"التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها"

مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18 جانفي 2022

من إعداد الباحثة: سويسي فتيحة

قاضية باحثة بمركز البحوث القانونية والقضائية

ملخص:

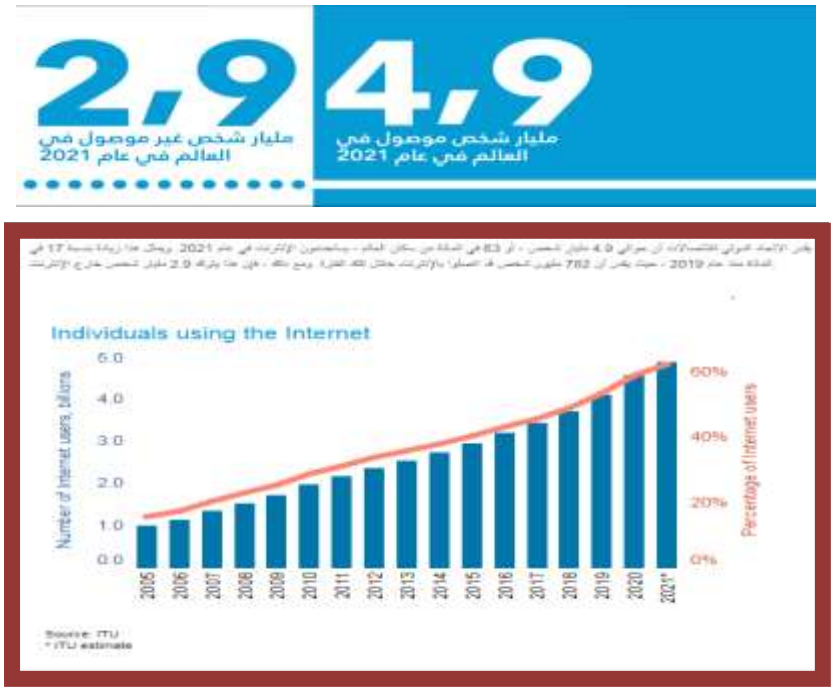
أدى التطور التكنولوجي المتسارع بفضل الاستخدام الواسع للتكنولوجيات الحديثة للإعلام والاتصال في جميع المجالات(NTIC)، Les nouvelles technologies d'information et communication إلى بروز نمط جديد من الإجرام وهو الإجرام المعلوماتي أو ما يعرف بالجريمة الالكترونية أو الجريمة السبيرانية. إذ يعتبر هذا النوع من الجرائم بشتى صوره وأنواعه من أكبر التحديات التي تواجهها الدول بسبب انتشاره الواسع لكونه يتسم بالطابع الدولي أي عابر للحدود وأصبح يهدد اليوم الأمن المعلوماتي للأفراد والمؤسسات مما تستدعي الضرورة للتصدي لهذا النوع من الإجرام.

يتمثل موضوع الندوة البحثية في مناقشة أحد أهم الجرائم المطروحة أمام القضاء والتي تتسم بالخطورة البالغة وهي: الجرائم المعلوماتية، وذلك من خلال تسليط الضوء على الإطار القانوني الذي ينظمها وكيفية إضفاء التكييف القانوني الصحيح للوقائع التي تكتسي طابع الجريمة المعلوماتية. كما تهدف هذه الندوة إلى مناقشة أهم الإشكالات العملية المطروحة في مجال الجرائم المعلوماتية والتي تواجه القاضي الجزائي وقضاة النيابة على ضوء الممارسة القضائية، ومحاولة إيجاد حلول لها من خلال المناقشات قصد المساهمة في توحيد العمل القضائي. وتكمن أهمية دراسة الموضوع لحداثته من جهة، وخطورته من جهة أخرى، وللوقوف على مدى مواكبة المشرع الجزائري للتطورات الحاصلة في مجال مواجهة جرائم تكنولوجيات الإعلام والاتصال باعتبارها من أكثر أنواع الجرائم تعقيدا لارتباطها بالنظام المعلوماتي.

الكلمات المفتاحية: المجرم المعلوماتي، الإجرام السبيراني، الدليل الالكتروني، الحق في الخصوصية، التعاون الدولي.

مقدمة

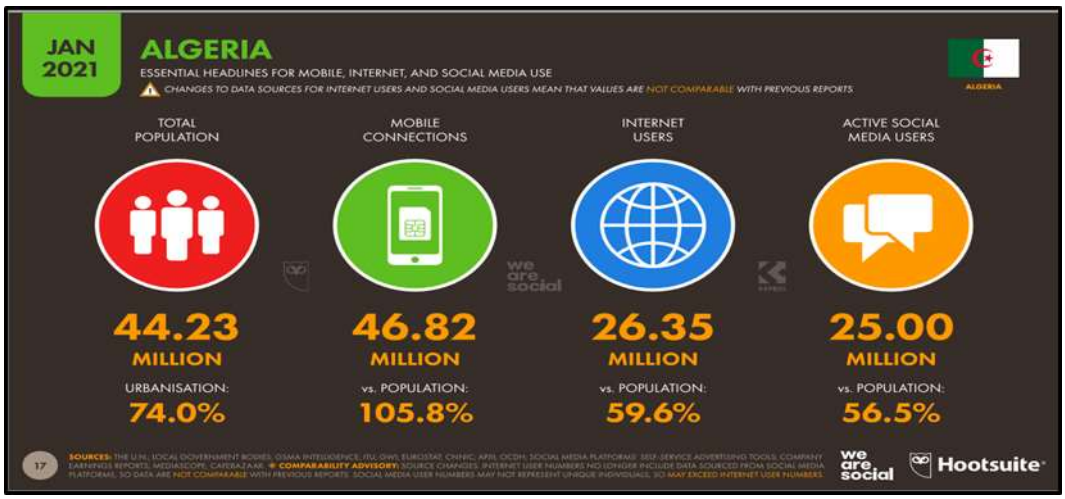
إن الـتطورات السريعة في مجال التكنولوجيا الرقمية نتيجة استخدام الشبكة العالمية الانترنت أدت إلى بروز نمط جديد من الإجرام وهو الإجرام الالكتروني أو ما يسمى بالجريمة المعلوماتية، نظرا لتوفر الوسائط المستحدثة لتكنولوجيات الإعلام والاتصال، والتي ساهمت بشكل كبير في انتشار الجريمة المعلوماتية وتطورها فحسب آخر الإحصائيات لسنة2021الصادرة عن الاتحاد الدولي للاتصالات وهي وكالة تابعة للأمم المتحدة متخصصة في مجال تكنولوجيا المعلومات والاتصالات.(ITU) أشارت إلى وجود نمو عالمي قوي في استخدام الأنترنت حيث ارتفع مستخدميها عبر العالم إلى 4.9 مليار شخص خلال سنة 2021 وفي المقابل يبقى 2.9 مليار شخص عبر العالم غير موصول بشبكة الانترنت، أي ما يعادل نسبة 37 بالمائة من مجموع سكان العالم.[1]



"مستخدمي الأنترنت في العالم إحصائيات سنة 2021"

[1]- الموقع الرسمي للاتحاد الدولي للاتصالات www.itu.int.

أما بالنسبة للجزائر وحسب نفس المصدر، فقد بلغ عدد مستخدمي الانترنت في جانفي **2021** حوالي 26.35 مليون شخص أي بنسبة 59.6 بالمائة من مجموع السكان. كما تزايد عدد مستخدمي مواقع التواصل الاجتماعي في الجزائر وبلغ 25 مليون شخص اي بنسبة 56,5 بالمائة من مجموع السكان.[1]



"مستخدمي الانترنت في الجزائر: إحصائيات جانفي 2021"

وبمجرد القراءة الأولية لهذه الإحصائيات الحديثة فإن الارتفاع الحاد في استخدام الأنترنت راجع أساسا إلى عدة عوامل ومن بينها الآثار الناجمة عن انتشار وباء كورونا في العالم والتدابير المتخذة من طرف الدول وزيادة الحاجة للجوء إلى الخدمات الالكترونية من خلال التحول الرقمي مثل: الخدمات المصرفية عبر الأنترنت، التعليم عن بعد، العمل عن بعد، التجارة الالكترونية...الخ.

كما أن هذه الأرقام لها مدلول إيجابي حول واقع الانترنت في الجزائر، إذ تعتبر خطوة مهمة نحو بناء مجتمع معلوماتي أكثر شمولا لكنها من جهة أخرى، تبرز الحاجة الملحة لزيادة الحماية الالكترونية على المستوى الوطني قصد تعزيز الأمن السيبراني في الجزائر.

[1]- نفس المصدر www.itu.int.

وتجدر الإشارة إلى أن حق الأشخاص في الاتصال وتبادل المعلومات يتطلب الحماية القانونية بما يضمن ممارسة هذا الحق، والتي تعتبر من الضمانات الدستورية حيث يترتب على سهولة الاتصال والحصول على المعلومات عبر شبكة الأنترنت وبواسطة الأنظمة المعلوماتية سهولة حدوث بعض الأفعال الإجرامية قد تتعدى آثارها الحدود الوطنية باعتبار أن الجريمة المعلوماتية من الجرائم العابرة للحدود، إلا أن مكافحة الجريمة المعلوماتية والتصدي لها لا يتأتى دون تسليط الضوء على الإشكالات التي تثيرها من خلال الممارسة القضائية لكون ذلك من شأنه أن يساعد في فهم ماهيتها مما يسهل محاربتها من خلال سد الثغرات. وللوقوف على مدى مواكبة المشرع الجزائري للتطورات الحاصلة في مجال مواجهة جرائم تكنولوجيات الإعلام والاتصال باعتبارها من أكثر أنواع الجرائم تعقيدا لارتباطها بالنظام المعلوماتي.

ولمعالجة هذه المسائل نطرح الإشكالية التالية:

ما مدى نجاعة الترسانة القانونية التي وضعها المشرع الجزائري لمكافحة الجريمة المعلوماتية والوقاية منها؟

وتتفرع عن هذه الإشكالية عدة تساؤلات فرعية تتمثل فيما يلي:

- كيف يمكن مباشرة إجراءات التحقيق في الجريمة المعلوماتية دون أن يتعارض مع الحق في الخصوصية؟
- ما مدى مسايرة المشرع الجزائري لتطور الإجرام المعلوماتي بالموازاة مع سرعة التكنولوجيات الحديثة؟
- ماهي الإشكالات العملية التي تثيرها الجرائم المعلوماتية على ضوء الممارسة القضائية؟
- ماهي الحلول المقترحة لمعالجة هذه الاشكالات؟

ولمعالجة هذه الإشكالية، تم تقسيم المداخلة إلى ثلاث محـــاور أساسية:

محور تمهيدي/ الإطار المفاهيمي لجرائم المعلوماتية

المحور الأول/ التكييف القانوني لجرائم المعلوماتية

المحور الثاني/ أهم الإشكالات الموضوعية والإجرائية التي تثيرها جرائم المعلوماتية

محور تمهيدي/ الإطار المفاهيمي للجرائم المعلوماتية

1- نشأة الجريمة المعلوماتية و تطورها ضمن التشريعات الدولية:

خلال سنة 1966 سجلت أول قضية في الولايات المتحدة الأمريكية تتعلق بارتكاب أفعال إساءة استعمال الحاسوب أين تمت محاكمة مهندس يعمل في البنك من أجل قيامه بالتحايل على برنامج الإعلام الآلي لاختلاس مبلغ مالي، كما تم تسجيل عدة قضايا مماثلة تتعلق بالدخول خلسة إلى الأنظمة المعلوماتية للاطلاع على محتواها وكان القضاء يتعامل مع هذه القضايا على أساس قضية سرقة بالإكراه وأحيانا يعتبرها إخلال بالتزامات المسؤولية العقدية.

وفي اليابان، سجلت أول قضية خلال سنة 1970 تتعلق بالمساس بالأنظمة المعلوماتية على إثر اكتشاف عملية سرقة ونشر معطيات شخصية لزبائن شركة تجارية.[1]

ونظرا لصعوبة التعامل مع هذا النوع من الجرائم بسبب خصائص البيئة المعلوماتية الافتراضية، تبلورت فكرة ضرورة وضع نصوص قانونية خاصة وبادرت عدة دول إلى إصدار تشريعات تجرم إساءة استعمال الكمبيوتر ونذكر على سبيل المثال:

- في الولايات المتحدة الامريكية في سنة 1970 صدر أول قانون خاص بحماية البيانات وحق الوصول إليها ثم في سنة 1977 أصدرت أول تشريع فدرالي خاص بجرائم الحاسوب.

- السويد – في سنة1973 أصدرت قانون المعطيات المعلوماتية.

---

[1]- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية: دراسة مقارنة، مذكرة رسالة ماجستير، جامعة الشرق الاوسط كلية الحقوق عمان، الأردن ،2014 ، ص.43.

- فرنسا – في سنة 1978 أصدرت قانون يتعلق بالمعلوماتية والحريات.

في سنة 1988 أصدرت قانون يتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات GODFRAIN.[1]

وفي مطلع الثمانينات تبنى مجلس أوروبا اتفاقية حماية المعطيات الشخصية والمعالجة الآلية لها.[2]

واستمر التطور التشريعي لمعالجة هذا النوع من الجرائم في العديد من الدول عبر العالم، وبرزت الحاجة إلى ضرورة التعاون الدولي في هذا المجال أين صدرت عدة اتفاقيات إقليمية ودولية من بينها اتفاقية بودابست والمتعلقة بمكافحة الجرائم الالكترونية التي أعدها مجلس أوروبا سنة 2001 ودخلت حيز التنفيذ في 2004 وتلاها بروتوكولين إضافيين في سنة 2006 والثاني في 2021.[3] وصادقت على هذه الاتفاقية عدة دول وتعتبر الإطار الدولي الوحيد إلى غاية اليوم في مجال مكافحة الجرائم المعلوماتية، تهدف أساسا لتوحيد الجهود الدولية وتوطيد التعاون الدولي للتصدي لهذا النوع من الإجرام.

2- تعريف الجريمة المعلوماتية:

في الـــواقع لا يوجد أي تعريف موحد أو متفق عليه للجريمة المعلوماتية لأن ذلك يتطلب إسقاط مفاهيم مادية في عالم لامادي IMMATERIEL أي افتراضي وهذا ما زاد في الأمر تعقيدا، بالرغم من أن العنصر الوحيد الذي لا يتغير هو ID IDENTIFIANT (المعرّف الرقمي).

وتجدر الإشارة إلى أن كل من اتفاقية بودابست، والقانون الاسترشادي العربي، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لم يتضمنوا أي تعريف للجريمة

---

[1]- مختار الاخضري، الإطار القانوني لمواجهة جرائم المعلوماتية في الفضاء الافتراضي، مداخلة ألقيت خلال أعمال الملتقى الدولي بالجزائر بعنوان "محاربة الجريمة المعلوماتية "، يومي 5-6 ماي 2010 ، مركز البحوث القانونية و القضائية، طبعة 2011 ، ص .54.

[2]- الاتفاقية رقم 108 المؤرخة في1981/01/28 لمجلس أوروبا المتعلقة بحماية الأشخاص اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، والبروتوكول الإضافي رقم 181 لسنة 2001 الخاص بسلطات المراقبة و انسياب و تدفق المعطيات عبر الحدود، للاطلاع على الاتفاقية و البروتوكول الإضافي من خلال رابط الموقع الرسمي لمجلس أوروبا. www.int.coe

[3]- الاتفاقية الأوروبية لمكافحة الجرائم الالكترونية، الموقعة ببودابست بتاريخ 23 نوفمبر 2001، وبروتوكولها الإضافي الأول الموقع بستراسبورغ بتاريخ 28 جانفي 2003، بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، والبرتوكول الإضافي الثاني المؤرخ في 2021/11/17 بشأن تعزيز التعاون و الكشف عن الأدلة الالكترونية.

المعلوماتية، فمسألة وضع تعريف لهذه الجريمة تم تناولها من طرف الفقهاء وبعض التشريعات والهيئات من عدة زوايا سواء من الجانب الفقهي، أو من الجانب التقني أو من الجانب التشريعي وهذا ما سنتناوله من خلال عرض بعض الـــتعاريف:

أ-التعريف الفقهي:

حسب الفقيه الألماني تاديمان: "هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستعمال الحاسب الآلي ".[1]

ب-التعريف التقني:

حسب مكتب تقييم التقنية في الولايات المتحدة الامريكية: "هي الجرائم التي تلعب فيها بيانات الكمبيوتر و البرامج المعلوماتية دورا رئيسيا".[2]

-التعريف حسب منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة (OCDE)

"كل سلوك غير مشروع أو مناف للأخلاق أو غير مرخص به يرتبط بالمعالجة الآلية للبيانات أو نقلها".[3]

-التعريف حسب منظمة الأمم المتحدة المؤتمر العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد بفيينا سنة 2000

"كل سلوك غير مشروع يتم عن طريق عمليات الكترونية والتي تستهدف أمن الأنظمة المعلوماتية والمعطيات التي تقوم بمعالجتها".[4]

ج-التعريف القانوني حسب المشرع الجزائري:

أدرج المشرع الجزائري الجريمة المعلوماتيـــة لأول مرة بموجـب قانون العقوبـات رقم 15-04 المعدل في 2004، استنادا إلى الالتزامات الدولية للجزائر من بينها الإعلان العالمي

---

[1]- إسماعيل جابو ربي، دور الأمن السيبراني في مواجهة التهديدات الالكترونية دراسة حالة الجزائر، مجلة تحولات جامعة ورقلة، المجلد الثالث: العدد الثاني ديسمبر 2020، ص 68.

[2]- نفس المرجع السابق، ص 67.

[3]- Myriam QUÉMÉNER, Yves CHARPENEL : Cybercriminalité, droit pénal appliqué, Edition ECONIMICA, 2010,8P.

[4]- نفس المرجع السابق.

لحقوق الانسان والعهدين الدوليين اتفاقية الأمم المتحدة الخاصة بالجريمة المنظمة العابرة للحدود الوطنية لتاريخ 2000/11/15، المصادق عليها بموجب المرسوم الرئاسي رقم 55/02، المؤرخ في 2002/02/05. ثم التعديل الذي شمل قانون العقوبات في 2006 أين قام المشرع بتشديد العقوبات إلا أن الملاحظ أن المشرع الجزائري لم يضع أي تعريف لهذه الجريمة وإنما جرّم إحدى صورها بموجب القسم السابع مكرر تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات ثم تدارك المشرع الجزائري الأمر سنة 2009، بموجب القانون رقم 09 -04 واستعمل مصطلح: الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها ضمن أحكام المادة الثانية على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية". ومن خلال أحكام هذا القانون حرص المشرع الجزائري على الموازنة بين الحق في الخصوصية وبين تنظيم القواعد الإجرائية للوقاية من الجرائم المعلوماتية ومواجهتها.[1]

وبموجب الأمر رقم 11/21 المتضمن تعديل قانون الإجراءات الجزائية واستحداث القطب الجزائي الوطني المتخصص في هده الجرائم،[2] عرّف المشرع الجزائري بموجب المادة 211 مكرر 22 الفقرة الثالثة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال على أنها: "أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال".

1- خصائص الجريمة المعلوماتية:

نظرا للطابع الخاص لجرائم المعلوماتية فإنها تمتاز بخصائص متنوعة مما جعلها تختلف عن الجرائم التقليدية المادية، وعليه سنعرض أهم هذه الخصائص والمتمثلة فيما يلي:

---

[1]- تجدر الإشارة إلى أن اغلب قواعد القانون رقم 09 -04 مستوحاة من أحكام اتفاقية بودابست لمكافحة الجرائم الالكترونية، لسنة 2001.

[2]- القانون رقم 21-11 المؤرخ في 2021/08/25 المتمم للامر رقم 66-155 المتضمن قانون الاجراءات الجزائية و الذي بموجبه قام المشرع الجزائري باستحداث القطب الجزائي الوطني المتخصص لمكافحة الجرائم المتصلة بتكنولوجياتالإعلام و الاتصال، المادة 211 مكرر 22 و ما بعدها.

أ- الجريمة المعلوماتية جريمة مستحدثة وعدم وجود تعريف مشترك لها:

تعتبر من أبرز أنواع الجرائم الجديدة التي أفرزتها ثورة التكنولوجيا كما أنه لا يوجد أي مفهوم أو تعريف أو مصطلح قانوني موحد للدلالة على هذا النوع من الجرائم، إذ اختلفت التسميات بشأنها كما سبق ذكره أعلاه وهذا راجع أساسا إلى تطور هذه الجريمة تزامنا مع التطور التكنولوجي.

الملاحظ هو وجود اختلاف في التسميات التي أطلقت على الجريمة الالكترونية نظرا لتطور هذا النوع من الإجرام المتصل بتقنية المعلوماتية إلا أن معظم المصطلحات المستعملة تحمل نفس الدلالة فمنهم من يطلق عليها مصطلح:

-الجرائم المعلوماتية،

-الجرائم الالكترونية، الجرائم السبيرانية، جرائم الكمبيوتر أو جرائم الحاسوب –جرائم الانترنيت،

-جرائم الفضاء السبيراني La criminalité dans le cyber espace

-الإجرام السبيراني Cybercriminalité - cyber crime

-جرائم التقنية العالية او جرائم التكنولوجيا المتقدمة Les crimes de la haute technologie

-جرائم الهاكرز HACKERS CRIMES

-الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

Infractions liées aux technologies d'information et communication.

ب – صعوبة الكشف عن الجريمة المعلوماتية وإثباتها:

تكمن صعوبة إثبات هذا النوع من الجرائم لأنها لا تترك أي آثار مادية ظاهرة وكذلك لسهولة محو الدليل الإلكتروني كما أنه من الصعب اكتشافها لكونها ترتكب في بيئة رقمية افتراضية وهي مسرح الجريمة، كما تمتاز بسرعة تنفيذها وبدون أي عنف أو إكراه.

ج- غالبا هي جريمة عابرة للحدود الوطنية:

أي أنها ذات طابع دولي وهذه الخاصية ناجمة من أن المجتمع المعلوماتي société de l'informations لا يعترف بالحدود الجغرافية أو المكانية أو الزمانية مما طرح مشكلة الاختصاص القضائي وهنا ظهرت الحاجة لضرورة صياغة تشريع قانوني دولي ومكافحة هذا النوع من الجرائم.

د- جريمة تتطلب خبرة فنية وتحكّم في تكنولوجيا المعلوماتية أثناء التحقيق والمتابعة:

نظرا للطبيعة التقنية للجريمة المعلوماتية لابد، أن يكون المحققين أو عناصر الضبطية القضائية متخصصين في هذا النوع من الجرائم والتعامل باحترافية ومهارة أثناء مرحلة البحث والتحري، كما تتطلب المتابعة المستمرة للتطورات التكنولوجية ومعرفة الوسائل التقنية والإجرائية لمواجهة الجرائم المعلوماتية، وكذلك ضرورة التدريب المستمر وتبادل الخبرات بين المتخصصين في هذا المجال سواء على المستوى الدولي أو الوطني وكذا تفعيل دور التعاون الدولي لاكتساب المهارات والخبرات من الدول المتقدمة. كما تساعد الخبرة العلمية والتقنية في الكشف عن الدليل الالكتروني وتحديد خصائصه كالمستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور، ...الخ .

هـ- جريمة تتسم بخطورة بالغة من شأنها المساس بالاقتصاد الوطني والدولي وتسبب في خسائر مالية كبيرة:

فحسب دراسة حديثة أصدرها مركز الدراسات الاستيراتجية والدولية CSIS تم التوصل إلى أن الجرائم الالكترونية تكلف الاقتصاد العالمي نحو 445 مليار دولار سنويا.[1]

4-تصنيفات الجريمة المعلوماتية حسب اتفاقية بودابست لسنة 2001:

صنفت الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية (بودابست 2001) الجرائم المعلوماتية إلى عدة أصناف تتمثل في:

[1]- مقال منشور في الموقع الرسمي لمركز الدراسات الاستيراتجية والدولية CSIS بعنوان: "الجرائم الالكترونية تكبد الاقتصاد العالمي خسائر باهضة"، https://www.csis.org.

-الصنف الأول/ الجرائم الماسة بخصوصية وسلامة الانظمة والبيانات: وتشمل جرائم النفاذ غير المشروع، جرائم الاعتراض والالتقاط غير المشروع، التدخل في البيانات، التدخل في الشبكات والأنظمة المعلوماتية، إساءة استخدام الأجهزة.

-الصنف الثاني/ الجرائم المتصلة بالكمبيوتر: وتشمل التزوير والاحتيال بواسطة الحاسوب.

-الصنف الثالث/ الجرائم المتصلة بالمحتوى: وتشمل إنتاج، توزيع، حيازة مواد إباحية يستخدم فيها الأطفال.

-الصنف الرابع/ الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف، والحقوق المجاورة.

- الجرائم الماسة بخصوصية وسلامة وتوفير بيانات ونظم الكمبيوتر:

وتشمل جرائم النفاذ غير المشروع: جرائم الاعتراض والالتقاط غير المشروع، التدخل في البيانات، التدخل في الشبكات والأنظمة المعلوماتية، إساءة استخدام الأجهزة.

"تصنيف الجرائم المعلوماتية حسب الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية (بودابست BUDAPEST (2001"

5-أطراف الجريمة المعلوماتية:

أ- المجرم المعلوماتي: إن التطور التكنولوجي أفرز صنفا جديدا من المجرمين وهم المجرمون المعلوماتيون cyber criminels، يتمتعون بقدرات عالية من الذكاء والتحكم في الوسائل

والاتصالات الالكترونية ويحرص المجرم المعلوماتي على إخفاء هويته باستمرار من خلال استعمال أفضل التقنيات والبرامج لذا من الصعب الكشف عنه وتحديد هويته الحقيقة وينقسم المجرمون المعلوماتيون إلى عدة أصناف من بينهم: القراصنة، الهاكرز، الهواة، المتطفلون، الكراكرCRACKERS.....الخ

ب- الضحية: قد يكون ضحية الإجرام المعلوماتي أشخاصا طبيعية أو معنوية إذ أن المجرم المعلوماتي يقوم مباشرة بقرصنة الحواسيب أو الهواتف أو اختراق البريد الإلكتروني أو حسابات الأفراد على منصات مواقع التواصل الاجتماعي، كما تشكل الجرائم الالكترونية التي تستهدف الأشخاص المعنوية خطرا كبير سواء في القطاع العام أو القطاع الخاص كالشركات التجارية والبنوك، الوزارات، المستشفيات....إلخ.

وتزداد الخطورة إذا أدى للمساس بقطاعات حساسة في الدولة والمتعلقة بالدفاع والأمن الوطني و الوزارات لكونها فيها مساسا بالسيادة الوطنية.

ج- الشاهد المعلوماتي:

تختلف الشهادة في الجريمة المعلوماتية عن تلك المعتاد الأخذ بها في الجريمة التقليدية، نظرا للبيئة الافتراضية التي ترتكب فيها هذا النوع من الجرائم وبالتالي فإن الشهود غالبا ما يكونوا من الأشخاص المحيطون بهذه البيئة اللامادية وهم الأشخاص الذين لهم دراية وخبرة في مجال تكنولوجيا المعلومات والاتصال ونذكر على سبيل المثال: المبرمجون، القائم على تشغيل الحاسوب، مهندسو الصيانة والاتصالات مزودو خدمات الأنترنت والاستضافة، وللإشارة فقد ألزم المشرع الجزائري بموجب المادة 10 الفقرة الأولى من القانون 04/09 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية وإمدادهم بكل المعلومات المتعلقة بمحتوى الاتصالات.

6- الإطار القانوني للجريمة المعلوماتية في التشريع الجزائري:

أ- الدستور: (لاسيما المواد 41، 43، 47، 50،51، 52، 54، 55، المتعلقة أساسا بحماية الحريات الفردية، حماية الحياة الخاصة، الحق في سرية المراسلات والاتصالات الخاصة حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي).[1]

ب- الاتفاقيات الدولية و الاقليمية:

-الإعلان العالمي لحقوق الإنسان 1948،

- العهد الدولي الخاص بالحقوق المدنية و السياسية 1966،

- العهد الدولي الخاص بالحقوق الاقتصادية و الاجتماعية و الثقافية 1966،

- اتفاقية الأمم المتحدة الخاصة بالجريمة المنظمة العابرة للحدود الوطنية المؤرخة في 2000/11/15، المصادق عليها بموجب المرسوم الرئاسي رقم 55/02، المؤرخ في 2002/02/05.

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، المصادق عليها بموجب المرسوم الرئاسي رقم 252/14، المؤرخ في 08 سبتمبر 2014.

- مرسوم رئاسي رقم16-111 يتضمن التصديق على اتفاقية إنشاء المنظمة العربية لتكنولوجيات الاتصال والمعلومات المحررة بالقاهرة في 2002/02/13.

- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات والذي اعتمدته جامعة الدول العربية.

ج- الــقوانين:

✓ **تعديل قانون العقوبات** بموجب كل من:

❖ القانون رقم 01-09، المؤرخ في 26 جوان 2001.

[1]- لقد تم تكريس هذه المبادئ الدستورية ضمن كافة الدساتير الجزائرية لاسيما دستور سنة 2020 المؤرخ في 2020/12/30.

❖ القانون رقم 04-15، المؤرخ في10 نوفمبر2004. إضافة القسم السابع مكرر يتضمن مواد جديدة تعاقب على المساس بأنظمة المعالجة الآلية للبيانات.

❖ القانون رقم 14-01، المؤرخ في 14 فيفري 2014، المعدل والمتمم لقانون العقوبات.

❖ القانون رقم 16-02، المؤرخ في 10 يونيو 2016، المتمم لقانون العقوبات.

❖ قانون رقم 20-06 مؤرخ في 28 أبريل 2020، يعدل ويتمم الأمر رقم 66-156 والمتضمن قانون العقوبات، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، أين تم إضافة مواد جديدة تعاقب على نشر وترويج أخبار أو أنباء تمس بالنظام والأمن العمومين لاسيما عبر وسائل الاتصال الحديثة.

✓ **القواعد الإجرائية المقررة لمكافحة الجرائم الإلكترونية:**

❖ القانون رقم 04-14، المؤرخ في 10 نوفمبر 2004، المعدل لقانون الإجراءات الجزائية.

❖ القانون رقم 06-22، المؤرخ في 2006/11/20 المعدل لقانون الإجراءات الجزائية: يهدف إلى وضع قواعد إجرائية أكثر تكيفًا مع بعض أنواع معينة من الجرائم الجديدة أو الأكثر انتشارًا، بما في ذلك الهجمات على أنظمة المعالجة الآلية للبيانات، ومن بين المستجدات التي تم إدراجها: اعتراض المراسلات، تسجيل الصوت وأخذ الصورة.

❖ القانون رقم 06-01، المؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته.

❖ القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: هذا القانون يعكس السياسة الجديدة للجزائر في مكافحة الجريمة المتعلقة بتكنولوجيا الإعلام والاتصال ويتضمن تدابير إجرائية أهمها:

-تعزيز صلاحيات أجهزة التحقيق.

-إشراك المتعاملين التقنيين «شركات الاتصالات و مقدمو خدمة الأنترنت».

-تعزيز المساعدة القانونية والتعاون الدولي.

✓ **القوانين الخاصة ذات الصلة:**

❖ القانون رقم 08-01، المؤرخ في 23 جانفي 2008، يتمم القانون رقم 83-11 المؤرخ في 2 جويلية1983،المتعلق بالتأمينات الاجتماعية، تم بموجبه تحديد الجرائم الواقعة على البطاقة الالكترونية الشفاء .

❖ القانون العضوي رقم 12-05، المؤرخ في 12 جانفي 2012، المتعلق بالإعلام.

❖ القانون رقم 15-12، المؤرخ في 15 جويلية 2015، يتعلق بحماية الطفل.

❖ القانون رقم 15-13، المؤرخ في 15 جويلية 2015، يتعلق بأنشطة وسوق الكتاب.

❖ الأمر رقم 05-03، المؤرخ في 19 جويلية 2005، المتعلق بحقوق المؤلف والحقوق المجاورة.

❖ القانون رقم 16-03 المؤرخ في 19 جوان 2016 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية.

❖ القانون رقم 04-08، المؤرخ في 14 أوت 2004، المتعلق بشروط ممارسة الأنشطة التجارية، المعدل والمتمم.

❖ القانون رقم 18-04، المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.

❖ القانون رقم 18-05، المؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية.

❖ القانون رقم 18-07، المؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

❖ القانون رقم 09-03، المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش.

✓**بعض النصوص التنظيمية ذات الصلة:**

❖ المرسوم التنفيذي رقم 06-348، المؤرخ في 05 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

❖ المرسوم التنفيذي رقم 09-410، المؤرخ في 10 ديسمبر 2009، المحدد لقواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة.

❖ القانون رقم 15-04 الذي يضع القواعد العامة للتوقيع والتصديق الإلكترونيين.

❖ المرسوم التنفيذي رقم 16-134، المؤرخ في 25 أفريل 2016، الذي يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها.

7- الإطار المؤسساتي لمكافحة الجريمة المعلوماتية:

1-الهيئات الوطنية المتخصصة:

أ-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/07.يتضمن إعادة تنظيم هذه الهيئة .

ب-استحداث القطب الجزائي الوطني المتخصص لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال و مكافحتها:

بموجب الأمر رقم 21-11 المؤرخ في 26 اوت 2021 المتضمن تعديل قانون الإجراءات الجزائية وطبقا للمادة 211 مكرر 22 يختص هذا القطب بالمتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والجرائم المرتبطة بها و يمارس وكيل الجمهورية وقاضي التحقيق ورئيس القطب صلاحياتهم عبر كامل الإقليم الوطني كما حددت المادة 211 مكرر 24 الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال وهي: الجرائم الماسة بأمن الدولة أو الدفاع الوطني، جرائم نشر وترويج أخبار كاذبة ماسة بالأمن العام، جرائم نشر وترويج أخبار مغرضة ماسة بالنظام والأمن العموميين ذات الطابع المنظم والدولي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية، جرائم

الاتجار بالأشخاص أو الأعضاء البشرية أو تهريب المهاجرين، جرائم التمييز وخطاب الكراهية.

ج- استحداث القطب الجزائي المالي و الاقتصادي:

إذ تشير المادة 211 مكرر 11 الفقرة الثانية على أنه يؤول الاختصاص للقطب الاقتصادي والمالي في حالة الاختصاص المتزامن للقطب الجزائي الاقتصادي والمالي مع القطب الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ويؤول الاختصاص وجوبا لوكيل الجمهورية التابع للقطب الجزائي الاقتصادي والمالي لدى محكمة سيدي امحمد بالجزائر العاصمة.

د- المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني:

أنشأ بموجب المرسوم الرئاسي رقم 183/04 المؤرخ في 2004/06/26، ويعتبر مكسب مؤسساتي كبير للجزائر بفضل التقنيات الحديثة والمتطورة المستخدمة في مجال التحقيقات ومكافحة الجريمة وتبنيه نظام إدارة الجودة مما مكنه من الحصول على شهادة اعتماد على الصعيدين الوطني و الدولي، ومن بين المهام المسندة للمعهد:

-إنجاز الخبرات والتحاليل بناء على طلبات القضاة، المحققين والسلطات المؤهلة.

-الدعم التقني للوحدات أثناء التحقيقات المعقدة.

-تصميم بنوك معطيات وإنجازها وفقا للقانون.

-المشاركة في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.

- المساهمة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.

-المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة.

-العمل على ترقية البحث التطبيقي وأساليب التحريات الفعالة في ميدان علم الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.

- المشاركة في تنظيم دورات تحسين المستوى والتكوين.

كما يلعب المعهد الوطني للأدلة الجنائية وعلم الإجرام دورا فعالا في مجال مكافحة الجرائم السبيرانية إذ تكلف دائرة الإعلام الآلي والإلكتروني:

-بمعالجة و تحليل وتقديم كل دليل الكتروني لفائدة أجهزة العدالة.

- تقديم مساعدة تقنية للمحققين في التحقيقات المعقدة.

-السهر على تأمين اليقظة التكنولوجية من أجل تحيين المعارف والتقنيات والطرق المستعملة في الخبرات العلمية.[1]

وتنقسم دائرة الإعلام الآلي والإلكتروني إلى (03) مخابر وكل مخبر مزود بفصيلة تسند لها مهمة اقتناء المعطيات من دعامات المعلومات وضمان نزاهة وشرعية الدليل الالكتروني

وتتمثل هذه المخابر الثلاثة فيما يلي:

- مخبر الإعلام الآلي،
- مخبر الفيديو،
- مخبر الصوت لتحديد شرعية التسجيلات الصوتية مثلا .[2]

هـ- المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التابعة للمديرية العامة للأمن الوطني: التي تتمثل مهامها في:

- ✓ مساعدة مصالح الشرطة القضائية في مجال التحريات التقنية.
- ✓ المشاركة في تأمين و حماية الأنظمة المعلوماتية و الفضاء السيبيراني الوطني.
- ✓ التعاون و المشاركة في التحقيقات و التحريات ذات البعد الوطني و الدولي .

---

[1]- أنظر الموقع الرسمي لوزارة الدفاع الوطني .www.mdn.dz

[2]- أومدور نجاة، خصوصية التحقيق في مواجهة الجرائم المعلوماتية ، رسالة دكتوراه في القانون الخاص، كلية الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريرج، 2021،ص، 101.

✓ المساهمة في تكوين المتخصص لعناصر الشرطة المتواجدة على مستوى فرق مكافحة الجريمة المعلوماتية بأمن الولايات.

✓ المشاركة في أعمال الوقاية والتوعية.

✓تقنيات اليقظة الالكترونية

✓إنشاء فرق ولائية لمكافحة الجرائم المعلوماتية على المستوى الوطني تتمثل مهامها في:

- استقبال شكاوي المواطنين و إجراء التحقيقات الجنائية بالتنسيق مع الجهات القضائية
- المشاركة في البحث و التحري في الجرائم المعلوماتية.
- المشاركة في حملات التوعية و التحسيس.
- متابعة شبكة الأنترنت لرصد أي محتوى مجرم.
- تحليل الوضع السياسي، الاقتصادي و الاجتماعي المتداول في مواقع التواصل الاجتماعي من أجل العمل على وضع استراتيجية وقائية للحفاظ على النظام و الامن العمومين.

✓ إنشاء أقسام مختصة في تحليل الأدلة الرقمية على مستوى المخابر الثلاثة المتواجدة بكل من العاصمة، وهران و قسنطينة، تكمن مهامها في:

- وضع بروتوكولات العمل المتعلقة باستخلاص الأدلة الرقمية.
- تقديم الدعم التقني في ميدان مكافحة الجريمة المعلوماتية.
- إجراء الأعمال التقنية الجنائية بناء على طلبات ضباط الشرطة القضائية.
- إنجاز خبرات لفائدة الأجهزة القضائية في ميدان الأدلة الرقمية.

و-السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: تحت وصاية رئاسة الجمهورية أنشأت بموجب القانون رقم 18-07، مؤرخ في 10 ماي 2018، المتعلق بحماية الأشخاص

الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهي سلطة ادارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والاداري تحدث لدى رئيس الجمهورية، أسند لها المشرع الجزائري عدة مهام تصب في إطار حماية حق الشخص الطبيعي في حرمة حياته الخاصة، مما جعلها آلية مهمة لحماية معالجة المعطيات ذات الطابع الشخصي في إطار احترام الحياة الخاصة للأشخاص.

ي- المنظومة الوطنية لأمن الانظمة المعلوماتية التابعة لوزارة الدفاع الوطني: ينظمها المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 الذي يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، تم بمقتضى هذا المرسوم استحداث هيئة عليا مركزية تحت رئاسة وزارة الدفاع الوطني.

م- الوكالة الوطنية لتطوير الرقمنة: هي وكالة تابعة للوزارة الأولى، أنشأت بموجب المرسوم الرئاسي رقم 19-317 المؤرخ في 2019/11/26.

2- الهيئات والمنظمات الدولية المتخصصة:

- منظمتي الأنتربول و الأفريبول ودورهما الفعال في مواجهة الجريمة المعلوماتية،
- المنظمة العربية لتكنولوجيات الاتصال والمعلومات تم تأسيسها من طرف جامعة الدول العربية بتاريخ 2001/09/10 ودورها في التصدي لهذا النوع من الإجرام، وتعتبر الجزائر من ضمن الدول الأعضاء.
- هيئة الأمم المتحدة لاسيما الاتحاد الدولي للاتصالات وهي وكالة متخصصة في التكنولوجيات والاتصالات، و تعتبر الجزائر عضوا فيها.
- المنظمة العالمية للملكية الفكرية.

المحور الأول / التكييف القانوني للجرائم المعلوماتية

إن مسالة التكييف القانوني تتمثل في إعطاء الوصف القانوني الصحيح للوقائع بما يتطابق مع النص القانوني المناسب، إلا أن الأمر أكثر تعقيدا فيما يتعلق بالتكييف

القانوني للجرائم المعلوماتية نظرا لخصائصها إذ يتطلب الأمر إسقاط وقائع مادية في عالم افتراضي أي في بيئة رقمية و هي مسرح الجريمة. ومن هذا المنطلق يتعين التطرق لأركان الجريمة المعلوماتية (أولا)، والأحكام الخاصة المتعلقة بإحدى صورها وهي جرائم المساس بنظام المعالجة الآلية للمعطيات (ثانيا).

1- أركان الجريمة المعلوماتية:

أ-الركن المادي: الركن المادي في الجرائم المعلوماتية يتطلب وجود بيئة رقمية وهي مسرح الجريمة ويتطلب كذلك معرفة بداية النشاط والشروع فيه وبالتالي يتحقق هذا الركن بتوفر السلوك الإجرامي، والنتيجة والعلاقة السببية بينهما.

ب-الركن المعنوي: اشترط المشرع الجزائري لقيام بعض الجرائم قصدا عاما فقط وفي بعض الحالات اشترط وجوب توافر القصد الخاص ونذكر على سبيل المثال المادة 394 مكرر 2 كل من يقوم عمدا وعن طريق الغش.

وللإشارة قد ترتكب الجريمة المعلوماتية في إطار جماعة إجرامية منظمة لاسيما تلك التي تنطوي على دوافع مالية لغرض الربح مثلا إذ تتطلب درجة عالية من التنظيم وهي الصورة الغالبة في الوضع الحالي حسب الإحصائيات الحديثة.

2-الأحكام الخاصة المتعلقة بجرائم المساس بنظام المعالجة الآلية للمعطيات:

لقد خصص المشرع الجزائري منذ تعديل قانون العقوبات سنة 2004 ثم التعديل اللاحق في سنة 2006 القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات والذي يندرج ضمن الباب الثاني: الجنايات والجنح ضد الأفراد، الفصل الثالث الجنايات والجنح ضد الأموال (المواد من 394 مكرر إلى 394 مكرر 7 قانون العقوبات).

وتجدر الإشارة إلى أن المشرع الجزائري من خلال أحكام هذه المواد لم يضع أي تعريف لمصطلح نظام المعالجة الآلية للمعطيات،[1] إلا أنه تدارك الأمر من خلال القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقام بإدراج تعريف لهذا المصطلح ضمن أحكام المادة الثانية فقرة ب كما يلي: "المنظومة المعلوماتية هو نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

ومن خلال أحكام مواد قانون العقوبات فقد حددت المادة 394 مكرر صور المساس بأنظمة المعالجة الآلية للمعطيات وتشمل ما يلي:

- الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية المعطيات أو محاولة ذلك.

- حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تحريف نظام اشتغال المنظومة.

أما المادة 394 مكرر 1 أشارت إلى:

- إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنه.

أما المادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات كما يلي:

- 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.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

---

[1]- الدكتور مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، طبعة 2018، ص 125.

وشدد المشرع الجزائري العقوبة إذا استهدفت الجريمة مصالح الدفاع الوطني أو الهيئات و المؤسسات العمومية، كما طبق المشرع أحكام قانونية تتعلق بالشخص المعنوي في حالة إذا ارتكب إحدى هذه الجرائم.

وفي نفس السياق أكدت محكمة النقض الفرنسية بموجب القرار الصادر بتاريخ 2021/06/08 تحت رقم 00699 على أنه تعتبر التعديلات أو حذف المعطيات الواردة في نظام معالجة آلية احتيالية بالضرورة بالمفهوم الوارد ضمن احكام المادة 323-3 من قانون العقوبات عندما تم إخفاؤها عن قصد عن مستخدم آخر على الأقل لهذا النظام حتى ولم تكن لديه حقوق التعديل، وبرر قضاة الاستئناف قرارهم لما أدانوا المتهم لارتكابه جريمة المساس بنظام المعالجة الآلية للمعطيات، وأنه قام بحذف أصل الحكم في نسخته الرقمية والبيانات الهامشية مع علمه التام بالأفعال المنسوبة إليه دون علم المستخدم الآخر لهذا النظام. وللتوضيح أكثر للقرار تتلخص وقائع القضية أنه تمت إدانة المتهم وهو أمين ضبط بجنحة الحذف عن طريق الغش لمعطيات داخل نظام معالجة آلية للمعطيات بعد إعادة تكييف الوقائع، وذلك على إثر اكتشاف اختفاء أصل حكم قضائي على مستوى أمانة ضبط المحكمة التجارية وحذف النسخة الرقمية للحكم على مستوى النظام المعلوماتي لتسيير الملفات القضائية، وبعد إجراء التحقيق تم اكتشاف قيام أمين الضبط بارتكاب جنحة حذف معطيات ومضمون الحكم القضائي بالدخول عن طريق الغش لنظام المعالجة الآلية للمعطيات على مستوى المحكمة.[1]

المحور الثاني/ الإشكالات الموضوعية والإجرائية التي تثيرها الجريمة المعلوماتية

1- الإشكالات الموضوعية: يمكن حصر أهمها فيما يلي:

أ- إشكال يتعلق بالمصطلحات المستعملة، نظرا للطابع التقني والحديث للجريمة المعلوماتية فإنها تطرح إشكالا عمليا عند تطبيق النصوص القانونية يتعلق بالمصطلحات التقنية إذ تتضمن بعض النصوص القانونية المجرمة مصطلحات غامضة المفهوم مما يجعلها عائقا أمام فهم هذه النصوص، إذ لم يقم المشرع الجزائري بشرح وتعريف المصطلحات الواردة في المواد القانونية المتعلقة بتجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات لاسيما

[1]- موقع دالوز www.dalloz.fr.

أنها تعتبر مصطلحات حديثة وذات طابع تقني، مما يؤدي إلى عدم تحقيق الأمن القانوني والقضائي، وعلى سبيل المثال نذكر أحكام المادة 394 مكرر 2 إذ وردت بعض العبارات غامضة في تبيان السلوك المادي للجريمة والمتمثلة في عبارة: بحث، تصميم، توفير، تجميع، مما يثير صعوبة في تصور الجريمة وتحديد الفعل المجرم.

ب- استبدال مصطلح "المعطيات" DONNEES الواردة لدى تعريف الجرائم المدرجة ضمن أحكام المواد من 394 الى 394 مكرر 1 ، بمصطلح "معطيات معلوماتية"، تماشيا مع أحكام القانون 04/09.

وذلك حتى نضمن معايير الصياغة القانونية للنصوص التي تتطلب الدقة، الوضوح، وتفادي التأويل من جهة، ومن جهة أخرى فإن اختلاف المصطلحات يؤدي إلى انعدام الأمن القانوني مما يشكل عائقا امام التعاون الدولي.

ج- يوجد إشكال قانوني آخر يتعلق بعدم توحيد المصطلحات المستعملة فأحيانا يستعمل المشرع الجزائري عبارة "نظام" في المادة 394 مكرر 1، ثم استعمل عبارة "منظومة" من خلال المادة 394 مكرر، ثم أدرج عبارة "حذف أو تغيير" 394 مكرر، أما في المادة 394مكرر1 استعمل عبارة "إزالة أو تعديل"، وهو اختلاف في المفردات وعليه كان من الأجدر على المشرع الجزائري شرح وتعريف هذه المصطلحات واستبدال مصطلح "نظام معالجة آلية للمعطيات" (المادة 394 وما يليها من قانون العقوبات) بالمصطلح الذي ورد ضمن أحكام القانون 04/09، "نظام معلوماتي" لكونه مصطلح أدق وأشمل وذلك حتى نضمن معايير الصياغة القانونية للنصوص التي تتطلب الدقة، الوضوح، وتفادي التأويل.

د- إشكال يتعلق بالمادة 12 من القانون 04/09 التي تجعل الالتزام بالتدخل الفوري يقع على عاتق مقدم الخدمة، ونقترح إعادة تغيير عنوان المادة 12 السالفة الذكر بجعل الالتزام بالتدخل الفوري يقع على عاتق مقدم الخدمة وإيواء الخدمة معا.

هـ- إشكال عملي يتعلق بالفراغ القانوني: عدم تجريم بعض الأفعال التي تتسم بطابع الجريمة المعلوماتية (مبدأ الشرعية).

و- إشكال قانوني يتعلق أساسا بوجود فراغ تشريعي في القانون الجزائري فالعديد من صور الإجرام الالكتروني غير مجرمة ونذكر على سبيل المثال: جريمة انتحال الهوية الرقمية إذ أن المشرع الفرنسي جرم هذه الصورة في سنة 2011 بموجب قانون LOPPSI2، ضمن أحكام المادة 2 أين تم إدراج المادة 1-4-226 في قانون العقوبات الفرنسي في إطار الاستعمال عن طريق الغش لمعطيات ذات طابع شخصي.[1]

وفي هذا الصدد يتعين الإشارة إلى مسالة هامة وهي التصيد الالكتروني أو ما يسمى بـ PHISHING وهي تقنية حديثة لسرقة بيانات الهوية الرقمية مثل بيانات بطاقة الائتمان البنكية والتي أصبحت ظاهرة خطيرة في عالم الإجرام السبيراني، إذ تشير آخر الإحصائيات لسنة 2020 الصادرة عن الإنتربول أنها بلغت نسبة 59 بالمائة خاصة مع انتشار وباء كورونا.[2]

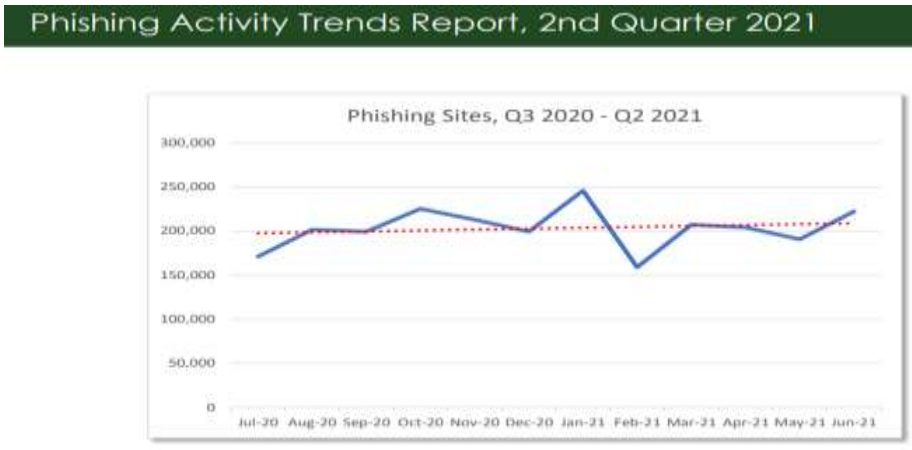
Fig. 2 - Répartition des principales cybermenaces liées aux COVID-19 d'après les réponses fournies par les pays membres

"زيادة استعمال تقنية التصيد الالكترونيPHISHINGمع انتشار وباء كوفيد 19إحصائيات 2020(الانتربول)"

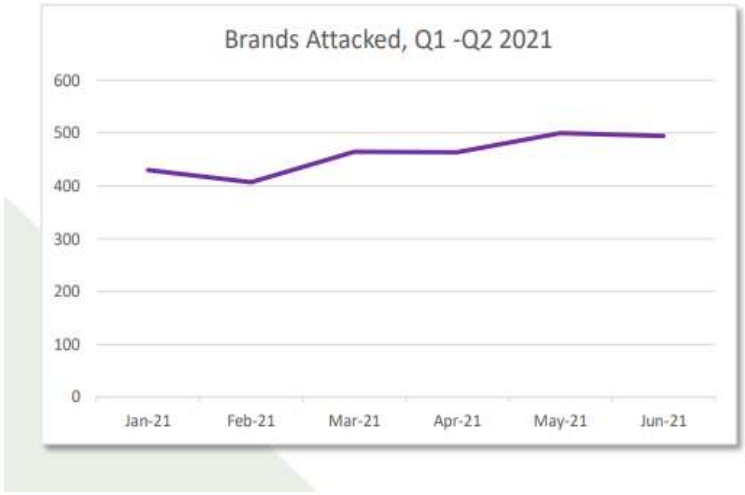
[1]-Loi n 2011-267 publié au journal officiel du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure dite LOPPSI2 . http://www.legifrance.gouv.fr/ .

[2]- انظر الموقع الرسمي للانتربول www.Intrerpol.int .

كما أكدت الإحصائيات الصادرة سنة 2021 عن مجموعة العمل لمكافحة التصيد الاحتيالي APWG زيادة في معدلات التصيد الاحتيالي .[1]



"ارتفاع نسبة استعمال تقنية التصيد الالكتروني PHISHING إحصائيات 2021"



www.apwg.org

[1]- انظر موقع مجموعة العمل لمكافحة التصيد الاحتيالي APGW: WWW.APGW.ORG

2- **الإشكالات الإجرائية**: يمكن حصر أهمها فيما يلي:

أ- إشكال يتعلق بصعوبة التعرف على مرتكب الجريمة المعلوماتية وتحديد هويته الحقيقة وأن الاعتماد على عنوان البرتوكول Internet protocole/ IP لا يؤدي حتما بجهات التحقيق إلى التوصل إلى الفاعل الحقيقي لأنه يمكن اختراق أجهزة كمبيوتر تابعة لأشخاص آخرين.

ب- إشكال يتعلق بامتناع الضحايا سواء أشخاص طبيعية أو معنوية عن التبليغ عن الجرائم المعلوماتية بسبب الحفاظ على سمعتهم الشخصية أو التجارية في حالة الشركات مثلا أو اكتشافهم للجريمة في وقت متأخر، أو عدم علمهم أصلا بأنهم وقعوا ضحايا جريمة معلوماتية.

ج- إشكال يتعلق بعدم تجاوب الضحايا أحيانا مع مصالح الضبطية القضائية المختصة في حالة إنذارهم بوجود هجوم سبيراني محتمل على النظام المعلوماتي التابع للشركة أو المؤسسة لوجود ثغرة في النظام المعلوماتي faille de sécurité إلا أن صاحب الشركة التجارية لا يتخذ أي إجراءات لتعزيز تأمين النظام المعلوماتي للشركة، مما يؤدي لوقوع الهجوم السبيراني بصفة فعلية.

د- عدم تمتع المحققين أحيانا بالخبرة الكافية أو نقص الاحترافية في التعامل مع الوسائل التقنية الحديثة مقارنة بالإجرام الإلكتروني الذي يتمتع فيه المجرمون أحيانا بمستوى عال من الاحترافية والذكاء، وهو ما يترتب عليه خرق قواعد إجراءات التعامل مع الدليل الإلكتروني أثناء التفتيش أو الضبط وبالتالي المساس بالشرعية الإجرائية مما يؤثر على مصداقية الدليل الالكتروني المستخلص.

هـ- صعوبات تتعلق بالدليل الالكتروني في حد ذاته لكونه دليل غير مادي وقد يتطلب الوصول إليه المساس ببيانات أخرى محاطة بالخصوصية المعلوماتية، بالإضافة إلى سهولة إتلاف الدليل الالكتروني أو تعديله أو نقله بعد تنفيذ الجريمة في مدة وجيزة.

و- إشكال ناجم عن التعاون الدولي يتعلق باختلاف التشريعات والنظم القانونية الإجرائية للدول مما نتج عنه عدم وجود نموذج موحد للتعامل مع النشاط الإجرامي، وكذلك يؤثر

مباشرة على إجراءات جمع الدليل الالكتروني، فمثلا الاجراء الذي يعتبر مشروعا في دولة ما قد تعتبره دولة أخرى خارج إطار الشرعية الإجرائية وهو ما يترتب عنه لاحقا عدم مشروعية الدليل الالكتروني.

وفي هذا الإطار أصدرت محكمة النقض الفرنسية قرار مهم بتاريخ 2020/11/25 تحت رقم 19.523-17الغرفة الاجتماعية، أكدت من خلاله على مسألة مشروعية الحصول على الدليل الالكتروني والتي تعتبر من أهم شروط قبول الدليل الالكتروني أمام القضاء، إذ اعتبرت محكمة النقض لأول مرة أن عنوان برتوكول الانترنيت Internet protocole/ IP والملفات اليومية تعتبر بمثابة معطيات ذات طابع شخصي وأن معالجتها تخضع وجوبا لترخيص سابق من طرف اللجنة الوطنية للمعلوماتية والحريات CNIL، وأكدت محكمة النقض على أنه يتعين على القضاة مناقشة مشروعية الدليل في إطار مبدأ تناسب الإجراء إذا فيه مساس بالحياة الخاصة للعامل.[1]

ونشير في هذا الصدد إلى أنه لا توجد معايير خاصة محددة نص عليها المشرع الجزائري فيما يتعلق بإنشاء أي تكوين أو قبول الدليل الالكتروني في قواعد الإثبات الجزائي أمام القاضي الجزائي production et admissibilité، وإنما يخضع إنشاء الدليل الالكتروني وقبوله من طرف القاضي إلى معيارين وهما:

- ✓معيار شرعية الدليل الجنائي légalité.
- ✓معيار مشروعية الدليل الجنائي loyauté (légitimité).

ي- إشكال يتعلق بالمساعدة القضائية الدولية التي تعتبر من أشكال التعاون الدولي في مجال التحقيق الجنائي في الجرائم الالكترونية ومن صورها الإنابة القضائية الدولية بين جهات التحقيق إلا أن بطء الإجراءات التي يتوجب على الدولة طالبة الإنابة القضائية أن تسلكها بعد تقديمها الطلب إلى البلد الآخر وانتظار الرد تشكل معوقات لجهات التحقيق في الجريمة الالكترونية من شأنه أن يؤدي إلى إتلاف وضياع الدليل الالكتروني، وفي هذا الإطار وبموجب اتفاقية بودابست تم إنشاء مراكز اتصال لتأمين عملية المتابعة، وجمع واعتراض

[1]- موقع دالوز www.dalloz.fr.

بيانات الحركة في الوقت الحقيقي en temps réel وتبادل المعلومات بين الدول الأطراف دون انقطاع أي على مدار الساعة 24/24 وطيلة أيام الاسبوع 7/7 وتعتبر مراكز الاتصال أساس فعالية التحقيق وتبادل المعلومات من خلال هذه الاتفاقية.

كذلك من بين التعقيدات التي أفرزتها الجريمة المعلوماتية هي تلك الصعوبات التي تواجه التعاون الدولي في مجال التحقيق ومن بينها مسألة تنازع الإختصاص القضائي على المستوى الدولي، فالسلوك الإجرامي في الجريمة الإلكترونية قد يرتكب في دولة معينة ولكن آثاره ونتيجته تتحقق في دولة أخرى، فالتحقيق يتطلب امتداد الإختصاص القضائي إلى الخارج وأن عملية جمع الأدلة الإلكترونية مثلا يتطلب الولوج إلى أنظمة معلوماتية متواجدة خارج إقليم الدولة المعينة وهو ما يتعارض مع السيادة الوطنية.[1] (وتجدر الإشارة إلى أن اتفاقية بودابست عالجت هذه المسألة من خلال المواد 31-32).

م- إشكال يتعلق بالاصطدام بالحق في الخصوصية المعلوماتية وتنعكس في الاجراءات التالية:

✓مسألة التسرب الالكتروني والتفتيش الالكتروني كإجراء فعال من إجراءات جمع الأدلة في الجريمة الالكترونية طبقا للمواد 65 مكرر 5 و 65 مكرر 11 ق ا ج.

✓الإجراء المتعلق برقابة الاتصالات الالكترونية من أجل اعتراض أشكال المراسلات التي تتم عبر وسائل الاتصال السلكية واللاسلكية وكذا عبر البريد الالكتروني، والتي قد يشكل محتواها دليلا لإثبات الجريمة الالكترونية إلا أن هذا الإجراء من شأنه أن يشكل تهديدا ومساسا بالخصوصية المعلوماتية مما يتطلب تقييد اللجوء لهذا الاجراء بشروط صارمة حفاظا على حرمة الحياة الخاصة للأفراد

[1]- أومدور نجاة، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، رسالة دكتوراه في القانون الخاص، كلية الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريرج ، 2021،ص.43.

ن- إشكال يتعلق بعدم الالتزام بحفظ المعطيات المتعلقة بحركة السير من طرف مزودي الخدمات عبر الانترنيت المحددة بمدة سنــة في التشريع الجزائري بموجب القانون 04/09 مما يعرقل حسن سير إجراءات التحريات الأولية والتحقيق القضائي.

ز- إشكال يتعلق أساسا بنقص تفعيل دور الأمن السبيراني في مواجهة التهديدات الالكترونية والهدف منه حماية الأنظمة المعلوماتية والشبكات والبرامج الحكومية من الهجمات الرقمية ويتم ذلك بوضع استيراتجية وطنية شاملة من أجل ضمان أمن المعلومات في الفضاء السبيراني.

كما أن المسألة تزداد تعقيدا في حالة لجوء بعض الإدارات العمومية وشركات كبرى في الجزائر إلى استخدام البرامج المقرصنة (الكراك)، أو استعمال أنظمة تشغيل مقرصنة (نظام التشغيل ويندواز مقرصن)، استعمال برامج مدفوعة عن طريق استخدام برامج قرصنة بها فيروسات، استعمال برامج مجانية تحتوي على برامج جوسسة، دون الأخذ بعين الاعتبار لمخاطرها الأمنية في المجال الالكتروني.

وللإشارة فإن التهديدات السبيرانية في تزايد مستمر حسب الاتحاد الدولي للاتصالات أين تم إطلاق مبادرة الرقم القياسي العالمي للأمن السيبراني في إطار البرنامج العالمي للأمن السبيراني والذي يقوم على خمسة (5) ركائز أساسية وهي:

- التدابير القانونية،
- التدابير التقنية والإجرائية،
- الهياكل التنظيمية،
- بناء القدرات،
- التعاون الدولي،

وبالتالي الهدف من هذا البرنامج هو بناء الثقة الرقمية والأمن في استعمال تكنولوجيا المعلومات والاتصالات، وحماية الفضاء السيبراني وتعزيز القدرات الفنية الوطنية في الدفاع ضد التهديدات السيبرانية.[1]

وخلال سنة 2018 صنّفت الجزائر ضمن البلدان العربية التي بدأت في تنفيذ التزامات في مجال الأمن السيبراني، بينما سجلت خمسة بلدان عربية مستويات عالية من الالتزام إزاء جميع ركائز الرقم القياسي العالمي للأمن السيبراني الخمس، بينما طورت أربعة بلدان عربية أخرى - الكويت والأردن وتونس والمغرب - التزامات معقدة وانخرطت في برامج ومبادرات للأمن السيبراني، وحصلت السعودية وعُمان وقطر على المراتب الثلاث الأولى في منطقة الدول العربية إزاء جميع ركائز الرقم القياسي العالمي للأمن السيبراني الخمس السالفة الذكر.[2]

"الاتحاد الدولي للاتصالات / خريطة التزام الأمن السيبراني الوطني"
"منطقة الدول العربية، الرقم القياسي العالمي للأمن السيبراني 2018"

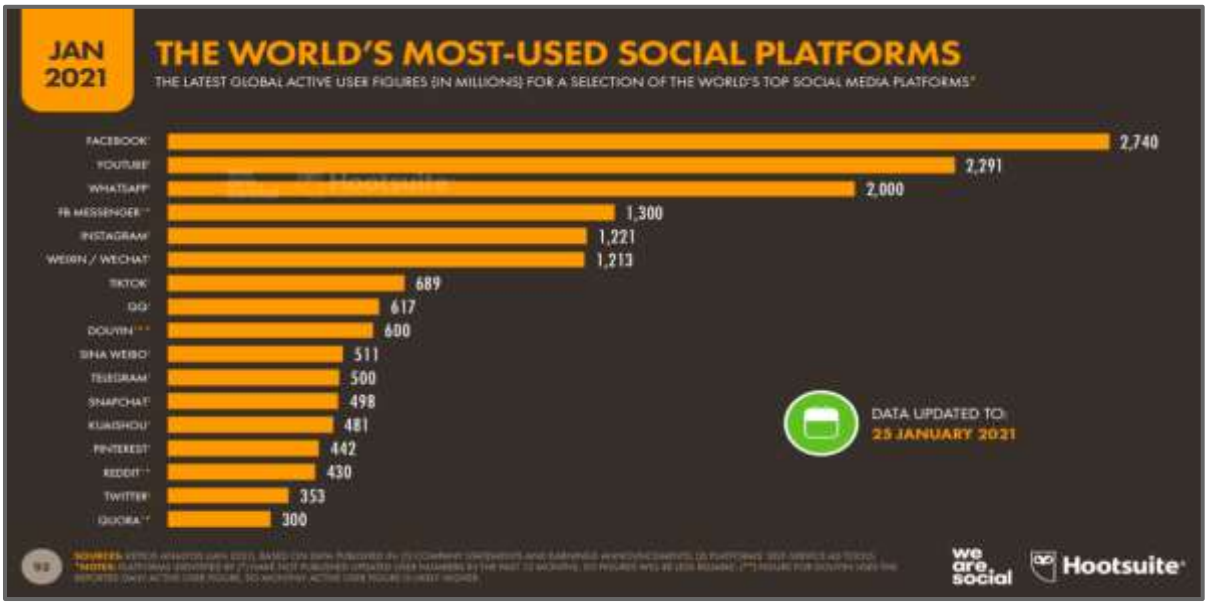
[1]- الموقع الرسمي للاتحاد الدولي للاتصالات www.itu.int.

[2]- تقرير مؤرخ في 2021/03/22، حول الاجتماع الإقليمي الافتراضي التحضيري للدول العربية للمؤتمر العالمي لتنمية الاتصالات لعام 2021المنعقد بتاريخ7-8 أفريل 2021، الاتجاهات الرقمية في الدول العربية في عام 2021 .متوفر على الموقع الرسمي للاتحاد الدولي للاتصالات www.itu.int .

وفي نفس السياق نشير إلى زيادة التهديدات الالكترونية عبر العالم باستعمال تقنيات أخرى مستحدثة في مجال الإجرام السبيراني ومن بينها:

- تقنية برامج الفدية الخبيثة / RANSOMWARE
- تقنية التصيد الالكتروني/ PHISHING
- تقنية ارسال بريد الكتروني غير مرغوب فيه /SPAMMING
- تقنية انتحال IPعنوان بروتوكول الانترنيت/ SPOOLING
- تقنية حجب الخدمة/ DENIAL OF SERVICES
- برمجة خبيثة/ MALWARE
- تقنية برامج الجوسسة/ SPYWARE
- تقنية قرصنة خادم DNS/ Pharming

كما يتعين لفت الانتباه أيضا إلى تفاقم الجرائم السبيرانية عبر مواقع التواصل الاجتماعي في سنة 2021 نظرا لزيادة المستخدمين عبر العالم، واحتل موقع الفايسبوك المرتبة الأولى ثم اليوتوب في المرتبة الثانية ثم الواتساب في المرتبة الثالثة وهو ما أدى لزيادة المخاطر السبيرانية كما هو موضح في الشكل البياني.[1]



"مواقع التواصل الاجتماعي الأكثر تداولا عبر العالم: إحصائيات جانفي 2021"

[1] www.datareportal.com.

خاتمـــة

في الـختام وعلى ضوء ما سبق تفصيله، نؤكد أن الرصيد التشريعي الجزائري الحالي غير كاف لمكافحة كل صور الجرائم المعلوماتية، بل لابد من تحيين القوانين حتى تشمل جرائم أخرى لم تشملها القوانين الحالية مثل قرصنة أسماء المواقع المجالات على شبكة الأنترنت أو انتحال الهوية الرقمية، كما أن أحكام التشريع الجزائري وآليات التعاون القضائي الدولي لازالت قاصرة على مواجهة الإجرام المعلوماتي الذي يصعب فيه إثبات الفعل المجرم أو ضبط الجاني بسبب طبيعة الدليل الالكتروني ولكون الجريمة المعلوماتية في أغلب الأحوال عابرة للحدود لارتكابها عبر شبكات الاتصال الحديثة.

لذلك أصبح من الضروري السعي لوضع اتفاقية عالمية تحت إشراف هيئة الأمم المتحدة قصد سنّ إطار دولي للإجرام الالكتروني وضمان تعزيز التعاون الدولي لتوحيد الجهود الدولية لمكافحة هذا النوع من الإجرام الخطير ولمواجهة الهجمات السبيرانية، لكون أن الجريمة المعلوماتية في أغلب الأحوال عابرة للحدود لارتكابها عبر شبكات الاتصال الحديثة، وبالتالي من الضروري مواكبة التطورات التكنولوجية واستحداث إجراءات خاصة تتناسب مع خصوصية التعامل مع البيئة الرقمية نظرا للتعقيدات والصعوبات التي تواجه السلطات المختصة أثناء استخلاص الأدلة الالكترونية والكشف عن الجناة، إلا أنه من جهة أخرى فإن استحداث هذه الإجراءات والقواعد الخاصة يجب أن يكون مراعيا لإقامة توازن بين الحق في استخدام الوسائل الحديثة للكشف عن الجريمة وجمع الأدلة فيها، وبين الحرية الشخصية للأفراد واحترام خصوصياتهم من خلال الالتزام بالضوابط القانونية الملائمة في ذلك.