولة وظهر رأيان فقهيان، وهما:

الرأي الأول: يرى بأنه من غير المشروع أن تقوم سلطات دولة ما بالتدخل وتفتيش النظم المعلوماتية الموجودة في إقليم دولة أخرى، بهدف كشف وضبط أدلة لإثبات جريمة كانت قد وقعت على أراضيها وذلك إستنادا لمبدأ الأقليمية.

الرأي الثاني: يرى بأنه يمكن السماح بتنفيذ هذه الإجراءات حال توافر ظروف معينة يتم تحديدها كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية([3]).

**الفرع الثاني: موقف الإتفاقيات الدولية من مسألة تنازع الإختصاص القضائي الدولي**

نظرا لعدم نجاعة الحلول الفقهية المقترحة في تجاوز مشكلة تنازع الإختصاص التي تثيرها عملية التحقيق في جرائم نظام المعالجة الآلية للمعطيات، لجأت الدول إلى تنظيم مسألة الإختصاص بنصوص واضحة في إتفاقيات دولية ذات الصلة

---

[1]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 568.

[2]- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق، ص 642،643.

[3]-عراب مريم، مرجع سابق، ص 682،683.

والإتفاقيات الدولية الثنائية لإيجاد حل لمسألة الإختصاص القضائي الدولي لهذه الجرائم ذات البعد الدولي، يتم من خلالها تحديد الضوابط التي بموجبها توزع الولاية القضائية بين الأطراف المتعاقدة لتفادي النزاع.

فنصت المادة 25 في فقرتها الخامسة والأخيرة من إتفاقية بودابست على أنه"

5- عندما يقوم أكثر من طرف بإدعاء الإختصاص بالنسبة لجريمة معينة مشار إليها في هذه الإتفاقية، فأنه يجب على هذه الأطراف، إذا كان ذلك مناسبا، التشاور فيما بينها، بهدف تحديد الطرف الأكثر ملائمة لمباشرة التحقيقات.

ويلاحظ أن هذه الفقرة تعالج مسألة تعدد الإختصاص، إذ يحدث أن تختص عدة دول ببعض أو كل الأشخاص المساهمين في إرتكاب الجريمة المعلوماتية، لذا فأنه من أجل تدعيم إعتبارات فاعلية وتحقيق عدالة الإجراءات، أوجبت على الأطراف المعنية إستشارة بعضها البعض لتحديد الجهة الأمثل للتقاضي ولإجراء التحقيقات([1]).

كما نصت المادة (15) من إتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة على أنه يتعين على كل دولة طرف أن تعتمد ما يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقررة في الحالات الآتية:

-ا حينما ترتكب الجريمة في إقليم تلك الدولة.

-ا حينما ترتكب الجريمة ضد أحد مواطني تلك الدولة.

-ا حينما ترتكب الجريمة من طرف أحد مواطني تلك الدولة أو من طرف شخص عديم الجنسية أتخذ مكان إقامته المعتاد في إقليمها.

وأضافت هذه المادة، أنه إذا بلغت الدولة التي تمارس ولايتها القضائية عن سلوك إجرامي ما بموجب المعايير السالفة الذكر أو علمت بطريقة أخرى أن دولة واحدة أو أكثر باشرت إجراءات التحقيق والمتابعة القضائية في السلوك ذاته، فعلى

[1]-هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، دار النهضة العربية، القاهرة، ب ط، سنة 2011، ص 233،237.

السلطات المختصة في هذه الدول أن تتشاور فيما بينها لغرض تنسيق ما تتخذه من التدابير"([1]).

وفي هذا الصدد أصدر المجلس الأروبي في 11 سبتمبر 1995 توصية من بين عدة توصيات تناولت مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، جاء فيها بأن تفترض إجراءات التحقيق مد الإجراءات إلى أنظمة حاسب آلي آخر قد تكون موجودة خارج الدولة وتفترض التدخل السريع وحتى لا يمثل مثل هذا الأمر إعتداء على سيادة الدولة أو القانون الدولي وجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة ملحة لإبرام إتفاقيات تنظم وقت وكيفية إتخاذ مثل هذه الإجراءات، كما يجب أن تكون هنالك إجراءات سريعة ومناسبة ونظام إتصال يسمح للجهات القائمة على التحقيق بالإتصال بجهات أجنبية لجمع أدلة معينة، وهذا كله لا يكون إلا من خلال تفعيل إتفاقيات التعاون الدولي وتكريسها([2]).

أما عن إتفاقية مجلس أروبا لمكافحة الجريمة الإلكترونية فنظمت بدورها مسألة الإختصاص القضائي الدولي من خلال المادة 22 التي نصت على أنه" يلتزم كل طرف بوضع ما يلزم من تدابير تشريعية لإقرار الإختصاص بشأن أي جريمة إلكترونية وذلك:

- عندما ترتكب الجريمة على إقليمه.
- عندما ترتكب الجريمة من أحد مواطنيه إذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي لمكان إرتكابها أو في حالة إرتكاب الجريمة خارج الإختصاص القضائي الإقليمي لأي دولة.

وحثت الإتفاقية الأطراف المتعاقدة في حالة وجود تنازع في الإختصاص بين أكثر من طرف بشأن أي جريمة إلكترونية تقررها هذه الإتفاقية باللجوء متى كان ذلك

---

[1]- مقتبس عن: محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 569.

[2]- عراب مريم، مرجع سابق، ص 288،289.

ممكنا إلى التشاور فيما بينها لغرض تحديد الإختصاص القضائي الأكثر ملائمة لمتابعة هذه الجريمة([1]).

كما نصت المادة 30 في فقرتها الثالثة من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أنه"

3- إذا إدعت أكثر من دولة طرف بالإختصاص القضائي لجريمة منصوص عليها في هذه الإتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا إتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم"([2]).

وفي نفس السياق حثت المادة 22 من القانون العربي الإسترشادي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات لسنة 2004، أنه على الدول العربية عقد إتفاقيات لتبني المعيار الأول (مبدأ الإقليمية) في حالة تنازع الإختصاص بين الدول([3]).

كما أن معظم الدول قد سعت لإيجاد حل لمسألة الإختصاص القضائي لجرائم نظام المعالجة الآلية للمعطيات، إلا أن الحلول إختلفت من دولة إلى أخرى فبعض الدول تبنت الحل عن طريق الإتفاقيات الدولية وبعضها الآخر توسع قضائها في تفسير هذه المبادئ والبعض الآخر ساير الإجتهاد القضائي([4]).

وعليه، فإنه لا بدا من التعاون بين الدول لحل مسألة تنازع الإختصاص القضائي الدولي من خلال عقد إتفاقيات دولية لتبني المعيار الأنسب لمكافحة جرائم نظام المعالجة الآلية للمعطيات، ووضع آليات دولية لتعزيز التعاون الدولي في مجال القضاء الدولي من أجل وضع حد لتنازع الإختصاص القضائي الدولي، وبالتالي نضمن عدم إفلات مرتكبي هذه الجرائم من العقاب.

---

[1]- مقتبس عن: محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق، ص 643،644.

[2]- المادة 30 الفقرة 3 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[3]- عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والأنترنت، مرجع سابق، ص 149.

[4]- عراب مريم، مرجع سابق، ص 288،289.

**المبحث الثاني: المساعدة القضائية الدولية المتبادلة**

تعرف المساعدة القضائية الدولية المتبادلة بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم([1])، فملاحقة مرتكبي الجرائم الإلكترونية وتقديمهم للعدالة من أجل توقيع العقاب عليهم يستلزم القيام بإجراءات جنائية خارج حدود الدولة التي أرتكبت الجريمة أو جزء منها، ومن هذه الإجراءات معاينة مواقع الأنترنت في الخارج أو ضبط الأقراص الصلبة أو تفتيش نظم الحاسب الآلي، وهذا كله يصطدم بمشاكل الحدود والولايات القضائية([2]).

وكان فيما مضى التعاون القضائي والقانوني بين الدول محدود لعدة أسباب أبرزها تعقيدات وبطء إجراءات تبادل المساعدة القضائية التقليدية وعدم فاعليتها فقد يستغرق إتخاذ الإجراء الشهور، الأمر الذي لايناسب طبيعة جرائم نظام المعالجة الآلية للمعطيات التي تستدعي ضرورة توخي السرعة في التعامل مع الأدلة الرقمية غير الملموسة وسريعة الزوال([3]).

لذلك تعتبر المساعدة القضائية الدولية المتبادلة في المسائل الجنائية من الآليات الفعالة لمواجهة جرائم نظام المعالجة الآلية للمعطيات، وتبقى أهم وسيلة في التعاون الدولي، خصوصا لما للتعاون في مجال الإجراءات الجنائية من دور التوفيق بين حق الدولة في ممارسة إختصاصها الجنائي داخل حدودها الإقليمية وحقها في توقيع العقاب.

فالمساعدة القضائية على الصعيد الدولي تعني الصلاحيات القانونية المقررة لإجهزة إدارة العدالة الجنائية في الدولة التي يتم بمقتضاها قيام تلك الأجهزة بإتخاذ إجراءات معينة بغرض تعقب وتتبع أي نشاط إجرامي تم في نطاق إختصاصها الإقليمي من خلال الإستعانة بالأجهزة المقابلة لها بالدول الأخرى، وذلك في أي من إجراءات التحقيق أو المحاكمة التي تجريها سواء لضبط الجناة أم للوصول إليهم لجمع الأدلة أم إستدعاء الشهود والإستعانة بالخبراء، أم لتوفير المعلومات اللازمة لحسن سير إجراءات التحقيق والمحاكمة بما يوفر كافة العناصر القانونية اللازمة

---

1- أمال فكيري، مرجع سابق، ص 645.

2- بن محمد محمد، مرجع سابق، ص 153.

3- محمد كمال محمود الدسوقي، مرجع سابق، ص 143 .

للفصل في الإتهامات المسندة للمتهم إما بالحفظ أو بالأمر بأن لا وجه لإقامة الدعوى الجنائية وإما بالإحالة للمحاكمة وتوقيع العقاب المقرر قانونا([1]).

ونصت إتفاقية بودابست في المادة 23 على أنه" سوف يتعاون الأطراف فيما بينهم طبقا للأحكام الواردة في هذا الفصل من خلال تطبيق الأدوات اللازمة في شأن التعاون الدولي في المسائل الجنائية والترتيبات المتفق عليها، وذلك على أساس التشريعات الموحدة أو النظيرة والقوانين المحلية وذلك إلى أبعد حد ممكن في مجال التحريات والإجراءات الخاصة بالأفعال الجنائية المتعلقة بنظم الحاسبات والمعلومات أو بجمع الأدلة في شكلها الإلكتروني في شأن الجرائم الجنائية"([2]).

وتتنوع وتتعدد مجالات المساعدة القضائية المتبادلة في مجال مكافحة الجريمة إلى مجالات عامة تستهدف مختلف الجرائم والتي غالبا ما تتضمنها إتفاقيات عامة مثل معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية والإتفاقية الأروبية لنقل الإجراءات الجنائية، النموذج الإسترشادي لإتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003، وإتفاقية الرياض العربية للتعاون القضائي 1983، ومجالات خاصة تتطلبها طبيعة الجريمة المستهدفة مثل مكافحة جرائم نظام المعالجة الآلية للمعطيات محل بحثنا والتي عادة ما ترد هذه المجالات ضمن الإتفاقيات الدولية والإقليمية التي أبرمت لغرض مكافحتها وأهمها إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000، وإتفاقية بودابست المتعلقة بالجريمة الإلكترونية 2001، والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010([3]).

فتتضمن معظم هذه الإتفاقيات نصوصا تقتضي ضرورة الجوء إلى المساعدة القضائية الدولية المتبادلة بين الدول من أجل تحقيق الفعالية والسرعة في إجراءات ملاحقة وعقاب مرتكبي جرائم نظام المعالجة الآلية للمعطيات.

---

1- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 672،671.

2- مقتبس عن: محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق، ص 839.

3- محمد كمال محمود الدسوقي، مرجع سابق، ص 146 .

كما نصت عليها المادة 23 من القانون القطري رقم 14 لسنة 2014، بإصدار قانون مكافحة الجرائم الإلكترونية، على أنه" يتعين على الجهات المختصة أن تقدم العون للجهات النظيرة في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة وتسليم المجرمين في التحقيقات والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القانون، وفقا للقواعد التي يقررها قانون الإجراءات الجنائية المشار إليه والإتفاقيات الثنائية أو متعددة الأطراف التي تكون الدولة طرفا فيها، أو مبدأ التعامل بالمثل، وذلك بما لا يتعارض مع أحكام هذا القانون أو أي قانون آخر"([1]).

أما بالنسبة للمشرع الجزائري فنص على المساعدة القضائية الدولية المتبادلة في المادة 16 من القانون 09-04، السالف الذكر، والتي تنص على أنه" في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الإدلة الخاصة بالجرائم في الشكل الإلكتروني..." ([2]).

لذلك سوف نقسم هذا المبحث إلى مطلبين يتناول المطلب الأول طلبات المساعدة القضائية الدولية المتبادلة، بينما يتناول المطلب الثاني مجالات المساعدة القضائية الدولية الخاصة بمكافحة جرائم نظام المعالجة الآلية للمعطيات.

**المطلب الأول: طلبات المساعدة القضائية الدولية المتبادلة**

إن تنفيذ طلبات المساعدة القضائية الدولية المستعجلة الرامية لتبادل المعلومات والحفاظ علي سريتها أو إتخاذ أي إجراءات تحفظية تتم وفقا للقواعد المقررة في الإتفاقيات الدولية ذات الصلة والإتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل، دون المساس بأمن الدولة وسيادتها أو نظامها العام أو مصالحها الأساسية، وهذا من أجل المساهمة في جمع الأدلة التي تدين مرتكبوا جرائم نظام المعالجة الآلية للمعطيات وتقديمهم للمحاكمة واستصدار إحكام قضائية بالتحفظ على الأجهزة أو المعدات التي إستخدمت في إرتكابها.

---

1- المادة 23 من القانون القطري رقم (14) لسنة 2014.

2- المادة 16 من القانون 09-04.

ونصت المادة 25([1]) من إتفاقية بودابست في الفصل الثالث بعنوان مبادئ عامة تتعلق بالمساعدة القضائية الدولية المتبادلة على ما يلي "

1- يجب على كل الأطراف أن توفر لبعضها البعض مساعدة قضائية متبادلة إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الإلكترونية للجريمة الجنائية.

2- يجب على كل طرف أيضا أن يتبنى الإجراءات التشريعية وأية أجراءات أخرى يرى أنها ضرورية للوفاء بالإلتزامات المنصوص عليها في المواد 27 إلى 35.

3- يمكن لكل طرف في حالة الإستعجال، أن يقدم طلبا للمساعدة المتبادلة أو الإتصالات عن طريق وسائل سريعة للإتصال كالفاكس أو البريد الإلكتروني، وذلك لما تقدمه هذه الوسائل من شروط كافية للأمن والتوثيق (بما في ذلك التشفير لو كان ضروريا)، مع التأكيد الرسمي اللاحق حينما يكون ذلك مطلوبا بواسطة الدولة الموجه إليها الطلب أن توافق وأن ترد على الطلب المقدم إليها عن طريق أية وسيلة من الوسائل العاجلة للإتصال.

4- بإستثناء ما يرد مخالفا ذلك صراحة في مواد هذا الفصل، فإن المساعدة المتبادلة تخضع للشروط المحددة عن طريق القانون الداخلي للطرف الموجه إليه الطلب أو عن طريق الإتفاقات المطبقة للمساعدة المتبادلة، بما في ذلك الأسباب التي بناء عليها يمكن للطرف الموجه إليه الطلب أن يرفض التعاون.

يجب على الطرف الموجه إليه الطلب إلا يمارس حقه في رفض المساعدة القضائية المتبادلة بالنسبة للجرائم المنصوص عليها في المواد من 2 إلى 11 من الإتفاقية، فقط إذا كان الباعث على تقديم الطلب يتصل بجريمة ذات طبيعة مالية.

5- عندما يسمح، وفقا لبنود هذا الفصل، للطرف المقدم إليه الطلب أن يخضع المساعدة المتبادلة لوجود تجريم مزدوج (مشترك)، فإن هذا الشرط يعتبر مستوفيا إذا كان السلوك المكون للجريمة في الطلب المقدم للطرف المطلوب منه المساعدة، يوصف بأنه جريمة جنائية في قانونه الداخلي، سواء أكان القانون الداخلي قد صنفه

[1]- تقابلها في نفس المعنى المادة 32 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

في نفس طائفة الجرائم أم لا، وسواء تم تجريده بنفس المصطلح الذي نص عليه قانون الطرف الملتمس أم لا([1]).

ويتضح من خلال فقرات هذه المادة أنها وضعت القواعد أو المبادئ العامة التي تحكم المساعدة القضائية الدولية المتبادلة، ومن أهمها:

- الإلتزام بالمساعدة القضائية المتبادلة يجب أن يتوفر لأقصى حد ممكن، فيجب أن تكون شاملة أو ممتدة لكافة التحقيقات أو الإجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الإلكترونية للجريمة الجنائية، طبقا لأحكام الفقرة 1 من هذه المادة.

- أن كل طرف يكون مطالبا أن يضع موضع التنفيذ الأسس القانونية التي تسمح له بالموافقة على الأشكال المحددة للتعاون الذي يتم وضعه في باقي بنود هذا الفصل، إذا كانت الإتفاقيات أو الإتفاقات أو القوانين الخاصة به تحتوي على مثل هذه النوعية من الشروط، طبقا لأحكام الفقرة 2 من هذه المادة.

- تسهيل عملية الإسراع في الحصول على المساعدة المتبادلة، بحيث لا تضيع المعلومات أو الأدلة الأساسية بسبب محوها قبل إعداد وإرسال الرد على طلب المساعدة، طبقا لأحكام الفقرة 3 من هذه المادة، وذلك من خلال أمرين:

الأول: السماح للأطراف بتقديم طلب المساعدة عن طريق وسائل سريعة الإتصال بدلا من ولوج وسائل تقليدية أكثر بطئا في نقل المستندات المكتوبة داخل مظروف مختوم عن طريق الحقيبة الدبلوماسية أو عن طريق البريد.

الثاني: إلزام الطرف المقدم إليه طلب المساعدة أن يستخدم وسائل سريعة للإتصال للرد على هذا الطلب.

– يجب أن تخضع المساعدة المتبادلة للشروط الواردة في الإتفاقيات وتلك الواردة في القانون الداخلي، ولا مراء في أن هذه التنظيمات تضمن حقوق الأفراد المتواجدين على أرض الطرف المطلوب منه المساعدة، والذين يمكن أن يكونوا موضوعا لطلب المساعدة، وهذا طبقا لأحكام الفقرة الرابعة من هذه المادة.

---

1- مقتبس عن: هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص ص 253-255.

- خضوع المساعدة المتبادلة لشرط التجريم المزدوج، بحيث يتم السماح للطرف المقدم إليه الطلب بإخضاع المساعدة المتبادلة لشرط تجريم مزدوج، كأن يكون هذا الطرف يحتفظ بالحق في إستلزام التجريم المزدوج كشرط من أجل تنفيذ التماس أو التحفظ على بيانات معلوماتية أو التحفظ العاجل على البيانات المعلوماتية المخزنة، وفي كل الحالات فإن هذا الشرط يعتبر متوافرا إذا كان السلوك المكون للجريمة محل المساعدة المتبادلة يشكل جريمة جنائية أيضا في القانون الداخلي للطرف المقدم له الطلب، حتى لو كان قانونه الداخلي يضع هذه الجريمة في طائفة مختلفة للجرائم أو كان يستخدم مصطلحا مختلفا في تحديد هذه الجريمة، وهو الشرط المشار له في الفقرة الخامسة من هذه المادة([1]).

ومن تم فإننا سنقوم بتقسيم هذا المطلب إلى فرعيين، بحيث نتطرق في الفرع الأول إلى تنفيذ طلبات المساعدة القضائية الدولية لمكافحة جرائم نظام المعالجة الآلية للمعطيات، أما الفرع الثاني نعالج فيه رفض تنفيذ طلبات المساعدة القضائية الدولية.

**الفرع الأول: تنفيذ طلبات المساعدة القضائية الدولية**

نصت إتفاقية بودابست على القواعد المتعلقة بتنفيذ المساعدة القضائية الولية المتبادلة في المادتين 27 في فقرتيها 3 و9، و28 في فقراتها 2، 3 و4.

فنصت المادة 27 من ذات الإتفاقية في فقرتيها 3 و9 بندين "أ" و"ب" على أنه"

3- سوف يتم تنفيذ طلب المساعدة المتبادلة في ظل هذه المادة وفقا للإجراءات التي يحددها الطرف الطالب بإستثناء حالة عدم توافقها مع القوانين السارية لدى الطرف المطلوب منه.

9-أ في حالة الإستعجال فإن طلبات المساعدة المتبادلة أو الإتصالات الخاصة بها يمكن أن ترسل مباشرة من السلطات القضائية للطرف الطالب إلى السلطات المختصة لدى الطرف المطلوب منه وفي أي من تلك الحالات فإن صورة من ذلك الطلب سوف ترسل في ذات الوقت للسلطة المركزية (المحددة طبقا للمعاهدة) لدى

[1]- هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص ص 256-259.

الطرف المطلوب منه من خلال السلطة المركزية (المحددة طبقا للمعاهدة) لدى الطرف الطالب.

ب- أي طلب أو إتصال تحت هذا البند يمكن أن يتم من خلال منظمة الشرطة الجنائية الدولية (الأنتربول).

كما نصت المادة 28 من ذات الإتفاقية، والتي تطبق في حالة عدم وجود معاهدة خاصة بالمساعدة المتبادلة، في فقراتها 2،3، و4، على أنه"

2- قد يشترط الطرف المطلوب منه توفير المعلومات أو المواد إستجابة لطلب الموجه إليه شريطة:

أ- وجوب الإحتفاظ بسرية طلب المساعدة المتبادلة في حالة عدم إمكانية الإستجابة له أو

ب- عدم إستخدام المعلومات أو المواد في غير التحريات والإجراءات المحددة في الطلب.

3- وفي حالة عدم قدرة الطرف الطالب على الإلتزام بالشروط الواردة في الفقرة 2 فأنه سوف يقوم فورا بإخطار الطرف الآخر بذلك فيقوم في حينه الطرف الآخر بتحديد إمكان إتخاذ القرار بتوفير المعلومات بالرغم من عدم إستيفاء الشروط الواردة في الفقرة الثانية من عدمه، عندما يقبل الطرف الطالب تلك الشروط فأنه يصبح ملزما بها.

4- يحق للطرف الذي يوفر معلومات أو مواد طبقا للشروط الواردة في الفقرة 2 أن يطلب من الطرف الآخر في ظل الشروط المشار إليها تقديم تفسير (إيضاح) لإستخدامه تلك المعلومات أو المواد التي تم توفيرها له"([1]).

ونص المشرع القطري على قواعد تنفيذ المساعدة القضائية الدولية المتبادلة لمكافحة جرائم نظام المعالجة الألية لمعطيات بصورة تفصلية في المواد 24و28, 33, 34, 35 من قانون رقم 14 لسنة 2014, المتعلق بإصدار قانون مكافحة الجرائم الإلكترونية, فنصت المادة 24 منه على أنه" يتولى النائب العام مسؤولية

[1]- مقتبس عن: محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 769-771.

وصلاحيات تلقي طلبات المساعدة القانونية المتبادلة أو الطلبات تسليم المجرمين من الجهات الأجنبية المختصة فيما يتعلق بالجرائم المنصوص عليها في هذا القانون، ويتعين عليه تنفيذ هذه الطلبات أو إحالتها إلى الجهة المختصة بتنفيذها في أسرع وقت ممكن.

ويجوز في الحالات المستعجلة، إرسال تلك الطلبات عن طريق المنظمة الدولية للشرطة الجنائية (الإنتربول) وبشكل مباشر من الجهات الأجنبية المختصة، إلى الجهة المختصة في الدولة، وفي هذه الحالات يتعين على الجهة التي تستلم الطلب إبلاغ النائب العام بذلك.

وترسل الطلبات والردود إما بواسطة البريد أو بأي وسيلة أخرى أسرع تتيح الحصول على سجل كتابي بالإستلام أو مايعادله في ظروف تسمح للدولة بالتحقق من صحتها، وفي جميع الأحوال، ترفق الطلبات ومرفقاتها بترجمة ملخصة لها باللغة العربية".

ونصت المادة 28 من ذات القانون على أنه" يجب التقيد بسرية الطلب إذا إشترط فيه ذلك، وفي حالة عدم إمكانية التقيد بذلك، يجب إخطار الجهة الطالبة على الفور".

ونصت المادة 33 من ذات القانون على أنه" تنفذ طلبات إتخاذ تدابير التحقيق وفقا للقواعد الإجرائية المعمول بها في الدولة، وذلك ما لم تطلب الجهة الأجنبية المختصة إتباع إجراءات معينة لا تتعارض مع تلك القواعد.

ويجوز أن يحضر تنفيذ التدابير موظف عام تفوضه الجهة الأجنبية المختصة".

ونصت المادة 34 من ذات القانون على أنه" تنفذ طلبات إتخاذ التدابير المؤقتة وفقا لقانون الإجراءات الجنائية المشار إليه، وإذا كان الطلب مصاغا بعبارات عامة، تطبق التدابير الأكثر ملائمة وفقا للقانون.

فإذا كانت التدابير المطلوبة غير منصوص عليها في قانون الإجراءات الجنائية المشار إليه، يجوز للجهة المختصة أن تستبدلها بما ينص عليه ذلك القانون من تدابير يكون أكثرها مماثلا قدر الإمكان للتدابير المطلوبة.

وتسري الأحكام المتعلقة برفع التدابير المؤقتة على النحو المنصوص عليه في هذا القانون، ويتعين قبل الأمر برفع التدابير المؤقتة إبلاغ الدولة طالبة المساعدة بذلك".

ونصت المادة 35 من القانون ذاته على أنه " في حالة تلقي الجهة المختصة طلب للمساعدة القانونية المتبادلة لإصدار أمر بمصادرة، يتعين على الجهة المذكورة إحالة الطلب إلى النيابة العامة لإستصدار أمر المصادرة، وتنفيذ هذا الأمر في حالة صدوره.

ويسري أمر المصادرة على الأجهزة وأنظمة المعلومات والبرامج والوسائل المستخدمة المنصوص عليها في أحكام المصادرة المنصوص عليها في هذا القانون، والموجودة على أراضي الدولة.

ويتعين على الجهة المختصة، لدى تنفيذها أمر المصادرة، أن تلتزم بالوقائع التي تم الإستناد إليها لإصدار الأمر"([1]).

أما بالنسبة المشرع الجزائري فنص على قواعد تنفيذ المساعدة القضائية الدولية المتبادلة في المادتين 16 و17 من القانون 09-04، السالف الذكر، بحيث تنص المادة 16 منه على أنه" في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم....

يمكن، في حالة الإستعجال، ومع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة أعلاه، إذا وردت عن طريق وسائل الإتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها"([2]).

ويتضح من هذه المادة أن تبادل المساعدة القضائية الدولية لجمع الإدلة المتعلقة بهذه الجريمة يكون في الشكل الإلكتروني نظرا للطابع الخاص لهذه الجرائم، بحيث أجاز المشرع الجزائري في حالة الإستعجال قبول طلبات المساعدة القضائية

---

[1]- المواد 24، 28، 33، 34، و35 من القانون القطري رقم (14) لسنة 2014.

[2]- المادة 16 من القانون 09-04.

حتى وأن وردت عن طريق وسائل الإتصال السريعة مثل الفاكس أو البريد الإلكتروني شريطة التأكد من صحتها، وتطبيقا لذلك نصت المادة 36 في فقرتها الثانية من الأمر رقم 05-06 الصادر بتاريخ 23 أوت 2005، المتعلق بمكافحة التهريب، على أنه" إذا ما وجه الطلب إلكترونيا يمكن تأكيده بواسطة أي وسيلة تترك أثرا مكتوبا"([1]).

ونصت المادة 17 من من القانون 09-04، على أنه" تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو إتخاذ أي إجراءات تحفظية وفقا للإتفاقيات الدولية ذات الصلة والإتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل"([2]).

والملاحظ أن هذه المادة أشارت إلى أنه تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات التي تتم على مستوى الدول إما بطريقة مباشرة (من دولة إلى دولة) أو من خلال المنظمة الدولية أو الأقليمية لتحديد هوية الأشخاص المشتبه في ضلوعهم في تلك الجرائم وتحديد أماكن وجودهم تمهيدا للقبض عليهم.

فضلا عن ذلك، فإن تبادل الدول المعلومات بالنسبة للوسائل والأساليب التي يستخدمها مرتكبي هذه الجرائم ، والتي تتسم بالتطور السريع والمستمر، يسهل من مهمة التصدي لتلك الجرائم، ويستوجب أن يتم تبادل تلك المعلومات بشكل أكثر سرعة دون إنتظار عقد إجتماعات ومؤتمرات لعرض تلك المعلومات وإستعراض هذه الأساليب([3]).

كما يمكن أن يتم إتخاذ إجرات تحفظية كالتحفظ على البيانات المعلوماتية أو التحفظ العاجل على البيانات المعلوماتية المخزنة، وذلك وفقا للإتفاقيات الدولية ذات الصلة والإتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل.

وبناء على ما سبق، فإن تنفيذ طلبات المساعدة القضائية الدولية المتبادلة في مجال مكافحة جرائم نظام المعالجة الآلية للمعطيات، يتم من خلال تبادل المعلومات

---

1- المادة 36 الفقرة 2 من الأمر رقم 05-06 المؤرخ في 23 أوت سنة 2005، المتعلق بمكافحة التهريب ، ج ر ج ج، ع 59 المؤرخة في 28 غشت سنة 2005.

2- المادة 17 من القانون 09-04.

3- محمد كمال محمود الدسوقي، مرجع سابق، ص 148، 149 .

أو إتخاذ أي إجراءات تحفظية من إجل جمع الإدلة المتعلقة بهذه الجرائم العابرة للحدود في إطار الإتفاقيات الدولية ذات الصلة والإتفاقيات الثنائية ومبدأ المعاملة بالمثل، وذلك وفقا للتوجيهات الواردة في هذه الطلبات التي تقتضي الحفاظ على سريتها ومحتوياتها وعدم إستخدام تلك المعلومات أو الأدلة لأي إستخدام في غير ما هو موضح في هذه الطلبات.

كما يجب أن تتوافر هذه الطلبات الواردة في الإتفاقيات على إجراءات سريعة ونظام إتصال يسمح للجهات القائمة على التحقيق بالإتصال بجهات أجنبية لجمع أدلة معينة([1])، ومن الأمثلة الواقعية لتنفيذ طلبات المساعدة القضائية الدولية، تمت متابعة ومحاكمة شاب جزائري وهو طالب جامعي بقسم الإعلام الآلي بعنابة من طرف سلطات الأمن الجزائري، وهذا الشاب تمكن من قرصنة عدد كبير من البطاقات البنكية عقب إختراقه لمواقع إلكترونية لمؤسسات أجنبية في أروبا والولايات المتحدة الأمريكية وكندا، وتمكن من سحب أموال معتبرة، وأثر المعلومات المتبادلة مع الأمن الجزائري في إطار المساعدة القضائية تمت متابعة البريد الإلكتروني الذي يستعمله "الهاكرز" المتهم المشار له والذي أدين من طرف محكمة الجنح بعنابة([2]).

وعليه، فإنه وجب العمل على إبرام إتفاقيات دولية ذات صلة أو ثنائية تنطوي على نصوص واضحة تتضمن كيفية تنفيذ المساعدة القضائية الدولية المتبادلة كآلية دولية فعالة لمكافحة جرائم نظام المعالجة الآلية للمعطيات، مع كفالتها في الوقت نفسه الحماية لحقوق الأفراد وحرياتهم وسيادة الدول.

**الفرع الثاني: رفض تنفيذ طلبات المساعدة القضائية الدولية المتبادلة**

نصت إتفاقية بودابست على حالات رفض تنفيذ طلبات المساعدة المتبادلة في المادة 27 في فقراتها 4،5،6، و7، بقولها"

4- يجوز للطرف المطلوب منه أن يرفض المساعدة المتبادلة إضافة إلى الأسس الأخرى الخاصة بالرفض والموضحة بالمادة 25 فقرة 4 على الأسس التالية:-

---

[1]- علي حسن الطوالبة، مقال بعنوان التعاون القضائي الدولي في مجال مكافحة الجرائم الإلكترونية، مركز الإعلام الأمني، ص 6.

[2]- مقتبس عن: زبيحة زيدان، مرجع سابق، ص 147.

أ- إذا كان الطلب يخص فعلة يعتبرها الطرف المطلوب منه جريمة سياسية أو جريمة متصلة بجريمة سياسية.

ب- إذا ما إعتبر أن تنفيذ الطلب ماسا بسيادته، أمنه، نظامه العام أو مصالح هامة أخرى.

5- يجوز للطرف المطلوب منه تأخير إتخاذ القرار في شأن الطلب إذا كان القرار يهدد تحريات جنائية أو إجراءات جنائية تتولاها سلطات الطرف المطلوب منه.

6- قبل رفض الطلب أو تأجيل المساعدة سوف يكون للطرف المطلوب منه حيثما كان ذلك ملائما وبعد التشاور مع الطرف الطالب الحق في النظر في مدى الموافقة جزئيا أو رهنا بشروط محددة على هذا الطلب حيثما رأى لزوم ذلك.

7- سوف يقوم الطرف المطلوب منه بسرعة بإخطار الطرف الطالب بنتائج تنفيذ طلب المساعدة وفي حالة رفض أو تأجيل تنفيذ الطلب فإن عليه أن يوضح أسباب الرفض أو التأجيل، كما إن الطرف المطلوب منه سوف يقوم بإعلام الطرف الطالب بأية أسباب تجعل تنفيذ الطلب امرا مستحيل التنفيذ أو توفر تنفيذه"([1]).

كما نصت المادة 35 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، على حالات رفض المساعدة، بقولها" يجوز للدولة الطرف المطلوبة منها المساعدة-بالإضافة إلى أسس الرفض المنصوص عليها في المادة الثانية والثلاثين الفقرة (4) أن ترفض المساعدة إذا:

1- كان الطلب متعلقا بجريمة يعتبرها قانون الدولة الطرف المطلوب منها المساعدة جريمة سياسية.

2- اعتبر أن تنفيذ الطلب يمكن أن يشكل إنتهاكا لسيادته أو أمنه أو نظامه أو مصالحه الأساسية"([2]).

ونصت المادة 31 من القانون القطري رقم 14 لسنة 2014، السالف الذكر، على حالات رفض تنفيذ طلبات المساعدة القضائية الدولية، بقولها" لا يجوز رفض طلب المساعدة القانونية المتبادلة إلا في الحالات الآتية:

---

[1]- مقتبس عن: محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، مرجع سابق، ص 845،846.

[2]- المادة 35 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

1- إذا لم يكن الطلب صادر عن جهة مختصة طبقا لقانون الدولة التي تطلب المساعدة، أو إذا لم يرسل الطلب وفقا للقوانين المعمول بها، أو إذا كانت محتوياته تتضمن مخالفة جوهرية لأحكام هذا القانون أو أي قانون آخر.

2- إذا كان تنفيذ الطلب يحتمل أن يمس بأمن الدولة أو سيادتها أو نظامها العام أو مصالحها الأساسية.

3- إذا كانت الجريمة التي يتعلق بها الطلب، تمثل موضوع دعوى جنائية منظورة أو فصل فيها بحكم قضائي في الدولة.

4- إذا كانت هناك أسباب جوهرية تدعو للعتقاد بأن التدبير أو الأمر المطلوب إصداره لا يستهدف الشخص المعني إلا بسبب عنصره أو ديانته أو جنسيته أو عرقه أو آرائه السياسية أو جنسه أو حالته.

5- إذا كانت الجريمة المذكورة في الطلب غير منصوص عليها في قوانين الدولة، وفقا لحكم المادة (23/فقرة ثانية) من هذا القانون، ومع ذلك فإنه يتعين خلافا لذلك تقديم المساعدة إذا كانت لا تنطوي على تدابير جبرية.

6- إذا كان من غير الممكن إصدار أمر بإتخاذ التدابير المطلوبة أو تنفيذها بسبب قواعد التقادم المنطبقة على الجريمة المنصوص عليها في هذا القانون بمقتضى قوانين الدولة أو الدولة التي تطلب المساعدة.

7- إذا كان الأمر المطلوب تنفيذه غير قابل للنفاذ بمقتضى القانون.

8- إذا كان إصدار القرار في الدولة الطالبة، قد جرى في ظروف لم تتوفر فيها الضمانات الكافية فيما يتعلق بحقوق المتهم".

كما نصت المادة 32 من ذات القانون، على أنه" لا يجوز رفض طلب المساعدة القانونية المتبادلة، إستنادا إلى شروط مقيدة بشكل مبالغ فيه.

ويخضع القرار الصادر بشأن طلب المساعدة القانونية المتبادلة، للطعن عليه وفقا للقواعد القانونية المقررة.

وفي حالة رفض تنفيذ الطلب، يتعين على النائب العام أو الجهة المختصة، إبلاغ الجهة الأجنبية المختصة على الفور، بأسباب الرفض"([1]).

[1]- المادتين 31 و32 من القانون القطري رقم (14) لسنة 2014.

أما بالنسبة للمشرع الجزائري فقد نص في المادة 18 من القانون 09-04، السالف الذكر، على القيود الواردة على تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، بقولها" يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن إن تكون الإستجابة لطلبات المساعدة مقيدة بشرط المحافظة على على سرية المعلومات المبلغة أو بشرط عدم إستعمالها في غير ما هو موضح في الطلب"([1]).

ونستشف من هذه المادة أن المشرع الجزائري يرفض تنفيذ طلبات المساعدة القضائية الدولية، إذا كان من من شأنها المساس بالسيادة الوطنية أو المساس بالنظام العام، وفي المقابل يمكن الإستجابة لها مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم إستعمالها في غير ما هو موضح في الطلب.

وفي هذا السياق نصت المادة 6 في الفقرة الأولى في النقطة أ من إتفاقية تتعلق بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية والبوسنة والهرسك، على ما يلي:" 1- يرفض التعاون القضائي إذا:

أ- كان تنفيذ الطلب من شأنه المساس بالسيادة أو بالأمن أو بالنظام العام للطرف المطلوب منه التعاون"([2]).

لذلك فإنه يجب من الناحية العملية على الدولة المطلوب منها المساعدة أن تقوم قبل تأجيل أو رفض المساعدة بإجرائين هامين وهما:

أولا: إخطار الدولة الطالبة فورا بسبب إعتزامها تأجيل أو رفض الطلب.

ثانيا: التشاور مع الدولة الطالبة لتحديد ما إذا كانت المساعدة يمكن أن تمنح وفق بنود وشروط معينة قد تراها الدولة المطلوب إليها ضرورية، فإذا قبلت الدولة الطالبة المساعدة وفقا لهذه الشروط كان عليها أن تتقيد بها، أما إذا ما رفضت الدولة المطلوب إليها المساعدة أو طلبت تأجيلها كان عليها أن تخطر الدولة الطالبة باسباب الرفض أو التأجيل حسب الأحوال، وتطبيقا لذلك نصت المادة السابعة عشر

---

[1]- المادة 18 من القانون 09-04.

[2]- المادة 6 الفقرة 1 النقطة أ من إتفاقية تتعلق بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية والبوسنة والهرسك، ج ر ج ج، ع 36، المؤرخ في 17 يونيو سنة 2020، ص 10.

من إتفاقية التعاون بين مصر وفرنسا على أن" كل رفض للتعاون القضائي يجب أن يكون مسببا([1]).

**المطلب الثاني: المجالات الخاصة بالمساعدة القضائية الدولية المتبادلة لمكافحة جرائم نظام المعالجة الآلية للمعطيات.**

تتمتع المساعدة القضائية الدولية المتبادلة بأهمية كبيرة في مجال مكافحة جرائم نظام المعالجة الآلية للمعطيات بصفة خاصة، حيث أن جرائم الدخول أو البقاء غير المشروع في نظام المعالجة الآلية والتلاعب بالمعطيات تمثل الصورة الحقة لهذه الجرائم العابرة للحدود الدولية، ذلك أن العديد من الإجراءات الرسمية المتعلقة بمجالات المساعدة القضائية الدولية المتبادلة التقليدية أثناء تبادل المعلومات ونقل الإجراءات تتسم بنوع من البطء والتعقيد الذي لا يتناسب مع طبيعة هذه الجرائم .

لذا فإنه كان من اللازم إستحداث وسائل أكثر سعة وفاعلية لمكافحة جرائم نظام المعالجة الآلية للمعطيات، تمكن من الحصول على المعلومات بصورة عاجلة، وهو ما تضمنته الإتفاقيات الخاصة بالجرائم المعلوماتية مثل إتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة 2001 والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، من خلال إستحداثها لبعض صور مجالات التعاون القضائي التي تتناسب مع طبيعة هذه الجرائم، وتتمثل في المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة والمساعدة القضائية في مجال سلطات التحقيق.

وسنقوم بدراسة كل مجال على حدى من خلال الفرعين التاليين، فنتناول في الفرع الأول المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة، أما الفرع الثاني نخصصه للمساعدة القضائية في مجال سلطات التحقيق.

**الفرع الأول: المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة**

تشمل المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة المجالين الآتيين وهما:

- التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي

---

[1]- محمد علي سويلم، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، مرجع سابق، ص 776،777.

- الإفشاء العاجل لسرية بيانات المرور المتحفظ عليها.

**أولا: التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي**

تناولت هذا الإجراء المادة 29 من إتفاقية بودابست، والتي نصت على أنه"

1- يجوز لأي طرف أن يطالب طرف آخر أن يأمر أو بالأحرى يتحفظ على بيانات مخزنة، بواسطة نظام كومبيوتر، يقع داخل أقليم ذلك الطرف الآخر والتي بشأنها ينوي الطرف الطالب تقديم طلب المساعدة المتبادلة من أجل البحث أو الدخول على أو مصادرة أو تأمين أو كشف هذه البيانات...

3- عند إستلام الطلب من الطرف الآخر، يقوم الطرف المطلوب منه، بإتخاذ كافة الإجراءات الملائمة وذلك لسرعة التحفظ على البيانات المحددة وفقا للقانون الوطني، لأغراض الإستجابة، لا يلزم وجود إزدواجية في الجريمة كشرط لتوفير مثل هذا التحفظ.

4- يجوز لأي طرف يشترط وجود إزدواجية في الجريمة كشرط للإستجابة لطلب المساعدة المتبادلة من أجل البحث في بيانات الكومبيوتر، أو الدخول عليها، أو مصادرتها أو تأمينها أو الكشف عنها بالنسبة للجرائم خلاف تلك المنصوص عليها وفقا للمواد من 2-11 من هذه الإتفاقية، أن يحتفظ بالحق في رفض طلب التحفظ بموجب هذه المادة في الحالات التي يتوافر لديه فيها أسباب تدعوه للإعتقاد بأنه في وقت عملية الكشف أو الإفصاح عن هذه المعلومات بتعذر إستيفاء الشرط الخاص بوجود إزدواجية في الجريمة([1]).

والملاحظ أن هذه المادة أقرت آلية فعالة على المستوى الدولي لمكافحة الجرائم المعلوماتية بصفة عامة، بحيث سمحت الفقرة الأولى من هذه المادة لكل طرف أن يطلب، أما الفقرة الثالثة فقررت أنه على طرف أن يكون لديه الطرق القانونية للحصول على التحفظ العاجل على بيانات مخزنة لدى نظام معلوماتي في أقليم الطرق المقدم إليه الطلب، حتى لا يتم تغيير هذه البيانات، أو نقلها، أو حذفها،

[1]- مقتبس عن: محمد كمال محمود الدسوقي، مرجع سابق، ص 156،157 .

خلال الفترة الزمنية اللازمة لإعداد ونقل وتنفيذ طلب المساعدة المتبادلة بخصوص الحصول على هذه البيانات([1]).

ونصت المادة 37 في فقراتها 1،3،4، و5، من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، في نفس السياق، على أنه"

1- لأي دولة طرف أن تطلب من دولة أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلبا بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات.

3- عند إستلام إحدى الدول الأطراف الطلب من دولة طرف أخرى فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل عاجل بحسب قانونها الداخلي، ولغايات الإستجابة إلى الطلب فلا يشترط وجود إزدواجية التجريم للقيام بالحفظ.

4- إي دولة طرف تشترط وجود إزدواجية التجريم للإستجابة لطلب المساعدة يجوز لها في حالات الجرائم عدا المنصوص عليها في الفصل الثاني من هذه الإتفاقية، أن تحتفظ بحقها برفض طلب الحفظ حسب هذه المادة إذا كان هناك سبب للإعتقاد بأنه لن يتم تلبية شرط إزداواجية التجريم في وقت الكشف.

5- بالإضافة لذلك، يمكن رفض طلب الحفظ إذا:

أ- تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية.

ب- إعتبار الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها"([2]).

أما بالنسبة للمشرع الجزائري فقد نص على إجراء التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي في المادة 17 من القانون 09-04، على هذا الإجراء

---

[1]- هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص 279.

[2]-المادة 37 في فقراتها 1،3،4، و5 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

بقولها" ...أو إتخاذ أي إجراءات تحفظية وفقا للإتفاقيات الدولية ذات الصلة أو الإتفاقيات الثنائية ومبدأ المعاملة بالمثل"([1]).

والمساعدة المتبادلة في التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي هو أمر ضروري تستلزمه طبيعة الأدلة في جرائم نظام المعالجة الآلية للمعطيات، وذلك لتفادي إي تغيير في هذه الأدلة أونقلها أو إتلافها أو محو آتار الجريمة خلال تلك المدة التي تستغرقها إجراءات طلب المساعدة المساعدة المتبادلة للحصول على تلك البيانات بالطرق التقليدية.

وإن عملية التحفظ عبارة عن إجراء ذو طبيعة وقتية للتدخل بطريقة أكثر سرعة من مجرد تنفيذ إلتماس أوطلب المساعدة المتبادلة التقليدية، كما أن هذا الإجراء ليس فيه مساس بسرية المعلومات والبيانات محل الإجراء الوقتي موضوع الطلب فلا يتم كشفها ولا فحصها من قبل سلطات إنفاذ القانون إلا في بعض الحالات ووفقا للشروط المقررة قانونا بما يكفله حق الشخص المعني بالخصوصية في سرية معلوماته([2]).

**ثانيا: الإفشاء العاجل لسرية بيانات المرور**

نصت المادة 30 في فقرتها الأولى من إتفاقية بودابست، على أنه"

1- في حالة إذا ما أكتشف الطرف المطلوب منه، أثناء تنفيذ الطلب المقدم إليه وفقا للمادة (29) من أجل التحفظ على خط سير بيانات تتعلق بإتصال محدد، أن أحد مقدمي الخدمة في دولة أخرى مشتركا في نقل الإتصال يقوم الطرف المطلوب منه على الفور بالكشف عن القدر الكافي من خط سير البيانات للتعرف على مقدم الخدمة هذا والمسار الذي سلكه الإتصال"([3]).

وفي نفس السياق نصت المادة 38 في فقرتها 1 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، على أنه"

1- حينما تكشف الدولة المطلوب منها -في سياق تنفيذ الطلب حسب المادة السابعة والثلاثين لحفظ معلومات تتبع المستخدمين الخاصة بإتصالات معينة- بأن مزود

---

1- المادة 17 من القانون 09-04.

2- محمد كمال محمود الدسوقي، مرجع سابق، ص 157،158.

3- مقتبس عن: هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص 284.

خدمة في دولة أخرى قد إشترك في بث الإتصال فيجب على الدولة الطرف المطلوب منها أن تكشف للدولة الطرف الطالبة قدرا كافيا من معلومات تتبع المستخدمين من أجل تحديد مزود الخدمة ومسار بث الإتصالات"([1]).

وبتجسد الإفشاء العاجل لسرية بيانات المرور عندما يقوم الطرف المقدم إليه الطلب بتنفيذ ما طلب منه بالتحفظ على بيانات المرور المتعلقة بنقل الإتصال بواسطة مزودي الخدمة بفرض تتبع مصدر الإتصال لتحديد هوية فاعل الجريمة أو تجميع الأدلة القاطعة، بيدا أنه قد يكتشف أثناء ذلك أن بيانات المرور التي وجدت في أقليمه تشير إلى أن الإتصال قد تم إرساله من خلال مزود خدمات موجود في أقليم دولة ثالثة أو حتى في أقليم الدولة مقدمة الطلب([2])، فأنه في هذه الحالة يجب على الدولة المقدم إليها الطلب أن تقوم بالكشف للدولة الطالبة عن القدر الكافي من البيانات من خط سير البيانات الذي يمكنه من التعرف على مزود الخدمة هذا والمسار الذي سلكه الإتصال، وفي ذلك فائدة للدولة مقدمة الطلب بحيث تتمكن من خلال هذه المساعدة معرفة الدولة التي تقدم إليها طلب المساعدة العاجلة بشأن التحفظ على البيانات والمعلومات المخزنة في النظام المعلوماتي، وبالتالي يتم الوصول إلى المصدر الحقيقي للإتصال([3]).

**الفرع الثاني: المساعدة القضائية المتبادلة في مجال سلطات التحقيق**

يمكن لسلطات التحقيق تبادل المساعدة القضائية الدولية في عدة مجالات تشمل المساعدة المتبادلة بالولوج إلى البيانات المعلوماتية المخزنة والوصول إليها عبر الحدود، والجمع الفوري لبيانات المرور وكذا إعتراضها.

**أولا: المساعدة المتبادلة بالولوج إلى البيانات المعلوماتية المخزنة في النظم المعلوماتية**

نصت المادة 31 من إتفاقية بودابست، على المساعدة المتبادلة بالولوج إلى البيانات المعلوماتية المخزنة في النظم المعلوماتية، بقولها"

---

1- المادة 38 الفقرة 1 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

2- هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص 285.

3-محمد كمال محمود الدسوقي، مرجع سابق، ص 159،160.

1- بمقدور كل طرف أن يطلب من الطرف الآخر أن يفتش أو أن يقوم بالولوج إلى البيانات المعلوماتية المخزنة في نظام معلوماتي يتواجد على أرض هذا الطرف الآخر، لضبطها أو الحصول عليها أو الكشف عنها، بما في ذلك البيانات التي تم التحفظ عليها تبعا للمادة 30.

2- يجب على الطرف المقدم إليه الطلب أن يستجيب لهذا الطلب من من خلال تطبيق المعاهدات الدولية والإتفاقيات والتشريعات المشار إليها في المادة 23، وعلى نحو يتوافق مع البنود الأخرى المتصلة بذلك الفصل..." ([1]).

وتتشابه هذه المادة مع البند "ج" من الفقرة 2 من المادة (18) من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والخاصة بتقديم المساعدة القانونية المتبادلة بالكامل بمقتضى قوانين الدولة متلقية الطلب ومعاهداتها وإتفاقاتها وترتيباتها ذات الصلة، بشأن تنفيذ عمليات التفتيش والضبط والتجميد([2]).

وفي نفس السياق نصت المادة 39 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، على أنه"

1- يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها بحسب المادة السابعة والثلاثين.

2- تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقا للأحكام الواردة في هذه الإتفاقية.."([3]).

ويتضح من خلال هذه النصوص أنه يمكن لسلطات تحقيق دولة طرف في هذه الإتفاقيات بمناسبة تحقيقات تجريها في جرائم النظام أن تطلب من دولة طرف أخرى يقع على إقليمها النظام المعلوماتي الولوج إلى البيانات المعلوماتية المخزنة فيه لضبطها أو تأمينها أو الحصول عليها أو الكشف عنها أو مصادرتها، وأن تكون هذه

---

1- مقتبس عن: هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص 287،288.

2- محمد كمال محمود الدسوقي، مرجع سابق، ص 160.

3- المادة 39 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

الدولة مؤهلة لتلبية تلك الطلبات من الناحية الفنية والتقنية، وذلك فقا للأحكام الواردة في هذه الإتفاقيات.

**ثانيا: الوصول عبر الحدود إلى البيانات المعلوماتية المخزنة بموافقة صريحة أو من خلال إتاحتها للجمهور**

هذا المجال تضمنته المادة 32 من إتفاقية بودابست، فنصت على أنه" يمكن لأي طرف دون تصريح من الطرف الآخر:

أ- أن يصل إلى البيانات المعلوماتية المخزنة والمتاحة للجمهور (مصدر مفتوح) بغض النظر عن موقعها الجغرافي، أو

ب- أن يصل، أو أن يتلقى عبر نظام معلوماتي يقع على أقليمه، بيانات معلوماتية مخزنة في دولة أخرى، إذا حصل هذا الطرف على موافقة قانونية وإرادية من شخص لديه سلطة قانونية للكشف عن هذه البيانات إلى هذا الطرف من خلال هذا النظام المعلوماتي"([1]).

وفي نفس السياق، نصت المادة 40 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، على أنه" يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى:

1- أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة(مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات.

2- أن تصل أو تستقبل- من خلال تقنية المعلومات في إقليمها- معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة"([2]).

ومن تم فإنه يمكن لسلطات تحقيق دولة طرف في هذه الإتفاقيات بمناسبة تحقيقات تجريها في جرائم النظام، وبدون الحصول على تصريح أو تفويض من أي طرف آخر، الدخول عبر الحدود إلى البيانات المعلوماتية المخزنة في نظام

---

1- مقتبس عن: هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص 288.

2- المادة 40 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

معلوماتي لدولة أخرى، حيثما تكون متاحة علنا للجمهور أو بعد الحصول على موافقة صريحة من الشخص الذي يملك السلطة القانونية في الكشف عن هذه البيانات.

**ثالثا: المساعدة المتبادلة بخصوص جمع بيانات المرور في الوقت الفعلي**

نصت المادة 33 من إتفاقية بودابست، على المساعدة المتبادلة بخصوص جمع بيانات المرور في الوقت الفعلي، بقولها"

1- يجب على الأطراف أن تقدم المساعدة المتبادلة إلى بعضها البعض بالنسبة لجمع بيانات المرور في الوقت الفعلي، والتي تكون مرتبطة بإتصالات معينة على أرضهم، ومرسلة عن طريق نظام معلوماتي، ووفقا للأوضاع المنصوص عليها في الفقرة "2" فإن هذه المساعدة، سوف تحكمها الشروط والإجراءات المنصوص عليها في القانون الداخلي.

2- يجب على كل طرف أن يقدم هذه المساعدة على الأقل فيما يتعلق بالجرائم الجنائية من حيث جميع بيانات المرور في الوقت الفعلي التي يمكن أن تكون متاحة في قضية موازية على المستوى الداخلي"([1]).

وفي نفس السياق، نصت المادة 41 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، على أنه"

1- على الدول الأطراف توفير المساعدة الثنائية لبعضها البعض بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لإتصالات معينة في إقاليمها والتي تبث بواسطة تقنية المعلومات.

2- على كل دولة طرف توفير تلك المساعدة على الأقل بالنسبة للجرائم التي يتوفر فيها الجمع الفوري لمعلومات تتبع المستخدمين لمثيلتها من القضايا الداخلية"([2]).

والملاحظ أنه في حالات كثيرة لا يكون بمقدور سلطات التحقيق ضمان تتبع خط سير بيانات المرور للوصول إلى مصدرها من خلال تتبع أثرها، فوجب على كل

---

[1]- مقتبس عن: هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص 290،291.

[2]- المادة 41 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

الأطراف أن تقدم المساعدة المتبادلة إلى بعضها البعض بصورة عاجلة وفي الوقت الفعلي بالنسبة لجمع بيانات المرور.

وفي العديد من الدول يتم توفير المساعدة المتبادلة لأمر جوهري يتعلق بالتجميع في الوقت الفعلي للبيانات الخاصة بالمرور، لأن هذا التجميع يكون أقل تطفلا أو تدخلا من إعتراض بيانات المحتوى أو التفتيش أو الضبط.

كما أن تجميع بيانات المرور بصورة عاجلة وفي الوقت الفعلي قد يكون الطريقة الوحيدة الجوهرية لتحديد هوية مرتكب جرائم النظام، باعتباره الإجراء الأقل تطفلا أو تدخلا، فأن الفقرة 2 لكلا المادتين قد إستخدمت مصطلح (على الأقل) لتشجيع جميع الدول الأطراف على السماح بأوسع نطاق ممكن للمساعدة المتبادلة بهذا الشأن حتى في ظل غياب مبدأ التجريم المزدوج([1]).

**رابعا: المساعدة المتبادلة في مسألة إعتراض بيانات المحتوى**

نصت المادة 34 من إتفاقية بودابست على المساعدة المتبادلة في مسألة إعتراض بيانات المحتوى، بقولها" يقدم الأطراف المساعدة المتبادلة لبعضهم البعض، فيما يتعلق بتجميع أو تسجيل محتوى البيانات بصورة عاجلة والتي تتعلق بإتصالات محددة يتم نقلها بواسطة نظام كومبيوتر وذلك بالحد الذي تجيزه الإتفاقيات والقوانين الوطنية واجبة التطبيق"([2]).

وفي نفس السياق، نصت المادة 42 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، على أنه" تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضهما فيما يتعلق بالجمع الفوري لمعلومات المحتوى لإتصالات معينة تبث بواسطة تقنية المعلومات إلى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية"([3]).

ونظرا لما يشكله الجمع الفوري لمحتوى بيانات المرور من مساس بحقوق الأفراد في الخصوصية، باعتباره ينطوي على تجميع وتسجيل البيانات التي يتم نقلها بواسطة نظام معلوماتي معين، فقد تم تحديد الإلتزام بتوفير المساعدة المتبادلة

---

1- هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص 292.

2- مقتبس عن: مناصرة يوسف، مرجع سابق، ص 376.

3- المادة 42 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

المتعلقة بإعتراض بيانات المحتوى ، بحيث يجب تقديمها في الحدود التي تسمح بها المعاهدات والقوانين الداخلية المطبقة لدى الدول.

وبما أن التطبيق العملي للمساعدة المتبادلة المتعلقة بإعتراض بيانات المحتوى له تداعياته، فقد تم إتخاذ قرار بخصوص هذا الإجراء، وذلك بأن يتم تنظيمه وفقا للقوانين الداخلية المعمول بها من حيث مدى الإلتزام بتقديم هذا النوع من المساعدة والقيود التي ترد عليه([1]).

وبالمجمل يمكن القول أن المساعدة القضائية الدولية المتبادلة تعتبر آلية دولية فعالة لمكافحة جرائم نظام المعالجة الآلية المعطيات ذات البعد الدولي والمرتكبة في بيئة إفتراضية، لذا فإن تنفيذها وفق القواعد المنصوص عليها في الإتفاقيات الدولية ذات الصلة والإتفاقيات الثنائية ومبدأ المعاملة بالمثل، وإستحداث مجالات خاصة بالمساعدة القضائية الدولية للمواجهة هذا النوع من الإجرام، يتلائم مع طبيعة هذه الجرائم التي تقتضي التعامل مع أدلة رقمية غير ملموسة وسريعة الزوال.

1- هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مرجع سابق ، ص 293.

## خلاصة الباب الثاني

إتجهت غالبية الدول كمرحلة أولى إلى تعديل قوانينها الإجرائية بصفة دورية ومستمرة بما يضمن مواكبة متغيرات وتطورات جرائم النظام، وإلى إرساء قواعد قانونية جديدة تواجه المشكلات المعاصرة التي أسفرت عنها هذه الجرائم المستحدثة وتطوراتها اللامتناهية، ثم قامت كمرحلة ثانية باستحداث نصوص قانونية خاصة أكثر إنسجاما مع الطبيعة الخاصة لهذه الجرائم، بحيث قام المشرع الجزائري كمرحلة أولى بتعديل قانون الإجراءات الجزائية بصفة دورية ومستمرة لمكافحة جرائم ذات خطورة بالغة حددها على سبيل الحصر من بينها جرئم المساس بأنظمة المعالجة الآلية للمعطيات، ثم قام كمرحلة ثانية بسنه القانون 09-04،السالف الذكر، الذي يمثل الجانب الإجرائي لكافة جرائم تكنولوجيات الإعلام والإتصال بما فيها جرائم نظام المعالجة الآلية للمعطيات، وتضمن جملة من التدابير المستحدثة غير المألوفة في القوانين السابقة والأكثر ملائمة مع خصوصيات جرائم نظام المعالجة الآلية للمعطيات، تتنوع بين تدابير وقائية تتمثل في مراقبة الإتصالات الإلكترونية والإلتزمات المترتبة على مقدمي الخدمة وأخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائية وتتمثل في تفتيش الإنظمة المعلوماتية وحجز المعطيات المعلوماتية، باعتبارهما إجراءين حاسمين خلال التحقيق في هذه الجرائم، وملائمين كذلك لخصوصية الدليل الرقمي الذي يتم الحصول عليه من خلالهما.

فضلا عن ذلك، فإن البعد الدولي لهذه الجرائم فرض على المجتمع الدولي ضرورة البحث عن وسائل أكثر ملائمة لطبيعة جرائم نظام المعالجة الآلية للمعطيات، والعمل على تضييق الثغرات القانونية التي برع مرتكبوها في إستغلالها لتهرب من العقاب ونشر نشاطهم الإجرامي في مناطق مختلفة من أنحاء العالم، وذلك من خلال وجود آليات تلزم الدول بتوحيد تشريعاتها المختلفة بشأن قواعد الإختصاص والسهر على تطبيقها، ووجوب تفعيل آليات المساعدة القضائية الدولية المتبادلة بالنسبة لتبادل المعلومات في هذه الجرائم والمساعدة على التحقيق فيها وتتبع مرتكبيها، وهذا كله وفقا للقواعد التي تقررها الإتفاقيات الثنائية أو المتعددة الأطراف أو وفقا لمبدأ المعاملة بالمثل.

# الخاتمة

## خاتمة

إن نظام المعالجة الآلية للمعطيات ينطبق على أي نظام مهما كان مسماه يحتوي على مجموعة من العناصر مرتبطة مع بعضها البعض تهدف الى تحقيق نتيجة معينة، وهي معالجة المعطيات، كما يقوم على أساس الروابط بين مختلف أجزاء النظام، ويتطلب الوجود المتزامن للأجهزة والبرامج والمعطيات.

إلا أن المساس بهذا النظام والإعتداء عليه إدى الى ظهور ما يعرف بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، وهي طائفة من الجرائم المعلوماتية، وتنحصر في المفهوم الضيق لها، إذن فهي جزء من كل، وقد تطرق لها المشرع الجزائري في قانون العقوبات بإستحداثها بقسم سابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، بحيث أن المساس بنظام المعالجة يختلف عن المساس بالمعطيات و البرامج، ويترتب على ذلك أن المساس بمكونات مادية معزولة أو معنوية معزولة لا يشكل مساسا بنظام المعالجة الآلية للمعطيات إلا إذا كانت جزءا منه، أو لها القدرة على ذلك، ويكون لها دورا في تحقيق الغاية الأساسية للنظام.

كما أنه وبالرغم من الجهود التي بذلت ولازالت تبذل لتكريس حماية جنائية فعالة لنظام المعالجة الآلية للمعطيات إلا إنها تبقى غير كافية في ظل غياب سياسة جنائية واضحة للتعامل مع هذه الطائفة من الجرائم ومرتكبيها، لا سيما بالنسبة للدول التي لم تبادر بعد إلى تعديل تشريعاتها بما يكفل تجاوز النصوص التقليدية التي أصبحت قاصرة في مكافحة هذا النوع من الإجرام.

ولقد توصلنا من خلال هذه الدراسة إلى النتائج والإقترحات التالية:

**أولا: النتائج**

1- إن المعطيات والبرامج هي جزء من نظام المعالجة الآلية للمعطيات، وإن الإعتداء على إحداها منفردا لا يعد إعتداء على هذا النظام أو مساسا به، ذلك أن الحماية الجنائية للنظام أوسع من الحماية الجنائية للمعطيات و البرامج.

2- إن نظام المعالجة الآلية للمعطيات يعتبر الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الإعتداء على نظام المعالجة، فإذا تخلف هذا الشرط لا

يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة بنظام المعالجة الآلية للمعطيات، والتي تؤدي إما إلى المساس بالنظام في حد ذاته أو إلى المساس بالمعطيات الموجودة داخل نظام المعالجة الآلية أو التي لها علاقة به.

وهو ما جعل الفقه يتجه إلى وضع معيارا للتفرقة بين الإعتداء على النظام والإعتداء على المعطيات التي يتضمنها، وذلك على أساس ما إذا كان الإعتداء يشكل وسيلة أم غاية، فإذا كان الإعتداء مجرد وسيلة فإن الفعل يشكل جريمة إعتدء على نظام المعالجة الآلية أما إذا كان الإعتداء غاية فهو يشكل جريمة إعتداء على المعطيات الموجودة داخل هذا النظام.

**3-** لقد تعاظم الدور الذي يؤديه نظام المعالجة الآلية للمعطيات باعتباره مستودعا لكم هائل وضخم من البيانات والمعلومات الشخصية والاقتصادية والمالية والعسكرية، وأصبح عرضة للكثير من الإعتدءات التي تمس بسلامته مما أدى الى ظهور شركات متخصصة في صناعة برامج الحماية الفنية ونظم الأمان الهدف منها حماية هذه الأنظمة من الإختراقات والفيروسات، ورغم هذا التطور الذي بلغته هذه الصناعة فإن الإعتداءات لم تتوقف بل على العكس من ذلك ذهب مرتكبوها إلى تطوير تقنيات وسائل إرتكابهم لهذه الجرائم وأهمها تقنيتي الإختراق والفيروسات بما يحبط آمان هذه النظم وإلحاق أضرارا إقتصادية كبيرة بالدول والمؤسسات من خلال الولوج اليها بطرق غير مشروعة، الأمر الذي جعل الشرائع الدولية والتشريعات الداخلية تأذن بوضع نصوص ومبادئ قانونية لتجريم مختلف أنواع العدوان على نظم المعالجة الآلية للمعطيات.

4- إن مميزات جرائم نظام المعالجة الآلية للمعطيات سواء تلك المتعلقة بالمجرم المعلوماتي أو بطبيعة الجريمة في حد ذاتها تستدعي من النصوص القانونية المتعلقة بهذه الجرائم أن تواكب الواقع الإجرامي من أجل تحقيق الحماية الجنائية المثلى للحد من جرائم نظام المعالجة الآلية للمعطيات، وهو المسلك الذي أنتهجه المشرع الفرنسي بتعديله للنصوص القانونية المتعلقة بهذه الجرائم برفع قيمة العقوبة والغرامة في سنوات 1994، 2004 و2015، لذلك نهيب بالمشرع الجزائري أن يشدد العقوبة

والغرامة المتعلقة بجرائم نظام المعالجة الآلية للمعطيات مسايرة للواقع الإجرامي القاتم لهذه الجرائم.

5- توصلنا إلى إن جرائم نظام المعالجة الآلية للمعطيات لما تتسم به من خطورة بالغة على كافة مجالات الحياة الإقتصادية والشخصية والعسكرية والأمنية، نظرا لإرتكابها من بين فئات متعددة من المجتمع، وتبعا لحجم الخسائر والأضرار الناجمة عنها قياسا بالجرائم التقليدية، تسلزم وجود منظومة قانونية فعالة توازي الواقع الإجرامي لهذه الجرائم، لذلك فعلى التشريعات المقارنة أن تستعجل بإصدار نصوص قانونية أخرى نظرا لقصور التشريعات القائمة بالأحاطة بكافة أشكال الإعتداءات التي تمس بالكيانات المعنوية لهذه النظم، لا سيما وأن المشرع الجزائري يتجه نحو حكومة إلكترونية تستوجب منه أصدار نصوص قانونية تضمن أن تتم المعاملات الإلكترونية فيها عبر قنوات إلكترونية آمنة.

6- إن محل جرائم نظام المعالجة الآلية هو نظام المعالجة الآلية بمكوناته المعنوية التي ينصرف مدلولها الواسع إلى جميع المعطيات التي تمت معالجتها من نصوص أو صور أو أصوات أو رموز أو برامج ومهما كانت الحالة التي تكون عليها سواء كانت معالجة أو مخزنة أو في طريقها إلى المعالجة والتبادل ضمن وسائل الإتصال المندمجة مع نظام المعالجة الآلية، والمشرع يقوم بحمايتها باعتبارها جزء من النظام سواء بوجودها داخل النظام أو خارجه تربطها به علاقة غير مباشرة، أما المكونات المادية لنظام المعالجة الآلية للمعطيات فالإعتداء عليها مجرم بنصوص تقليدية.

7- إن المشرع الجزائري وسع نطاق الحماية الجنائية في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات بصورتيها البسيطة والمشددة المنصوص عليهما في المادة 394 مكرر وذلك حينما جرم فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من نظام المعالجة الآلية حتى ولو لم يصحب إتيانهما إي مساس بمكونات نظام المعالجة الآلية، وهو نفس الإتجاه الذي سلكه المشرع الفرنسي.

8- في رأينا أن المشرع الجزائري لم يرد النص على جريمة إفساد أو تعطيل النظام كجريمة خاصة مستقلة مثلما هو الحال في بعض التشريعات المقارنة كالتشريع

الفرنسي، وإنما إكتفى بجعلها صورة مشددة من جريمة الدخول أو البقاء غير المصرح به في نظام المعالجة الآلية للمعطيات، وذلك نتيجة إلى التشابه الكبير بين جريمة إفساد أو تعطيل النظام وجريمة التلاعب بالمعطيات التي يصعب في الكثير من الأحيان التمييز بينهما لإن الأفعال التي تتضمنها جريمة التلاعب بالمعطيات ( الدخول، الإزالة، التعديل) هي الأخرى تؤدي إلى إعاقة النظام وإفساده، وهو الأمر الذي جعل المشرع الفرنسي يفرق بين هذه النتيجة (إعاقة النظام وإفساده) باعتبارها ظرف تشديد غير مقصود نص عليه في المادة 323-1 من قانون العقوبات الفرنسي وبين إعتبارها جريمة خاصة مستقلة نص عليها في المادة 323-2 من قانون العقوبات الفرنسي وهي جريمة إعاقة أو تعطيل نظام المعالجة الآلية .

9- بالرغم من تدارك المشرع الجزائري في القانون(04-15) للفراغ القانوني في مجال الإجرام المعلوماتي، بتجريمه لكافة الإعتداءات التي تمس نظم المعالجة الآلية للمعطيات من خلال النصوص القانونية الخاصة به، إلا أنه أغفل تجريم الإعتداءات الواردة على منتوجات الإعلام الآلي التي تتم عن طريق التزويرالمعلوماتي.

10- نظرا لخطورة ما يترتب على معالجة البيانات الشخصية من تهديد لخصوصيات الأفراد فقد تضمن القانون رقم 18-07 السالف الذكر، عدة مخالفات تشكل جرائم ماسة بتلك المعطيات التي ترتكب إما أثناء عملية جمعها أو أثناء معالجتها أو أثناء إستعمالها أو التصرف فيها، والى جانب ذلك قام بتوفير حماية جنائية لهذه المعطيات، وحسنا ما فعله المشرع الجزائري لاسيما وأن المعطيات الشخصية للجزائريين كانت وإلى وقت قريب في متناول شركات أجنبية ناشطة في الجزائر في مجالات حساسة جدا على غرار شركات الهاتف النقال والهاتف الأرضي ومزودي خدمات الأنترنت وغيرها، والتي لا يعرف طبيعة معالجتها لهذه المعطيات ولا الغرض من تلك المعالجة، إلا أنه تأخر في حمايتها مقارنة بالعديد من الشرائع الدولية والتشريعات الداخلية ولا سيما منها التشريع الفرنسي.

11- إن المشرع الجزائري قد نص على جريمة أخرى في المادة 394 مكرر 8 بموجب القانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016، المعدل والمتمم لقانون العقوبات، والمتمثلة في مخالفة الإلتزامات الخاصة بمقدمي خدمات الأنترنت،

والتي لم نتطرق لها في الجانب الموضوعي لكونها تمثل الجانب الإجرائي لجرائم نظام المعالجة الآلية للمعطيات، باعتبارها آلية فعالة في البحث والتحري والكشف عن مرتكبي هذه الجرائم، وموضعها حسب نظرنا هو القانون 09-04 الذي ينص على إلتزامات مقدمي خدمات الأنترنت ويعاقب على مخالفة القواعد الإجرائية في عدة مواد، ولذلك كان من الأحسن النص على هذه الإلتزامات ضمن هذا القانون الذي يجمع بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة بتحديد مصدرها والتعرف على مرتكبها.

12- نص المشرع الجزائري على ظرف مشدد لعقوبة الإعتداء على نظام المعالجة الآلية للمعطيات في المادة 394 مكرر3 وذلك تبعا لصفة المجني عليه، بحيث تصبح تضاعف العقوبات في حال ما إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام نظرا لما تشكله من تهديد لأمن الوطن والمصالح العامة، وهذا الظرف المشدد لا نجد له ذكرا لا في التشريع الفرنسي ولا في إتفاقية بودابست.

أما الظرف المشدد الثاني فيكون تبعا للنتيجة المترتبة عن جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات في صورتها المشددة في حالتين:

الحالة الأولى: إذا نجم عن هذا الدخول أو البقاء حذف أو تغيير لمعطيات النظام.

الحالة الثانية: إذا نجم عن هذا الدخول أو البقاء تخريب إشتغال النظام.

أما بالنسبة للمشرع الفرنسي فقد جعل بدوره من جسامة النتيجة ظرف مشددا، ألا أنه لم يرفع عقوبة جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية إلى ضعف عقوبة الجريمة البسيطة كما فعل المشرع الجزائري، وذلك في تقديرنا يرجع إلى سببين، يتمثل السبب الأول في أن عقوبة الجريمة البسيطة تضاعفت ولا يمكن مضاعفتها مرة أخرى بالنسبة للجريمة المشددة، بينما يتمثل السبب الثاني في إن عدم مضاعفة العقوبة تم إستجابة لإنتقاد الفقه بوجود فارق كبير بين العقوبة البسيطة والمشددة.

13- إن المشرع الجزائري ورغبة منه في التصدي بكل فعالية وحزم للإعتداءات الواردة على نظام المعالجة الآلية للمعطيات، فقد وسع نطاق الحماية الجنائية لتشمل من حيث الأفعال أعمال البدء في التنفيذ ومن حيث الأشخاص الذين يشاركون في الإعداد لجنح نظام المعالجة الآلية للمعطيات في إطار إتفاق جنائي.

14- بالنسبة للعقوبات التكميلية إقتصر المشرع الجزائري على عقوبة المصادر والغلق باعتبارهما عقوبتان تكمليتان وجوبيتان للعقوبة السالبة للحرية في جرائم نظام المعالجة الآلية للمعطيات ، وهو نفس المسلك الذي أتبعته بعض التشريعات المقارنة كالتشريع الفرنسي الذي نص على غيرها من العقوبات التكملية الوجوبية سعيا منه لتحقيق مبدأ تفريد العقوبة.

15- لا يمكن تطبيق الظرف المشدد في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة إذا قصد النتيجة المشددة لإن ذلك يقع مباشرة تحت طائلة المادة 394 مكرر1 من قانون العقوبات الجزائري والمادة 323-3 من قانون العقوبات الفرنسي والمتعلقتين بجريمة التلاعب بالمعطيات والتين تضمنتا فعلي التعديل والإزالة العمديين.

16- إن جريمة التلاعب بالمعطيات تقوم متى قصدها الجاني، ولا يهم بعد ذلك أن يكون الدخول مشروعا أو غير مشروع، وإن كان يثير في الحالة الأخيرة مسألة التعدد المادي للجرائم بالنسبة لجريمتي الدخول غير المشروع وجريمة التلاعب بالمعطيات فتطبق العقوبة الأشد وفقا للمواد 33 -38 من قانون العقوبات الجزائري.

17- إن جريمة التعامل في معطيات متحصل عليها من إرتكاب جريمة تعد من الجرائم التي إنفرد بها المشرع الجزائري والتي لا نجد لها ذكرا لا في القانون الفرنسي ولا في إتفاقية بودابست، وهي تلم عن رغبة المشرع الجزائري في تضييق نطاق الأشخاص الذين يمكنوا أن يتعاملوا في هذه المعطيات التي تم الحصول عليها بطريقة غير مشروعة، سعيا منه للحفاظ على سريتها والتخفيف من الآثار والضرر الذي يمكن أن يترتب عن إرتكاب إحدى الجرائم السابقة.

18- إن ما يميز مصطلحي التوفير أو العرض والوضع تحت التصرف الذي نص عليهما المشرع الفرنسي عن مصطلح الإتجار هو حصول هذا الأخير بمقابل بينما

التصرفات الأخرى تتم بدون مقابل، والظاهر أن المشرع الفرنسي لا يقيم اعتبارا للمقابل فيعتبر تقديم المعطيات مجرما سواء تم بمقابل أو بغير مقابل، بينما أراد المشرع الجزائري أن يشمل بالنص الحالتين معا.

19- إن المادة 394 مكرر2 في بندها الثاني تعاقب على حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم، ولو كان المشرع يتطلب بقوله"عن طريق الغش" قصدا خاصا فلماذا يعود في نفس المادة ويقرر أن الجريمة تقوم "لأي غرض كان" أي مهما كان قصد الجاني والوقائع التي ينصرف إليها من خلال التعامل في هذه المعطيات فإن الجريمة تقوم.

20- إن المشرع الجزائري أستعمل عبارة "الغش وعمدا" في المادة 394 مكرر2 للتأكيد على صفة العمدية، وكان يجب عليه أن يقتدي بالمشرع الفرنسي الذي لا يتطلب وجود قصد خاص لقيام هذه الجريمة وأضاف عبارة "بدون مبرر شرعي" التي تقوم بحماية الشخص الذي يقوم بإستخدامها لأغراض مشروعة مثل الأعمال العلمية والتقنية.

إضافة إلى أنه أستعمل أسلوبا غامضا وغير واضح في هذه المادة للدلالة على عمدية الجريمة بإضافته لمصطلح عمدا، وذلك أن الصورة الثانية من هذه الجريمة لا تحتاج الى العمد لأن التعامل فيها يتم أصلا في معطيات متحصل عليها من جريمة، أما في الصورة الأولى فعبارة الغش وحدها تدل على عمدية الجريمة، إضافة الى أنها لم تستثني الذين يستخدمون هذه المعطيات في أبحاث علمية، وكان من الواجب على المشرع أن يضع عبارة واضحة ودقيقة كعبارة بدون مبرر شرعي أو بدون سبب شرعي.

21- إن العقوبات المقررة لجرائم نظام المعالجة الآلية للمعطيات تظل لوحدها غير قادرة على تحقيق الوقاية من هذه الجرائم ذلك أن التهديد بهذه العقوبات كأسلوب وقائي رادع يعتبر جزء من الحل ولا يكفي وحده لإبعاد هذا الخطر إذ لا بدا من تدعيمه بوسائل وقائية أخرى تتناسب والطبيعة التقنية لهذه الجرائم ومن أهمها إتخاذ مسألة أمن المعلومات من الناحية التقنية بشكل أكثر فعالية، والبحث عن طرق وأساليب جديدة لمكافحة جرائم نظام المعالجة الآلية للمعطيات تساهم في الحد من

إنتشارها، من قبل خبراء أمن المعلومات ورجال الصناعة، والعمل كذلك على تكييف هذه الوسائل التقنية للقيام بدورها في مراقبة الإتصالات الإلكترونية دون أن تتعرض حقوق الإفراد وحرياتهم ومعطياتهم الشخصية للخطر، لا سيما وأن المشرع الجزائري أصدر مؤخرا القانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

22- إتجهت غالبية الدول كمرحلة أولى إلى تعديل قوانينها الإجرائية بصفة دورية ومستمرة بما يضمن مواكبة متغيرات وتطورات جرائم النظام، وإلى إرساء قواعد قانونية جديدة تواجه المشكلات المعاصرة التي أسفرت عنها هذه الجرائم المستحدثة وتطوراتها اللامتناهية، ثم قامت كمرحلة ثانية باستحداث نصوص قانونية خاصة أكثر إنسجاما مع الطبيعة الخاصة لهذه الجرائم.

في حين إقتصرت بعض الدول على تعديل قوانينها الإجرائية بما يتماشى والتطورات الحاصلة في هذا النوع من الإجرام والإعتماد على بعض النصوص القانونية المتفرقة في بعض التشريعات الخاصة كقوانين حماية الملكية الفكرية وقوانين حماية حقوق المؤلف وقوانين التوقيع الإلكتروني.

أما بالنسبة للمشرع الجزائري فقد قام كمرحلة أولى بتعديل قانون الإجراءات الجزائية بصفة دورية ومستمرة لمكافحة جرائم ذات خطورة بالغة حددها على سبيل الحصر من بينها جرئم المساس بأنظمة المعالجة الآلية للمعطيات، ثم قام كمرحلة ثانية بسن القانون 09-04،السالف الذكر، والذي يمثل الجانب الإجرائي لكافة جرائم تكنولوجيات الإعلام والإتصال بما فيها جرائم نظام المعالجة الآلية للمعطيات، لكونه يجمع بين القواعد الوقائية التي تسمح بالرصد المبكر لهده الجرائم والتعرف على مرتكبها والقواعد الإجرائية المكملة لقانون الإجراءات الجزائية وكذا القواعد المتعلقة بالإختصاص القضائي والمساعدة القضائية الدولية.

وفي رأينا أن الجمع بين مختلف الأساليب مثل ما فعل المشرع الجزائري هو الطريق الأنسب لمكافحة هذا النمط الخطر والمستجد من أنواع الإجرام المعلوماتي الذي يتطلب حسب نظرا الجمع بين مختلف الأساليب لتوفير الحماية الفنية أو التقنية وكذا الحماية الجنائية بشقيها الموضوعي والإجرائي لنظم المعالجة الآلية للمعطيات .

23- إن الحماية الموضوعية لنظام المعالجة الآلية وأن كانت لازمة وهامة فإنها تظل قاصرة وغير كافية لمواجهة الإعتداءات التي يتعرض لها النظام مما أستدعى تدخل المشرع الجنائي لفرض حماية جنائية خاصة بوضعه إطار قانوني أكثر ملائمة وإنسجاما مع خصوصية الجريمة الإفتراضية يتمثل في القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، والذي أنشأهيئة خاصة للوقاية من جرائم تكنولوجيا الإعلام والإتصال تتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، ألا أن المشرع الجزائري تأخر في تشكيلها وتنظيمها وكيفيات سيرها وترنح بين إلحاقها تحت أي سلطة ليتم وضعها مؤخرا تحت سلطة رئيس الجمهورية بموجب المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو سنة 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، إضافة إلى غياب بعض القرارات الوزارية المنصوص عليها في المادتين 14 و15 من المرسوم الرئاسي رقم 20-183 ، والتي تحدد تنظيم وكيفيات سير مكونات المديرية العامة للهيئة، وكذا كيفيات تطبيق الأحكام المنصوص عليها في المادة 15 من نفس المرسوم.

24- كان جدير بالمشرع الجزائري حسب رأينا باستعماله لمصطلح منظومة للدلالة على النظام لأن مجموعة نظام هي أنظمة وليس منظومة، وذلك تماشيا مع تعريف المنظومة الوارد في المادة 2 النقطة "ب" من القانون 09-04" أي نظام منفصل أو مجموعة من الأنظمة.."، وكذلك أيضا مع عنوان القسم السابع مكرر" المساس بأنظمة المعالجة الآلية للمعطيات"، بالإضافة إلى ذلك فإن النظام يقصد به مجموعة من الأجزاء المترابطة والتي تعمل معا لتحقيق هدف معين بينما المنظومة هي التي تهدف إلى تنظيم مرفق عام وترتيبه وتنسيق سير العمل بين مختلف مصالحه مثل المنظومة المعلوماتية المركزية لوزارة العدل.

25- إن المشرع الجزائري قام بإرساء جملة من التدابير المستحدثة غير المألوفة في القوانين السابقة والأكثر ملائمة مع خصوصيات جرائم نظام المعالجة الآلية للمعطيات، تتنوع بين تدابير وقائية تتمثل في مراقبة الإتصالات الإلكترونية

والإلتزمات المترتبة على مقدمي الخدمة وأخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائية وتتمثل في تفتيش الإنظمة المعلوماتية وحجز المعطيات المعلوماتية، باعتبارهما إجراءين حاسمين خلال التحقيق في هذه الجرائم، وملائمين كذلك لخصوصية الدليل الرقمي الذي يتم الحصول عليه من خلالهما.

وتعتبر هذه التدابير من أهم الضمانات القانونية التي أقرها المشرع الجزائري في سبيل تحقيق الحماية الإجرائية لنظم المعالجة الآلية للمعطيات والتي أثبتت فاعليتها في مكافحة هذا النوع من الإجرام، وهي نفس التدابير التي إعتمدتها إتفاقية بودابست والإتفاقية العربية لمكافحة جرائم تقنية المعلومات والعديد من التشريعات المقارنة ولا سيما منها التشريع الفرنسي.

إلا أنه وبالنظر لكون جرائم نظام المعالجة الآلية للمعطيات تعتمد بشكل كبير على التكنولوجيا التي تسبق دائما القانون فإنه يجب على هذا الأخير أن يسعى دائما لمواكبتها من خلال إيجاد تدابير مستجدة لسد النقص الحاصل في التدابير الإجرائية لنظم المعالجة الآلية للمعطيات وإستحداث تدابير أخرى تلائم التطور الحاصل في إساليب إرتكاب هذه الجرائم،

26- إن جرائم نظام المعالجة الآلية للمعطيات تعتبر من أهم الجرائم العابرة للحدود الإقليمية، الأمر الذي آثار معه العديد من الصعوبات في مجال تفعيل الآليات الإجرائية الدولية لمكافحة جرائم نظام المعالجة الآلية للمعطيات، وخصوصا مسألة الإختصاص القضائي الدولي من حيث الجهات المختصة وما يثور عنها من تنازع الإختصاص القضائي وذلك نتيجة لإختلاف التشريعات في المعايير والمبادئ المطبقة في تحديده، وكذا مسألة المساعدة القضائية الدولية المتبادلة بخصوص تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، وعدم كفاية مجالاتها التقليدية (تبادل المعلومات ونقل الإجراءات والإنابة القضائية) المخصصة لمجابهة كافة الجرائم الخطيرة بما فيها جرائم نظام المعالجة الآلية للمعطيات للتصدي لهذا النوع من الجرائم.

فالبعد الدولي لجرائم نظام المعالجة الآلية للمعطيات يفرض على المجتمع الدولي ضرورة البحث عن وسائل أكثر ملائمة لطبيعة هذه الجرائم، والعمل على تضييق الثغرات القانونية التي برع مرتكبوها في إستغلالها للتهرب من العقاب ونشر نشاطهم الإجرامي في مناطق مختلفة من أنحاء العالم من خلال خلق سياسة جنائية مشتركة في مجال جرائم نظم المعالجة الآلية للمعطيات، وهو نفس المسلك الذي دعت إليه العديد من الإتفاقيات الدولية والإقليمية ويأتي على رأسها إتفاقية بودابست والأتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذا العديد من التشريعات الداخلية ولا سيما منهما التشريعين الجزائري والفرنسي.

27- إن الإختلاف في التشريعات الداخلية بشأن قواعد الإختصاص وعدم وجود آليات إلزام الدول بتوحيد هذه التشريعات والسهر على تطبيقها يساهم أيضا في إنتشار هذه الجرائم وإفلات مرتكبيها من العقاب، وهو الأمر الذي يستحيل معه مكافحة هذا النوع من الإجرام بغير تفعيل الآليات الإجرائية الدولية سواء على صعيد الإختصاص القضائي الدولي أو المساعدة القضائية الدولية المتبادلة بالنسبة لتبادل المعلومات في هذه الجرائم والمساعدة على التحقيق فيها وتتبع مرتكبيها، وذلك كله وفقا للقواعد التي تقررها الإتفاقيات الثنائية أو المتعددة الأطراف أو وفقا لمبدأ المعاملة بالمثل.

كما أن تفاقم مسألة تنازع الإختصاص القضائي الدولي وتحولها إلى عائق حقيقي أمام مكافحة جرائم نظام المعالجة الآلية للمعطيات، جعلت التشريعات المقارنة تفكر بضرورة وضع ضوابط إسناد جنائية لتحديد الإختصاص القضائي الدولي لجرائم نظام المعالجة الآلية للمعطيات فإختلفت الحلول من دولة إلى أخرى فبعض الدول تبنت الحل عن طريق الإتفاقيات الدولية وبعضها الآخر توسع قضائها في تفسير هذه المبادئ والبعض الآخر ساير الإجتهاد القضائي

لذلك فإنه لا بدا من التعاون بين الدول لحل مسألة تنازع الإختصاص القضائي الدولي من خلال عقد إتفاقيات دولية لتبني المعيار الأنسب لمكافحة جرائم نظام المعالجة الآلية للمعطيات، ووضع آليات دولية لتعزيز التعاون الدولي في مجال

القضاء الدولي من أجل وضع حد لتنازع الإختصاص القضائي الدولي، وبالتالي نضمن عدم إفلات مرتكبي هذه الجرائم من العقاب.

28- إن المساعدة القضائية الدولية المتبادلة تعتبر آلية دولية فعالة لمكافحة جرائم نظام المعالجة الآلية المعطيات ذات البعد الدولي والمرتكبة في بيئة إفتراضية، لذا فإن تنفيذها وفق القواعد المنصوص عليها في الإتفاقيات الدولية ذات الصلة والإتفاقيات الثنائية ومبدأ المعاملة بالمثل، وإستحداث مجالات خاصة بالمساعدة القضائية الدولية للمواجهة هذا النوع من الإجرام، يتلائم مع طبيعة هذه الجرائم التي تقتضي التعامل مع أدلة رقمية غير ملموسة وسريعة الزوال.

وحسنا مافعل المشرع الجزائري بنصه على المساعدة القضائية الدولية في القانون 09-04، كآلية فعالة في مكافحة هذا النوع من الإجرام مقتفيا بذلك أثر بعض التشريعات المقارنة كالتشريع الفرنسي، وكذا الإتفاقيات الدولية ذات الصلة (إتفاقية بودابست، الإتفاقية العربية لمكافحة جرائم تقنية المعلومات).

لذلك نتوقع في الأخير أن يحمل المستقبل عدة أنواعا جديدة غير متوقعة من جرائم نظم المعلومات، التي تحرص وسائل الإعلام على إبراز المثير والغريب منها، وتستلزم من كافة خبراء أمن المعلومات أن يظلوا في حالة إستنفار دائمة لمواجهتها.

## ثانيا: الإقترحات

على ضوء النتائج التي توصلنا إليها في هذه الدراسة نقترح ما يلي:

1- يستحسن على المشرع الجزائري الإقتداء بالتشريعات المقارنة الأخرى بوضعه نصوص قانونية تحمي مكونات النظام المعزولة (معطيات أو برامج) التي لم تكن جزء منه و ليس لها علاقة به، وتجرم كذلك الإعتداءات على منتوجات الإعلام الآلي مثل التزوير المعلوماتي والسرقة المعلوماتية...

2- وجوب توفير حماية جنائية فعالة لنظام المعالجة الآلية للمعطيات تعنى بتطوير نظم الحماية والآمان لمواجهة الخسائر الكبيرة التي تهدد مصالح الأشخاص والدول، باعتباره مستودعا لكم هائل وضخم من البيانات والمعطيات الشخصية والإقتصادية والمالية والعسكرية لتشمل حماية كل المعطيات مع تشديد الحماية على طوائف معينة

من المعطيات الشخصية ذات الطبيعة الخاصة المتعلقة بالأصل العرقي، والأطفال، والصحة أو الحالة الجسدية أو النفسية، والمعتقدات الدينية، والعلاقة الزوجية...

3- إن الإلتزامات الخاصة بمقدمي خدمات الأنترنات تعد تدابير وقائية فعالة للبحث والتحري في الكشف عن مرتكبي جرائم نظام المعالجة الآلية للمعطيات ويترتب على مخالفتها مسؤولية جزائية نصت عليها المادة 394 مكرر8 من قانون العقوبات المعدل والمتمم، لذلك وجب على المشرع الجزائري حذفها من هذا القانون وإدراجها في موضعها المتضمن هذه الإلتزامات ألا وهو القانون 09-04 السالف الذكر، الذي يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية والقواعد الوقائية.

4- تصحيح مصطلح منظومة للدلالة على النظام في القانون 09-04، بوضع بدل منظومة نظام لأن مجموع نظام أنظمة وليس منظومات، ولتتطابق بذلك مع العنوان الأساسي للقسم السابع مكرر" المساس بأنظمة المعالجة الآلية للمعطيات".

5- ضرورة وضع المشرع الجزائري نصوص إجرائية تكميلية إلى جانب التدابير الإجرائية المستحدثة يتم من خلالها الحصول على هذه المعلومات بطريقة آمنة تلائم طبيعة هذه الجرائم الإفتراضية التي يخبئ لنا منها المستقبل أنواع جديدة وغير متوقعة.

6- إن البعد الدولي لجرائم نظام المعالجة الآلية للمعطيات يستوجب على المجتمع الدولي توحيد الجهود وعقد إتفاقيات ثنائية ودولية ذات الصلة للعمل على تضييق الثغرات القانونية التي برع مرتكبوها في إستغلالها لنشر نشاطاتهم في مختلف أنحاء العالم، وأهمها توحيد التشريعات الداخلية بشأن قواعد الإختصاص ومطابقتها مع قواعد الإختصاص القضائي الدولي لتفادي تنازع الإختصاص، وكذا تفعيل آليات المساعدة القضائية الدولية المتبادلة بالنسبة لتبادل المعلومات في هذه الجرائم والمساعدة على التحقيق فيها في مجالات البحث والتفتيش وجمع الأدلة وتسليم المجرمين بل وحتى تنفيذ الأحكام الأجنبية الصادرة في هذا المجال مع مرعاة مبدأ المعاملة بالمثل.

7- تشديد العقوبات في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات بصورتيها وكذا جريمة التلاعب بالمعطيات أسوة بالمشرع الفرسي الذي عدلها في العديد من المرات وآخرها كان سنة 2015، مع إدراج ظروف أخرى للتشديد مثل الدخول إلى النظام بنية إرتكاب عدة جرائم، والأخذ بعين الإعتبار وظيفة أو صفة الفاعل التي تسهل له إرتكاب هذه الجرائم.

8- من الضروري على المشرع الجزائري النص على جريمة إعاقة أو إفساد نظام المعالجة الآلية للمعطيات كجريمة مستقلة بذاتها بما لا يتعارض مع جريمة التلاعب بالمعطيات قدوة بالتشريعات المقارنة الأخرى وتماشيا مع ما إتجهت إليه إتفاقية بودابست في مادتها 05.

9- حبذا لو يحذو المشرع الجزائري حذو المشرع الفرنسي بالعقوبة على جريمة التعامل في معطيات غير مشروعة بالعقوبة نفسها المقررة لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات، لأنه من غير المعقول المعاقبة على جريمة التعامل في معطيات غير مشروعة بصفتها أعمال تحضيرية بعقوبات أشد من عقوبات تلك الأخيرة.

10- نهيب بالمشرع الجزائري الإقتداء بالمشرع الفرنسي بتنويع العقوبات التكميلية بما يحقق مبدأ تفريد العقوبة بدل حصرها في المصادرة والغلق، مع تعديل المادة 394 مكرر 6 باستبدال عبارة "المواقع التي كانت محلا للجريمة" بعبارة "المواقع التي كانت وسيلة للجريمة".

11- الإقتصار على مصطلح الغش للدلالة على قصدية جرائم التعامل في معطيات غير مشروعة بدل إستعمال مصطلحي الغش والعمد باعتبارها جرائم عمدية.

12- حبذا لو يقوم المشرع الجزائري بحدف فعل الشروع من المادة 394 مكرر المنصوص والمعاقب عليه في المادة 394 مكرر 7 لأن ذلك يعد من قبيل التكرار.

13- ضرورة إستثناء الأبحاث العلمية والتقنية التي تهدف إلى تطوير وسائل الحماية الأمنية من الإختراق والمعاقب عليها في المادة 394 مكرر 2 بإضافة عبارة لتكون صياغتها كالآتي:"...كل من يقوم عمدا عن طريق الغش **وبدون سبب شرعي** بما يأتي:...".

14- منح الإعفاء من العقاب للفاعل في جرائم نظام المعالجة الآلية للمعطيات في حالة قيامه بالتبليغ عن الجريمة قبل بدء أي إجراء من إجراءات التحقيق فيها، أو التخفيف في حالة ما إذا كان التبليغ عنها يمكن السلطات المختصة من القبض على الجناة الآخريين حتى بعد التحقيق فيها أو يكون قبل إتمامها، وهذا قصد تشجيع المجرمين على العودة عن إرتكاب هذه الجرائم وتسهيل عمل المحقيقين فيها.

15- تعزيز الوعي بمخاطر وأضرار جرائم نظام المعالجة الآلية والآثار المترتبة عليها التي تمس مختلف القطاعات وتهدد مصالح الأشخاص والدول، وتوجيه رسالة قوية للمجرمين عن طريق الإعلام بأن مرتكبيها ليس في مأمن من المتابعات القضائية وإلحاق العقاب بهم في حالة إرتكابها.

16- الإسراع في إصدار النصوص التنظيمية الخاصة بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها التي شهدت عدة تعديلها بإلحاقها أولا بوزارة العدل ثم ثانيا بوزارة الدفاع الوطني وأخيرا برئاسة الجمهورية لا سيما وأنها تساهم في مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجرى بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال.

17- إن تطور الفكر الإجرامي في جرائم نظام المعالجة الآلية للمعطيات لا بدا أن يقابله تفعيل الفكر القانوني، بحيث يجب أن يكون هناك تطور موازي ومواكب في الإطار القانوني خاصة في ظل واقع المعلوماتية الذي يتسم بالحركية والتحول الدائمين وبالتالي العمل بشكل دائم على إستحداث آليات وتدابير جديدة لتوفير الحماية الجنائية للنظم المعلوماتية والبيانات التي تتدوال عبرها.

وفي الأخير تجدر الإشارة إلى أنه تم التطرق إلى أهم الآليات والتدابير الفعالة في مكافحة جرائم نظام المعالجة الآلية للمعطيات والتي تتلائم مع طبيعة وخصوصية هذه الجرائم، إذ أن هناك العديد من الآليات والتدابير الأخرى المقررة لكافة الجرائم المستحدثة ولجرائم تكنولوجيا الإعلام والإتصال التي تندرج ضمنها جرائم نظام المعالجة الآلية للمعطيات.

# قائمة المراجع

# قائمة المصادر والمراجع

## القرآن الكريم

**المصادر:**

- مرسوم رئاسي رقم 20-442 مؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 ديسمبر سنة 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه في إستفتاء أول نوفمبر سنة 2020، في الجريد الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، ج ر ج ج، ع 82، المؤرخة في 30 ديسمبرسنة 2020.

- دستور جمهورية مصر العربية المعدل بسنة 2014 الجريدة الرسمية، العدد 3، مكرر(أ) في 18 يناير 2014.

**الإتفاقيات الدولية والإقليمية والقرارات ذات الصلة**

**أ- الإتفاقيات الدولية**

1-إتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001، الموقعة في 23 نوفمبر 2001 بالعاصمة المجرية بودابست.

**ب- الإتفاقيات الإقليمية**

1-الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، الشبكة القانونية، العربية .

2-إتفاقية تتعلق بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية والبوسنة والهرسك، الجريدة الرسمية للجمهورية الجزائرية، العدد 36، المؤرخ في 17 يونيو سنة 2020.

**ج-القرارات ذات الصلة**

3- قرار رقم 417 بشأن مشروع قانون عربي إسترشادي لمكافحة جرائم المعلوماتية، جامعة الدول العربية، الدورة 21، لسنة 2004.

**النصوص القانونية والتنظيمية**

**أ- التشريع الجزائري**

**1- القوانين**

1- قانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، ج رج ج، ع 71 المؤرخة في 10 نوفمبر سنة 2004، الرابط: https :// www.joradp.dz

2- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 06 جوان 1966، المتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 84 المؤرخة في 24 ديسمبر 2006، الرابط: https :// www.joradp.dz

3- قانون 08-01 المؤرخ في 2008/01/23 المتمم لقانون رقم 83-11 المؤرخ في 1983/07/02، المتعلق بالتأمينات الإجتماعية، ج رج ج ، ع 04 المؤرخة في 27 جانفي 2008، الرابط:https :// www.joradp.dz

4- قانون 09-04 المؤرخ0 في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتهما، ج رج ج ، ع 47، المؤرخة في 16 غشت سنة 2009، الرابط:https :// www.joradp.dz

5- القانون 15-04، المؤرخ في أول فبراير سنة 2015، الذي يحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج رج ج ، ع 06، المؤرخة في 10 فبراير سنة 2015، الرابط: https :// www.joradp.dz

6- قانون رقم 16-02 مؤرخ في 14 رمصان عام 1437 الموافق 19 يونيو سنة 2016، يتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 والمتصمن قانون العقوبات، ج رج ج ، ع 37، المؤرخة في 22 يونيو سنة 2016، الرابط: https :// www.joradp.dz

7- قانون رقم 16-03 مؤرخ في 19 يونيو 2016، يتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرق على الأشخاص، ج رج ج ، ع رقم 37، المؤرخة في 19 يونيو 2016، الرابط: https :// www.joradp.dz

8- قانون 18-04، المؤرخ في 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية ، ج رج ج ، ع 27، المؤرخة في 13 مايو سنة 2018، الرابط: https :// www.joradp.dz

9- قانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعين في مجال المعطيات ذات الطابع الشخصي، ج رج ج، ع 34، المؤرخة في 29 ديسمبر 2018، الرابط: https :// www.joradp.dz

10- القانون رقم 20-06 المؤرخ في 28 أبريل سنة 2020، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966، والمتضمن قانون العقوبات، ج ر ج ج، ع 25، المؤرخة في 29 أبريل سنة 2020، الرابط: https :// www.joradp.dz

**2- الأوامر**

1-الأمر رقم 03-05 المؤرخ في 19 جويلية سنة 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج رج ج ، ع 44، المؤرخة في 23 يوليو 2003.

الرابط: https :// www.joradp.dz

2- الأمر رقم 05-06 المؤرخ في 23 أوت سنة 2005، المتعلق بمكافحة التهريب ، ج رج ج ، ع 59 المؤرخة في 28 غشت سنة 2005.

الرابط: https :// www.joradp.dz

**3- المراسيم**

1-مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، يتضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 12 ديسمبر سنة 2010، ج رج ج ، ع 57، المؤرخة في 28 سبتمبر سنة 2014، الرابط: https :// www.joradp.dz

2- المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات

الإعلام والإتصال ومكافحتها ، ج ر ج ج، ع 53، المؤرخة في 8 أكتوبر 2015، الرابط: https :// www.joradp.dz

3- المرسوم الرئاسي رقم 19-172 المؤرخ في 6 يونيو 2019، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج رج ج ، ع 37، المؤرخة في 9 يونيو سنة 2019، الرابط: https :// www.joradp.dz

4- مرسوم رئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج رج ج ، ع 04، المؤرخة في 26 جانفي سنة 2020 م،

الرابط: https :// www.joradp.dz

5- المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج رج ج، ع 40، مؤرخة في 18 يوليو 2020،

الرابط: https :// www.joradp.dz

6- مرسوم تنفيذي رقم 98-257 مؤرخ في 03 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998، يضبط شروط وكيفيات أقامة خدمات"أنترنات" واستغلالها، ج رج ج ، ع 63، المؤرخة في 4 جمادى الأولى عام 1419 هـ،

الرابط: https :// www.joradp.dz

**ب- التشريع المصري**

**1- القوانين**

[1]- قانون رقم 175 لسنة 2018، بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية المصرية، العدد 32 مكرر (ج) الصادرة بتاريخ 2018/08/14.

**ج- التشريع التونسي**

**1- القوانين**

-قانون أساسي عدد 63 لسنة 2004، المؤرخ في 2004/07/27، المتعلق بحماية المعطيات الشخصية، الرائد الرسمي للجمهورية التونسية، الصادرة بتاريخ 2004/07/30، عدد 61.

- قانون أساسي عدد 42 لسنة 2017 مؤرخ في 30 ماي 2017، يتعلق بالموافقة على إنضمام الجمهورية التونسية إلى الإتفاقية رقم 108 لمجلس أروبا المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي وبروتوكولها الإضافي رقم 181 الخاص بسلطات المراقبة وأنسياب وتدفق المعطيات عبر الحدود، الرائد للجمهورية التونسية، عدد45 المؤرخ في 6 جوان 2017.

**د- التشريع القطري**

**1- القوانين**

1- قانون رقم 11 المؤرخ في 10 ماي 2004، المتضمن قانون العقوبات القطري، جريدة رسمية، ع 7 المؤرخة في 30 ماي 2004.

2- القانون القطري رقم (14) لسنة 2014 المؤرخ في 2014/09/15، المتعلق بإصدار قانون مكافحة الجرائم الإلكترونية، الجريدة الرسمية القطرية، المؤرخة في 2014/10/02، العدد 15.

3- قانون رقم 13 لسنة 2016، بشأن حماية خصوصية البيانات الشخصية، الجريدة الرسمية القطرية، المؤرخة في 2006/12/29، العدد 15.

**هـ- التشريع المغربي**

**1- القوانين**

- القانون رقم 03-07 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات لسنة 2007

-قانون رقم 08-09 المؤرخ في 10 يونيو 2009، المتعلق بحماية الأشخاص الذاتيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية المغربية، المؤرخة في 2009/02/23، العدد 5711.

**و- التشريع الأردني**

- قانون جرام أنظمة المعلومات الأردني رقم 30 لسنة 2010.

- قانون المعاملات الالكتروني الإردني رقم 85 لسنة 2001، الجريدة الرسمية للمملكة الأردنية الهاشمية رقم 4524 الصادرة بتاريخ 2001/12/31.

**ز- التشريع البحريني**

-القانون البحريني رقم 60 لسنة 2014، بشأن جرائم تقنية المعلومات، الجريدة الرسمية البحرينية، المؤرخة في 9 أكتوبر 2014، العدد 3178.

**ح- التشريع السعودي**

- نظام مكافحة الجرائم المعلوماتية رقم 17 الصادر بتاريخ 2007/03/26 ، الجريدة الرسمية، مجموعة الأنظمة السعودية.

**ط- التشريع العماني**

- مرسوم سلطاني رقم 12 الصادر بتاريخ 2011/02/06، بشأن قانون مكافحة جرائم تقنيات المعلومات، الجريدة الرسمية لسلطنة عمان، العدد 929.

**ي- التشريع السوري**

**1- القوانين**

-قانون حماية حقوق المؤلف والحقوق المجاورة السوري الذي صدر بالمرسوم رقم 62 لعام 2014 المؤرخ في 16 أيلول 2013، وبدأ به العمل بعد ستة أشهر من تاريخ نشره في الجريدة الرسمية للجمهورية السورية.

-القانون السوري رقم 9 لعام 2018، القاضي بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والإتصالات ، مديرية المعلومات والتوثيق، رئاسة مجلس الوزراء، سنة 2020.

**2- المراسيم**

-المرسوم الشريعي السوري رقم 17 لعام 2012 المؤرخ في 2012/02/08، المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، مجلس الشعب السوري.

**ك- الشريع الإمارتي**

**1- المراسيم**

1- مرسوم بقانون إتحادي رقم (5) لسنة 2012، في شأن مكافحة جرائم تقنية المعلومات، سلسلة التشريعات الإتحادية، دائرة القضاء، أبوظبي، سنة 2013.

**ل-التشريع السوداني:**

**1- القوانين**

- قانون جرائم المعلوماتية السوداني لسنة 2007.

**م-التشريع الكويتي:**

**1- القوانين**

- القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.

**ن-التشريع الفلسطيني:**

**- التنظيم**

- قرار السلطة الفلسطيني الذي صدر بموجب قانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية

**التشريع الفرنسي:**

**1-** Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés , modifiè par LOI N° 2004-801 du 06 août 2004-ART 1, JORF 7 août 2004.

2-Loi n°88-19 du 05 janvier 1988, relative à la fraude l'informatique , JORF du 06 janvier 1988 , (LOI GODFRAIN).

3-Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur, JORF n° 0298 du 23 décembre 1992.

4- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, modifiè par LOI N° 2020-766 du 24 juin 2020.

5- Loi n° 2004-801 du 6 août 2004 relative à la protection des personne physiques à l'ègard des traitements de donnèes à caractère personnel et modifiant la loi n 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertès.

6- Code pènale, modifiè par LOI N° 2015-912 DU 24 JUILLET 2015-ART 4, JORF N° 0171 du 26 JUILLET 2015

7- Code de procèdure pènale, modifiè par LOI N° 2019-222 du 23 mars 2019.

## المراجع:

### باللغة العربية

### أولا- المؤلفات العامة

1-أحسن بوسقيعة، الوجيز في القانون الجزائي الخاصن جرائم الفساد،المال،الأعمال والتزوير، ج2، دار هومة، الجزائر، سنة 2006.

2- أحمد خليفة الملط، الجرائم المعلوماتية ، دار الفكر الجامعي، الأسكندرية، ط الثانية، 2006.

3-أشرف السعيد أحمد، القرصنة الإلكترونية، مطابع الشرطة، مصر، ب ط، سنة 2013.

4- امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط الثانية، سنة 2007.

5- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، الأسكندرية، سنة 2009.

6- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والأنترنت، مكتبة الوفاء القانونية، الأسكندرية-مصر، ط الأولى، سنة 2011.

7- الديربي عبدالعال، محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، ط الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.

8- بلعيات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط الأولى، 2007.

9- بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، ج2، دار الخلدونية، الجزائر، ط 1438هـ - 2017م.

10- حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الإعتداء على التوقيع الإلكتروني، دار الكتب القانونية-دار شتات للنشر والبرمجيات، مصر-الإمارات، 2013،

11- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض-السعودية، ط الأولى، سنة 2000.

12- حسن عماد مكاوي، تكنولوجيا الإتصال الحديث في عصر المعلومات، الدار المصرية البنانية، ط الثانية، 1998.

13- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، عمان، ط الأولى، سنة 2011.

14- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الأسكندرية، ط الأولى، سنة 2009، ص .232

15- ختير مسعود، الحماية الجنائية لبرامج الكومبيوتر أساليب وثغرات، دار الهدى، عين مليلة-الجزائر، 2012.

16- خيرات علي محرز، التحقيق في جرائم الحاسب، دار الكتاب الحديث، القاهرة، سنة 2012، ص .68

17- ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالأنترنت والمعلوماتية-دراسة تطبيقية مقارنة، مركز الدراسات العربية للنشر والتوزيع، جهورية مصر العربية، ط الأولى، سنة 2017.

18- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، المكتب الجامعي الحديث ، سنة 2013.

19- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، سنة 2011.

20- طارق صديق رشيد كه ردى، حماية الحرية الشخصية في القانون الجنائي (دراسة تحليلية مقارنة)، منشورات الحلبي الحقوقية، بيروت، لبنان، ط الأولى، سنة 2011.

21- طعباش أمين، الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الأسكندرية، ط الأولى، سنة 2015.

22- مجدي محمد أبو العطاء، أمن المعلومات والأنترنت، شركة علوم الحاسب كمبيوساينس، مصر، سنة 2016

23- محمد إبراهيم سعد النادي، جرائم الأنترنت بين الشريعة الإسلامية والقوانين الوضعية-دراسة مقارنة، مكتبة الوفاء القانونية، الأسكندرية، ط الأولى، سنة 2017.

24- محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، مصر، سنة 2005.

25- محمد أمين الرومي، جرائم الكومبيوتر والأنترنت، دار المطبوعات الجامعية، الأسكندرية ، سنة 2004.

26- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط الأولى، 2009.

27- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، ط الأولى، سنة 2014.

28- محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، ط الأولى،سنة 2006.

29- محمد دباس الحميد، ماركو ابراهيم نينو، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، الأردن عمان، ط الأولى ، سنة 2007.

30- محمد طارق عبدالرؤف الحق، جريمة الإحتيال عبر الأنترنت، منشورات الحلبي الحقوقية، لبنان، ط الأولى، سنة 2011.

31- محمد عبدالله إبراهيم، المواجهة الأمنية لجرائم شبكات المعلومات الدولية، مطابع الشرطة للطباعة والنشر والتوزيع، سنة 2016.

32- محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت(دراسة مقارنة) ، دار النهضة العربية، القاهرة، سنة 2005.

33- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الأسكندرية ، سنة 2004.

34- محمد علي سويلم ، الحماية الجنائية للمعاملات الإلكترونية الجرائم المعلوماتية والإلكترونية، دار المطبوعات الجامعية، الأسكندرية، مصر، ط الأولى، 2018.

35- محمد نصر محمد، المسؤولية الجنائية لإنتهاك الخصوصية المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، جهورية مصر العربية، ط الأولى، سنة 2016.

36- محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الأسكندرية، ط الأولى، سنة 2014.

37- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع، عمان الأردن، ط الأولى، 2009.

38- محمود أحمد عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان،الأردن، ب ط، سنة 2005.

39- مروك نصر الدين، محاضرات الإثبات الجنائي، الجزء الأول( النظرية العامة للإثبات الجنائي)، دار هومة، الجزائر، سنة 2007.

40- مسرة خالد الحمد، الدليل الرقمي ومعايير جودته، مركز الكتاب الأكاديمي، عمان، ط الأولى، سنة 2014.

41- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة للطباعة والنشر والتوزيع، ط الأولى، سنة 2009.

42- معتز سيد محمد أحمد عفيفي، قواعد الإختصاص القضائي بالمسؤولية الإلكترونية عبر شبكة الأنترنت، دار المطبوعات الجامعية، الأسكندرية-مصر، ط الأولى، سنة 2013.

43- ممدوح عبد الكريم، القانون الدولي الخاص- تنازع القوانين، دار الثقافة للنشر والتوزيع، عمان، ط 1، سنة 2005.

44- منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت لبنان، ط الأولى، 2018.

45- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية (دراسة نظرية وتطبيقية)، منشورات الحلبي الحقوقية، بيروت-لبنان، ط الأولى، سنة 2005.

46- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنثرنت في مرحلة جمع الإستدلالات- دراسة مقارنة، دار الفكر الجامعي، الأسكندرية، مصر، سنة 2013.

47- نعيم مغبغب ، حماية برامج الكومبيوتر، الأساليب والثغرات، دراسة في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، ط الأولى، سنة 2006.

48- نعيم مغبغب، مخاطر المعلوماتية والأنترنت، منشورات الحلبي الحقوقية، بيروت لبنان، ط الثانية، 2008.

49- نهلا عبدالقادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط الأولى، سنة 2008.

50- عبدالفتاح بيومي حجازي ، التجارة الإلكترونية في القانون العربي النموجي لمكافحة جرائم الكومبيوتر والأنترنت، دار الفكر الجامعي، الأسكندرية، مصر، ط الأولى، 2006.

51- عبدالفتاح بيومي حجازي ، الجريمة في عصر العولمة، دار الفكر الجامعي،الأسكندرية-مصر، 2008.

52- عبدالفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والأنترنت، دار الكتب القانونية، مصر، سنة 2007.

53- عبدالفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والأنترنت في القانون العربي النموذجي(دراسة متعمقة في القانون المعلوماتي، دار الكتب القانونية، مصر، سنة 2007.

54- عبدالفتاح مراد، شرح جرائم الكومبيوتر والأنترنت، شركة البهاء للبرمجيات والكومبيوتر والنشر الإلكتروني، الأسكندرية.

55- عبدالله سيف الكيتوب، الأحكام الإجرائية لجريمة الإحتيال المعلوماتي، دار النهضة العربية، القاهرة، سنة 2013.

56- على جعفر، جرائم تكنولوجيات المعلومات الحديثة الواقعة على الأشخاص والحكومة-دراسة مقارنة، مكتبة زين الحقوقية والأدبية، ط الأولى، سنة 2013.

57- علي حسن الطوالبة، الجرائم الإلكترونية،جامعة العلوم التطبيقية، مملكة البحرين، 2008.

58- علي عبدالقادر القهواجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، سنة 1999.

59- علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية- دراسة مقارنة، ماجستير قانون، كلية الحقوق، جامعة الموصل، المكتب الجامعي الحديث، الأسكندرية .

60- عمار تركي السعدون الحسيني، الحماية الجنائية للحرية الشخصية في مواجهة السلطة العامة، منشورات الحلبي الحقوقية، بيروت-لبنان، ط الأولى، سنة 2012.

61- عمار عباس الحسيني، جريمة الإتلاف المعلوماتي-دراسة مقارنة، منشورات زين الحقوقية، بيروت-لبنان، ط الأولى، سنة 2019.

62- عفيفي كامل، حماية أنظمة المعلومات، ط الأولى، دار الحامد للنشر والتوزيع، الأردن عمان، سنة 2007.

63- فتوح الشادلي، عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون- دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، ب س ن.

64- فهد عبيد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ، دار الجامعة الجديدة، الأسكندرية، سنة 2016.

65- قادري أعمر، الجرائم الخطيرة بين القانون والشريعة على ضوء بنود الإتفاقيات والتشريعات الخاصة ذات الطابع الجزائي ، دار هومة، الجزائر، سنة 2017.

66- سامر سلمان الجبوري، جريمة الإحتيال الإلكتروني، منشورات زين الحقوقية، بيروت-لبنان، ط الأولى، سنة 2018.

67- سامي جلال قفي حسين ، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي-دراسة مقارنة، دار شتات للنشر والبرمجيات، مصر، سنة 2011.

68- سامي منصور، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، المنشورات الحقوقية صادر، بيروت-لبنان، ب ط، ب س ن.

69- سعيدي سليمة، أمن المعلومات وأنظمتها في العصر الرقمي، دار الفكر الجامعي، الأسكندرية، ط الأولى، سنة 2018.

70- شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت-دراسة مقارنة، دار النهضة العربية، القاهرة، سنة 2009.

71- شيماء عبدالغني محمد عطاالله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، مصر، سنة 2007.

72- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية القاهرة، 1992.

73- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية-دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط-مصر، سنة 1994.

74- هشام صادق، تنازع الإختصاص القضائي الدولي، دار المطبوعات الجامعية، الأسكندرية-مصر، سنة 2007.

75- ياسر مطيع، محمد نصر الله، حمزة الغولة، طه عثمان، أكرم أبوزر، مفاهيم أساسية في تحليل و تصميم نظم المعلومات، مكتبة المجمع العربي للنشر والتوزيع، دار اجنادين للنشر و التوزيع، ط الأولى، سنة 2006.

**ثانيا - المؤلفات المتخصصة**

1- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع الجزائري والمقارن، ماجستير في القانون، ط الأولى، دار الفكر الجامعي، سنة 2008.

2- بولين أنطونيوس، الحماية القانونية للحياة الخاصة في مجال المعلوماتية -دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت لبنان، ط الأولى، 2009.

3- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، دار البداية، الأردن، ط الأولى، سنة 2007.

4- جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية- دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، سنة 2010.

5- جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة الكتاب الأول الجرائم الناشئة عن إستخدام الحاسب الآلي، دار التهضة العربية، القاهرة، ط الثانية، سنة 2012.

6- دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية-دراسة مقارنة، دار الفكر الجامعي، الأسكندرية، ط الأولى، سنة 2016.

7- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، لبنان، ط الاولى، 2012.

8- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الأسكندرية، 2007.

9- محمد علي سويلم ، مكافحة الجرائم الإلكترونية-دراسة مقارنة بالتشريعات العربية والأجنبية، دار المطبوعات الجامعية، مصر، ط الأولى،سنة 2019.

10- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات-دراسة مقارنة، ، دار المطبوعات الجامعية، مصر، ط الأولى، سنة 2019.

11- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية-دراسة مقارنة، ماجستير في القانون وباحث دكتواره، دار الفكر والقانون، المنصورة، ط الأولى، سنة 2017.

12- مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات(ماهيتها، صورها، الجهود الدولية لمكافحتها)-دراسة مقارنة-، دار الخلدونية، الجزائر، ط 1439هـ-2018م .

13- ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيات المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان-الجزائر، سنة 2018.

14- عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والأنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، لبنان، ط الأولى، سنة 2007.

15- هلالي عبداللاه أحمد ، إتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها، دار النهضة العربية، القاهرة، ط الأولى، سنة 2007.

16- هلالي عبداللاه أحمد ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست الموقعة 23 نوفمبر 2001، دار النهضة العربية، القاهرة، ط الأولى، 2003.

17- هلالي عبداللاه أحمد ، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، دار النهضة العربية، القاهرة، سنة 2011.

18- هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، دار النهضة العربية، ط الأولى، 1997.

**ثالثا: الرسائل العلمية**

**أ-أطروحات الدكتوراه**

1-براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة مولود معمري تيزي وزو، سنة 2018.

2- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت-دراسة مقارنة-، رسالة مقدمة لنيل درجة الدكتواره في القانون الجنائي، كلية الحقوق-جامعة عين الشمس.

3- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية قسم القانون الخاص -جامعة أبوبكر بلقايد-تلمسان، سنة 2018/2017.

4- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة باتنة 1، الموسم الجامعي 2015،2016.

5- ملياني عبد الوهاب، أمن المعلومات في بيئة إلكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية-جامعة أبوبكر بلقايد، تلمسان، سنة 2017/2016.

6- عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة مقدمة لنيل شهادة دكتواره علوم في القانون الجنائي، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة العربي التبسي –تبسة، الموسم الجامعي 2017،2018.

7- فايز محمد راجح غلاب ، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق -جامعة الجزائر1، سنة 2010/2009.

8- هروال هبة نبيلة ، جرائم الأنترنت، أطروحة من أجل الحصول على شهادة الدكتوراه، كلية الحقوق والعلوم السياسية-جامعة أبوبكر بلقايد، تلمسان، سنة 2014/2013.

**ب- مذكرات الماجستير**

1-الغسلان عبد العزيز بن سليمان، جرائم الإعتداء على برامج الحاسوب-دراسة مقارنة، أطروحة مقدمة لاستكمال متطلبات درجة الماجستير، كلية المعهد العالي للقضاء، جامعة الأمام محمد بن سعود الإسلامية، الرياض-السعودية، 2000.

2- جدي نسيمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق-جامعة وهران، الموسم 2014/2013.

3- حرية شعبان محمد الشريف، مخاطر نظم المعلومات المحاسبية الإلكترونية، رسالة مقدمة للحصول على درجة الماجستير في المحاسبة والتمويل، كلية التجارة-الجامعة الإسلامية غزة، 2006.

4- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري و المقارن، رسالة ماجستير شعبة القانون الجنائي، كلية الحقوق- جامعة قسنطينة، الموسم 2013/2012.

5- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية-جامعة أبوبكر بلقايد، تلمسان، سنة 2012/2011.

6- طارق عثمان، الحماية الجنائية للحياة الخاصة -دراسة مقارنة-، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة، 2007/2006.

7- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية ، جامعة الجزائر1، الموسم الجامعي 2012،2011.

8- مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم 09-04، مذكرة مقدمة لنيل شهادة الماجستير تخصص قانون جنائي، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة قاصدي مرباح –ورقلة، الموسم الجامعي 2013،2012.

9- معتوق عبداللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و القارن، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية- جامعة العقيد الحاج لخضر-باتنة، الموسم 2012/2011.

10- عبدالرحمن جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي- دراسة مقارنة، أطروحة مقدمة لاستكمال متطلبات درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس فلسطين، 2008.

11- عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية-دراسة مقارنة، مذكرة لنيل درجة الماجستير في القانون العام، جامعة الشرق الأوسط، سنة 2014.

12- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية- تخصص العلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر- باتنة، الموسم 2013/2012.

13- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية-جامعة أبوبكر بلقايد، تلمسان، سنة 2011/2010.

14- شنين صالح، الحماية الجزائية لبرامج الحاسب الآلي، مذكرة مكملة لنيل شهادة الماجستير في الحقوق تخصص قانون جزائي، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، الموسم 2007/2006.

**رابعا: المجلات العلمية**

1- أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، المجلد 10، العدد 1، مارس 2017.

رابط المقال: http://asjp.cerist.dz/en/downArticle/315/10/1/18306

2- آمال فكيري، إشكالات الإثبات والإختصاص في جرائم تكنولوجيا الإعلام والإتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية،جامعة الوادي، المجلد 9، العدد 1، جانفي 2018، رابط المقال: http://asjp.cerist.dz/en/downArticle/110/9/1/33853

3- أمحمدي بوزينة أمنة، الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري(دراسة تحليلية لقانوني العقوبات وحقوق المؤلف)، مجلة القانون والمجتمع، جامعة أحمد دراية-أدرار، المجلد 3، العدد 2، ديسمبر 2015. رابط المقال: http://asjp.cerist.dz/en/downArticle/133/3/2/34479

4- المعمري، عادل عبد الله خميس، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مركز بحوث الشرطة- القيادة العامة لشرطة الشارقة، الإمارات، المجلد 22، العدد 86، يوليو 2013.

رابط المقال: http://Search.Mandumah.com/Record/606358

5- المعيني، سرحان حسن، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، مركز بحوث الشرطة- القيادة العامة لشرطة الشارقة، الإمارات، المجلد 20، العدد 79، أكتوبر 2011.

رابط المقال: http://Search.Mandumah.com/Record/605735

6- العيداني محمد، يوسف زروق، حماية المعطيات الشخصية في الجزائر على ضوء القانون 18-07 (المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي)، مجلة معالم للدراسات القانونية والسياسية ، لبنان، العدد 5، ديسمبر 2018.

رابط المقال: http://asjp.cerist.dz/en/downArticle/520/2/3/73171

7- بخوش هشام، الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في ظل التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 4، العدد 1، جانفي 2017. رابط المقال: http://asjp.cerist.dz/en/downArticle/76/4/1/30826

8- برادل سمير، الجريمة المعلوماتية في التشريع الجزائري، مجلة القانون، كلية الحقوق والعلوم السياسية، المركز الجامعي لغيلزان ، المجلد 1، العدد 2 ، جويلية 2010. رابط المقال: http://asjp.cerist.dz/en/downArticle/325/1/2/45479

9- بن زيطة عبد الهادي، ضرورة إنشاء سلطة إدارية مستقلة كآلية للحماية القانونية للبيانات الشخصية في مواجهة إستخدامات المعلوماتية، مجلة الحقيقة، العدد 39، سنة 2017.

10- بن محمد محمد، تنازع الإختصاص في الجرائم الإلكترونية، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح ورقلة، العدد 2، ديسمبر 2009.

11- بوبرقيق عبدالرحيم، مفهوم أنظمة المعالجة الآلية للمعطيات في الجرائم المحددة في المواد 394 مكرر إلى 394 مكرر 2 من قانون العقوبات الجزائري، مجلة الدراسات والبحوث القانونية، جامعة المسيلة، المجلة 4، العدد 1، جوان 2019. رابط المقال: http://asjp.cerist.dz/en/downArticle/461/4/1/95905

12- بومعيزة جابر، الإعتداء على المعطيات الآلية في الحكومة الإلكترونية، مجلة البحوث والدراسات القانونية والسياسية، جامعة لونيس علي البليدة 2، المجلد 6، العدد 2، جوان 2017.

13- جاسم خريبط خلف، الدليل الجنائي في الجريمة المعلوماتية، قسم القانون، كلية شط العرب، الجامعة.

14- حديدان سفيان، الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، المجلد 2، العدد 4، ديسمبر 2017.

رابط المقال: http://asjp.cerist.dz/en/downArticle/457/2/4/80500

15- حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي دراسة على ضوء القانون 18-07، مجلة الإجتهاد للدراسات القانونية والإقتصادية، المركز الجامعي تمنراست، المجلد 08، العدد 04، جوان 2019. رابط المقال: http://asjp.cerist.dz/en/downArticle/222/8/4/94785

16- حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد1، سبتمبر 2009.

رابط المقال: http://asjp.cerist.dz/en/downArticle/20/1/1/4425

17-حمادي كردلاس، حماية المعطييات الشخصية، مجلة قانونك، المغرب، ص 1، على الموقع www.ganonak.com

18-حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الاكاديمية للبحث القانوني ، المجلد 14، العدد2 لسنة 2016.

رابط المقال: http://asjp.cerist.dz/en/downArticle/72/7/2/4923

19-حمي أحمد، كيسي زهيرة، صور جرائم تقنية المعلومات وفقا للإتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 10، العدد 1، أفريل 2019.

رابط المقال: http://asjp.cerist.dz/en/downArticle/110/10/1/91408

20- خليفي محمد، إشكالية الإختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية، مجلة الميزان، المركز الجامعي بالنعامة، العدد1، ديسمبر 2016.

21- درياد مليكة، المساس بأنظمة المعالجة الآلية للمعطيات، حوليات جامعة الجزائر 1، الجزء الأول، العدد 33، ، مارس 2019.

رابط المقال: http://asjp.cerist.dz/en/downArticle/18/33/1/83941

22- دليلة العوفي، إشكالية مواكبة الجزائر لمجتمع المعلومات من الفجوة الرقمية إلى الجريمة المعلوماتية، مجلة الحكمة للدراسات الإعلامية والإتصالية، المجلد 4، العدد 8، نوفمبر 2016.

23- رابح وهيبة، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد الرابع، ديسمبر 2014.

24- رابحي أحسن، الجريمة الإلكترونية: النقطة"المظلمة" بالنسبة للتكنولوجية المعلوماتية، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد1، سبتمبر 2009.

رابط المقال: http://asjp.cerist.dz/en/downArticle/20/1/1/4420

25- رامي حليم، جرائم الإعتداء على أنظمة المعالجة الآلية للمعلومات، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجلد 1، العدد 1، سبتمبر 2009.

رابط المقال: http://asjp.cerist.dz/en/downArticle/20/1/1/4431

26- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة ورقلة، المجلد 3، العدد 2، جوان 2012.

27- زياد خليف العنزي، إختصاص القضاء الإمارتي بنظر المنازعات الإلكترونية ذات العنصر الأجنبي، مجلة جامعة الشارقة، أبوظبي-الإمارت، المجلد 15، العدد 2، ديسمبر 2018.

28- طباش عزالدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري- دراسة في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، لبنان، العدد 2، سنة 2018.

رابط المقال: http://asjp.cerist.dz/en/downArticle/72/9/2/71027

29- كريمة علة، الجهات القضائية الجزائية ذات الإختصاص الواسع، مجلة revue Academique de la Recherche jurdique، جامعة عبدالرحمان ميرة بجاية، المجلد 6، العدد1، سبتمبر 2015.

30- ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة الحقوق والعلوم السياسية، جامعة الوادي، المجلد 8، العدد 2، جوان 2017. رابط المقال: http://asjp.cerist.dz/en/downArticle/110/8/2/46702

31- محمد حماد مرهج الهيتي، جريمة الدخول الى النظام الآلي لمعالجة المعطيات عن طريق الغش، مجلة كلية الحقوق، جامعة النهرين، المجلة 9، العدد 10، السنة محرم 1427-شباط 2006.

32- محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد1، سبتمبر 2009.

رابط المقال: http://asjp.cerist.dz/en/downArticle/20/1/1/4433

33- محمد خليفة، دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية للقانون والعلوم السياسية( revue critique de drait et sciences politiques)، جامعة مولود معمري تيزي وزو، المجلد 13، العدد 1، جوان 2018.

رابط المقال: http://asjp.cerist.dz/en/downArticle/381/13/1/100754

34- محمد هاشم ماقورا، الحماية الجنائية لبرامج الحاسب الآلي، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد1، سبتمبر 2009. رابط المقال: http://asjp.cerist.dz/en/downArticle/20/1/1/4423

35- مريم لوكال، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 18-07، مجلة العلوم القانونية والسياسية ، جامعة الوادي، المجلد 10، العدد 01، أفريل 2019.

رابط المقال: http://asjp.cerist.dz/en/downArticle/110/10/1/91438

36- مزاولي محمد، المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الإلكترونية في القانون الجزائري، مجلة دراسات وأبحاث، جامعة عاشور زيان الجلفة، المجلد 1،العدد 1 ، سبتمبر 2009.

رابط المقال: http://asjp.cerist.dz/en/downArticle/20/1/1/4428

37- مصطفى الفوركي، الجرائم الماسة بالنظم المعلوماتية في القانون المغربي، مجلة البحوث القانونية والإقتصادية، المركز الجامعي لافلو، المجلد 2، العدد 1، جانفي 2020.

38- نبيلة هبة هروال، دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية للقانون والعلوم السياسية(revue critique de drait et sciences politiques)، جامعة مولود معمري تيزي وزو، المجلد 13، العدد 1، جوان 2018.

39- نبيلة هبة هروال، ماهية جرائم الأنترنت، مجلة المعيار، المركز الجامعي تيسمسيلت، المجلد 3، العدد 5، جوان 2012.

40- صالح شنين، إجراءات التحري والتحقيق في جرائم تكنولوجيات الإعلام والإتصال في التشريع الجزائري(قانون 09-04)، مجلة الدراسات الحقوقية، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي سعيدة، العدد الأول،سنة 2014.

41- عائشة بن قارة مصطفى، ضرورة آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم(18-07)، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 10، العدد 01، أفريل 2019. رابط المقال: http://asjp.cerist.dz/en/downArticle/110/10/1/91406

42- عباوي نجاة، الإشكالات القانونية في تجريم الإعتداء على أنظمة المعلومات، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية جامعة ورقلة، المجلد9، العدد 16 ، جانفي 2017.

43- عثمان بكر عثمان، المسؤولية عن الإعتداءات على البيانات الشخصية لمستخدمي شبكات التواصل الإجتماعي، كلية الحقوق، جامعة طنطا، مصر، بدون سنة.

44- عراب مريم، الإختصاص القضائي في الجرائم المعلوماتية، مجلة annales de facute de droit، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد وهران، المجلد 7، العدد3، ديسمبر 2015.

45- عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد 1، العدد 1، سبتمبر 2009.
رابط المقال: http://asjp.cerist.dz/en/downArticle/20/1/1/4438

46- علي حسن الطوالبة، التعاون القضائي الدولي في مجال مكافحة الجرائم الإلكترونية، مركز الإعلام الأمني.

47- عمراني أحمد، الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في التشريع الجزائري والمقارن، مجلة الحضارة الإسلامية، جامعة وهران السانية، المجلد 13، العدد16، ماي 2012.
رابط المقال: http://asjp.cerist.dz/en/downArticle/45/13/16/51820

48- غزال نسرين، حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، المجلة الجزائرية للعلوم القانونية والسياسية ، جامعة بن يوسف بن خدة الجزائر، المجلد 56، العدد 01،جوان 2019.
رابط المقال: http://asjp.cerist.dz/en/downArticle/32/56/1/97108

49- سامح عبدالواحد التهامي، ضوابط معالجة البيانات الشخصية"دراسة مقارنة بين القانون الفرنسي والقانون الكويتي"، مجلة كلية القانون الكويتية العالمية، الكويت، بدون سنة.

50- شرف الدين وردة، بلجراف سامية، الجوانب الموضوعية والإجرائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية، جامعة فارس يحي المدية، المجلد 1، العدد 3، ديسمبر 2017.

51- شوقي يعيش تمام، عزيزة شبري، تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الإجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 9، العدد15، جوان 2017.

52- يزيد بوخلط، تفتيش المنظومات المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل ET-Tawassal ، كلية الحقوق والعلوم السياسية، جامعة باجي مختار عنابة، المجلد 22، العدد 2، ديسمبر 2016.

53- يعيش تمام شوقي، خليفة محمد، نظام المعالجة الآلية المعطيات كأساس للحماية الجزائية في التشريع الجزائري، مجلة جيل للأبحاث القانونية المعمقة، مركز جيل البحث العلمي، العام الثالث، العدد 25، مايو 2018.

**خامسا: بحوث ومداخلات**

**بحوث:**

1- أمحمدي بوزينة أمنة ، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، أعمال الملتقى الوطني: مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل للبحث العلمي، الجزائر 29 مارس 2017.

2- الهادي خضراوي، عبدالحليم بوقرين، تجربة الجزائر في مكافحة الجريمة الإلكترونية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية-السعودية، نوفمبر 2015.

3- جورج أسحق حنين، دراسة عن الجرائم المعلوماتية والإلكترونية عبر شبكة الأنترنت وسبل مواجهتها، الإدارة العامة المركزية للمعلومات الإحصائية، الإدارة المركزية لمركز المعلومات والتوثيق، قطاع مكتب الوزير، وزير المالية، ستة 2015.

4- حفوظة الأمير عبد القادر، غرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، مركز جيل البحث العلمي، أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة 29 مارس 2017.

5- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحوث مؤتمر القانون والكومبيتر والأنترنت، المجلد الثالث من 1 الى 3 مايو 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الطبعة الثالثة، 2004.

5- مصطفى محمد عرجاوي، الحماية المدنية لبرامج الكومبيوتر في القوانين الوضعية، بحوث مؤتمر القانون والكومبيتر والأنترنت، المجلد الثاني من 1 الى 3 مايو 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الطبعة الثالثة، 2004.

6- موسى مسعود أرحومة، بحث بعنوان الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس خلال الفترة 28- 29 أكتوبر 2009.

7- سعدات، محمود فتوح محمد، بحث بعنوان خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات-جامعة الأمام محمد بن سعود الإسلامية، الرياض- المملكة العربية السعودية، نوفمبر 2015.

**المداخلات:**

[1]- حسين نوارة، مقال بعنوان آليات تنظيم المشرع الجزائري لجريمة الإعتداء على الحق في الحياة الخاصة إلكترونيا، مركز جيل البحث العلمي، أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة 29 مارس 2017.

2- مزياني عبدالغني قاضي تحقيق لدى محكمة المسيلة، مداخلة بعنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعلومات، محكمة المسيلة، مجلس قضاء المسيلة، وزارة العدل.

**المواقع الإلكترونية:**

https:akhbarak.net.news

**باللغة الأجنبية**

## Ouvrages gènèraux:

1-Myriam Quéméner, yves charpenal (cybercriminalité droit penal appliqué), économica ,paris ,France , 2010.

2- MEUNIER.C : ia loi du 28 novembre 2000 relative à la Criminalitè informatique, formation Permanent CUP, fevrier 2001.

3 -Michel veron, droit pènal spècial, 6ème èdition armand colin, paris, 1998.

## Sites internet:

1-Alain-ben soussan , fraude informatique, la protèction d'un sustème informatique par un dispositif de sècuritè n èst pas une condition dàpplication de la loi God frain, art, disponble en lingne à làdresse suivante http://www.alain-bensossan.com/page/2903.

## Jurisprudencesur:

1 - cass. Crim 8 dècember 1999,
2- cass crim 5 janvier 1994.

.

.

# الفهرس

| العنوان | الصفحة |
|---|---|
| **إهداء** | أ |
| **شكر وتقدير** | ب |
| **قائمة المختصرات** | ج |
| **مقدمة** | 2 |
| **الفصل التمهيدي.**<br>**الإطار المفاهيمي لنظام المعالجة الآلية للمعطيات** | 16 |
| **المبحث الاول**: ماهية نظام المعالجة الآلية للمعطيات | 17 |
| **المطلب الاول**: مفهوم نظام المعالجة الآلية للمعطيات | 17 |
| **الفرع الأول**: تعريف النظام | 17 |
| **الفرع الثاني**: تعريف نظام المعالجة الآلية للمعطيات | 20 |
| **المطلب الثاني**: تمييز نظام المعالجة الآلية للمعطيات عن المصطلحات المشابهة لها | 30 |
| **الفرع الأول**: تمييز نظام المعالجة الآلية للمعطيات عن الجريمة المعلوماتية | 30 |
| **الفرع الثاني**: تمييز المساس بنظام المعالجة الآلية للمعطيات عن المساس بالمعطيات والبرامج | 34 |
| **الفرع الثالث**: تمييز جرائم نظام المعالجة الآلية للمعطيات عن جرائم المعطيات الشخصية | 36 |
| **الفرع الرابع**: تمييز جرائم نظام المعالجة الآلية للمعطيات عن جرائم الأنترنت | 37 |
| **المبحث الثاني**: عناصر نظام المعالجة الآلية للمعطيات | 38 |
| **المطلب الاول**: العناصر المادية | 38 |
| **الفرع الأول:** وحدات الإدخال | 38 |
| **الفرع الثاني:** وحدة المعالجة المركزية | 39 |
| **الفرع الثالث:** وحدات الإخراج | 42 |

| | |
|---|---|
| **المطلب الثاني**: العناصر المعنوية | 43 |
| **الفرع الأول:** البرامج | 43 |
| **الفرع الثاني:** المعطيات | 47 |
| **المطلب الثالث**: شبكات الإتصال | 51 |
| **المبحث الثالث**: أهمية الحماية لنظام المعالجة الآلية للمعطيات | 55 |
| **المطلب الاول**: مبررات حماية نظام المعالجة الآلية للمعطيات | 55 |
| **الفرع الأول:** أهمية المعطيات المدرجة في النظم المعلوماتية | 55 |
| **الفرع الثاني:** إرتباط النظم المعلوماتية بالأنترنت | 57 |
| **الفرع الثالث:** النظم المعلوماتية تتطلب أساليب مستحدثة للمواجهة | 57 |
| **الفرع الرابع:** وجوب مقابلة تطور الفكر الإجرامي بتفعيل الفكر القانوني | 58 |
| **المطلب الثاني**: خصائص جرائم نظام المعالجة الآلية للمعطيات وتقنيات إرتكابها | 59 |
| **الفرع الأول:** خصائص جرائم نظام المعالجة الآلية للمعطيات | 59 |
| **الفرع الثاني:** تقنيات إرتكاب جرائم نظام المعالجة الآلية للمعطيات | 70 |
| **المطلب الثالث**: قصور الحماية الفنية لنظام المعالجة الآلية للمعطيات | 71 |
| **الفرع الأول:** عدم كفاية الحماية الفنية لنظام المعالجة الآلية للمعطيات | 71 |
| **الفرع الثاني:** دور الحماية الجنائية في الوقاية من جرائم نظام المعالجة الآلية للمعطيات | 74 |
| **الباب الأول.**<br>**الحماية الموضوعية لنظام المعالجة الآلية للمعطيات.** | 77 |
| **الفصل الأول.**<br>**الحماية الجنائية للمعطيات ذات الطابع الشخصي.** | 81 |
| **المبحث الاول**: الإطار القانوني لحماية المعطيات ذات الطابع | 86 |

| | |
|---|---|
| الشخصي | |
| **المطلب الاول**: مفهوم المعطيات ذات الطابع الشخصي | 86 |
| **الفرع الأول**: تعريف المعطيات ذات الطابع الشخصي | 86 |
| **الفرع الثاني**: المصادر التي تهدد خصوصية المعطيات ذات الطابع الشخصي | 91 |
| **المطلب الثاني**: القواعد القانونية للحماية الجنائية للمعطيات ذات الطابع الشخصي | 96 |
| **الفرع الأول**: حقوق الشخص المعني بالمعطيات المزمع معالجتها | 96 |
| **الفرع الثاني**: الإلتزامات الملقاة على عاتق المسؤولين عن المعالجة | 108 |
| **المبحث الثاني**: الجرائم المرتبطة بالمعطيات ذات الطابع الشخصي | 116 |
| **المطلب الاول**: صور جرائم المعطيات ذات الطابع الشخصي | 118 |
| **الفرع الأول**: تجريم الجمع والإستغلال غير المشروع للمعطيات ذات الطابع الشخصي | 118 |
| **الفرع الثاني**: تجريم المخالفات المرتكبة أثناء إنشاء المعالجة | 126 |
| **المطلب الثاني**: آليات الحماية الجنائية للمعطيات ذات الطابع الشخصي | 130 |
| **الفرع الأول**: المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي | 131 |
| **الفرع الثاني:** السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي | 136 |
| **الفرع الثالث**: العقوبات المقررة لجرائم المعطيات ذات الطابع الشخصي | 140 |
| **الفصل الثاني.**<br>**أركان جرائم نظام المعالجة الآلية للمعطيات.** | 155 |

| | |
|---|---|
| **المبحث الأول**: أركان جرائم المساس بنظام المعالجة | 157 |
| **المطلب الأول**: أركان جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة | 157 |
| **الفرع الأول**: الركن المادي | 159 |
| **الفرع الثاني**: الركن المعنوي | 168 |
| **الفرع الثالث**: العقوبات المقررة لهذه الجريمة | 171 |
| **المطلب الثاني**: أركان جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة | 175 |
| **الفرع الأول**: الركن المادي | 176 |
| **الفرع الثاني**: الركن المعنوي | 180 |
| **الفرع الثالث**: العقوبات المقررة لهذه الجريمة | 182 |
| **المبحث الثاني**: أركان جرائم المساس بمعطيات نظام المعالجة الآلية | 185 |
| **المطلب الأول**: أركان جريمة التلاعب بالمعطيات | 186 |
| **الفرع الأول**: الركن المادي | 190 |
| **الفرع الثاني**: الركن المعنوي | 201 |
| **الفرع الثالث**: العقوبات المقررة لهذه الجريمة | 206 |
| **المطلب الثاني**: أركان جريمة التعامل في معطيات غير مشروعة | 208 |
| **الفرع الأول**: الركن المادي | 210 |
| **الفرع الثاني**: الركن المعنوي | 225 |
| **الفرع الثالث**: العقوبات المقررة لهذه الجريمة | 235 |
| **خلاصة الباب الأول** | 239 |
| **الباب الثاني.**<br>**الحماية الإجرائية لنظام المعالجة الآلية للمعطيات.** | 241 |
| **الفصل الأول.**<br>**التدابير المستحدثة للوقاية وللبحث والتحري في الكشف عن** | 246 |

| | |
|---|---|
| **جرائم نظام المعالجة الآلية للمعطيات.** | |
| **المبحث الأول**: التدابير المستحدثة للوقاية من جرائم نظام المعالجة الآلية للمعطيات | 248 |
| **المطلب الأول**: التدابير الوقائية المتعلقة بمراقبة الإتصالات الإلكترونية | 248 |
| **الفرع الأول**: مراقبة الإتصالات الإلكترونية عن طريق القضاء | 249 |
| **الفرع الثاني**: مراقبة الإتصالات الإلكترونية عن طريق هيئات خاصة | 251 |
| **المطلب الثاني**: التدابير الوقائية المتعلقة بإلتزامات مقدمي الخدمة بالنسبة للإتصالات الإلكترونية | 256 |
| **الفرع الأول**: الإلتزامات العامة لمقدمي الخدمات بالنسبة للإتصالات الإلكترونية (الأنترنت) | 257 |
| **الفرع الثاني**: الإلتزامات الخاصة لمقدمي الخدمات بالنسبة للإتصالات الإلكترونية (الأنترنت) | 262 |
| **المبحث الثاني**: التدابير الإجرائية للبحث والتحري في الكشف عن جرائم نظام المعالجة الآلية للمعطيات | 268 |
| **المطلب الأول**: التدابير الإجرائية المتعلقة بالتفتيش في النظام المعلوماتي | 296 |
| **الفرع الأول**: إجراءات التفتيش في النظام المعلوماتي | 271 |
| **الفرع الثاني**: تمديد التفتيش في النظم المعلوماتية | 277 |
| **المطلب الثاني**: التدابير الإجرائية المتعلقة بحجز المعطيات المعلوماتية | 283 |
| **الفرع الأول**: الحجز عن طريق نسخ المعطيات المعلوماتية | 286 |
| **الفرع الثاني**: الحجز عن طريق منع الوصول إلى المعطيات | 293 |
| **الفصل الثاني.**<br>**الآليات الإجرائية الدولية لمكافحة جرائم نظام المعالجة الآلية** | 300 |

| | |
|---|---|
| **للمعطيات.** | |
| **المبحث الأول**: الإختصاص القضائي الدولي في جرائم نظام المعالجة الآلية للمعطيات | 302 |
| **المطلب الأول**: تنظيم الإختصاص القضائي الدولي في جرائم نظام المعالجة الآلية للمعطيات | 305 |
| **الفرع الأول**: تنظيم الإختصاص القضائي الدولي في الإتفاقيات الدولية | 305 |
| **الفرع الثاني**: تنظيم الإختصاص القضائي الدولي في القوانين الداخلية | 309 |
| **المطلب الثاني**: تنازع الإختصاص القضائي الدولي في جرائم نظام المعالجة الآلية للمعطيات | 313 |
| **الفرع الأول**: موقف الفقه الجنائي من مسألة تنازع الإختصاص القضائي الدولي | 315 |
| **الفرع الثاني**: موقف الإتفاقيات الدولية من مسألة تنازع الإختصاص القضائي الدولي | 317 |
| **المبحث الثاني**: المساعدة القضائية الدولية المتبادلة | 321 |
| **المطلب الأول**: طلبات المساعدة القضائية الدولية المتبادلة | 323 |
| **الفرع الأول**: تنفيذ طلبات المساعدة القضائية الدولية المتبادلة | 326 |
| **الفرع الثاني**: رفض تنفيذ طلبات المساعدة القضائية الدولية المتبادلة | 331 |
| **المطلب الثاني**: المجالات الخاصة بالمساعدة القضائية الدولية المتبادلة لمكافحة جرائم نظام المعالجة الآلية للمعطيات | 335 |
| **الفرع الأول**: المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة | 335 |
| **الفرع الثاني**: المساعدة القضائية المتبادلة في مجال سلطات التحقيق | 339 |

| | |
|---|---|
| **خلاصة الباب الثاني** | 345 |
| **الخاتمة** | 347 |
| **قائمة المراجع** | 363 |
| **فهرس الموضوع** | 392 |
| **الملخص** | 400 |

# الملخصات

## الملخصات


### - باللغة العربية

تعتبر جرائم نظام المعالجة الآلية للمعطيات من الجرائم المستحدثة وذات طابع دولي ولها مميزاتها الخاصة، الأمر الذي جعل الشرائع الدولية والتشريعات الداخلية تقوم بتكريس حماية جنائية فعالة لنظام المعالجة الآلية للمعطيات لمواجهة الخسائر الكبيرة التي تهدد مصالح الأفراد والدول، وذلك من خلال إرساء جملة من التدابير المستحدثة غير المألوفة في القوانين السابقة والأكثر ملائمة مع خصوصيات جرائم نظام المعالجة الآلية للمعطيات، تتنوع بين تدابير وقائية وأخرى إجرائية.



**الكلمات الفتاحية:** المعالجة الآلية، المعطيات، النظام، الحماية الجنائية، تفتيش النظام ، حجز االمعطيات، المعطيات ذات الطابع الشخصي.


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -


### - باللغة الفرنسية

Les crimes de traitement automatisé des données sont considérés comme de nouveaux crimes de nature internationale et ont leurs propres caractéristiques, ce qui a fait que les lois internationales et la législation interne consacrent une protection pénale efficace au système de traitement automatique des données pour faire face aux pertes importantes qui menacent les intérêts des individus et des États.en établissant un ensemble de nouvelles mesures inhabituelles dans les lois, le précédent et les plus appropriés aux spécificités du système de traitement automatique des crimes variaient entre les mesures préventives et procédurales.



**Mots clés:** Traitement automatisé des données-système de données-système de protection pénale-inspection-taille des données-données personnelles du personnel.


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -


### - باللغة الإنجليزية

Automated data processing crimes are considered to be new crimes of an international nature and have their own characteristics, which made international laws and internal legislation devote effective criminal protection to the automatic data processing system to confront the large losses that threaten the interests of individuals and states by establishing a set of new unfamiliar measures in lawsthe precedent and the most appropriate to the specifics of the Automatic Processing System crimes varied between preventive and procedural measures.



**The Key Word:** Automated data processing-data-system-penal protection-inspection system-sized data-private personnel data.