

الجريمة المعلوماتية بين التكييف الوطني والمجابهة الدولية

Information crime between national conditioning and international confrontation

د. درار عبد الهادي

كلية الحقوق والعلوم السياسية.

جامعة جيلالي ليايس-سيدي بلعباس-

الايمل:derrarm@hotmail.fr

ملخص:

إن التطور الحاصل في مجال تكنولوجيا الإعلام والاتصال وظهور شبكات الإنترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام لأنه بقدر ما أحدث آثار إيجابية وغير نمط حياة المجتمعات وذهب بهم إلى التطور والرفق في جميع المجالات ولا سيما المعاملات الإلكترونية. بقدر ما كان له أثر سلبي على حياة الناس ومصالحهم ومصالح الدول، هذا كله تجلى في تطوير الإنترنت ووسائله المعلوماتية لتكون عالما من عوالم الجريمة. وهكذا ظهرت إلى الوجود الجرائم الإلكترونية بشتى أنواعها. لذلك سوف نخوض في التعرف على معنى هذه الجريمة المعلوماتية وكيف تم التعامل معها من أجل مواجهتها.

الكلمات المفتاحية: تكنولوجيا الإعلام والاتصال ، المجرم الإلكتروني ، الإنترنت ، الجرائم السيبرانية.

Summary:

The development in the field of information and communication technology and the emergence of the Internet with all its progress and services did not pass safely to the world because, to the extent that it has brought positive effects and changed the lifestyle of societies, it has taken them to development and advancement in all fields, especially electronic transactions. As much as it had a negative impact on people's lives, their interests, and the interests of nations, all this was manifested in the development of the Internet and its information means to be a world of crime. Thus, cybercrime of all kinds appeared. Therefore, we will delve into the meaning of this information crime and how it was dealt with in order to confront it.

Keywords: Media and communication technology, cyber criminal, internet, cybercrime.

تواجه رقعة العلوم الجنائية اليوم أحدث وأخطر صور الجريمة التي انتشرت نتيجة المزاوجة بين تقنيات الإعلام الآلي و تكنولوجيا الإتصالات أو ما يعرف بثورة تكنولوجيا المعلومات وهي الجريمة المعلوماتية، الأمر الذي فرض على الدول ضرورة التدخل والتصدي لهذه الجرائم المستحدثة وكبح مخاطرها سواء على الأموال أو الأشخاص التي لم تعد منحصرة في إقليم الدولة الواحدة وإنما تعداها ليصبح الأمر ذو شأن دولي. مما جعل الدول - ومنها الجزائر - تضع نصوص وتشريعات تواجه بها الإجرام ولكن في غالبيتها تصطدم بفكرة تنازع الاختصاص القضائي إما على أساس مبدأ الاختصاص الشخصي في جانبه الايجابي أو على أساس مبدأ الاختصاص العيني، الأمر الذي يفرض أن يكون هناك تعاون دولي يتفق مع طبيعة الإجرام السيبراني الذي يتميز بطابع خاص يقتضي أن تكون هناك ردود فعل سريعة لأن هذا التنسيق الفعال والعاجل يساعد على الحد من الأضرار الناجمة عن هذه الجرائم المعلوماتية وكذلك تجنب المجرم المعلوماتي الإفلات من العقاب.

من خلال ما سبقتساغ الإشكالية التالية: مدى كفاية النصوص التشريعية الجزائرية للتصدي للجريمة المعلوماتية؟ وهل تم حصرها ومجابتها في إطار ما يعرف بالإتفاق أو التعاون الدولي؟
لتمحيص هذه الدراسة تم الإعتماد على المنهج الاستدلالي المقارن لعرض بعض التجارب الدولية ومطابقتها للإتفاقيات و المعاهدات التي تناولت الموضوع. لذلك تم تقسيم هذا الموضوع إلى الإطار المفاهيمي للجريمة المعلوماتية (المبحث الأول) ثم إلى ثبات النص الجزائري وتكامله مع الإتفاق الدولي لمواجهة الجريمة المعلوماتية (المبحث الثاني).

المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية

تتعدد أشكال السلوك السلبي وتتطور وتتخذ أشكالا لا حصر لها تبعا لما يتوفر بين يدي الإنسان من وسائل لإيقاع الفعل وتحقيق نتائجه في الواقع العملي.

وإنطلاقا من ذلك فقد ظهرت للوجود سلوكيات سلبية خطيرة تبعا لظهور تقنية نظم المعلومات والإتصالات التي وضعت بين يدي البعض وسائل وطرق حديثة لإيقاع جرائمهم بسهولة وخفة، فكان أن أحدثت هذه السلوكيات المستحدثة ثورة هائلة في النظرية العامة للجريمة على اختلاف مستوياتها¹.

¹ جلال محمد الزغي وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة)، ط 1، دار الثقافة للنشر والتوزيع، الاردن 2010، ص

وتعد الجريمة الإلكترونية من الجرائم التي استحضرتها الممارسة السيئة لثورة تكنولوجيا المعلوماتية التي تختلف كثيرا عن الجريمة التقليدية في طبيعتها وأنواعها وأدواتها، وحتى في خصوصية وتمييز مرتكبيها. وهذا ما سنخرج إليه من خلال هذا المبحث.

المطلب الأول : تعريف الجريمة الإلكترونية

قبل الخوض في إعطاء تعاريف الجريمة الإلكترونية لابد من الإشارة إلى المصطلحات المتعلقة بهذه الجريمة والتي نذكر منها:

1. الحاسب الآلي: هو عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما، وذلك بتنفيذ ثلاث عمليات أساسية هي : إستقبال البيانات المدخلة (الحصول على حقائق المجردة)، ومعالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المداخلات)، وإظهار المعلومات المخرجة (الحصول على نتائج)² كما يعرف بأنه : " أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو إستقبالها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له"³ ومن بين التعريفات التي أجمع عليها الفقه حول تعريف الحاسب الآلي : " مجموعة من الأجزاء المتداخلة المادية والمعنوية وبتكامل هذه الأجهزة يقوم الجهاز ب إستقبال البيانات ومعالجتها من خلال مجموعة من عمليات حسابية بسرعة عالية وتسلسل منطقي تظهر بعدها النتائج المطلوبة ويمكن تخزينها والإستفادة منها مرات عديدة"⁴

2. المعلومات: وهي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنيته المعلومات بوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها.⁵

3. كلمة إلكتروني: يقصد بها تقنية إستعمال وسائل كهربائية أو كهرومغناطيسية أو بصرية أو أي شكل آخر من وسائل التقنية المتشابهة.⁶

² نحلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2008، ص 20.

³ محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت (دراسة مقارنة)، ط1، دار الفكر والقانون للنشر والتوزيع، مصر، 2013، ص 8.

⁴ خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الاسكندرية، 2008، ص 20.

⁵ محمود أحمد طه، المرجع السابق، ص 8.

⁶ خالد ممدوح إبراهيم، المرجع السابق، ص 26.

4. المجرم المعلوماتي: وهو شخص يتمتع بالمهارة والمعرفة والوسيلة والسلطة وكذلك الباعث⁷ من أجل تنفيذ نشاطه الإجرامي.

فالجاني في جرائم التقنية شخص طبيعي، يتوافر لديه كشرط أساسي معرفة كافية بآلية عمل وتشغيل الحاسب الآلي، ولا نقصد هنا المستوى الرفيع العالي من المعرفة، فإن الجريمة وإن كانت ترتبط بتقنية نظم المعلومات والحاسب الآلي من حيث السعة والأسلوب والنتيجة، إلا أن الحد الأدنى من المعرفة يكفي لظهور الجريمة وإمكانة ارتكابها خصوصا إذا ما اتسعت دائرة الإجماع فإستعان الفاعل ذاته بغيره ممن يساعده في إيقاع الجريمة وإرتكابها.⁸

ويُقسم مجرمو المعلوماتية (Cyber Criminels) إلى مجموعة من الطوائف المختلفة، وهذا التصنيف كان قائما على أساس أغراض الإعتداء، وقد وجد الباحثون صعوبة في إيجاد تصنيف منضبط لمجرمي هذه التقنية والسبب راجع إلى التغير السريع الحاصل في نطاق هذه الظاهرة المرتبطة أساسا بالتسارع الرهيب في ميدان الكمبيوتر والانترنت.

ومن أفضل التصنيفات لمجرمي التقنية تقسيم المجرمين إلى ثلاث طوائف وهي:

أ- المخترقون أو المتطفلون: وهذه الفئة من المجرمون ينطلقون من دوافع التحدي وإثبات الذات والمقدرة التقنية، ويتسمون كذلك بصغر السن، وكذلك لا تتوافر لديهم دوافع حاقدة أو تخريبية أو ربحية فهم يسعون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها.⁹

⁷ الدافع أو الباعث أو الغرض أو الغاية : تعبيرات لها دلالة اصطلاحية في القانون الجنائي، وهنا الباعث يكون إما من أجل : السعي الى تحقيق المكسب المالي او الانتقام من رب العمل والحاق جلال محمد الزغي وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة)، ط1، دار الثقافة للنشر والتوزيع، الاردن 2010، ص 21.

⁷ نخلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2008، ص 20.

⁷ محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت (دراسة مقارنة)، ط1، دار الفكر والقانون للنشر والتوزيع، مصر، 2013، ص 8.

⁷ خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، دار الجامعية، الاسكندرية، 2008، ص 20.

⁷ محمود أحمد طه، المرجع السابق، ص 8.

⁷ خالد ممدوح ابراهيم، المرجع السابق، ص 26.

⁷ الدافع أو الباعث أو الغرض أو الغاية : تعبيرات الضرر بمال الرغبة في اختراق نظام الكمبيوتر والتفوق على تعقيد وسائل التقنية ، دوافع سياسية أو اقتصادية أو دينية راجع: نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2013، ص 60. وأيضا : يوسف صبيدي، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص ص 40-41.

⁸ أسامة احمد المناعسة وجمال مُجد الزغي، المرجع السابق، ص 71.

⁹ محمود أحمد طه، المرجع السابق، ص 14.

ب- مجرمو الكمبيوتر المحترفون: تتمتع هذه الطائفة بسعة الخبرة والإدراك للمهارات التقنية كما تتميز بالتخطيط والتنظيم للأنشطة التي يرتكبها أفرادها فهم يسعون من وراء ذلك إلى تحقيق الربح المادي بطريقة غير مشروعة، ويتم عمل هذه المجموعة في إطار منظم ينطبق على أفعالهم وصف الجريمة المنظمة¹⁰ وتعد هذه الطائفة الأخطر من بين مجرمي التقنية.

ج-الحاقدون: تسعى هذه الطائفة من المجرمين إلى الرغبة في الإنتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف النشأة المعنية عندما لا يكونوا موظفين فيها. وتغلب على أنشطتهم من الناحية التقنية إستخدام تقنيات زراعة الفيروسات والبرامج الضارة وتخريب النظام أو إتلاف كل أو بعض معطياته.¹¹

وتجدر الإشارة إلى أنه إزاء التصدي لظاهرة الإجرام المعلوماتي لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، حيث ذهب جانب إلى تناولها بالتعريف على نحو ضيق، وجانب آخر عرفها على نحو متسع.

أما بالنسبة للمشرع الجزائري لم يعرف الجريمة الإلكترونية وإنما تبنى للدلالة على الجريمة بالمصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة.

أ - التعريف الضيق للجريمة الإلكترونية

ما ذهب اليه الفقيه MERWE حيث يرى أن الجريمة المعلوماتية¹² هي: "الفعل غير المشروع الذي يتورط في إرتكابه الحاسب الآلي، أو هي مختلف صور السلوك الإجرامي التي ترتكب ب إستخدام المعالجة الآلية للبيانات"¹³.

ويرى الأستاذ MASS أن المقصود بالجريمة المعلوماتية : " الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح "¹⁴

¹⁰ طارق ابراهيم الدسوقي عطية، عولمة الجريمة (الشراكة العالمية في الممارسات الاجرامية)، دار الجامعة الجديدة، د.ط، الاسكندرية، 2010، ص 238.

¹¹ محمود أحمد طه، المرجع السابق، ص 15. وأيضا طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 237.

¹² مصطلح المعلوماتية Informatique : هي اختصار مزجي لكلمتي معلومة Information وكلمة آلي Automatique، وهي تعني المعالجة الآلية للمعلومة.

¹³ طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 208.

¹⁴ فله عبد القادر المومني، المرجع السابق، ص 48.

كما أن مجرد استخدام الحاسب الآلي لا يضيف إلى السلوك غير المشروع جديداً، ولكن استخدام البيانات والمعلومات والبرامج هو الذي يمكن أن يضيف إلى الجريمة سمة الجريمة المعلوماتية.¹⁵ وجل هذه التعريفات تعرضت للنقد من قبل الفقه، لذلك حاول جانب آخر من الفقه تعريف الجريمة الإلكترونية على نحو واسع من أجل محاولة تفادي أوجه القصور التي شابت تعريفات الاتجاه المضيق في التصدي لظاهرة الإجرام المعلوماتي.

ب - التعريف الواسع لمفهوم الجريمة الإلكترونية

من بين التعريفات الموسعة للجريمة المعلوماتية ما ذهب إليه من الفقه الأستاذ هلالي عبد الله أحمد بقوله : " عمل أو إمتناع عن عمل يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات ويفرض للإعتداء عليها عقاباً"¹⁶ ويمتاز هذا التعريف بالمزايا التالية:

- ✓ أنه يحتوي على كل صور الإعتداء الإيجابية أو السلبية التي توقع أضرار بمكونات الحاسب المادية أو المعنوية.
- ✓ أنه يتضمن الأثر الجنائي المترتب على العمل أو الإمتناع غير المشروعين والذي يتمثل في الجزاء الجنائي بشتى صورته وأنواعه.
- ✓ يحافظ على الشرعية الجنائية : " لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"¹⁷.

ونظراً لخطورة هذه الجريمة وآثارها الممتدة التي قد تصل من دولة لأخرى، فإن بعض الهيئات الدولية المعنية بجرائم الكمبيوتر قد أرست قواعد لتعريف هذا النوع من الجرائم، من هذه الهيئات هيئة التعاون الإقتصادي للتنمية OECD، التي إتخذت التعريف التالي كتعريف لجريمة الكمبيوتر بأنها : " أي سلوك غير قانوني أو غير أخلاقي أو غير مفوض يتعلق بالنقل أو المعالجة الآلية للبيانات يعتبر إعتداء على الكمبيوتر "¹⁸.

¹⁵ محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الاسكندرية، 2001، ص 72.

¹⁶ عبد الله أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2000، ص 105.

¹⁷ راجع المادة الأولى من الأمر 66 / 154 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم

¹⁸ طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 214 و 215.

بعد التطرق إلى تعريف الجرائم الإلكترونية التي تعد إفرازا ونتاجا لتقنية المعلومات نخوض في البحث عن خصائص هذه الجريمة التي تميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من السمات قد يتطابق بعضها مع صفات أنواع أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فإن إختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية أكسبها خصوصية غير عادية.

المطلب الثاني : خصائص الجريمة الإلكترونية

يصعب متابعة جرائم الحاسب الآلي والإنترنت وكذا الكشف عنها، لأن هذه الجرائم لا تترك أثرا فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات ومعظم جرائم الحاسب الآلي تم إكتشافها بالصدفة وبعد وقت طويل من إرتكابها، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، وتعود أسباب صعوبة إثبات هذا النوع من الجرائم إلى الأمور التالية:

- ✓ أنها جريمة لا تترك أثرا بعد إرتكابها ويصعب الإحتفاظ بأثرها إن وجدت.¹⁹
- ✓ تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.
- ✓ أنها تعتمد على الخداع في إرتكابها والتضليل في التعرف على مرتكبها.
- بالإضافة إلى أن إرتباط الجريمة الإلكترونية بجهاز الحاسب الآلي وشبكة الأنترنت أضفى عليها مجموعة من الخصائص التي تميزها عن الجرائم التقليدية، ولعل من أهمها ما يلي:
- الخاصة الأولى : جرائم الحاسوب ترتكب بواسطة الحاسب الآلي وكذلك عبر شبكة الأنترنت فهي حلقة الوصل الرئيسية بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات وغيرها من الأهداف التي تكون غالبا الضحية لتلك الجرائم.²⁰

• الخاصية الثانية : أنها جريمة عابرة للحدود، فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود، وهو خلق العديد من المشاكل حول تحديد الدولة صاحبة الإختصاص القضائي بهذه الجريمة وكذلك حول تحديد القانون

¹⁹ طارق إبراهيم دسوقي عطية، المرجع السابق، ص 222.

²⁰ أمير يوسف فرج، المرجع السابق، ص 16.

الواجب تطبيقه بالإضافة إلى شكيلات تتعلق بإجراءات الملاحقة القضائية وغيرها من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.²¹

• الخاصية الثالثة : صعوبة التحري والتحقيق نظرا لإرتكابها في الخفاء، وعدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من أفعال إجرامية، فالتحري عنها ينطوي على العديد من المشكلات والتحديات الإدارية والقانونية، والتي تتصل ابتداء من عملية ملاحقة الجناة، فإذا تحققت إمكانية الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الإقرار القانوني بطبيعة الأدلة المتعلقة بهذه الجريمة.²²

• الخاصية الرابعة : تتسم بالخطورة البالغة من عدة جوانب، فمن ناحية أولى نجد الخسائر الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية خاصة جرائم الأموال، ومن ناحية ثانية نجدها ترتكب من فئات متعددة تجعل من التنبؤ بالمشيئة فيه أمرا صعبا ومن ناحية ثالثة تنطوي على سلوكيات غير مألوفة. ولا أدل على ذلك من أن الخسائر المادية الناجمة عن هذه الجرائم تبلغ وفقا لتقديرات المركز الوطني لجرائم الحاسب في الولايات المتحدة الأمريكية في نهاية القرن الماضي حوالي 500 مليون دولار في السنة، وذلك في نهاية القرن العشرين.²³

• الخاصية الخامسة : الصورة التقليدية للمجرم تكاد تختفي في هاته الجرائم بل وعلى العكس من ذلك فالمجرم المعلوماتي عادة ما ينتمي إلى مستوى إجتماعي مرتفع عن غيره من المجرمين ونادرا ما يكون محترفا للإجرام أو عائدا، كما أنه لا ينظر إليه كمجرم بالمعنى المتعارف عليه لهذه الكلمة وذلك لكون الأسباب والعوامل التي تقف وراء إرتكاب الجريمة المعلوماتية تختلف بالمقارنة بالجريمة التقليدية.²⁴

• الخاصية السادسة : قلة الإبلاغ عن وقوع الجريمة المعلوماتية، وذلك راجع لسببين أولهما الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الإنترنت تم الكشف عنها بالصدفة أو بعد فترة طويلة

²¹ فتية رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماجستير، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011-2012، ص 43.

²² محمود أحمد طة، المرجع السابق، ص 13.

²³ طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 287.

²⁴ سفيان سوير، جرائم للمعلوماتية، مذكرة ماجستير، تخصص العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010 - 2011، ص 18 و 19.

من إرتكابها، والسبب الثاني هو عدم إكتشاف الضحية للجريمة مما يعني أن الجرائم التي حدثت ولم يتم إكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها.²⁵

وعليه فالجريمة الإلكترونية تعتبر من أحدث أنواع الجرائم، مسرحها العالم الافتراضي غير ملموس بعيدة عن أي مظهر من مظاهر الجريمة التقليدية فهي جريمة عابرة للحدود يرتكبها مجرمون ذو مستوى عالي، أذكاء و متميزون في المجال التقني، مما يؤدي إلى تشتيت الجهود الدولية في محاولة تعقبها والتحري عنها، أو الوصول إلى مرتكبها.

وقد صنف الفقهاء والدارسون جرائم الكمبيوتر والإنترنت ضمن فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، وهذا ما سنتعرض إليه فيما يلي.

المطلب الثالث: تصنيف الجرائم الإلكترونية.

يصعب تصنيف الجرائم نظرا لإختلافها من مجتمع لآخر من حيث تطوره، ومدى إستخدامه للحاسوب ودرجة إعتماده عليه في مختلف جوانب الحياة، وقد أوجد مشروع إتفاقية جرائم الكمبيوتر والإنترنت لعام 2001 (إتفاقية بودابست 2001) تضمن أربع طوائف رئيسية:

أ- الجرائم التي تستهدف سلامة وسرية المعطيات والنظم: وتضم الدخول غير قانوني (غير مصرح به)، الإعتراض غير القانوني، تدمير المعطيات، إعتراض النظم

ب- الجرائم المرتبطة بالكمبيوتر: تضم التزوير المرتبط بالكمبيوتر، الإحتيال المرتبط بالكمبيوتر.

ج- الجرائم المرتبطة بالمحتوى: وهي تضم طائفة واحدة وفق لهذه الإتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.²⁶

د- الجرائم المرتبطة بالأشخاص والأموال : وتضم السرقة والإحتيال والتزوير والإطلاع على البيانات الشخصية، المعلومات المضللة والزائفة، أنشطة الإعتداء على الخصوصية وإساءة إستخدام المعلومات، القرصنة ... وغيرها من الجرائم.²⁷

وعليه، فقد تعدد الجهود الفقهية التي بذلت على الصعيد الدولي أو الوطني من أجل وضع تقسيم يمكن الإعتداد عليه لجرائم المعلوماتية، وفي هذا المجال يمكن تقسيمها إلى مجموعتين أساسيتين

²⁵ خالد ممدوح إبراهيم، المرجع السابق، ص 19 و 20.

²⁶ محمود أحمد طة، المرجع السابق، ص 18.

²⁷ جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، ط1، دار البداية، عمان، 2012، ص 134.

المجموعة الأولى : الجرائم التي تقع على الأنترنت

أي أن شبكة العنكبوتية تكون عنصر سلبي في الجريمة أي محل للجريمة فقط، فإن هدف المجرم ينصب حول البيانات والمعلومات المخزنة والمنقولة عبر قنوات الخاصة أو العامة وإختراق الحواجز الأمنية إن وجدت والإعتداء على الأموال، والتي نذكرها على التوالي.

أ- سرقة المال المعلوماتي

أضحى لبرامج المعلومات قيمة غير تقليدية لإستخداماتها المتعددة في كافة المجالات الإجتماعية والإقتصادية فهذه القيمة المميزة لبرامج المعلومات تجعلها محلا للتداول، وهنا تبدو أهمية الأنترنت بصفته مصدر المعلوماتية، مما أدى إلى ظهور قيمة إقتصادية جديدة وأموال جديدة، عرفت بالأموال المعلوماتية، وصاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم المعلوماتية وهذه الجرائم يمكن تصورها من زاويتين:

أن تكون المعلوماتية أداة أو وسيلة للإعتداء، وأن تكون المعلوماتية موضوعا للإعتداء رأي سرقة تلك المعلومات.

فالزاوية الأولى يستخدم الجاني المعلوماتية لتفويض جرائم سواء ما تعلق منها بجرائم للإعتداء على الأشخاص أو الأموال كالسرقة والنصب وخيانة الأمانة، أما الجرائم من الزاوية الثانية يكون المال المعلوماتي موضوعا لها.²⁸

ب- إستخدام البروكسي للدخول المواقع المحجوبة هو عبارة عن برامج وسيط يقوم بحصر إرتباط جميع مستخدمى الأنترنت في جهة واحدة ضمن جهاز موحد وهذا البرنامج يستخدم لتجاوز المواقع المحجوبة، والتي عادة ما تكون إما مواقع جنسية أو سياسية معادية للدولة.²⁹

ج - جرائم الإختراق: يمثل الإختراق المعلوماتي تحديا على قدر كبير من الأهمية لإنجازات تكنولوجيا المعلومات، ويعرفه شراح القانون المعاصرون بأنه : "فعل مشروع يوظف المعرفة العلمية السائدة في ميدان ثقافة الحاسوب والمعلوماتية لإقتراف إساءة أو هجوم على الغير".³⁰

²⁸ منال هلال المزاهرة، تكنولوجيا للإتصال والمعلومات، دار السيرة، الأردن، 2014، ص 376.

²⁹ محمد عبد الله منشاوي، المرجع السابق، ص 32.

³⁰ مصطفى عثمان ضياء، المرجع السابق، ص 40.

فهي عملية إقحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر، يقوم المستخدمون المخولون بفتح حسابات الشركات أو المؤسسات للأغراض الشرعية مثل اللعب بالحسابات الشخصية ومزاولة بعض أنواع الألعاب في الحاسوب للوصول إلى الأسرار الخاصة بالمؤسسة عن طريق كسر كلمات السر الخاصة بالأنظمة خلال خطوط شبكات الهاتف³¹.

و فيها تعرض بعض الأساليب المستخدمة في عمليات الإختراق:

1. الإقحام أو التسلسل.

2. الفيروسات.

د - المواقع المعادية: بعض المواقع يتم إنشائها لمعاداة سياسية أو معاداة الدين أو للأشخاص أو الجهات.

هـ - جرائم القرصنة: تواجه شبكة الأنترنت ما يسمى بظاهرة القرصنة، والتي تكون من قبل بعض الجماعات التي تؤمن بالحرية المطلقة في الرأي والتعبير والإستخدام أيضا، وهي جماعات تستطيع أن تدخل عبر طرق خاصة تحترق أجهزة الحاسوب، وكذا الأرقام السرية للأشخاص وإلى يريدتهم الإلكتروني.

فهي تعتبر سرقة للخدمات أو الإستعمال غير المصرح به للنظام المعلوماتي.³²

و - جرائم التجسس الإلكتروني: هي الجرائم التي يتم بواسطتها إختراق أجهزة المستخدمين بطرق غير شرعية ولأغراض غير سلمية، من أجل سرقة المعلومات تتعلق بذلك المستخدم سواء على الصعيد الشخصي، أو السياسي أو العلمي أو الإجتماعي حيث لم يعد هناك سرية يمكن الإحتفاظ بها من دون أن يقوم الشخص بعمليات كثيرة لتجنب عمليات التجسس أو "الهاكرز".

فهي ممارسات غير مشروعة على شبكات الحاسب الآلي، تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيا.³³

³¹ علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، الأردن، 2007، ص432.

³² طارق إبراهيم الدسوقي عطية، المرجع السابق، ص، 248.

³³ إطلع على الموقع الإلكتروني <www.abahe.co.uk>71102-piracy: تاريخ الإطلاع : 2019/03/13، ساعة الإطلاع : 19:45.

ي - الإرهاب الإلكتروني: يعد الإرهاب المعلوماتي من أخطر أصناف الجرائم المرتبطة بتكنولوجيا المعلوماتية نظرا لأثرها ودوافعها فالإرهاب الإلكتروني هو تحطيم أو إتلاف أنظمة معلوماتية بهدف المساس، أو إحداث خلل يمس باستقرار دولة أو بهدف الضغط على حكومة ما.³⁴

فهو هجوم مع سبق الإصرار، ذو أهداف سياسية ضد المعلوماتية، ضد أهداف مسلحة كالشرطة، الدرك أو أهداف عسكرية، أو غير مسلحة كالإدارات المدنية الوطنية، من طرف جماعات وطنية أو دولية خفية.³⁵

و خطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة التي تضار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدفا سهلا للمال فبدلا من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية وإغلاق المواقع الجوية وشل أنظمة القيادة.

المجموعة الثانية : جرائم تقع بواسطة الأنترنت

أي أن الشبكة دورها إيجابي في ارتكاب الجريمة، فهي تسهل للمجرم المعلوماتي تحقيق غايته ويلاحظ أن أغلب صورها في هذه الحالة تشكل جرائم الواقعة على الأشخاص.

1. الجرائم الجنسية والممارسات غير أخلاقية

2. الجرائم المالية : والتي تضم كلا من:

أ. جرائم السطو على أرقام البطاقات الائتمانية : والتي يتم ارتكابها باستخدام تكنولوجيا المعلومات سرقة الأقراص الصلبة والمرنة، بغرض الحصول على المعلومات التي تحولها ويتولى قراصنة المعلومات بيعها بعد الحصول عليها، نظير الحصول على عائد مادي، مثل ذلك :

الوصول إلى أجهزة الحاسب الخاصة بمكاتب الائتمان الرئيسية وسرقة المعلومات الائتمانية، تم استخدامها بإعادة بيعها لأشخاص آخرين، وتدمير المشروعات المهمة للشركات بغرض ابتزازهم.³⁶

³⁴ نسيم درود، جرائم للمعلوماتية على ضوء القانون الجزائري، مذكرة ماجستير، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2012 - 2013، ص 155.

³⁵Sophie Revol, (DESS) Droit du Multimédia et de l'informatique, « Terroriste et Internet », sous la direction de N.KOSTIC , Université Paris II Pantheon Assas année 2002-2003(France), page.9

³⁶ فضيل دليو، تكنولوجيا الإعلام والاتصال الجديدة، ط1، دار الهومة للطباعة والنشر والتوزيع، الجزائر، 2014، ص 247.

ب. **القمار عبر الإنترنت** : مع الانتشار الواسع والتطور الكبير لشبكة الإنترنت على مستوى العالم ظهر إلى الوجود. صيحات القمار يتمثل في الكزنيوهات الافتراضية، وهي عبارة عن مواقع ويب تم تصميمها على طراز كازينوهات " لاس فيغاس " الأمريكية وتتوفر كل أنواع القمار وألعابه ابتداء من ألعاب الورق إلى إنتهاء بآلات المقامرة، وهي موجودة على الشبكة المعلوماتية.

ج. **تزوير البيانات** : لا تكاد تخلو جريمة من عملية تزوير للبيانات بشكل أو بآخر، ويتم تزوير البيانات الحاسب إما بإدخال بيانات مغلوبة إلى الموظفين المسموح لهم بإدخال البيانات، ثبت أنه كان لهم ضلع كبير في الكثير من جرائم نظم المعلومات³⁷.

د. **الجرائم المنظمة** : هي عنف منظم قصد الحصول على مكاسب مالية، بطرق وأساليب غير مشروعة وتمارس الجريمة على شكل نصي وإحتيال وتزوير وسطو وخطف من أجل الإبتزاز والقتل....الخ، إلا أنها تختلف عن الجرائم المعروفة كونها تنفذ عن بعد تدبير وتنظيم، لذا سميت بـ "الجريمة المنظمة"³⁸.

المبحث الثاني: ثبات النص الجزائي وتكافؤ مع الإتفاق الدولي لمواجهة الجريمة المعلوماتية.

لقد أثبت الواقع العملي على أنه لا يمكن لدولة وحدها مكافحة الجريمة المعلوماتية وكسر شوكة تقشي هذه الظاهرة المستحدثة كيف ما كانت الإمكانيات التي تتوفر عليها في هذا الإطار. حيث أنه ليس من المهم التوفر على ترسانة تشريعية وقضائية وفنية في مجال مكافحة الجريمة المعلوماتية بل أن تكون هذه القوانين متجانسة وملائمة مع قوانين مختلف الدول هذا من جهة، وملائمة قوانين هذه الدول مع نصوص الاتفاقية التي صادقوا عليها من جهة أخرى وذلك بهدف خلف منظومة قانونية موحدة بين دول تهدف إلى حماية المصلحة المشتركة.

المطلب الأول: سعي المشرع الجزائري للتصدي للجريمة الإلكترونية

سعيًا من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولة منه تدارك الفراغ التشريعي القائم في

³⁷ منال هلال المزاهرة، المرجع السابق، ص 40 و 41.

³⁸ بشير مصطلح الجريمة المنظمة: إلى جماعات ترتكب أفعالاً تخترق بها القانون للحصول على مساعدات مادية، كما تحتم بالإبتزاز والخدع والإنتاج والتوزيع غير القانون لإدمان المخدرات والتعامل مع السلع الممنوعة مثل الأسلحة غير القانونية، فهي تمتاز بخصيتين : التنظيم، والكسب المادي. راجع : نصره تامي، الإعلام القضائي والإرهاب، ط1، دار أسامة للنشر والتوزيع، الأردن، 2015، ص 87.

هذا المجال من جهة أخرى، عمد منذ الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال، وقام بإستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية.

أولا : أركان الجريمة الإلكترونية

تتشترك أركان الجريمة الإلكترونية مثل الجريمة العادية في الركن المادي والمعنوي وكذا الركن الشرعي.

• الركن المادي:

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتائجها. يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب م مثلا : جريمة التجسس الإلكتروني، الركن المادي فيها هو : الحصول مباشرة على الدعامة الإلكترونية الحاوية لهذا السر أو المعلومات، كالحصول على "CD" مخزنة فيه الأسرار والوثائق.³⁹

• الركن المعنوي:

يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين أي العلم والإرادة

• العلم : هو إدراك الفاعل للأمر.

• الإرادة : فهي إتجاه السلوك الإجرامي لتحقيق النتيجة.

و طبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما وخصوصا. وعليه فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء، ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص مثلا : جرائم تشويه السمعة عبر الإنترنت، وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.

ثانيا : القوانين المتعلقة بالجريمة الإلكترونية

قد أخص المشرع الجزائري تنظيم الجريمة الإلكترونية بقوانين عامة وأخرى خاصة وهذا ما سنتطرق إليه.

³⁹ أسامة أحمد المناعسة، جلال محمد الزعبي، المرجع السابق، ص 49 و 50

أ. قانون العقوبات

لقد تعرض المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي في قانون العقوبات بموجب القانون 15/04⁴⁰ تحت عنوان : “المساس بأنظمة المعالجة الآلية للمعطيات ” ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 8.

و في عام 2006 أدرج المشرع تعديل آخر على قانون العقوبات بموجب القانون 23/06⁴¹ حيث مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال.

و يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث من الإجرام بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى.

أما بالنسبة لأنواع الجرائم الإلكترونية المنصوص عليها في قانون العقوبات والتي يمكن تصنيفها إلى مايلي:

1. الغش أو الدخول أو البقاء غير المشروع في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات.
2. حذف أو تغيير لمعطيات المنظومة.
3. إدخال أو تعديل في نظام المعطيات.
4. تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار.
5. حيازة أو إفشاء أو نشر أو إستعمال المعطيات.
6. تكوين جمعية الأشرار.

و عليه، يمكن تكليف هذه الأفعال الإجرامية بأنها جرائم ضد أموال الغير والمضرة بالمجتمع.

وتجدر الإشارة إلى أن المشرع قد قام بتعديل قانون العقوبات في سنة 2016، مستحدثا بذلك نصا جديدا وهو المادة 87 مكرر 12 والتي أحدثت لنا جريمة جديدة وهي جناية تجنيد الأشخاص لصالح إرهابي أو منظومة إرهابية بإستخدام وسائل تكنولوجيا الإعلام والإتصال.⁴²

⁴⁰ القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات ،ج.ر. عدد 71

⁴¹ القانون رقم 23/06 المؤرخ في 20 ديسمبر المعدل والمتمم لقانون العقوبات ،ج.ر. عدد 84

⁴² القانون رقم 02/16 المؤرخ في 19 ماي 2016 المعدل والمتمم لقانون العقوبات ،ج.ر. عدد 37

ب. قانون الإجراءات الجزائية

فيما يتعلق بمتابعة الجريمة الإلكترونية فهي تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالنتيش والمعاينة، وإستجواب المتهم والضبط والتسرب والشهادة والخبرة. غير أن المشرع الجزائري فقد نص على تمديد الإختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية.⁴³ كما نص على التفتيش في المادة 45 الفقرة 7 من نفس القانون⁴⁴ المعدلة حيث إعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد العامة من حيث الشروط الشكلية والموضوعية.

ونص كذلك المشرع على التوقيف للنظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذلك على إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور.

أما بالنسبة لباقي الإجراءات من تحقيق ومحاكمة فإنه تطبق عليه نفس إجراءات الجريمة التقليدية.

ج. قانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

يهدف هذا القانون⁴⁵ إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام

و الإتصال ومكافحتها.

وقد تبنى هذا القانون تعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكل مايتعلق

بالمنظومة المعلوماتية وكذا معطيات المعلومات ومقدمو الخدمات.⁴⁶

وقد خول هذا القانون بعض الإجراءات التي تطبق على الجرائم الإلكترونية من:

- مراقبة الإتصالات الإلكترونية.
- تفتيش المنظومة المعلوماتية.
- حجز المعطيات المعلوماتية.

⁴³ انظر المادة 37 من القانون رقم 07/17 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجراءات الجزائية ، ج.ر. عدد 20

⁴⁴ المادة 45 الفقرة الثانية من نفس القانون 07/17 السالف الذكر

⁴⁵ القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، ج.ر.

عدد 47.

⁴⁶ راجع المادة 2 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

ومكافحتها

وقد أنشأ بموجب هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتي من مهامها:

- تفعيل التعاون القضائي والأمني وإدارة وتنسيق العمليات الوقائية.
- تبادل المعلومات مع الجهات الأجنبية من أجل تفعيل الحماية على المنظومة المعلوماتية من كل خطر يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني⁴⁷.

المطلب الثاني: الجهود الإقليمية لمجابهة الإجرام المعلوماتي

لأن الجريمة السيبرانية عابرة للحدود غير مكرثة بالحواجز الطبيعية أو الثقافية، ومن شواهد ذلك كثرة إنتشار فيروسات الكمبيوتر بسرعة وعلى نطاق واسع، ولأن مرتكبيها غالبا ما يكونون متواجدين في أماكن غير تلك التي تُنتج فيها الجريمة آثارها، فقد إقتضى الأمر من دول العالم التنسيق والتعاون في مجال محاربتها ووضع التصورات المشتركة بشأنها وذلك من خلال أطر التعاون والتكتل الإقليمي وكذلك على الصعيد الدولي، وفي هذا السياق جاء إتفاق الدول العربية على وضع آلية تعاون خاصة بها تتمثل في:

أولا: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بتاريخ 21 ديسمبر 2010 والتي تهدف بحسب مقتضيات مادتها الأولى إلى تعزيز التعاون بين الدول الأعضاء في مجال مكافحة جرائم تقنية المعلومات بما تمثله من خطر على أمن ومصالح الدول والمجتمعات والأفراد.⁴⁸

و يتضح من خلال بنية نص الإتفاقية ومضمون الترتيبات التي قضت بها أنها ألهمت النصوص العربية اللاحقة على توقيعها وقد جاء ذلك صريحا في بعض هذه النصوص، من ذلك ما جاء في المذكرة الإيضاحية لقانون مكافحة جرائم تقنية المعلومات الكويتي، والذي أخذ بنفس التسمية التي أعطتها الإتفاقية لهذه الجرائم، من أن أعداد هذا القانون يأتي إلزاما (بأحكام الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها دولة الكويت بموجب القانون رقم 60 لسنة 2013).⁴⁹ وقد حددت الإتفاقية مجال تطبيقها في أربع نقاط وردت على النحو التالي:

⁴⁷ راجع المادة 04، 05، 06 والمادتين 13، 14 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

⁴⁸ المادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

⁴⁹ المذكرة الإيضاحية للقانون الكويتي رقم 63 لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات

- إذا ارتكبت إحدى هذه الجرائم في أكثر من دولة
- إذا كانت الجريمة المرتكبة في الدولة العضو قد تم التخطيط والإعداد لها أو الإشراف والتوجيه بشأنها، في دولة أو دول أخرى.
- إذا كانت الجهة الضالعة في ارتكاب الجريمة، جماعة إجرامية منظمة، لها أنشطة في أكثر من دولة.
- إذا كان للجريمة المرتكبة في إحدى الدول آثار بالغة الخطورة والضرر على دولة أو دول أخرى.⁵⁰

و على الرغم من تأكيد الاتفاقية على احترام سيادة الدول الأعضاء، لاسيما في مجال الولاية القضائية وغيرها من وظائف السيادة، فإنها ألزمت كل دولة في نطاق احترام تشريعاتها وأنظمتها الداخلية، بتجريم الدخول والبقاء غير المشروعين إلى تقنية المعلومات أو إعتراض سير بياناتها وإساءة استخدام وسائلها والإحتيال بواسطتها وكذا الإعتداء على الحياة الخاصة والملكية الفكرية والجرائم المتعلقة بالإرهاب والمواد الإباحية وبالإستخدام غير المشروع لأدوات الدفع الإلكترونية⁵¹ كما ألزمت الاتفاقية في مادتها الحادية والعشرين، الدول الأطراف بتشديد العقوبات المقررة للجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

و لأن الأمر يتعلق باتفاقية بين عدة دول فقد تم تكريس فصل كامل للتعاون القانوني والقضائي شمل مسائل الاختصاص وتسليم المجرمين والمساعدة المتبادلة مع التوصية بإنشاء جهاز خاص بطاقم بشري مؤهل من أجل ضمان حسن سير هذا التعاون.⁵²

وعلى غرار الدول العربية وفي سياق الوعي المتنامي بخطورة الجريمة السيبرانية وضرورة مواجهتها بالوسائل التشريعية، الفنية والمؤسسية اللازمة، نحت الدول الافريقية نفس المنحى وذلك من خلال:

⁵⁰ المادة 03 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

⁵¹ المواد من 05 إلى 18 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

⁵² المواد من 30 إلى 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

ثانياً: إتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي: وقد تم تبنيها من قبل دول الاتحاد الإفريقي بمناسبة إنعقاد مؤتمره الثالث والعشرين في دورة عادية، بتاريخ 27 يونيو 2014 بمالابو.

تضمنت هذه الإتفاقية بنص واحد من ثمانية وثلاثين مادة، أربعة مجالات تناولها المشرع الموريتاني بنصوص منفصلة على النحو الذي تقدم، وهذه المجالات هي:

- الجريمة السيبرانية بأبعادها المختلفة الموضوعية والإجرائية.
 - حماية البيانات ذات الطابع الشخصي.
 - تنظيم المبادلات الإلكترونية.
 - رسم أهداف ووضع ضوابط لتنظيم وترقية مجتمع المعلوماتية في دول الاتحاد.
- و نرى أن أفراد مشرعنا لكل من هذه الميادين الأربع بنص، مسلك موفق لا يحول دون تكاملتها من حيث الأهداف والتنظيم.

وعلى الصعيد شبه الإقليمي تبنت المجموعة الإقتصادية لدول غرب إفريقيا المعروفة إختصاراً بـ (CEDEAO) في الدورة السادسة والسنتين لمجلس وزرائها المنعقد في أبوجا أيام 17، 18 و 19 أغسطس 2011 إتفاقية لمحاربة الجريمة السيبرانية في فضاء المجموعة إشتملت تقريباً على نفس محاور ومضمون النصوص الوطنية، الإقليمية والدولية في هذا المجال.⁵³

المطلب الثالث: التصدي الدولي للإجرام المعلوماتي

إتفاقية مجلس أوروبا (Convention sur la cybercriminalité – Conseil de l'Europe)

التي إعتدتها لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة المنعقدة بتاريخ الثامن من ديسمبر 2001 والمعروفة بإتفاقية بودابست؛ المدينة التي فُتح فيها باب التوقيع على الإتفاقية بتاريخ الثالث والعشرين من نفس الشهر والسنة، وذلك بمناسبة إنعقاد المؤتمر الدولي حول الجريمة الإلكترونية،

⁵³ Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO

⁵⁴ مجلس أوروبا هو منظمة دولية تأسست في عام 1949 ويتكون من 47 دولة أوروبية، يقع مقر للمجلس في مدينة ستراسبورغ الفرنسية وعضويته مفتوحة لكل دول أوروبا الديمقراطية وهو ليس جزء من الاتحاد الأوروبي ويختلف عن مجلس الاتحاد الأوروبي والمجلس الأوروبي

ولم تقتصر هذه الإتفاقية على الدول الأعضاء في مجلس أوربا بل أنها قد سمحت بمقتضيات مادتها السادسة والثلاثين بالتوقيع عليها، حتى قبل دخولها حيز التنفيذ، من دول من خارج المجلس وهو ما حصل بالفعل مع كل من كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية،⁵⁵ ليستمر بعد ذلك الإنضمام إلى هذه الإتفاقية من قبل المزيد من الدول، بما جعل منها آلية دولية لمكافحة الإجرام المرتكب بوسائل تقنيات المعلوماتية وضدّها.

و قد نظمت الوزارة المكلفة بتقنيات الإعلام والاتصال بالتعاون مع خبراء دوليين في هذا المجال ورشة تحت عنوان: إعداد مسار إنضمام موريتانيا إلى إتفاقية بودابست حول الجريمة السيبرانية، الأيام من 17 الى 19 جانفي 2018 وهو ما يمكن إعتباره خطوة في طريق الإنضمام الفعلي لهذه الإتفاقية.⁵⁶ و تستفيد الدول التي تنظم إلى الإتفاقية من الخبرات والإمكانات التي تتمتع بها الدول الأعضاء المتقدمة تكنولوجياً كالدول الأوروبية والولايات المتحدة الأمريكية واليابان، كما تستفيد كذلك من تعاون الفاعلين الأساسيين في مجال تقنية المعلومات والاتصال كـ **Gmail, Gool** ، **Facebook وYouTube**، وذلك في التحريات والتصدي للجريمة كسحب فيديو من اليوتوب مثلاً، أو الحصول على معلومات من شأنها المساعدة في التعرف على هوية صاحب حساب في Yahoo متورط في إرتكاب جريمة، أو توقيف حساب على الفيسبوك ينشر محتوى مجرماً بالنصوص الوطنية أو الدولية.⁵⁷

ولأن هذه الإتفاقية قد جاءت سابقة على الكثير من القوانين الوطنية والإتفاقيات الإقليمية، فإن شكلها من حيث البنية النصية، ومضمونها من حيث وضع معانٍ للمصطلحات المستخدمة في هذا المجال وتعداد الأفعال المجرّمة سواء منها ما تعلق بالإعتداء على شبكة تقنية المعلوماتية نفسها، أو ما استخدمت له هذه التقنية من أغراض الإعتداء على حقوق الأفراد وثقافة المجتمعات وأمن الدول، وكذلك وضع القواعد الإجرائية وأسس التعاون الدولي في مجال مكافحة هذه الجريمة، كل ذلك قد عكسته النصوص اللاحقة على نفاذها وذلك على النحو الذي سبق التطرق إليه في معرض تناول التدابير التشريعية في مجال محاربة الجريمة السيبرانية على الصعيد الوطني والإقليمي

⁵⁵ التقرير التفسيري لاتفاقية الجريمة الالكترونية <https://rm.coe.int/explanatory-report...convention-in>

⁵⁶ www.ami.mr/Depeche-56093.html

⁵⁷ <http://www.mf-ctrf.gov.dz/presse/Bulletin%2032%20Cyber.pdf>

من كل ما تقدم نخلص إلى أن الثورة الرقمية، التي غيرت الشكل التقليدي للمجتمعات، وجعلت من سوق تقنيات الإتصال؛ من حواسيب وهواتف و ألواح إلكترونية وغيرها، السوق الأكثر رواجًا، وعلى الرغم مما حملت معها من مزايا على صُعد الحياة المختلفة، فإنها لم تسلم من سوء الإستعمال والإستغلال في ارتكاب جرائم تطل الفرد والمجتمع والدولة.

لقد تجاوز تطور تكنولوجيا المعلوماتية من خلال شبكة الاتصال فائقة السرعة، المفاهيم القانونية السائدة لاسيما بالنسبة للقانون الجنائي الذي تم وضعه للتعامل مع واقع مادي لا إفتراضي وليطبق في نطاق حدود الدولة الواحدة لا على الصعيد العالمي.

لقد مثلت ضرورة تحديث وتطوير ومواءمة قواعد القانون الجنائي؛ الموضوعي منها والشكلي، مع هذا الواقع الجديد تحديًا، إن اختلفت الدول في الترتيبات الفنية للتعامل معه، فقد إتحدت في الوعي بضرورة مواجهته.

الخاتمة:

جالت بنا هذه الاوراق البحثية إلى التعرّيج بأن العالم يعيش اليوم ثورة ثالثة، أو الموجة الثالثة كما يسميها البعض وهي ثورة تكنولوجيا المعلومات والمعرفة والتي أصبحت أساسا للتنمية وزيادة الإنتاج، وسرعة إتخاذ القرار الصحيح، وقد تمخض عن هذا التطور إنتشار ما يعرف بالجريمة الإلكترونية والتي تتمتع بطبيعة قانونية خاصة تميزها عن الجريمة التقليدية

ومن المؤكد أن المشرع على غرار نظرائه وضع ترسانة قانونية جزائية في مجال مكافحة الجرائم المعلوماتية، و إتضح أن قانون العقوبات تضمن فصولا تشكل الأداة الأساسية لمكافحة هذا النمط الجديد من الإجرام- في محاولة منه للتصدي لهذا النوع من الجرائم ومكافحتها بشتى الطرق -، كما أن هناك مجموعة من المقتضيات الزجرية المتفرقة في المعاهدات الإقليمية والدولية- التي صادقت الجزائر عنها- ذات علاقة بالمجال المعلوماتي، والتي تكمل تلك الموجودة بالمجموعة الجنائية الجزائرية.

وكما لوحظ بأن المشرع الجزائري خطى منهج خطوات إيجابية في مجال سن تشريعات حديثة لمواجهة الجريمة المعلوماتية، وبالتالي أصبح للقاضي الجزائري آليات البث في قضايا الجريمة الإلكترونية، وخصوصا القضايا المتعلقة بالمعطيات الشخصية والمساس بها. أما في مايخص التوصيات التي تخرج بها هذه الاوراق البحثية فتكمن في:

أنه لا يمكن القول بأن المشرع الجزائري قد بلغ العلى بالقوانين التي وضعها بصدد مكافحة صور الجرائم المعلوماتية، بل لابد من ترفيتها وتكاملتها بحيث تشمل جرائم أخرى لم تشملها بحكم أن الإجراء السبراني متحدد وحديث وكما أن الآليات التعاون القضائي الدولي لازالت قاصرة على أن تكون ملائمة للإجرام المعلوماتي الذي يصعب فيه إثبات الفعل المجرم أو ضبط الجاني بسبب طبيعة الدليل الالكتروني، ولكون الجريمة المعلوماتية في اغلب الأحوال عابرة للحدود لكونها ترتكب عبر شبكات الاتصال الحديثة خصوصا الانترنت.

زيادة على ذلك على الدولة أن تضع نصوصا قانونية بنود تنظيمية بغرض فرض دورات تدريبية للأفراد في مجال مكافحة الجريمة، وأيضا الإحتكاك بالخبراء سواء الوطنيين أو الدوليين من أجل خلق رجال أمن متخصصين في مكافحة الجريمة في المجال المعلوماتي والسبراني.

قائمة المراجع :

أولا: الكتب و المؤلفات

1. جلال محمد الزغبى وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة)، ط1، دار الثقافة للنشر والتوزيع، الاردن 2010.
2. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2008.
3. محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت (دراسة مقارنة)، ط 1، دار الفكر والقانون للنشر والتوزيع، مصر، 2013.
4. خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، دار الجامعية، الاسكندرية، 2008.
5. جلال محمد الزغبى وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة)، ط1، دار الثقافة للنشر والتوزيع، الاردن 2010.
6. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2008.
7. طارق ابراهيم الدسوقي عطية، عولمة الجريمة (الشراكة العالمية في الممارسات الاجرامية)، دار الجامعة الجديدة، د.ط، الاسكندرية، 2010.
8. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الاسكندرية، 2001.
9. عبد الله أحمد هلالى، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2000.

10. فضيل دليو، تكنولوجيا الإعلام والاتصال الجديدة، ط 1، دار الهومة للطباعة والنشر والتوزيع، الجزائر، 2014.

11. نصرة تامي، الإعلام القضائي والإرهاب، ط 1، دار أسامة للنشر والتوزيع، الأردن، 2015.

12. علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، الأردن، 2007.

13. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، ط 1، دار البداية، عمان، 2012.

14. منال هلال المزاهرة، تكنولوجيا للاتصال والمعلومات، دار السيرة، الأردن، 2014.

15. Sophie Revol, (DESS) Droit du Multimédia et de l'informatique, « Terroriste et Internet », sous la direction de N.KOSTIC , Université Paris II Pantheon Assas année 2002-2003(France).

ثانيا: الرسائل والأطروحات العلمية.

1. درار نسيم، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني ، أطروحة

دكتوراه، كلية الحقوق والعلوم السياسية ، جامعة تلمسان، 2016-2017.

2. نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة

ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة،

2013.

3. وأيضا :يوسف صعيدي، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، تخصص قانون

دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

4. فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماجستير، تخصص

قانون عام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011-2012.

5. سفيان سوير، جرائم للمعلوماتية، مذكرة ماجستير، تخصص العلوم الجنائية، كلية الحقوق

والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010-2011.

ثالثا: أهم النصوص القانونية

1. القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم

المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر. عدد 47.

2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات متوفرة على الرابط التالي :

Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO

3. مجلس أوروبا هو منظمة دولية تأسست في عام 1949 ويتكون من 47 دولة أوروبية، يقع مقر

للمجلس في مدينة ستراسبورغ الفرنسية وعضويته مفتوحة لكل دول أوروبا الديمقراطية وهو

ليس جزء من الاتحاد الأوروبي ويختلف عن مجلس الاتحاد الأوروبي والمجلس الأوروبي

<http://www.mf-ctrf.gov.dz/presse/Bulletin%2032%20Cyber.pdf>