

## مجتمع المعلومات والقانون الجنائي

### Information Society and Criminal Law

د. جمال خفيف\*

كلية الحقوق، سعيد حمدين، جامعة الجزائر 1، dj.khefif@univ-alger.dz

تاريخ الاستلام: 2025/02/27؛ تاريخ القبول: 2025/05/07؛ تاريخ النشر: 2025/06/07

#### ملخص:

تأثر الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات والجرائم السيبرانية في المصالح الفردية والجماعية التي تعتبر حاسمة في وقتنا الحالي، وذلك لارتباطها بنوعية حياة عدد كبير من الأشخاص في العالم، وذلك بمساسها للحريات الشخصية وبسرية المعلومات، مما جعل الجمعية الدولية للقانون الجنائي تهتم بهذا النوع من الإجرام المستحدث، وهذا ما دفعنا لتسليط الضوء على طريقة معالجة هذا الموضوع من قبل هذه الجمعية، من جهة، وتحليل مختلف عناصر مثل هكذا جرائم لم تعرف من قبل، حيث غيرت من بعض قواعد القانون الجنائي، أي التطرق للمصالح المحمية بالقوانين التي تواجه الجرائم المتصلة بتكنولوجيات المعلومات والاتصالات.

الكلمات المفتاحية: جرائم سيبرانية؛ تكنولوجيات المعلومات؛ الإجرام المستحدث؛ المعلوماتية؛ أمن المعلومات.

#### Summary:

Crimes related to information and communications technology and cybercrimes affect individual and collective interests, which are considered crucial in our current time, because of their connection to the quality of life of a large number of people in the world, and by affecting personal freedoms and the confidentiality of information, which made the International Society of Criminal Law interested in this type of new crime. This is what prompted us to shed light on the method of dealing with this issue by this association, on the one hand,

\* المؤلف المرسل.

and to analyze the various elements of such crimes that were not known before, as they changed some of the rules of criminal law, that is, addressing the interests protected by the laws that confront crimes related to information and communications technologies.

**Keywords:** cybercrimes; information technologies; new crimes; informatics; information security.

### المقدمة:

إنّ الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات والجرائم السيبرانية. تؤثر على المصالح الفردية والجماعية التي تعتبر حاسمة في الوقت الراهن، وذلك لارتباطها بنوعية حياة عدد كبير من الأشخاص في العالم إن لم نقل الكل، وما جعل البحوث والدراسات والندوات والمؤتمرات تتزايد وتتطور في اطار التعاون الدولي على مختلف أنواعها، وجعل كذلك عدة وكالات ومنظمات أو جمعيات تبحث في هذا الموضوع بجدية نظرا للمخاطر التي يوفرها هذا المجال، وأمام هذا الوضع المفزع والمخيف الذي أصبح يسيطر على كافة بلدان العالم، خاصة مقابل إتاحتها فرص واسعة وغير متناهية في المجتمعات برمتها، حيث نتج عن ذلك تكبد خسائر مالية ضخمة، من جهة، ومساس هذه الجرائم بالحريات الفردية المقدسة ومن بينها سرية المعلومات الشخصية، من جهة أخرى .

ومن بين الجمعيات التي أردنا أن نسلط عليها الضوء في هذه الورقة البحثية والتي أعطت أهمية كبيرة لمجال الاعتداءات في عالم تكنولوجيا المعلومات والاتصالات نجد الجمعية الدولية للقانون الجنائي.

قامت الجمعية الدولية للقانون الجنائي بإنشاء فريق خبراء حكوميين لبحث "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، وبمناسبة التحضير للمؤتمر الدولي التاسع عشر للقانون الجنائي المنعقد بمدينة (ريو دي جانيرو) بالبرازيل سنة 2014 بتقديم تقرير اعتمد على الاستبيان الذي أرسلته هذه الجمعية لمجموعة من الدول، وتلقت الجمعية الجواب عنه من ستة عشرة دولة، فكانت هذه الأرضية معتمدة على ستة عشرة نظام قضائي مختلف، ولكن وبالرغم من أن هذا الموضوع يتعلق بتكنولوجيات المعلومات والاتصالات والذي كان من المفروض أن تعالجه إحدى اللجان التقنية التابعة للجمعية إلا أن أعضاء الجمعية كلفوا اللجنة الأولى والتي تهتم عادة بالمواضيع المتعلقة بالقانون الجنائي العام، وهذا ما جعلنا نطرح التساؤل الآتي:

هل استطاعت الفرق المختصة التابعة للجنة الدولية للقانون الجنائي أن تستوعب امتداد هذه التكنولوجيات والحد من مخاطرها دون الحد من مزايا هذا التطور التكنولوجي؟

كما تتفرع عن هذه الإشكالية عدة تساؤلات لا تقل أهمية نختصرها فيما يلي:

لماذا اسند هذا التقرير للجنة الأولى بالجمعية الدولية للقانون الجنائي والتي تختص بالمواضيع ذات الصلة بالقانون الجنائي العام؟

ماهي أهم المسائل القانونية التي جاءت في هذا التقرير الذي يعتبر لبنة صلبة وأرضية اعتمدت عليها كل الأجهزة القضائية للدول في العالم؟

لمعالجة أهم النقاط التي ستطرح منطقياً أثناء البحث عن الأجوبة على السؤالين المذكورين أعلاه، قسمنا هذا البحث إلى ثلاثة أقسام، أولهما: نعالج فيه أهمية حالة موضوع تكنولوجيات المعلومات والاتصالات وعلاقته بالاعتداءات التي يمكن أن تقع عليهما أو بواسطتهما على هذه اللجنة غير المختصة، وثانيهما: نتطرق فيه إلى المصالح المحمية في الجرائم المتصلة بتكنولوجيات المعلومات والاتصالات، أما الثالث نحلل فيه الأركان المادية والمعنوية لجرائم تكنولوجيا المعلومات والاتصالات والجرائم السيبرانية.

1- أهمية إحالة موضوع تكنولوجيات المعلومات والاتصالات على لجنة القانون الجنائي العام:

إنّ إسناد المسائل التي يطرحها القانون الجنائي العام إلى اللجنة الأولى بالجمعية الدولية للقانون الجنائي بحكم تخصصها أصبح أمراً بديهياً، ولكن هذه المرة طلب من هذه اللجنة البحث في مسائل تقنية أخرى والنظر في ماذا تأثيرها على بعض مبادئ القانون الجنائي العام، ألم تجري العادة على أن تخضع جميع الأفعال بغض النظر عن طبيعتها إلى المبادئ التي تنظم وتحكم القانون الجنائي العام؟

1-1: أسباب إحالة موضوع التكنولوجيات الحديثة على لجنة ذات الاختصاص العام: جرت العادة أن يحيل المختصون بالجمعية الدولية للقانون الجنائي المواضيع التقنية ذات الاختصاص الدقيق على لجان خاصة تتكون من مختصين لهم علاقة بالاختصاص المعروض عليهم من أجل البحث فيه، ولكن هذه المرة تدخلت عدة أسباب، منها أسباب عامة وأخرى خاصة، جعلت الجمعية تعرض هذا النوع من المواضيع على لجنة

تتكفل بمعالجة المواضيع العامة، وهذا ما سنعالجه في النقاط الآتية:

### 1-1-2: الأسباب العامة: يرجع السبب في اتخاذ قرار الجمعية الدولية للقانون

الجنائي في إحالة المسائل التي تتعلق بتكنولوجيات المعلومات والاتصالات والجرائم السيبرانية على اللجنة الأولى المتخصصة في النظر في المسائل المتعلقة بالقانون الجنائي العام لدفع مستوى المناقشات على نطاق أوسع لتغطية كل المسائل التالية<sup>(1)</sup>:

- حماية المصالح القانونية المرتبطة مباشرة بتكنولوجيا المعلومات والاتصالات<sup>(2)</sup> وتحديات الفضاء السيبراني.

- توسيع نطاق التجريم، على سبيل المثال (تجريم بعض الأعمال التحضيرية، وحياسة بعض الأجهزة...).

- مشكلة احترام مبدأ الشرعية، لا سيما شرط الدقة في صياغة التهم الجنائية.

- حدود تغييرات في مفهوم حقوق التأليف والحقوق المجاورة، خاصة فيما يتعلق بمقدمي خدمات الأنترنت والمضيفين.

- دور القانون الجنائي في إيجاد طرق بديلة لحماية المصالح القانونية، بما في ذلك استعمال وسائل خاصة بشبكة الأنترنت لو تطلب الأمر، مثل منع الدخول أو إغلاق الموقع.

- الاستجابات التشريعية لتحدي إخفاء هوية مستخدم الأنترنت.

- القيام بجهود دولية لتنسيق ومواءمة القانون في منطقة تتجاوز (بحكم تعريفها) الحدود الجغرافية، مخترقة بذلك القاعدة القانونية المتعلقة بالمكان.

### 1-1-3: الأسباب الخاصة: وما لفت انتباهنا أنّ الطبيعة غير التقليدية لجدول أعمال

المناقشات في اللجنة الأولى المذكورة أعلاه ترتبط ارتباطاً مباشراً بالتحديات المحددة لتكنولوجيا المعلومات والاتصالات والجرائم السيبرانية، مما يميزها من عدة نواحٍ عن الأشكال القديمة أو التقليدية للجريمة، هذه التحديات هي التي تجعل موضوع تكنولوجيا المعلومات والاتصالات والجرائم السيبرانية مثيراً للاهتمام وصعباً في نفس الوقت، واتضح

(1) <https://www.penal.org/fr/colloques-internationaux>. Consulté le 04/02/2024 à 10h.

(2) TIC

جلياً أنّ المفاهيم التي كانت تستخدم في إطار الجرائم التقليدية ليست مناسبة ولا يصلح استخدامها في ميدان الجرائم التي لها علاقة بتكنولوجيات المعلومات والاتصالات أو في ميدان الجرائم السيبرانية، مما يتطلب تكييفها بطريقة مرنة إلى حد ما، ومن ناحية أخرى، سيكون من الضروري إعادة تحديد تعريف الحماية المعتادة ضد مخاطر التفسير الواسع للقانون الجنائي، مثل مبادئ الشرعية مبدأ التقييد الصارم (Ultima Ratio)، في مواجهة خصوصيات تكنولوجيا المعلومات والاتصالات والجرائم الإلكترونية.<sup>(1)</sup>

عندما نتكلم عن تكنولوجيا المعلومات والاتصالات والجرائم السيبرانية، نشير بالضرورة إلى عدة ظواهر مختلفة تمامًا، بحيث يمكننا التمييز بين ثلاثة أنواع من السلوكيات غير المشروعة أو المخالفة للقانون التي ستكون موضوع تحليلنا:

أولاً: - الجرائم "العادية" (أي التي كانت موجودة قبل ظهور هذه التكنولوجيات) والتي أصبحت اليوم ترتكب بفضل تكنولوجيا المعلومات والاتصالات، مثل الاحتيال، التحرش، السب والشتيم، التشهير والتقليد وغيرها.

ثانياً: - الجرائم التي ظهرت مع ظهور التكنولوجيات الحديثة والتي يكون هدفها الاعتداء على أنظمة تشغيل تكنولوجيا المعلومات والاتصالات، على سبيل المثال، القرصنة أو تشويه وإعاقة تشغيل نظام أو إتلاف البيانات المنقولة وما شبهها.

ثالثاً: - الجرائم ضد المصالح التي تكون خاصة بالويب، على سبيل المثال، التلاعب بالهويات الافتراضية أو سرقتها.

ومن المؤكد أن المشكلات القانونية والعملية المتعلقة بهذه الأنواع الثلاثة<sup>(2)</sup> من الجرائم تختلف اختلافاً كبيراً من نوع إلى آخر، وأمام هذا التنوع المختلط من هذه الأنواع من الجرائم يبقى السؤال المطروح هو: هل بإمكاننا أو هل ينبغي تطوير قواعد مشتركة بين لتكنولوجيا المعلومات والاتصالات والجرائم المتعلقة بها.

(1) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت-لبنان، 2005. ص 17.

(2) - هناك من الباحثين من يصنفها إلى أربعة أنواع من الجرائم بإضافة الجرائم العادية التي ترتكب عن بعد، لكننا نرى أن هذا النوع يتشابه مع النوع الأول ويتميز بنفس مميزات، ولهذا أدرجناه مع النوع الأول؛ لأن ارتكاب الجرائم عن بعد لا يمكنه أن يتحقق إلا باستعمال التكنولوجيات الحديثة.

بعد تفحص دقيق لهذا التقرير والبحث فيه عن العقوبات التي تعترض رجال القانون وما هي الحلول التي قدمت من الخبراء الذين أعدوه لاحظنا ما يلي:

- أنه لم يتم بذل جهود محددة لتطوير "نظام" تكنولوجيا المعلومات والاتصالات وقانون الجرائم الإلكترونية التي من شأنها أن تحتوي على قواعد لجميع هذه الجرائم.

- اقتصر دور المقرر العام على تقديم "أحدث ما توصلت إليه التقنية"، بطريقة مختصرة وبمبسطة للغاية، فيما يتعلق بالبيانات الناتجة عن الأنظمة القانونية المختلفة المدرجة في هذه الدراسة.

وبناء على ذلك وحسب رأينا فإن الجمعية الدولية للقانون الجنائي لم ترق إلى التطلعات التي كانت منتظرة من قبل المختصين في هذا المؤتمر، ولم تقم بالإجابة عن مختلف المسائل العالقة التي نتجت عن تزاوج هذه التقنيات الجديدة بالقانون وخاصة منها القانون الجنائي.

## (2) المصالح المحمية بالقوانين التي تواجه الجرائم المتصلة بتكنولوجيات المعلومات والاتصالات:

إن الحياة الاجتماعية التي تتسم بالروابط المتعددة بين أفراد المجتمع ينتج عنها تعدد في العلاقات مما ينشأ عنه عدة منازعات، وكل هذا ناتج عن تداخل مصالح هؤلاء الأفراد، ومن ثم وجب تدخل القانون للتوفيق بين تلك المصالح المتضاربة، ولهذا يجب تبين بعض الجوانب العامة لهذا النوع من الجرائم قبل الغوص في هذا المحور.

1-2: الجوانب العامة: لقد مكنت تكنولوجيا المعلومات والاتصالات والفضاء الإلكتروني المجرمين من أن يصبحوا "أكثر كفاءة" من ذي قبل عند التخطيط لارتكاب جرائم تقليدية باستعمال مثل هكذا تقنيات، ومن ثم أصبحت تطرح عدة مشاكل قانونية سنحاول الإجابة عنها في المحاور التالية.

### 1-1-2: تحول الجرائم العادية (التقليدية) إلى جرائم إلكترونية:

أصبح بإمكان المجرمين التخطيط لارتكاب جرائم تقليدية مثل جرائم الاحتيال والتشهير وانتهاك حقوق الطبع والنشر وغيرها من الجرائم التقليدية باستخدام أجهزة الكمبيوتر و/أو الإنترنت، بنقرة واحدة على الفأرة، للوصول إلى ملايين الضحايا المحتملين

أو التسبب في ضرر - أوسع بكثير من الخطر الذي يمكن أن تسببه هذه الجرائم لما تستعمل بالطريقة التقليدية أي دون استخدام التكنولوجيات الحديثة - يمس بسمعة أي شخص أو بحقوق الطبع والنشر الخاصة به، في هذه الحالات يرى الكثير من الفقهاء<sup>(1)</sup> أنه لم تتغير سوى الوسيلة والطريقة التي ارتكبت بها هذه الجرائم، أما المصالح التي مستها هذه الجرائم والتي يحاول القانون أن يحميها لم تتغير بل بقيت هي نفسها، وكل ما تغير هو الوسيلة التي ارتكبت بها، مع العلم أن القانون غالباً ما لا يأخذ بعين الاعتبار الوسائل التي ترتكب بها الجرائم ولا يعطي لها اهتماماً بالغاً.

ولكننا نخالف هذا الرأي الذي يأخذ بكل بساطة تساوي الأفعال الإجرامية التقليدية، سواء ارتكبت بالطريقة العادية أو بالطريقة الالكترونية، بحيث كل التقارير التي اطلعنا عليها والتي أعدتها كثير من الدول التي شاركت في هذا الاستبيان<sup>(2)</sup>، تبين أنه عند إعادة تعريف الجرائم التقليدية من خلال إنشاء جرائم جديدة يمكن ارتكابها "من خلال استخدام الحاسوب"، من الضروري توخي الدقة لتجنب التداخل أو النسخ غير الدقيق للأحكام الجنائية التي من شأنها أن تشمل أكثر أو أقل نفس السلوك المرتكب في الحالتين (بالطريقة التقليدية أو بالطريقة الجديدة التي تستعمل فيها الطرق الالكترونية) بحيث لا يمكن مساواتها، فقد تطرح بعض الصعوبات في مبدأ الشرعية هذا عندما يتم تعريف الفعل الذي لا يعاقب عليه (أو يعاقب عليه بدرجة أقل) في العالم الحقيقي والواقعي أثناء ارتكاب الجرائم التقليدية، إلا أنه يمكن أن يصبح جريمة خطيرة عندما يستخدم مرتكب الجريمة التقليدية تكنولوجيا المعلومات والاتصالات أو الإنترنت، وبالتالي نكون قد مسسنا بأحد المبادئ المقدسة في القانون الجنائي ألا وهو مبدأ الشرعية الجنائية.

ومن أمثلة الجرائم التقليدية التي يمكن ارتكابها من خلال استخدام الوسائل الالكترونية المختلفة، والتي تضمنتها عدة قوانين جنائية بعدة دول، نجد عمليات الاحتيال

(1) ومنهم الكاتب والباحث هشام محمد فريد رستم في أحد بحوثه المقدمة إلى مؤتمر حول القانون والكمبيوتر والأنترنت الذي انعقد في شهر ماي 2000 بكلية الشريعة والقانون بدولة الإمارات العربية تحت عنوان "الجرائم المعلوماتية - أصول التحقيق الجنائي الفني"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، الطبعة الثالثة، العين: جامعة الإمارات، 2004، ص 29-30.

(2) سبق أن أشرنا إلى هذا الاستبيان أعلاه.

باستخدام أنظمة تكنولوجيا المعلومات والاتصالات، والكشف عن أسرار الدولة المسجلة إلكترونياً، وتزوير البيانات الرقمية. التشهير أو التهديد ("التحرش المعنوي عبر الإنترنت").<sup>(1)</sup>

وتعد انتهاكات حقوق الطبع والنشر من خلال العروض غير القانونية أو تنزيل المواد المحمية بحقوق الطبع والنشر من الإنترنت مثلاً آخر على الانتهاكات بالطرق التقليدية التي تأخذ أبعاداً كمية (وربما نوعية) مختلفة تماماً لما ترتكب باستعمال الوسائل الالكترونية، ويصبح البعد الذي تتخذه هذه الجرائم عندما يتم تسهيل ارتكاب الجريمة من خلال الفرص التي توفرها شبكة الإنترنت بعداً آخر له عواقب جد خطيرة، سواء من حيث سرعة تنفيذ الجريمة أو من حيث انتشارها السريع أو من حيث بقائها بالفضاء الافتراضي مدة طويلة وتبقى متاحة لجميع الأشخاص متى أرادوا الاطلاع عليها فعلوا ذلك ليس بالحدود الإقليمية للدولة بل يتعداها لكل دول العالم على المعمورة وأخيراً إمكانية ارتكاب الجريمة دون وجود المجرم بمسرح الجريمة كما هو الحال بالجرائم التقليدية.

## 1-1-2: وضع التشريع الجزائي فيما يخص هذه الحالات: أما فيما يخص المشرع

الجزائري فبالرغم من أنه اعتبر أن كل جريمة ارتكبت أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام اتصالات الكترونية يعتبر جريمة الكترونية إلا أنه لم يغير لا من وصف هذه الجرائم ولا من العقوبات المسلطة عليها بالرغم من شدة خطورتها كما بيناه أعلى هذه الورقة البحثية، بل ترك الأمور كما كانت عليه قبل ظهور هذه التكنولوجيات التي أصبحت تستعمل في ارتكاب هذه الجرائم، وهذا ما نهت إليه عدة دول في تقاريرها التي أرسلتها إلى الأمم المتحدة.<sup>(2)</sup>

ما ننصح به مشرعنا هو القيام ببعض التعديلات التي يجب أن تمس بعض النصوص القانونية في قانون العقوبات ومنها: إضافة فقرات ببعض المواد التي تنص على الجرائم التي يمكن أن ترتكب باستعمال تكنولوجيات المعلومات والاتصالات الالكترونية وخاصة بمواقع التواصل الالكتروني، كجرائم الاعتداءات على الشرف واعتبار الأشخاص، وعلى حياتهم الخاصة وإفشاء الأسرار التي وردت في القانون رقم 23-06 مثلاً، ومنها جريمة

(1) [https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime\\_Study\\_French](https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_French), Office des nations unies contre la drogue et le crime, Étude détaillée sur la Cybercriminalité, P77. Consulté le 03/03/2024 à 14h.

(2) Thomas Weigend, <https://droit.cairn.info/revue-internationale-de-droit-penal-2013-1-page-19?lang=fr#re2no2>. p1. Consulté le 03/03/2024 à 16h: 25mn.

القذف وجريمة السب وجراء إدلاء الأطباء والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم وظائفهم بأسرار من ائتمنهم، أو استعمال الوسائل الالكترونية من مواقع التواصل الاجتماعي في عملية استدراج الأشخاص من أجل اختطافهم مثلاً، أو جرائم التمييز وخطاب الكراهية لما تستعمل بالوسائل الالكترونية كذلك، يجب أن ينص المشرع الجزائري في هذه الفقرات على تشديد العقوبات في حالة استعمال الجريمة التقليدية بالوسائل الالكترونية، وهذا ما قام به التشريع الفرنسي، حيث اعتبر انتهاك حقوق الطبع والنشر عبر الإنترنت أو على شبكة اتصالات الكترونية بصفة عامة ظرفاً مشدداً<sup>(1)</sup>.

- إضافة مواد قانونية جديدة إذا تعلق الأمر بأفعال خطيرة يمكن أن يتغير وصفها الجنائي ولو تظاهر في ظاهرها أنها تتشابه مع الجريمة التقليدية لما كانت ترتكب بالطرق والوسائل التقليدية، وهذا ما قامت به بعض الأنظمة القانونية ببعض الدول لما أدخلت نصوص قانونية جديدة بها أحكام جنائية محددة تتعلق بالمواد الإباحية عبر الإنترنت (بما في ذلك المواد الإباحية المتعلقة بالأطفال) وتوزيعها إلكترونياً في أغلب الأحيان،<sup>(2)</sup> لأنه وحسب رأينا، عندما يستخدم الجناة الوسائل الالكترونية أو التكنولوجيات الحديثة مثل وسائل التواصل الاجتماعي لإقامة اتصال مع ضحاياهم المحتملين في الجرائم الجنسية، وخاصة لما يتعلق الأمر بالجرائم التي تقع على الأطفال، فإننا نتجاوز بالفعل الخط الفاصل بين الجرائم التقليدية وتلك التي تتطلب وجود الإنترنت، لإن استخدام خدمات المواعدة - إن صح التعبير- عبر الإنترنت من قبل البالغين الذين يسعون إلى إغواء القُصّر بهدف ارتكاب الاعتداء الجنسي يمكن اعتباره جريمة مستقلة قائمة بذاتها، ودليلنا في ذلك أن العديد من الأنظمة القانونية المختلفة في العالم اعتبرته كذلك، ومنها التشريع الفرنسي والتشريع البلجيكي وغيرها من الدول الأوروبية الأخرى.

**2-1-2: الجرائم المستحدثة:** هناك أشكال أخرى من جرائم تكنولوجيا المعلومات والاتصالات والجرائم السيبرانية، وهي الجرائم التي يمكن أن تضر بمصالح جديدة لم تكن

(1) للتوسع أكثر يستحسن النظر إلى قانون الملكية الفكرية والأدبية الفرنسي.

(2) البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية، اعتمد وعرض للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 263 الدورة الرابعة والخمسون المؤرخ في 25 ماي 2000، دخل حيز النفاذ في 18 يناير 2002.

<http://hrlibrary.umn.edu/arab/pro-chlid2.html> Consulté le 03/03/2024 à 16h:25mn.

موجودة من قبل، أي قبل استخدام أجهزة الكمبيوتر وما نتج عنها من معلوماتية ووسائل الكترونية وقبل حتى ظهور شبكة الاتصالات العالمية (الأنترنت)، وهذا ما يعتبر من بين أحد تحديات القانون الجنائي في القرن الحادي والعشرين، ويتمثل هذا التحدي في تحديد هذه المصالح القانونية بشكل صحيح، واضح ودقيق، وذلك من أجل شيئين اثنين وهما على التوالي:- توفير الحماية القانونية لهذه المصالح من التدخل غير المناسب.

### 1-2-1: توفير الحماية القانونية لهذه المصالح من التدخلات غير المناسبة:

كان لزاما على المشرعين أن يتدخلوا تدخلا سريعا لحماية هذه المصالح الجديدة (كمصلحة ملكية المعطيات الشخصية لشخص ما مخزنة على مستوى بنك معلوماتي معين) والتي لم تكن معروفة قبل ظهور الفضاء الالكتروني أو الافتراضي كما يحلو للبعض تسميته، لأن حماية هذه المصالح الجديدة من المساس بها عن طريق الاستعمال غير المشروع ( يمكن أن يتجسد هذا المساس في صورة الإتلاف أو كشف سريتها) وبالتالي الاعتداء على خصوصية الأشخاص التي ترتبط ومبدأ الكرامة الإنسانية،<sup>(1)</sup> اذا حمايتها بالنصوص التي كانت سارية المفعول آنذاك لم يجدي نفعا، لعدم كفاية إنفاذ النصوص القانونية بالتشريعات الوطنية وضعف وعدم فعالية الضمانات الإجرائية التي كانت موجودة آنذاك، لأن هذا النوع من الإجرام لا يمس الفرد مستقلا عن المجتمع بل يمس أمن المجتمع ككل ويجعلنا نترقب بنشوء جيل جديد من الإجرام على مستوى جد مرتفع من الخطورة، وهذا ما جعل الأنظمة القانونية تستحدث نصوص قانونية تتلاءم وهذا النوع من الجرائم المستحدثة ذات المصالح الجديدة.

بالإضافة إلى أن الظروف السياسية والثقافية والاجتماعية والاقتصادية هي التي كانت بمثابة الفاعل الذي تتأثر به القاعدة القانونية أثناء إنشائها أو تعديلها أو حتى تفسيرها لمواجهة الجرائم التقليدية، إلا أنه في هذا النوع الجديد من الجرائم تدخلت عناصر أخرى أصبحت بمثابة المحرك الأساسي في إنشاء وصناعة القواعد القانونية ومن بينها النمو التكنولوجي غير المتناهي والذي أصبح يزداد تعقيدا لما ظهرت معه مصطلحات علمية

(1) - الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة، بتاريخ 10/12/1948 القرار رقم 217 المادة 12 منه.

<https://www.un.org/ar/about-us/universal-declaration-of-human-right>

جديدة والكم الهائل من المعطيات التي أصبحت تعالج آلياً وبالسّعة الإلكترونية الخارقة، مما جعل أحياناً رجال القانون عاجزين على فك ألغاز بعض الإشكالات الناتجة عن ذلك.

### 2-2-1-2 تحديد حدود نطاق تطبيق القانون الجنائي:

إنّ تحديد حدود نطاق تطبيق القانون الجنائي مهم جداً، لأنّ اختراع تكنولوجيا المعلومات والاتصالات وإنشاء الفضاء الإلكتروني قد فتحا أمام الناس عدداً من الإمكانيات الجديدة ومجالاً جديداً من الحرية، ليس فقط لجمع المعلومات، ولكن أيضاً لقضاء وقتهم والإبداع والتواصل مع الآخرين ومتابعة بعض المصالح منها الرياضية والتجارية وغيرها، بحيث لا يجب تطبيق القانون الجنائي على نطاق واسع للغاية إلى حد حرمان الأفراد من هذه الحرية الجديدة والإمكانيات الرائعة للتنمية الشخصية التي اكتسبوها من خلال الفضاء الافتراضي، بحيث إذا أصبح أفراد المجتمع يخافون من تصفح الإنترنت أو استخدام الخدمات التي تقدمها تكنولوجيا المعلومات والاتصالات في حياتهم اليومية، سيدفعون ثمنها باهظاً، خوفاً من التعرض لعقوبات جنائية بسبب أدنى خطأ، ولذلك فمن المهم جداً أن يتم تحديد الجرائم الجنائية بطريقة تحد من الأفعال الخطيرة والضارة ولكن لا تقيد بشدة حرية التصفح في العالم السيبراني الذي أعطى الشخص عبر العالم التواصل فيما بينهم ومنحهم حرية واسعة لم يتحصلوا عليها من قبل أبداً.<sup>(1)</sup> إنّ العديد من الأنظمة القانونية<sup>(2)</sup> تؤكد على ضرورة حماية عمل الأنظمة الفردية المتعلقة بتكنولوجيا المعلومات والاتصالات (أجهزة الكمبيوتر، اللوحات الرقمية، الهواتف الذكية والاتصال بشبكة الإنترنت، وما إلى ذلك) من خلال اللجوء إلى نصوص القانون الجنائي.

وعلى نطاق أوسع، فإن من الضروري ضمان هذه الحماية القانونية حتى يكتسب مستعملي الأنظمة ذات الصلة بتكنولوجيا المعلومات والاتصالات والفضاء الإلكتروني الثقة الكاملة في التعامل مع هذه الوسائل الحديثة، لأنها مصلحة تعلو على المصالح التي تشمل جميع المصالح الأخرى والتي بدونها يستحيل الاتصال الآمن في الفضاء السيبراني

(1) جمال بوزرتيني، تطور تكنولوجيات الإعلام والاتصال وعلاقتها بتطور الجريمة، أعمال الملتقى الدولي المنعقد بالجزائر يومي 5 و6 ماي 2010، تحت عنوان محاربة الجريمة المعلوماتية، مركز البحوث القانونية والقضائية، 2012، ص.38.

(2) Thomas Weigend, Op. Cit, p3. Consulté le 03/03/2024 à 18h: 10 mn.

الذي أصبحت تحل به الكثير من المسائل والمشاكل اليومية للمواطن، سواء في علاقته مع الإدارة أو في علاقته مع الأشخاص الآخرين في المجتمع، وتتمثل المصلحة الرئيسية في الحماية هنا في سرية<sup>(1)</sup> وسلامة وتوافر نظم المعلومات والبيانات دون عرقلة أو عرقلة الوصول إليها، لأنه في كل مرة يتعرض فيها عمل الفضاء الإلكتروني للخطر تكون على المحك حريات فردية لا محال.

خلاصة الموضوع في هذا المحور تتمثل في أنّ المصلحة القانونية الرئيسية التي يجب أن يحميها القانون الجنائي فيما يتعلق بالفضاء السيبراني هي حرية الفرد وأمنه، من منظور محدد موجه نحو الفضاء السيبراني بالطبع. لذلك، يُنظر إلى الحق في العلاقات مع الآخرين، مثل الحق في خصوصية الأشخاص، وعنصر ثقة الأفراد في الأنظمة الإلكترونية وفي المستندات والبيانات المخزنة في هذه الأنظمة، كما يتمتع بالحماية أيضاً حق الشخص في تحديد المعلومات التي يرغب في حمايتها (أي حق الشخص في اتخاذ القرار بحرية، على سبيل المثال، بشأن إدارة المعلومات ذات الطبيعة الشخصية، ومدى ونوع البيانات التي يتم الكشف عنها المتعلقة بشخص معين)، كذلك الحق المكفول دستورياً في الخصوصية وسرية الاتصالات. إنّ الاهتمام العام بالحفاظ على السلامة "المؤسسية" لتكنولوجيا المعلومات والاتصالات والعالم السيبراني يمكن أن تتحول أو أن تنقسم إلى اهتمامات خاصة، وكلها يمكن أن تتحول إلى مجالات تجذب مرتكبي الجرائم السيبرانية<sup>(2)</sup>.

**2-2: الجوانب الخاصة:** بعد تعرضنا إلى الجوانب العامة التي تتعلق بالمصالح المحمية سواء بالقوانين الخاصة بالتكنولوجيات المعلومات والاتصالات أو بالقوانين التي تواجه الجرائم السيبرانية سنعرض إلى الجوانب الخاصة والتي تتمثل في كل من الاعتداءات التي تمس بأنظمة هذه التكنولوجيات الحديثة وبالمراقبة غير القانونية بهذه الأنظمة وأخيراً بالجرائم الجنائية التي ابتكرت نتيجة هذه التقنيات الحديثة.

## 2-2-1: الاعتداءات الواقعة على أنظمة تكنولوجيا المعلومات والاتصالات:

تتمثل المصلحة الأساسية في هذا الميدان في "سلامة" الأنظمة العامة أو الخاصة

(1) د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 34.

(2) Wikipédia, l'encyclopédie libre, Technologies de l'information et de la communication, revue électronique, Consulté le 07/03/2024 à 09H.

المرتبطة بتكنولوجيا المعلومات والاتصالات، وبعبارة أخرى، تشغيل هذه الأنظمة وفقاً لقواعد التشغيل مع البيانات المقدمة من المالك الشرعي. ونظراً لأن الانتهاكات غير الشرعية يمكن أن تسبب أضراراً جسيمة، ويمكنها أيضاً أن تهدد المصداقية في الأداء الصحيح لنظام تكنولوجيا المعلومات والاتصالات، وحتى نحافظ على هذه الثقة التي يضعها الأشخاص في هذه التقنيات الجديدة فقد نصت العديد من الأنظمة القانونية<sup>(1)</sup> على فرض عقوبات جنائية على مثل هذه السلوكيات غير الشرعية.

إن نقل البيانات وتعديلها بشكل غير شرعي أو تغيير الحصول على ترخيص من صاحب الحق، أو محو البيانات والبرمجيات وتدميرها، أو إعاقة الوصول إلى النظام هي جرائم نموذجية في هذا المجال ويمكن أن نطلق عليها مصطلح "التخريب المعلوماتي"، إنَّ أغلب الأنظمة القانونية اليوم تعتبر تدمير أو تزوير أو إخفاء البيانات المخزنة في أي نظام لتكنولوجيا المعلومات والاتصالات جريمة قائمة بحد ذاتها، عادة ما تكون عملية إدخال برنامج ضار "فيروس" بنظام المعلومات والاتصالات يعتبر من نفس نوع الاعتداءات الموجودة في الأحكام العامة المتعلقة بالهجمات على أنظمة المعلومات والاتصالات، بحيث في بعض الدول يمكن أن يعاقب على مجرد الحيازة العمدية لمثل هذه البرامج الضارة، على عكس إصابة أحد الأنظمة عن طريق فيروس بطريقة غير عمدية (نتيجة اللامبالاة أو لعدم الاحتياط) لا تشكل جريمة جنائية في أغلب الأنظمة القانونية.

**2-2-2: المراقبة غير القانونية:** وهناك جريمة أخرى مرتبطة بتكنولوجيا المعلومات والاتصالات ولكنها ذات طبيعة مختلفة تتمثل في انتهاك سرية نظام الاتصالات والمعلومات عن طريق تركيب أو استخدام وسائل وبرامج معلوماتية لهذا الغرض. ما يجب توضيحه هنا هو أن المراقبة غير القانونية تختلف عن القرصنة من حيث أن مرتكب الجريمة لا يدخل النظام دون إذن فحسب، بل يسعى أيضاً للحصول على المعلومات التي تم تسجيلها أو سيتم إرسالها بواسطة النظام.

**2-2-3: الجرائم الجنائية المبتكرة:** لم يفتح العالم السيبراني إمكانيات جديدة للاتصالات والتجارة ونشر المعلومات والآراء فحسب، بل أنشأ أيضاً مصالح أخرى جديدة يمكن أن يلحق

(1) ومنها النظام الهولندي والبلجيكي والفرنسي والألماني ودول أخرى بأوروبا وآسيا والدول العربية منها أغلب دول الخليج ومصر العربية والأردن وغيرها.

أطراف آخرين بها بعض الأضرار، مما ينتج بعض الصعوبات القانونية غير المعتادة، ولهذا تعين على القانون التفاعل مع هذه الصعوبات الجديدة، وهذا ما دفع بعض الأنظمة القانونية بوضع تعريفات جديدة للجرائم الموجهة بشكل خاص نحو حماية المصالح الفردية في العالم السيبراني.<sup>(1)</sup> ووضعت بعض الترتيبات من أجل حماية البعض منها (المصالح) في هذا الميدان، ووفقاً لهذه الترتيبات أصبح قيام أي شخص باستخدام شبكة أو خدمة اتصالات إلكترونية أو وسيلة إلكترونية أخرى لإزعاج مراسله أو إلحاق الضرر به أو تركيب أي وسيلة تعتبر جريمة مكتملة وحتى الشروع في ذلك يعتبراً شروعا مكتملاً يعاقب عليه.

وإذا تساءلنا عن مدى شدة الخطورة التي تكمن في كل اعتداء يرتكب باستخدام تكنولوجيا المعلومات والاتصالات عن بعد مقارنة بتلك التي ترتكب وجهاً لوجه كالجرائم التقليدية مثلاً، فالجرائم التي ترتكب بالتكنولوجيات الحديثة بالإضافة لتحقيق الأضرار التي تتوفر بنفس الجرائم لما ترتكب بالوسائل العادية تتوفر على خطر آخر يرتبط عادةً بالإنترنت وهو التوزيع السريع للصور الفوتوغرافية وصور الأشخاص دون موافقتهم أو ضد إرادتهم، وأشياء تمس بسمعهم أحياناً كما هو الشأن في جرائم السب العلني والشتيم وما يشبههما ويعلم بها جمهور واسع على الشبكة العنكبوتية وتبقى متاحة مدة طويلة من الزمن على عكس النقس الجريمة إذا ما ارتكبت بالطرق التي كانت ترتكب عليها قبل ظهور هذه الوسائل الحديثة.

لقد عالجت عدة تشريعات هذه المسألة ومن بينها التشريع الإسباني<sup>(2)</sup> من خلال تجريم نشر أو الكشف أو تقديم "صور أو تسجيلات صوتية وبصرية لصاحب البيانات، والتي تم الحصول عليها في المنزل أو في مكان آخر، إلى طرف ثالث، دون إذن من صاحب البيانات". الوصول إلى أطراف ثالثة، لأن الكشف عن هذه الصور ينتهك بشكل خطير الحق في الحياة الخاصة لذلك الشخص.

ومن المثير للاهتمام ملاحظته حسب رأينا أن نطاق هذه الجريمة لا يشمل التسجيلات أو الصور الفوتوغرافية غير المصرح بها أو غير المسموح بها، بل يقصد به أن يشمل تجريم نشرها بالاستخدام غير المصرح به على الأنترنت فقط. قمنا بهذه الملاحظة لأن أغلب

(1) في هذا الصدد تم تقديم حكم عام يتعلق بالتحرش عبر الإنترنت في عام 2005 في بلجيكا، أنظر

Emilio C. Viano, Rapport général, Revue internationale de droit pénale, n° 84(3-4) nouvelle série ; Edition Eres, Toulouse, France, 2013, p331.

(2) Emilio C. Viano, Revue internationale de droit pénale, op. cit, p329.

الباحثين في هذا المجال خاصة في الدول العربية يخلطون بين نية هؤلاء المشرعين ونية هيئات الأمم المتحدة (المتخصصة في مكافحة جرائم التكنولوجيات الحديثة) بين الاعتداءات التي تقع على الصور والتسجيلات وبين انتهاك سرية وخصوصية هذه الصور والتسجيلات التي تنتهك لما تستعمل عبر وسائط الأنترنت، بحيث أغلب هؤلاء الباحثين يظنون أن التجريم كان يقصد به حماية الصور الفوتوغرافية والتسجيلات على مختلف أنواعها ولا ينتهون لانتهاك سريتها بنشرها على مواقع التواصل الاجتماعي. ونسعى هنا إلى لفت الانتباه لحل مشاكل الإثبات عندما تمر معلومات سرية عبر الإنترنت وليس من السهل دائما معرفة ما إذا كان الشخص الذي قام بتوزيع هذه المعلومات مسؤولا أيضا عن الحصول عليها بطريقة غير مشروعة.

وخلاصة القول لما أردنا تبيانها هنا تتمثل في شيء لا يختلف عليه اثنان ألا وهو "أنّ العالم الافتراضي للفضاء السيبراني يختلف عن العالم الحقيقي"، ولكن ما استنتجناه في حقيقة الأمر أنّه كثيرا ما نجد هناك روابط بين الاثنين، كما يمكن أن يتأثر الأشخاص بخسارة "ممتلكاتهم السيبرانية" بنفس المقدار الذي يفقدون فيه ممتلكاتهم المادية في العالم الحقيقي.

وتثير هذه الحقيقة التساؤل حول ما إذا كان ينبغي أيضا تطبيق حماية الحقوق ضد السرقة والاحتيال، والتي تتعلق في المقام الأول بالأموال والملكية في العالم "الحقيقي"، على عالم الإنترنت، لأن بعض الدول في العالم ومن بينها الجزائر لا تزال لم تقنن في تشريعها بعض الاعتداءات التي تمس بعدة مصالح لما تمس أو لما يعتدى عليها باستعمال الاتصالات الناتجة عن التكنولوجيات الحديثة، ومن أمثلة ذلك أن يقوم أحد الأشخاص بالحصول وبشكل غير قانوني على بيانات الولوج الالكترونية الخاصة بالضحية ويقوم بعدها بطلب بضائع على أحد الموقع التجارية تاركا دفع الفاتورة للضحية لأنها سجلت باسمه، لا يوجد لدى بعض الأنظمة القانونية حتى الآن تشريعات محددة بشأن هذا النوع من الجرائم وهي لا تزال تطبق القواعد القانونية التقليدية التي وضعت قبل ظهور هذه التكنولوجيات وكان الهدف منها قمع أفعال آخرها ترتكب في ظروف غير الظروف التي توجد الآن، وهذا ما يمس أحيانا بمبدأ الشرعية الجنائية، في حين أن البعض الآخر لديه تعريفات أوسع لهذه الفعل أو الاعتداءات، وبالتالي، وعلى سبيل المثال، يجرم القانون الجنائي الفرنسي<sup>(1)</sup> انتحال هوية طرف ثالث أو استخدام

(1) المادة 1-4-226، القانون رقم 936-20 المؤرخ في 30 جويلية 2020، المعدل والمتمم للقانون الجنائي الفرنسي، الجريدة الرسمية رقم 187 المؤرخة في 31 يوليو 2020. دخل حيز التنفيذ في 1 أوت 2020.

واحدة أو أكثر من بيانات تحديد الهوية من أي نوع - بما في ذلك عنوان IP أو الاسم المستعار على شبكة اجتماعية - مما يسمح بالتعرف على هويته بهدف لتعكير راحته أو استقراره أو صفو وراحة الآخرين أو الإضرار بشرفه أو باعتباره<sup>(1)</sup>، أما في أنظمة قانونية أخرى، طبقت المحاكم في مثل هذه القضايا تجريم الغش المعلوماتي<sup>(2)</sup>.

وهنا نطرح تساؤل هل يجب وضع نصوص تعاقب على سرقة أشياء افتراضية لا وجود لها في العالم الحقيقي؟

نستطيع الإجابة بالإيجاب أي يمكن وضع أحكام خاصة لتجريم السرقة التي تقع في العالم الافتراضي، ولكن ينبغي للتشريع عند إدخال أحكام محددة لمعاقبة السرقة السيبرانية، أن يأخذ بعين الاعتبار الحالات التي لا تكون فيها الأشياء التي حصل عليها مرتكب الجريمة بطريقة غير مشروعة في الواقع أموالاً تمثل وجوداً مادياً، ولكنها مجرد صور لا قيمة لها إلا في العالم السيبراني، حيث سبق أن اعتبر القضاء في عدة دول ومنها القضاء الفرنسي أن السرقة في المجال الافتراضي لا تتوفر فيها كل العناصر الواجب توافرها في السرقة التي ترتكب في العالم الحقيقي (الجريمة التقليدية)<sup>(3)</sup>.

كما يجب أن ننوه ببعض الجرائم الافتراضية التي ينبغي أن ينتبه لها رجال القانون ومنها الاعتداء على الهوية الافتراضية نظراً للأهمية المعطاة لسمعة ونزاهة هذه الهوية، لا سيما على شبكات التواصل الاجتماعي، حيث ينبغي للتشريعات أن ترى ضرورة تجريم اغتصاب الهوية الافتراضية للشخص أو تزويرها، حتى في حالة عدم نية مرتكب الفعل التسبب في ضرر مادي معين، لأن التعبير عن آراء معينة أو وضع إعلانات أو نشر معلومات

[https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000042193593/](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193593/) Consulté le 10/04/2024 à 12H

أحكام مماثلة في بعض المقاطعات في الولايات المتحدة، حيث ينص القانون الفيدرالي الأمريكي وكذلك هناك<sup>(1)</sup> القانون الكندي على قمع حيازة أو استخدام وسيلة لتحديد الهوية بقصد ارتكاب عمل غير قانوني.

<https://documents.un.org/doc/undoc/gen/n04/561/50/pdf/n0456150>

Lettre datée du 12 octobre 2004, adressée au Président du Comité par la permanente adjointe des États-Unis d'Amérique auprès de l'Organisation des Nations Unies, p35.

(2) ومنها القضاء البلجيكي.

(3) حكم محكمة فارسي (VERSAILLES) بتاريخ 1988/09/29، حيث جاء المنطوق "أن عناصر الركن المادي لجريمة السرقة لم تكتمل في حالة ارتكابها في المجال الافتراضي".

كاذبة تحت الهوية الافتراضية لشخص آخر يمكن أن يتسبب في ضرر معنوي جسيم للشخص الحقيقي المعني في عالم الإنترنت، ويمكن أن يمتد هذا الضرر إلى أضرار مادية أخرى لم يكن يقصدها الجاني كما سبق أن قلنا، ويمكن اعتبار هذا الضرر أكبر وأخطر من ضرر خسارة الأموال من خلال أفعال أخرى سبق تجريمها مثل الطلبات الكاذبة على مواقع التسوق عبر الإنترنت، ومن أمثلة ذلك: قيام أحد الأشخاص بوضع إعلاناً عبر الإنترنت تحت اسم شخص آخر وهو صبي يبلغ من العمر 12 عاماً يُزعم أنه يبحث عن ممارسة الجنس مع صبي آخر<sup>(1)</sup>.

### 3) الأركان المادية والمعنوية لجرائم تكنولوجيا المعلومات والاتصالات والجرائم السيبرانية:

ونظراً لحدثة تكنولوجيا المعلومات والاتصالات والجرائم السيبرانية، فمن المثير للاهتمام ملاحظة كيفية عمل التشريعات لتعريف هذه الجرائم الجديدة. هل هناك خصائص نموذجية في تعريف هذه الجرائم الجديدة؟

3-1- تعريف العنصر المادي: الجرائم التقليدية، غالباً ما يتم تعريفها على أساس الضرر الذي يصيب المتضرر ويعتبر جزءاً من الركن المادي للجريمة، مثل القتل لأنه يسبب ضرراً جسدياً، أو الاحتيال لأنه يسبب ضرراً مادياً لأصول مالية، أما فيما يتعلق بجرائم تكنولوجيا المعلومات والاتصالات والجرائم السيبرانية، يبدو ذلك بمثابة الاستثناء وليست القاعدة، حيث نلاحظ أنه في معظم الحالات يتم تجريم ارتكاب الأفعال في هذا الميدان، بغض النظر عما إذا كان هذا الفعل قد يكون له أو لا يكون له عواقب على المصالح المحمية، على سبيل المثال، يشكل الوصول إلى شبكة اتصالات ومعلومات محمية أو نقل صور إباحية عبر الإنترنت جريمة تامة، من المؤكد أن هذه الأفعال تؤدي إلى نتيجة، وعلى سبيل المثال، الشخص الذي يحاول توزيع صور إباحية ولكنه لا يستطيع الوصول إلى الإنترنت من هاتفه النقال لم "ينقل" الصور، ولكن الضرر الذي تريد التشريعات محاربته - انتهاك سرية بعض المعلومات في حالة القرصنة، وتحفيز سوق استغلال الأطفال في المواد الإباحية - لا تتطلب

(1) <https://www.coe.int/fr/web/portal/-/despite-finland-s-high-standards>, « Malgré des normes sévères en matière de protection des mineurs contre les violences sexuelles et de garantie de leur bien-être, certaines lacunes subsistent », Consulté le 22/05/2024 à 22h10.

حدوث الضرر حتى يمكن معاقبة مرتكب الجريمة على الجريمة المرتكبة. يمكن أيضاً تصنيف غالبية جرائم تكنولوجيا المعلومات والاتصالات والجرائم السيبرانية على أنها جرائم تعرض للخطر، والدليل على ذلك أنه لا توجد تعريفات كثيرة التي تعتمد على اختلال النظام كشرط لقيام الجريمة في هذا النوع من الجرائم.<sup>(1)</sup> لأنه يكثر من الأحيان، يعتبر التسبب في ضرر حقيقي، (والذي يهدف التجريم الجنائي إلى الوقاية منه) -على سبيل المثال -إتلاف البيانات عن طريق التدخل في نظام المعلومات والاتصالات - ظرفاً مشدداً في بعض الإدانات، وهذا ما لاحظناه في أغلب التشريعات ومنها التشريع الجزائري<sup>(2)</sup>.

ما يمكن الإشارة إليه في مجال الجرائم السيبرانية هو أن صفة الشخص الذي يرتكب هذا النوع من الجرائم تؤثر كثيراً على نوع العقبة وعلى شدتها، وذلك يرجع إلى المسؤولية التي أوكلت إليه، على سبيل المثال، في القانون الجزائري، قد تتم معاقبة الشخص الذي ينتهك سرية البيانات بشكل أشد إذا كان هو مقدم خدمة اتصالات أو ممثله القانوني أو شخصاً مسؤولاً عن حماية سرية البيانات.

### 3-2- تعريف الركن المعنوي (القصد الجنائي)

تتطلب معظم الجرائم التقليدية المرتكبة بالوسائل تكنولوجيا المعلومات والاتصالات وجود نية من جانب مرتكب الجريمة، ويشمل ذلك، في العديد من الأنظمة القانونية، شكلاً من أشكال إمكانية وجود "الاحتيال" الذي يتمثل في الوعي والاستعداد لتحمل المخاطر التي تنتج عن الفعل المجرم.

### 4- عقوبات ذات طابع خاص:

بالإضافة إلى السجن والغرامات، تنص بعض الأنظمة القانونية على عقوبات خاصة بالجرائم التي ترتكب في مجال الانتهاكات الواقعة على تكنولوجيات المعلومات والاتصالات وفي الجرائم السيبرانية بحيث يمكن مصادرة الأجهزة والبرمجيات الضارة كما يمكن استخدام جميع الوسائل التقنية لحجب البيانات وجعل الوصول إليها غير ممكناً إذا كانت هذه

(1) وهذا ما نلاحظه كذلك في القوانين التي تواجه هذا النوع من الجرائم ومنها القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، الجريدة الرسمية عدد 71، المؤرخة في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 جوان 1966 يتضمن قانون العقوبات.

(2) المادة 394 مكرر من القانون العقوبات الجزائري.

البيانات تشكل موضوع الجريمة، أو كانت نتاجاً لها أو إذا كانت مخالفة للنظام العام، أو تشكل خطراً على سلامة الدولة، وهذا ما لاحظناه في بعض دول التي تقدمت في مجال التشريع المتعلق بالتكنولوجيات الحديثة والاعتداءات الواقعة عليها، ومن بينها بلجيكا<sup>(1)</sup>.

هناك من يرى<sup>(2)</sup> أن بعض الدول تميل أثناء قيامها بسن تشريعاتها إلى المبالغة في رد فعلها تجاه التهديد الذي تشكله تكنولوجيات المعلومات والاتصالات والجرائم السيبرانية، وذلك من خلال فرض عقوبات شديدة للغاية على هذه الجرائم الجديدة، معتمدين على المبدأ العام المتمثل في: "أن العقوبات لا ينبغي أن تكون متناسبة مع خطورة الجريمة"، ولكن وحسب رأينا أن هذا المبدأ يتأرجح بين القبول والرفض من قبل الأخصائيين القانونيين، أو بالأحرى بين الاستغناء عنه في بعض الحالات، نظراً لتحول الجريمة المعنية بالتشريع إلى ظاهرة اجتماعية إجرامية تنخر بأحد عناصر المجتمع أو الدولة، كالمساس بالاقتصاد الوطني<sup>(3)</sup>، أو باستقرار الأمن والحفاظ على النظام العام، وبين وجوب استعماله وتطبيقه بحيث يكفي وضع عقوبات خفيفة تكفي لتحقيق الردع العام والخاص، أمّا فيما يخص التهديدات التي تشكلها تكنولوجيات المعلومات والاتصالات وكذا الجرائم السيبرانية تعتبر خطيرة وتهدد استقرار المجتمع وتمس بأكثر من مصلحة محمية في آن واحد، ومن بينها المصالح المقدسة للفرد والتي يحميها الدستور في نصوصه القانونية بكل وضوح، ومنها الحريات الشخصية للأفراد، وسرية المعطيات الشخصية لهم وغيرها، ولهذا يجب أن يعتمد المشرعون على وضع عقوبات أشد لما يتعلق الأمر بالاعتداءات التي تقع في هذا المجال.

وإن شئنا أن نضرب مثالا على ذلك، فلا نجد أحسن من جريمة "الشتم والسب"، بحيث يمكن أن ترتكب بالطرق التقليدية ما يمكنها أن ترتكب بالطرق التي تعتمد على تكنولوجيات الحديثة باستعمال مواقع التواصل الاجتماعي على مختلف أشكالها، بحيث

(1) Catherine Forget, Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict, Revue du droit des technologies de l'information - N° 66-67/2017, p25.

- لاحظنا أن المدعي العام في بلجيكا يقوم باستخدام هذه السلطة، حيث يمكنه أن يأمر مزود خدمة الإنترنت بإزالة اسم المجال لموقع ينتهك القانون، على سبيل المثال، لأنه يجعل المواد الإباحية للأطفال متاحة. انظر:

Thomas Weigend, op. cit, p27. Consulté le 06/07/2024 à 10h

(2) Thomas Weigend, op. cit, p30.

(3) وهذا ما لاحظناه في التشريع الجزائري فيما يتعلق بجريمة المضاربة، أين أخذ المشرع الجزائري بعين الاعتبار خطورة الجريمة ووضع لها عقوبات شديدة، ونفس الشيء بالنسبة لجريمة عصابة الأحياء.

في الحالة الأولى تقع الجريمة بين شخصين في مكان معين وفي وقت معين، أي المكان والزمان محددين، وبمجرد وقوع الفعل المادي للسب أو الشتم وانتهائه تنتهي الواقعة، ولا يسمع الغير بهذه الجريمة إلا من كان حاضرا في المكان المحدد وأثناء وقوع الواقعة أي في الزمان المحدد كذلك، أما وقوع هذه الجريمة باستعمال مواقع التواصل الاجتماعي تنتج أثارا أخرى أكثر خطورة؛ منها أن مرتكب الجريمة له سهولة في ارتكابها متى شاء، لأنه يرتكبها عن بعد (من مكان العمل، البيت، خارج حدود الوطن، وأيضا كان تواجهه)، أي سهولة ارتكاب الفعل وأحيانا يستطيع أن يقوم بالجريمة وهو متسترا عن هويته، على عكس الجريمة التقليدية التي كان ينبغي على المرتكب أن يبحث عن الضحية وعن مكان تواجهه، مع احتمال عدم العثور عليه، وإذا ارتكبها يكون معلوم الهوية، هذا من جهة، ومن جهة أخرى، ويمكن كذلك أن يطلع على هذا السب والشتم عدد كبير من الأشخاص (كل من يدخل إلى الموقع أو الصفحة التي نشر بها السب)، ولهذه الأسباب كنا قد اقترحنا في عدة مناسبات أن يضيف المشرع فقرة في نفس المادة التي تتعرض لفعل السب والشتم ويخصص لها ظرفا مشددا وبالتالي عقوبة مشددة إذا توفر هذا الظرف المتمثل في الحالة التي ترتكب فيها هذه الجريمة باستعمال وسائل التكنولوجيات الحديثة أو بالطرق الالكترونية (المصطلح الذي استعمله المشرع الجزائري في القانون رقم 04/09<sup>(1)</sup>).

### خاتمة

تعرضنا في هذه الورقة البحثية إلى أهم المسائل القانونية التي عالجتها اللجنة الأولى للجمعية الدولية للقانون الجنائي فيما يخص أهم التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن السيبراني، وتوصلنا إلى عدة نتائج مهمة، كما قمنا بتقديم بعض الاقتراحات التي من شأنها التقليل من ارتكاب هذا النوع من الاعتداءات. ففيما يخص الاستنتاجات، لاحظنا ما يلي:

أولا: أن المهمة أسندت إلى اللجنة الأولى للجمعية الدولية للقانون الجنائي، التي من العادة تسند إليها المواضيع المتعلقة بالقانون الجنائي العام ولا المواضيع المتخصصة (مثل هذا الموضوع) الذي كان من المفروض أن يسند إلى اللجان التقنية للجمعية.

(1) القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر بتاريخ 05 أوت 2009، الجريدة الرسمية العدد 47.

ثانيا: إن الانتقادات التي وجهت من قبل المختصين في هذا الميدان فيما يخص إسناد هذه المهمة للجنة غير متخصصة رد عليها أعضاء الجمعية الدولية للقانون الجنائي بالحجج التالية:

- حماية المصالح القانونية المرتبطة بشكل مباشر تكنولوجيا المعلومات والاتصالات وتحديات الفضاء الإلكتروني بالقانون الجنائي العام.
- مشكلة احترام مبدأ الشرعية، وخاصة ضرورة الدقة في صياغة التهم الجنائية لما يتعلق الأمر بمثل هكذا مواضيع تقنية مستعصية.
- دور القانون الجنائي في البحث عن طرق بديلة لحماية المصالح القانونية من خلال وسائل خاصة بالويب مثل حظر الوصول إلى الموقع الإلكتروني أو إزالته.
- ردود الفعل التشريعية على تحدي عدم الكشف عن هوية مستخدم الإنترنت.

أرى من وجهة نظري أن هذه الردود كانت جد مقنعة لتبرير إسناد هذه المهمة للجنة القانون الجنائي العام وليس للجان تقنية، إلا أنه يجب الإشارة إلى أن اللجان التقنية شاركت في هذا العمل مع لجنة القانون الجنائي العام بطريقة غير مباشرة، لما كلفت الجمعية الدولية خبراء الدول بإجراء تقارير عدة دول حول أهم المسائل القانونية المتعلقة بالجرائم المتصلة بتكنولوجيات المعلومات والاتصالات.

ثالثا: أن المسائل القانونية التي عولجت من قبل الجمعية الدولية للقانون الجنائي، والتي طرحت أمام المؤتمر الدولي التاسع عشر للقانون الجنائي المنعقد بمدينة (ريو دي جانيرو) بالبرازيل سنة 2014 كانت جد مهمة، وكانت اللبنة أو الأرضية التي اعتمدت في مختلف التشريعات لمعظم الدول في العالم ومنها التشريع الجزائري.

أما فيما يخص الاقتراحات، فنقدم التي نرى أنها فعالة ويمكن أن تجنبنا عدة تساؤلات طرحت في هذا الميدان، وتتمثل في:

أولا: يمكن بسهولة تجنب بعض جرائم تكنولوجيا المعلومات والاتصالات والجرائم الإلكترونية من خلال اتخاذ التدابير الاحترازية المناسبة من قبل أولئك الذين يصبحون ضحايا لهذه الجرائم، وخاصة عن طريق استخدام برامج مكافحة الفيروسات وحماية جهاز الكمبيوتر الخاص بهم والوصول إلى الإنترنت ومواقع معينة باستخدام كلمات مرور قوية. وهذا يثير التساؤل حول ما إذا كان من الممكن تحويل عبء منع مثل هذه الانتهاكات

إلى المستخدم، مما يجعله مسؤولاً عن حماية مصالحه الخاصة بدلاً من فرض عقوبات على مرتكب الانتهاكات التي كان من الممكن تجنبها بسهولة.

ثانياً: إن إحدى الطرق غير المباشرة لمنع الجرائم الإلكترونية والجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات تتمثل في الحد من إخفاء هوية المستخدم، لأنه تحت غطاء عدم الكشف عن الهوية، يتم تشجيع الأفراد على طلب أو تلقي محتوى غير مشروع، معتقدين أنهم لا يخشون أي اكتشاف. إذا تمكن المستخدمون من التنقل عبر الفضاء الإلكتروني باستخدام هوياتهم الحقيقية أو الكشف عن بيانات اعتمادهم، فقد يتم تقليص جاذبية الجرائم الإلكترونية بشكل كبير. ومن ناحية أخرى، يعد الفضاء الإلكتروني جذاباً أيضاً لأن الناس يستطيعون تغيير هوياتهم أو اللعب بها.

ثالثاً: الطريقة الأكثر موثوقية لتسجيل المستخدمين أثناء قيامهم بأنشطة معينة بصفتهم أشخاص طبيعيين عبر الإنترنت (على سبيل المثال: وضع محتوى محظور على موقع ويب أو عرض موقع ويب يحتوي على مثل هذا المحتوى) هي تسجيل أرقام IP الخاصة بهم وتخزينها، بمساعدة أرقام IP والعناوين ذات الصلة، من الممكن تتبع أنشطة الويب للمستخدمين، سواء على أجهزة الكمبيوتر أو الهواتف المحمولة.

### قائمة المراجع

#### المراجع باللغة العربية:

##### القوانين:

- القانون رقم 04-15 المتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات المؤرخ في 10 نوفمبر 2004 الجريدة الرسمية عدد 71، المؤرخة في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات.
- القانون رقم 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر بتاريخ 05 أوت 2009، الجريدة الرسمية العدد 47.

##### الكتب:

- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي

الحقوقية، بيروت-لبنان، 2005.

### المجلات والمقالات:

- بحوث مؤتمر القانون والكمبيوتر والإنترنت، الطبعة الثالثة، العين: جامعة الإمارات، 2004.

- جمال بوزرتيني، تطور تكنولوجيات الإعلام والاتصال وعلاقتها بتطور الجريمة، أعمال الملتقى الدولي المنعقد بالجزائر يومي 5 و6 ماي 2010، تحت عنوان محاربة الجريمة المعلوماتية، مركز البحوث القانونية والقضائية، 2012.

### المواقع الالكترونية:

- <https://www.un.org/ar/about-us/universal-declaration-of-human-right>  
- <http://hrlibrary.umn.edu/arab/pro-chlid2.html>

### المراجع باللغة الأجنبية:

#### Lois :

- Loi n° 2020-936 du 30 juillet 2020 parue au JO n°187 du 31 juillet 2020 code pénal français.

#### Revues :

- Catherine Forget, Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict, Revue du droit des technologies de l'information - N° 66-67/2017.  
- Emilio C. Viano, Rapport général, Revue internationale de droit pénale, n° 84(3-4) nouvelle série ; Edition Eres, Toulouse, France, 2013.

#### Sites Web:

- <https://www.penal.org/fr/colloques-internationaux>.  
- [https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime\\_Study\\_French](https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_French), Office des nations unies contre la drogue et le crime, Étude détaillée sur la Cybercriminalité  
- <https://droit.cairn.info/revue-internationale-de-droit-penal-2013>  
- <https://www.Wikipédia>, l'encyclopédie libre, Technologies de l'information et de la communication, revue électronique.  
5[https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000042193593/](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193593/)  
- <https://documents.un.org/doc/undoc/gen/n04/561/50/pdf/n04561507>  
- <https://www.coe.int/fr/web/portal/-/despite-finland-s-high-standards>