المجلة الدولية للإتصال الإجتماعي
جامعة عبد الحميد بن باديس- مستغانم
ISSN: 2437 – 1181
EISSN: 2710-8139

المجلد 09 / العدد 02 (2022)، ص 219 – ص 241

تداعيات جائحة كوفيد-19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر

The repercussions of the Covid-19 pandemic and its impact on achieving cybersecurity

وفاء مطروح* [1] ، ابتسام أونيس[2]

[1] جامعة العربي التبسي تبسة (الجزائر)، ouafa.metrouh@univ-tebessa.dz

[2] جامعة العربي التبسي تبسة (الجزائر)، ibtissem.ounis@univ-tebessa

تاريخ الاستلام: 2022/04/24 تاريخ القبول: .2022/06/05 تاريخ النشر: 2022/06/30

DOI : 10.53284/2120-009-002-037

ملخص :

في الوقت الذي أصاب فيه فيروس كوفيد-19 قرابة 200 دولة حول العالم وما فرضه من عزلة اجتماعية كانت في بعض الأحيان بصفة كلية، مما اضطر الأفراد الشركات والمؤسسات في هذه الدول لتبني نمط التواصل، العمل والتعليم عن بعد بالاعتماد على تكنولوجيات الاتصال والانترنت؛ أصبح الفضاء الرقمي (السيبراني) بمثابة بديل للفضاء الواقعي، وأصبح في نفس الوقت بيئة جاذبة لكثير من قراصنة المعلومات لممارسة هوايتهم المفضلة في الاختراق وارتكاب الجرائم الالكترونية بأنواعها المختلفة.

والجزائر كغيرها من دول العالم التي تأثرت بتداعيات جائحة كورونا، من جهة، ومن جهة أخرى تعرف ارتفاعا متناميا لاستخدام تكنولوجيات الاتصال، فهي تواجه تحديات جدية لتحقيق الأمن السيبراني والحد من مخاطر الجريمة الالكترونية التي لا تعرف حدودًا، على مختلف الأصعدة (أفراد، مؤسسات، حكومة)، وهو ما ستحاول الباحثتان دراسته في هذه الورقة العلمية.

- **الكلمات المفتاحية:** الفضاء السيبراني، الأمن السيبراني، كوفيد-19.

- **Abstract** :

At a time when the Covid-19 virus has infected nearly 200 countries around the world and the social isolation it has imposed, sometimes completely, forcing individuals, companies and institutions in these countries to adopt a pattern of communication, work and distance education based on communication technologies and the Internet; the digital space has become (Cyber) serves as an alternative to the real space, and at the same time has become an attractive environment for many information hackers to practice their favorite hobby of hacking and committing various types of cybercrime.

Algeria, like other countries of the world that have been affected by the repercussions of the Corona pandemic, on the one hand, and on the other hand, knows a growing increase in the use of communication technologies, as it faces serious challenges to achieve cyber security and reduce the risks of cyber crime that knows no borders, at various levels (individuals, institutions, government), which is what the researchers will try to study in this scientific paper.

Keywords: cyber space, cyber security, Covid-19.

* المؤلف المرسل

- **مقدّمة:**

إنّ قضية أمن وحماية المعلومات تعتبر من أهم قضايا العصر، حيث بات نجاح أيّ مؤسسة يعتمد بشكل كبير على ما تمتلكه من معلومات وكيفية تأمينها، إذ أنّ العديد من المعلومات والأنظمة والبُنى التحتية المتصلة بالشّبكات عرضة للخطر بين الحين والآخر، فهي تواجه أنواعًا شتى من الخروقات والهجمات، كما تتعرّض لأنشطة إجرامية (الهاكرز) التي تعطّل خدماتها وتدمّر ممتلكاتها، ومن جانب آخر انتقلت العمليات الإجرامية التهكيرية من تهديد سلامة أمن المؤسّسات إلى سلامة أمن الأشخاص والمواطنين.

وفي ظل جائحة كورونا التي عصفت بالعالم، وما فرضته من تحديات في مواجهة الأزمات؛ فضلا عن التداعيات الاقتصادية الاجتماعية والسياسية، وما لازمها من عزل اجتماعي للأفراد عن المجتمع وعن مختلف المؤسسات التي ينتمي إليها، بل وعزل الدول عن بعضها البعض، وهو ما دفع إلى ضرورة التكيف مع الوضع والاعتماد الحصري على تكنولوجيا المعلومات والاتصال كبديل لا يمكن الاستغناء عنه للتعايش مع هذه الوضعية الوبائية، وصولا إلى المجال المعلوماتي الذي شهد في ظل هذه الجائحة تزايدا في أعداد وأشكال الهجمات الالكترونية والترويج للأفكار الهدامة، وتقويض الثقة في الحكومات بشكل يؤدي إلى زعزعة أمن واستقرار البلدان؛ ممّا أدى إلى تكاثف الدعوة حول اتخاذ المؤسسات والأفراد الإجراءات اللازمة لتفادي الوقوع في مخاطر أكثر حدّة.

- **مشكلة الدراسة :**

بينما ارتكز الاهتمام في ظل جائحة كورونا على المجالات الطبية، الاجتماعية، السياسية، الاقتصادية، والثقافية وهو ما تفرضه الطبيعة الوجودية للتهديد؛ فقد أصبحت هذه الأزمة محور السياسة الأمنية أيضًا.

فرغم ما وفّره تطور تكنولوجيا الإعلام والاتصال من تسهيل للمهام المنوطة بالمؤسّسات والحكومات في مختلف المجالات، وما أرساه من قواعد حياتية جديدة يعيشها الأفراد ويجسّدها بالفضاء الافتراضي (السيبراني)، وما ساهم به من دعم وتثمين للتخاطب والتواصل بين أفراد المجتمع الواحد، وبين الأمم والشعوب، إلّا أنّ الواقع يعكس تفاصيل أخرى؛ كان أهمّها ما خلّفه ارتفاع مستويات استخدام تكنولوجيا الاتصال والتدفق السّريع للمعلومات؛ الّذي أدّى إلى ظهور تجاوزات كبيرة وخطيرة بالفضاء السيبراني، حتّى أنّه تحوّل إلى مخابر للجرائم الالكترونية حالت دون حماية حقوق الأفراد والمؤسسات (جمال بوازدية، 2019،ص ص 1264-1265) ،وأمام ما شهده العالم خلال الثلاث سنوات الأخيرة من تفشي لوباء كوفيد-19 وكلّ ما صحب الأزمة من تحولات مسّت جميع القطاعات دون استثناء؛ ودفع الأفراد إلى عزلة اجتماعية لم يسبق لها مثيل، انعكست عواملها على كيفية ونسبة استخدام تكنولوجيا الإعلام والاتصال؛ وطرق تداول المعلومات واستعمالها، ما ساهم بطريقة أو بأخرى في تضاعف عمليات الهاكرز، وزيادة انتشار مظاهر التجسس والتهديد السيبراني، وانتقلت الاختراقات بهدف التخريب لتنال المؤسسات والأجهزة الأمنية والشركات الكبرى والبنوك في أكبر دول العالم، وبات هذا الخطر لا يعرف حدودا بسبب تنوع تطبيقاته وأساليبه ما دفع بالكثير إلى إطلاق صافرات الإنذار لإعادة بناء ترسانة الأنظمة التقنية للتمكن من تحقيق الأمن السيبراني.

والجزائر كغيرها من دول العالم، تأثرت بالتطور التكنولوجي وشهدت ارتفاعا مستمرا في استخدام تكنولوجيات الإعلام والاتصال، مما يجعلها عرضة للتهديدات السيبرانية على مختلف المستويات بسبب ضعف البنية التحتية الرقمية التي تعتمدها خاصة

مع تفشي جائحة كورونا، وهو ما يستلزم وضع استراتيجيات وقائية وردعية من أجل حماية مواطنيها ومؤسساتها على حد سواء لمكافحة الجريمة الالكترونية وحماية فضائها السيبراني وتحقيق أمنه في الوضع الراهن وعلى الدوام.

وعليه فإنّ دراستنا هذه تتمحور حول التساؤل التالي: ماهي تداعيات جائحة كوفيد-19 في ما يخص تحقيق الأمن السيبراني في الجزائر؟ وما هي الأساليب المناسبة لمكافحة الجريمة الالكترونية؟

- **أهداف الدّراسة:**

تهدف هذه الدّراسة إلى إبراز تداعيات أزمة فيروس كورونا على ظاهرة الأمن السيبراني، والذي شهد تأثرا في الطبيعة والممارسة منذ تفشي الوباء في بداية عام 2019، والوقوف على تحديد مفهوم الأمن السيبراني، مظاهره، أهميته وواقعه من خلال تقديم أرقام إحصائية عبر مختلف أرجاء العالم وفي الجزائر، بالإضافة إلى تحديد أنماط الممارسة والمخاطر التي تواجه هذا المجال الذي بات بالغ الأهمية مقارنة بأهمية وقيمة المعلومات اليوم، كما ولابد من إبراز الحاجة لمعرفة طبيعة العلاقة بين الأمن السيبراني وتداعيات تفشي فيروس كورونا، وصولا إلى رصد جهود الدولة في تحقيق الأمن السيبراني ومواجهة كافة المخاطر الرقمية والإرهاب الالكتروني الذي بات يهدد المؤسسات و الأفراد على حد سواء، كما تهدف هذه الدراسة إلى تقديم رؤية استشرافية حول الحلول الممكنة لمواجهة الخطر الالكتروني الذي يهدد الأفراد والمؤسّسات.

- **أهمية الدّراسة:**

تتمثّل أهمية الدّراسة في الموضوع نفسه:خاصّة في ظل التوجه الدّولي نحو حوكمة المعلومات؛ حيث أصبحت قضية الأمن السيبرياني أو المعلوماتي من التحديات الكبرى على الصعيدين الإقليمي والدّولي، لاسيما في ظل تزايد ظاهرة الإرهاب الالكتروني الّذي بات يهدّد المؤسّسات باختلاف أنشطتها، والأفراد باختلاف فئاتهم وجنسياتهم.

والجزائر كغيرها من الدّول سعت منذ تبنيها للإدارة الإلكترونية لحماية منظومتها المعلوماتية وقاعدتها البيانية من خلال العديد من الأجهزة والخلايا الأمنية وعبر مختلف الاستراتيجيات والوسائل اللّازمة للحدّ من تفشّي ظاهرة التهكير الّتي طالت مؤسّسات وهيئات ذات أنشطة حساسة، خاصة أثناء فترة انتشار جائحة كوفيد-19 في العالم بأسره، الّتي شهدت اعتمادًا شبه كلي على تكنولوجيات الإعلام والاتصال

كما وتكمن أهمية الدراسة في أساليب و طرق معالجة مجموع الجرائم الرقمية المرتكبة من أجل تحقيق الأمن المعلوماتي.

1- ماهية الأمن السيبرياني:

قبل عرض مفهوم الأمن السيبرياني الّذي يُعتبر خطوة هامّة وأسلوب إجرائي لمواجهة عمليات وممارسات صنفت في خانة الجرائم الالكترونية؛ لابدّ لنا من معرفة ماهية الجريمة السبريانية. والتي تعدّ من بين أهم المصطلحات المرتبطة بالعالم الإفتراضي.

1.1-الجريمة السيبريانية: تعرّف بشكل مبسط وعام بأنّها إساءة استخدام الحاسوب والانترنت، إذا أنّ تحديد معنى جرائم الانترنت أو العالم الإفتراضي ليست مهمّة سهلة، فهي بنية واسعة للعديد من الأنواع الناشئة من سوء المعاملة والجريمة الممكنة عبر تقنيات الاتصالات والمعلومات، كما وتحتضن السلوكيات الضارة التي تحدث عبر الفضاء الإلكتروني والتي تتجاوز اختصاص الجيوسياسي، وتكتيكات تحقيق إنفاذ القانون. (سمير، الأمن السيبراني في الجزائر: السياسات والمؤسسات، 2017).

كما تُعرّف أيضا على أنّها "مجموعة الأفعال والأعمال غير القانونية الّتي تتمّ عبر معدّات أو أجهزة إلكترونية عبر شبكة الانترنت وتتطلّب تحكّما خاصًّا بتقنيات الكومبيوتر ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها.

2.1 -**الأمن السيبراني:**

لغويا: الأمن السيبراني مكوّن من لفظتين" :الأمن"، و"السيبراني.

أ- الأمن: هو نقيض الخوف، أي بمعنى السّلامة. أي أنه اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِن من الشر.

ب- السيبراني: مصطلح السّيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وكلمة cyber" "لفظة يونانية الأصل مشتقة من كلمة" kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازًا للمتحكم" governor". وأشار بعض المؤرخين إلى أن أصلها يرجع إلى عالم الرياضيات الأمريكي (1894-1964) Wieners Norbertوذلك للتّعبير عن التحكم الآلي. (السمحان، 2020)

- **اصطلاحا**: الأمن السيبراني (Cybersecurity) ويطلق عليه أيضا "أمن المعلومات " و "أمن الحاسوب"، وهو فرع من فروع التكنولوجيا؛ يُعنَى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية التي تهدف عادة للوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية.

يعرّفه " إدوارد أمورسو" صاحب كتاب "الأمن السّيبرياني" الذي صدر عام 2007 بأنّه : " مجموع الوسائل التي من شأنها الحدّ من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشّبكات "، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات الرقمية ووقفها وتوفير الاتصالات المشفّرة (هارفارد بزنس ريفيو. الأمن السيبراني المفاهيم الإدارية)

كما يُعرَّف على أنّه: "مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات والتدريب وأفضل الممارسات، وضمان التقنيات التي يمكن أن يتم استخدامها لحماية البيئة الالكترونية وتنظيم أصول المستخدم". (سمير، الأمن السيبراني في الجزائر: السياسات والمؤسسات، 2017)

ومن خلال ما سبق ذكره يمكننا أن نقول أنّ الأمن السيبراني هو: مجموع الإجراءات والتدابير اللازمة لمواجهة كافة الأخطار التي تتعرض لها البيئة الإلكترونية أو العالم الافتراضي من ممارسات وهجومات تستهدف فيها مختلف المعلومات والبيانات والبرامج من أجل تحقيق أغراض غير قانونية من تهديد وابتزاز وإتلاف للمعلومات أو تغييرها، هذه المعلومات متعلقة بالمؤسسات أو بالأشخاص العاديين، و يشمل الأمن السيبراني توفير كافة الجهود التقنية والرقمية والبشرية لتحقيقه والحفاظ على مكتسباته من مختلف السلوكيات الضارة.

3.1- مصطلحات مرتبطة بالأمن السيبراني :

- **الفضاء السيبراني (Cyberspece)**:عبارة عن بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية ،مكونة من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات ، والمستخدمين سواء مشغلين أومستعملين ،ويطلق عليه" الذراع الرابعة للجيوش الحديثة".

- الردع السيبراني :(Cyer Deterrencer): يعرف بأنّه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي و بالأصول التي تدعم العمليات الفضائية .

- الهجمات السيبرانية : (Cyer attacks): أي فعل يقوض من قدرات ووظائف شبكة الكومبيوتر لغرض شخصي أو سياسي ،من خلال استغلال نقطة ضعف معينة ؛تمكن المهاجم من التلاعب بالنظام. (هارفارد بزنس ريفيو. الأمن السيبراني المفاهيم الإدارية)

- **الفرق بين الأمن السيبراني والأمن المعلوماتي :**

يعتبر مصطلحا الأمن المعلوماتي والسيبراني متشابهان جدًا، إلا إن هناك بعض الفروقات فيما بينهما، باعتبار الأمن المعلوماتي أكثر شمولًا وعمومًا من السيبراني، حيث يعتبر الأخير فرعًا أو مجالًا من مجالات علوم أمن المعلومات، كما يهتم الأمن المعلوماتي بتوفير الحماية للأنظمة والمعلومات بواسطة الوسائل والأدوات المختصة بالكشف المسبق للهجمات والتهديدات والتصدي لها، بينما يأتي الأمن السيبراني ليركز الاهتمام على تقنيات وأنظمة وإستراتيجيات الدفاع عن أنظمة الحواسيب والشبكات الذكية دون الاهتمام بالوسائل التأسيسية المستخدمة في ذلك كوسائل التشفير. (سامي عبد الله شعلان، 2020) وفي الجدول التالي حددنا أهم الفروق بين الأمن السيبراني وأمن المعلومات كالآتي:

الفروقات	الأمن السيبراني	أمن المعلومات
التعريف	✓ يعنى بحماية البيانات والتقنيات المتعلقة بها ومصادر التخزين من التهديدات ✓ يتعلق الأمن السيبراني بمجال الإنترنت والبيانات المرتبطة به	✓ يعنى بحماية المعلومات من الوصول غير المصرح به الذي قد يؤدي إما إلى تعديل البيانات أو حذفها ✓ ركز أمن المعلومات بشكل أساسي على المعلومات بحيث يضمن السرية والسلامة والتوافر.
الوسط الناقل	✓ يعنى الأمن الإلكتروني بحماية أي شيء وكل شيء موجود مرتبط بالإنترنت، وما يحتويه من البيانات أو المعلومات أوالأجهزة والتقنيات المرتبطة به ✓ ترتبط حماية ملفات وسائل التواصل الاجتماعي والمعلومات الشخصية عبر عالم الإنترنت بالأمن السيبراني	✓ يعنى بحماية المعلومات بنوعيها الرقمي والورقي. ✓ تعامل على وجه التحديد مع الأصول المعلوماتية من خلال ضمان السرية والسلامة والتوافر.
المعالجة	✓ دوّر الأمن الإلكتروني في المقام الأول الدفاع عن الفضاء الإلكتروني ومنع الهجمات الإلكترونية التي قد تحدث	✓ يعنى بحماية المعلومات من أي شكل من أشكال التهديد ويجنبها أي سيناريوهات تهدد المعلومات من نواحي السرية والسلامة والتوافر.

الحماية	✓ يتعامل الأمن الإلكتروني مع جميع المخاطر الكامنة في الفضاء الإلكتروني على سبيل المثال مع الجرائم السيبرانية والاحتيال السيبراني وتطبيق القوانين والتشريعات على الانتهاكات.	✓ حماية المعلومات من الوصول غير المصرح به الذي قد يؤدي إما إلى تعديل أو حذف هي من أهم القضايا التي تختص بجميع أشكال التهديدات على أمن المعلومات (سامي عبد الله شعلان، 2020)

4.1- فوائد و أهمية تحقيق الأمن السيبراني :

يعد الهدف الأسمى للأمن السيبراني في القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات؛ ويتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به،خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية.

كما تنبع أهمية الأمن السيبراني في ثلاث محاور رئيسية هي :

- السرية : (confidentiality): أي التحكم في الولوج إلى البيانات وإتاحتها لمن يسمح لهم فقط.
- السلامة (Integrity): الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة.
- الجاهزية (Availability): جاهزية جميع الأنظمة والخدمات والمعلومات وإتاحتها حسب طلب الشركة وعملائها.

وبذلك فإنّ في عالم اليوم المترابط بواسطة الشبكات ، أصبح يستفيد فيه الجميع من برامج الدفاع السيبراني . ونستطيع تلخيص أهمية الأمن السيبراني فيما يلي : (السمحان،2020)

- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها.
- تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها .
- حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيقِ مبادئ الأمن السيبراني.
- توفير بيئة عمل آمنة جد خلال العمل عبر الشبكة العنكبوتية.
- حماية الشبكات من الولوج غير المصرح به.
- تحسين مستوى حماية المعلومات وضمان استمرارية الأعمال.
- تعزيز ثقة المساهمين وأصحاب المصلحة في الشركة .
- استيراد البيانات المسربة في وقت أسرع في حالة حدوث خرق للنظام الأمني السيبراني. (هارفارد بزنس ريفيو. الأمن السيبراني المفاهيم الإدارية)

2-أسباب ظهور الأمن السيبراني :

برز الأمن السيبراني كقضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال، فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية والتي يعود منشأها إلى حد ما مع Arquilla و Ronfeldt's 1993 ، من خلال مفهوم حرب الإنترنت Netwar والحرب السيبرانية . cyber war وقد كان هناك تاريخ واسع من الاختبارات النظرية والأخلاقية بشأن المخاوف المتعلقة بالأمن السيبراني.

حيث إنه ومع نهاية الحرب الباردة، حدثت تحولات تدريجية، ظهرت على مستوى التفكير في الدراسات الأمنية وضمن مجال الدراسات الأمنية النقدية، يمكن فهم دور الأمن السيبراني وهو ما تجلّى في أعمال مدرسة كوبنهاغن وروادها أمثال :باري بوزان Barry Buzan وأولي ويفر Ole Waever .

ومن الأمور المتعارفة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو القوة السيبرانية (Cyber power) التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين ما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية أخرى منحت الفاعلين الأصغر قدرةً أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما يعني تغيرات في علاقات القوى في السياسة الدولية.

من هذا المنطلق أصبح الباحثون في حقل العلاقات الدولية وبقية الحقول الفرعية في الدراسات الأمنية والدراسات الاستراتيجية يركزون بشكل متزايد حول أثر التكنولوجيا على الأمن القومي والدولي، ويشمل ذلك تأثيرها على المفاهيم ذات الصلة كالقوة power والسيادة ,sovereignty الحوكمة العالمية global governance والأمننة. securitization

أما على مستوى الجانب الممارساتي للدول، فقد ارتبط ظهور الأمن السيبراني بظهور الهجمات السيبرانية والتي حدثت بسبب عاملين أساسين:

- **الأول**: باستحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً(Digital) ، رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توج بتطوير وحدة المعالجة المركزية(CPU) ، وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية.

- **الثاني**: مع ظهور الشبكة العنكبوتية-الإنترنت-، الذي أحدث انقلاباً مثيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة، وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن المنصرم، وذلك حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة Cyber Cold Warأو سباق التسلح السيبرانيCyber arms race . (فارس)

3- عناصر الأمن السيبراني: وتتمثّل أساسًا في: (التميمي، 2021)

- **التقنية**: تشكّل التكنولوجيا والتقنية دورًا في غاية الأهمية في حياة الأفراد والمنظّمات، حيث توفّر الحماية الفائقة لهم أمام الهجمات السّيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالإعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

–**الأشخاص**: يستوجب الأمر لزومًا على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ إحتياطية للبيانات.

–**الأنشطة والعمليات**: يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

كما يحدد جوزيف ناي ثلاثة أنواع من الفاعلين الّذين يمتلكون القوّة السّيبرانية:

–**الدّول**: التي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها فالدولة هي الفاعل المحوري بامتياز في هذا العام الافتراضي لما لها من مكانة على أساس التفوق التكنولوجي والمؤهلات التي ترشحها لتبني هذه المكانة.

–**الفواعل غير الدّولاتية**: ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، إلّا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثّر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطوّرة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية .وتشمل هذه الفواعل ما يلي:

–**الشّركات متعدّدة الجنسيات**: تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة الّتي ما زالت حكراً على الدول، فخوادم شركات مثل :جوجل Google وفايسبوك Facebook ومايكروسوفت Microsoft ، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

–المنظمات الإجرامية :تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الإنترنت المظلم Dark internet لتجارة المخدرات والأسلحة والبشر.

–**الجماعات الإرهابية**: تعدّ من أبرز الفواعل الدّولية، خاصّة بعد أحداث 11 سبتمبر، حيث تستغلّ الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجُدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التّحتية للدّول.

ومن أهم معايير الأمن السيبراني مايلي: (التميمي، 2021)

- إقامة علاقة تعاونية بين المجتمعات المعنية بصناعة الاتصالات والمعلومات.
- التصدي للجريمة السيبرانية وردعها ومنع وقوعها.
- ترسيخ جذور الثقافة المتعلقة بالأمن السيبراني و تحفيزها.
- العمل مليا على تطوير الاستراتيجيات ذات العلاقة وتوفير الحماية الفائقة للبنية التحتية للدولة بخصوص المعلومات الحساسة.

4- أبعاد الأمن السيبراني :

– **البعد السياسي**: تقوم على أساس حماية نظام الدولة السياسية وكياناتها، كما توجد عدة أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني ،كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات عويصة جدًّا على المستوى الداخلي والخارجي (فارس)، وقد نذكر على سبيل المثال ما حدث مع موقع ويكيليس الشّهير الّذي سرب اتفاقيات سياسية واقتصادية بين كثير من الدول كانت ذات طبيعة سرية جدا على مر سنوات.

حيث يمكن أنْ التقنيات في بثّ معلومات وبيانات قد يحدث من خلالها زعزعة استقرار أمن الدول والحكومات؛ انطلاقا من استغلال قوة مواقع التواصل الاجتماعي لتمرير رسائل وأفكار وإيديولوجيات في خدمة مصالح جماعات معينة.(حملات انتخابية ،تظاهرات افتراضية ، حركات احتجاجية ..).

– **البعد السياسي**: تقوم على أساس حماية نظام الدولة السياسية وكياناتها ،كما توجد عدة أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني ،كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات عويصة جدا على المستوى الداخلي والخارجي ، (فارس قرة ، د.س.ن) ،وقد نذكر على سبيل المثال ما حدث مع موقع ويكيليس الشهير الذي سرب اتفاقيات سياسية واقتصادية بين كثير من الدول كانت ذات طبيعة سرية جدا على مر سنوات.

حيث يمكن أنْ التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة استقرار أمن الدول والحكومات ؛انطلاقا من استغلال قوة مواقع التواصل الاجتماعي لتمرير رسائل و أفكار وإيديولوجيات في خدمة مصالح جماعات معينة.(حملات انتخابية ،تظاهرات افتراضية ، حركات احتجاجية ..). (قاسم بلشاء التميمي، 2021)

– **البعد الإقتصادي**: إن التلازم الواضح بين اقتصاد المعرفة وتوسع تقنيات المعلومات والاتصالات والتي تتيح تعزيز التنمية الاقتصادية لبلدان كثيرة. ما يربط الأمن السيبراني والاقتصاد ارتباطا وثيقا خاصة في ظل بحث كل إدارة عن تكلفة الانتاج بأفضل الشروط للحفاظ على مصالحها الاقتصادية، وهذا ما قد يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية .(منى عبد الله السمحان ، 2020،ص 15) ضف إلى ذلك دخول العالم عصر المال الإلكتروني ضمن بنية تقنية متحركة بعد إطلاق خدمة المحفظة الالكترونية® مما تزيد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي. ما لم تقم الدول بتعظيم معايير الأمن السيبراني فإنّها تبقى على الدوام في مواجهة خطر الجرائم السيبرانية المنظمة والخطيرة.

– **البعد الاجتماعي**: لقد أتاحت طبيعة الإنترنت والعالم الافتراضي عبر مختلف مواقعه ومدوناته من فتح المجال أمام الأفراد للتعبير عن أرائهم وأفكارهم المختلفة بالاضافة إلى الاطلاع على مختلف المعلومات والانفتاح على جميع الثقافات عبر العالم وهنا ما تظهر حاجة المجتمعات في الحفاظ على مقوماتها وعلى فضائها السيبراني من كل المخاطر التي قد تهدد استقراره وركائزه. وكل ما يعرض أخلاقيات المجتمعات للهدم والانهيار ومن تهديد للسلم الاجتماعي للدولة. وباقي المقومات الأخرى. وعليه فلا بد من توعية الأفراد على مخاطر الفضاء السيبراني والهجوم الإلكتروني. (فارس)

® المحفظة الإلكترونية أو الرقمية هي نظام مبني على أساس رقمي للقيام بالتبادلات والمعاملات التجارية الرقمية، وعبر استخدام هذه المحفظة، يمكن بسهولة القيام بعمليات الشراء من خلال الحواسب أو الهواتف الذكية أو أجهزة التابلت، وبشكل عام، يتم ربط حسابات الأفراد في البنوك مع محفظتهم الرقمية، والتي يتم فيها توثيق وحماية أموال المستهلك ومعاملاته التجارية من شراء وتبادل.

– **البعد العسكري**: لقد تجلت البدايات الأولى للانترنت كما هو معلوم في بيئة عسكرية بشكل مضاعف وانتقلت فيما بعد إلى الأوساط الأكاديمية والعلمية ومختلف المجالات. وكان البعد العسكري مهما من خلال قدرة الفضاء السيبراني في الربط بين الوحدات العسكرية ولتسهيل عملية تبادل المعلومات من أجل تحقيق الأهداف المرجوة (فارس قرة، د.س.ن).و تنشأ أهمية الأمن السيبراني في هذا البعد من خلال الوعي بخطورة الهجمات السيبرانية والاختراقات التي تطال أنظمة المنشآت النووية وما قد يحدث عنها من تهديدات لأمن الدول والحكومات والتي قد تقود الأحداث إلى كوارث.(أبحاث نت ،د.ن، د.س.ن /https://ab7as.net/cybersecurity).

– **البعد القانوني**: ارتبط ظهور المجتمعات المعلوماتية بظهور قوانين جديدة التي تعد البنية التنظيمية التشريعية المنظمة لحماية هذا المجتمع وحفظ حقوقه من خلال وضع أطر وتشريعات للأعمال القانونية على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه التشريعات.

5–أنواع الجرائم السيبرانية:

- **جرائم التعدي على البيانات المعلوماتية**: تشمل الجرائم التي يكون موضوعها البيانات المعلوماتية، أي التي تقع على بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية، وجرائم اعتراض بيانات معلوماتية، والبيانات هي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها.

- **جرائم التعدي على الأنظمة المعلوماتية**: تشمل جرائم الولوج غير المشرع إلى نظام معلوماتي أو المكوث فيه، مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل معلوماتي، ويتمثل النظام المعلوماتي في مجموعة البرامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

- **إساءة استعمال الأجهزة أو البرامج المعلوماتية**: تتضمن هذه الجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازا أو برنامجا معلوماتيا أو أي بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقا.

ويتضمن البرنامج المعلوماتي مجموعة من التعليمات والأوامر القابلة للتنفيذ باستخدام الحاسب الآلي ومعدة لإنجاز مهمة ما، إما البرامج المعلوماتية هي الكيان المعنوي غير المادي من برامج ومعلومات وما إليها ليكون قادرا على القيام بوظيفة.

- **الجرائم الواقعة على الأموال: أهمّها:**

✓ جرم الاحتيال أو الغش بوسيلة معلوماتية

✓ جرم التزوير المعلوماتي

✓ جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية

✓ جرم أعمال التسويق والترويج غير المرغوب فيها

✓ جرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشرع لها

✓ جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها.

- **جرائم الاستغلال الجنسي للقاصرات**: تظهرها الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، وتشمل:

✓ الرسومات أو الصور أو الكتابات أو الأفلام أو الإشارات

- ✓ أعمال إباحية يشارك فيها القاصرون.
- ✓ تتعلق باستغلال القاصرين في المواد الإباحية.
- ✓ إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.(محمد قاسم أسعد الردفاني،2014 ، صفحة 167).

- **جرائم التعدي على الملكية الفكرية للأعمال الرقمية:** تشمل جرام وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات، وجرم بيع أو عرض عمل مقلد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.
- **جرائم البطاقات المصرفية والنقود الإلكترونية:** تشمل أعمال تقليد بطاقات مصرفية بصورة غير مشروعة واستعمالها عن قصد، وتزوير إلكترونية بصورة غير مشروعة عن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي.
- **الجرائم التي تمس المعلومات الشخصية:** تتضمّن الأفعال الإجرامية الّتي تتعلق بمعالجة البيانات ذات الطّابع الشّخصي دون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.
- **جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية:**

- ✓ جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية
- ✓ جرم تهديد أشخاص أو التعدي عليهم بسبب انتهائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية
- ✓ جرم توزيع معلومات بوسيلة إلكترونية من شانها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية.
- ✓ جرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضدّ الإنسانية.

- **جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت:**

- ✓ تشمل جرم تملك وإدارة مشروع مقامرة، وجرم تسهيل وتشجيع مشروع مقامرة، وجرم ترويج الكحول للقاصرين، وجرم ترويج المواد المخدرة) .محمد قاسم أسعد الردفاني،2014 ، صفحة(168

- **الجرائم المعلوماتية ضد الدولة والسلامة العامة:** تتضمن الأفعال الإجرامية الناشئة عن المعلوماتية التي تطال الدولة وسامتها وأمنها واستقرارها ونظامها القانوني، وهي:

- ✓ جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية
- ✓ جرائم الإخفاق في الإبلاغ أو الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والاطلاع أو الحصول على معلومات سرية تخص الدولة وذلك من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية، بالإضافة إلى فعل العبث بالأدلة القضائية المعلوماتية أو إتلافها أو إخفائها، والأعمال الإرهابية التي ترتكب باستخدام شبكة الإنترنت أو أي وسيلة معلوماتية، وجرائم التحريض على القتل عبر الإنترنت أو أيه وسيلة معلوماتية.

- **جرائم تشفير المعلومات:** تشمل أفعال تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير، بالإضافة إلى أفعال تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة، وأيضاً بيع أو تسويق أو تأجير وسائل تشفير ممنوعة) .محمد قاسم أسعد الردفاني،2014 ،ص 170).

➢ **مرتكبي الجرائم السيبرانية:**

✓ الهواة : وهم من يرتكبون هذه الجرائم بغرض التسلية دون ضرر بالمجني عليه.

✓ القراصنة :وينقسم هذا الصنف إلى نوعين كالتالي:

o الهاكر : هم متطفلون على أمن النظم المعلوماتية والشبكات من خلال دخولهم إلى أنظمة الحاسبات وكسر الحواجز الأمنية وهدفهم الفضول أو إثبات الذات.

o الكراكر : وهم من يقومون بالتسلل إلى أنظمة المعالجة للإطلاع على المعلومات المخزنة لإلحاق الضرر إمّا بالسرقة أو العبث بها .

✓ -المهووسون : ويكون المجرم في حالة الجنون الذي يهدف إلى تحطيم كل الأنظمة.

✓ الجريمة المنظمة : فجهاز الحاسب أصبح أداة فعالة بأيدي عصابات المافيا.

✓ الحكومات الأجنبية : وذلك باستعمال أجهزة الحاسب في مجال الجاسوسية.

✓ المتطرفون : وهم من يستخدمون الشبكة المعلوماتية لنشر أفكارهم السياسية والدينية المتطرفة. (روان بنت عطية الله الصحفي، 2020،ص ص14-15).

➢ **معيقات تحقيق الأمن السيبراني:**

- عدم توفر إحصائيات ومعلومات حول الأفراد ضحايا الجريمة السيبرانية وذلك لعدم الإبلاغ عنها في الوقت المناسب أو عدم الإبلاغ عنها أبدا، وهذا يعود إلى عدم الوعي والمعرفة بالموضوع ومن جهة أخرى عدم وجود الثقة في الأجهزة الأمنية المختصة بل وعدم الدراية بوجود هذه الأجهزة على مستوى الدولة.

- عدم وجود مواصفات واضحة لمرتكبي الجرائم السيبرانية وضحاياهم، وبالتالي عدم إمكانية تحديد معالم الجريمة السيبرانية.

- الفضاء السيبراني؛ يشكل بيئة رقمية متغيّرة، ديناميكية ومتجدّدة مع كلّ التطورات الحاصلة في العالم الرقمي، ممّا يصعب فيها فهم ظاهرة الجرائم السيبرانية.

- الفضاء السيبراني؛ فضاء مختلف تماما عن العالم الحقيقي،حيث يبقى فيها فرد العالم الواقعي هو المؤثر الأهم والأساسي على العالم الإفتراضي. (criminalité, 6e Rapport international Prévention de la criminalité et sécurité quotidienne: prévenir la cybercriminalité, 2018)

6- الفضاء السيبراني في ظل جائحة كوفيد 19:

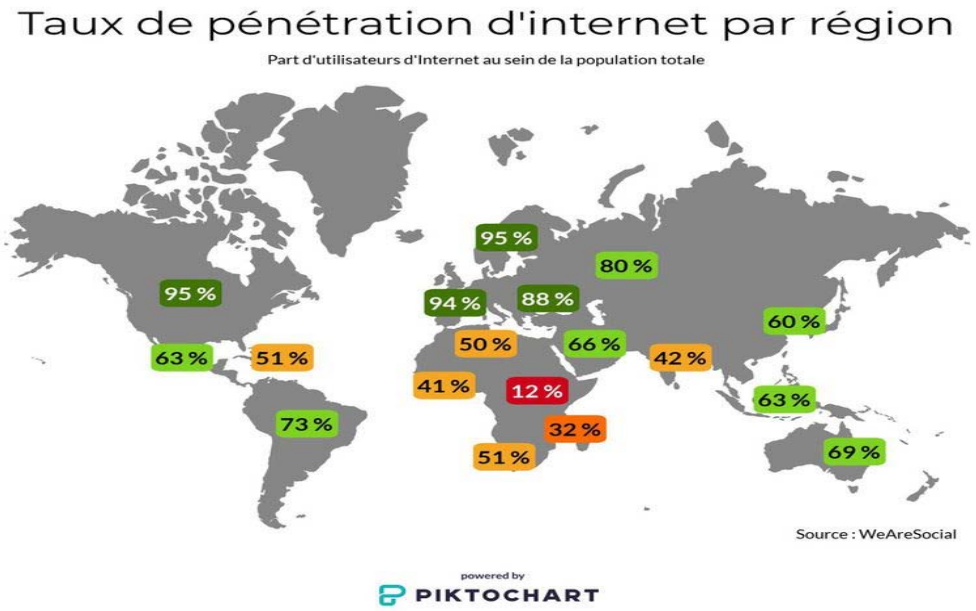
تتطلب التحوُّلات التي فرضها انتشار فيروس كوفيد-19 أن تعترف الدول بالأخطار المحدقة بالطبيعة المتعددة للأمن القومي وترابطه وتداخله مع الأمن الدولي، حيث يجب معالجة كليهما بشكل كُلّي، وألا يطرح أي حل نفسه بمعزل عن الآخر. ولا يعني ذلك أن الدول لم تكن تُدرك طبيعة الأمن القومي وما يشمله من أبعاد ترتبط ارتباطًا وثيقًا بعناصر القوة الوطنية، مثل: الأبعاد الاقتصادية والمادية والبيئية والغذائية والحدودية وغيرها، إلا أن ما أحدثه انتشار فيروس كوفيد-19 هو الكشف عن العديد من الثغرات في أنظمة الأمن والبنى التحتية الحيوية في جميع أنحاء العالم، وهشاشة الميكانيزمات المتبعة لاحتواء الأخطار المحيطة والمهدِّدة لهذه الأبعاد. في الوقت نفسه، برزت الأهمية المتزايدة لقدرة الإنترنت والأمن السيبراني، إلى جانب أهمية الذكاء

الاصطناعي. في الرفع من حدة التحديات والالتزامات الموجودة سلفًا أمام الدول لتحقيق التوازن بين مطالب أمن الدولة والصحة العامة والاقتصاد، دون تفاقم التهديدات الحالية أمام الحريات وحقوق الإنسان، كما يجب ألا تُغفَل النظم الصحية في تخطيط أو استراتيجية الأمن القومي. وبالمثل، فإن جائحة كوفيد-19 قد بدَّدت فكرة أننا لا نعيش في مجتمع عالمي (محجوب الزويري،2021، https://studies.aljazeera.net/ar/articl).

1.6- قراءة في أرقام وإحصائيات استخدام الانترنت عبر العالم في ظل جائحة كورونا:

مع تفشي جائحة كورونا والعزلة في المنازل، اجتاحت غالبية بقاع العالم ظاهرة الدراسة والعمل في البيت، حتى وصل الأمر إلى تلقى التعليم والتحصيل الدراسي عبر مختلف وسائط الانترنت وعلى كامل التطبيقات المعروفة (منصات فايسبوك، وخاصة خدمة مسنجر، وخدمات واتساب وانستغرام...إلخ)؛ نظرا لقدراتها على التحاور ونقل الصور والملفات بمختلف الأحجام. وهكذا بات كل ما يتعلق بالسوشيال ميديا ناشطاً بشكل استثنائي، حتى أنه في فترة من الفترات اشتكت الشبكة من اختناقها أمام الاستخدام المضاعف لهذه المواقع. وإصابة العديد منها بعطلات وتعثر بسبب حجم الاتصالات والملفات المرسلة عليه.

وحسب دراسة جاءت لإحصاء استخدام الانترنت لسنة 2019 فإنّه بين 7.7 مليار من سكان المعمورة، 5.1 مليار يملكون هاتفا نقالا، و 4.4 مليار منهم يستخدمون الانترنت أي 57% ، وخلال سنة واحدة ارتفع عدد مستخدمي الويب بنسبة 9.1% في حين أن نسبة ارتفاع عدد سكان الأرض لم يتجاوز نسبة 1.1%، كما أنّ مواقع التواصل الاجتماعي عرفت انتشارا واسعا حيث تم إحصاء 3.48 مليار مستخدم أي بنسبة 45 % من الإنسانية جمعاء، وفي ما يلي شكل يوضح نسب توزيع استخدام الانترنت على خريطة العالم . (Sophie Amsili, 2019).



(https://wearesocial.com/uk/)

المصدر: WeAre Social

ووفقا للتقرير الرقمي السنوي 2021 (وهي دراسة تسمح بمعرفة كافة الإحصائيات حول استخدام الويب وشبكات التواصل الاجتماعي عبر العالم) الذي أعدته We Are و HootSuite تبين في حين أنّ 4.4 مليار شخص موصول على شبكة لانترنت

Internautesعبر العالم، فإنّ 4.5 مليار مستخدم لشبكات التواصل الاجتماعي، 5.22 مليار موصول على شبكة الانترنت عبر الهاتف النقال Des Mobinautes ،بمعدل 6سا و45 د على الخط يوميا.

490 مليون مستخدم جديد لشبكات التواصل الاجتماعي خلال 2020. وبلغت 13.2 % مستخدم جديد للشبكات الاجتماعية خلال 12 شهرا الأخيرة ؛أي ما يساوي 1.3 مليون مستخدم جديد يوميا ما يمثل 15.5 مستخدم كل ثانية.و 4.15 مليون يستخدمون الهواتف النقالة للولوج إلى مواقع التواصل الاجتماعي.

بحيث بلغت نسبة 79% من الولوج في أوروبا الشمالية والغربية، 74% في أمريكا الشمالية، 66% في آسيا الشرقية، و8% في أفريقيا (النسبة الأقل). وسجلت هنا 53.6 % من سكان العالم من يستخدمون شبكات التواصل الاجتماعي ؛ما يساوي 217.5 مستخدم نشط عبر هذه المواقع ،كما تجدر الإشارة إلى أنّ تطبيقات التّراسل الآنية Applications de messagerie instantanées، احتلت الصدارة وفي مقدمتها الواتساب يليها الفايسبوك، عدا إثيوبيا التي يغلب فيها استعمال التلغرام وتطبيق إيمو IMO.

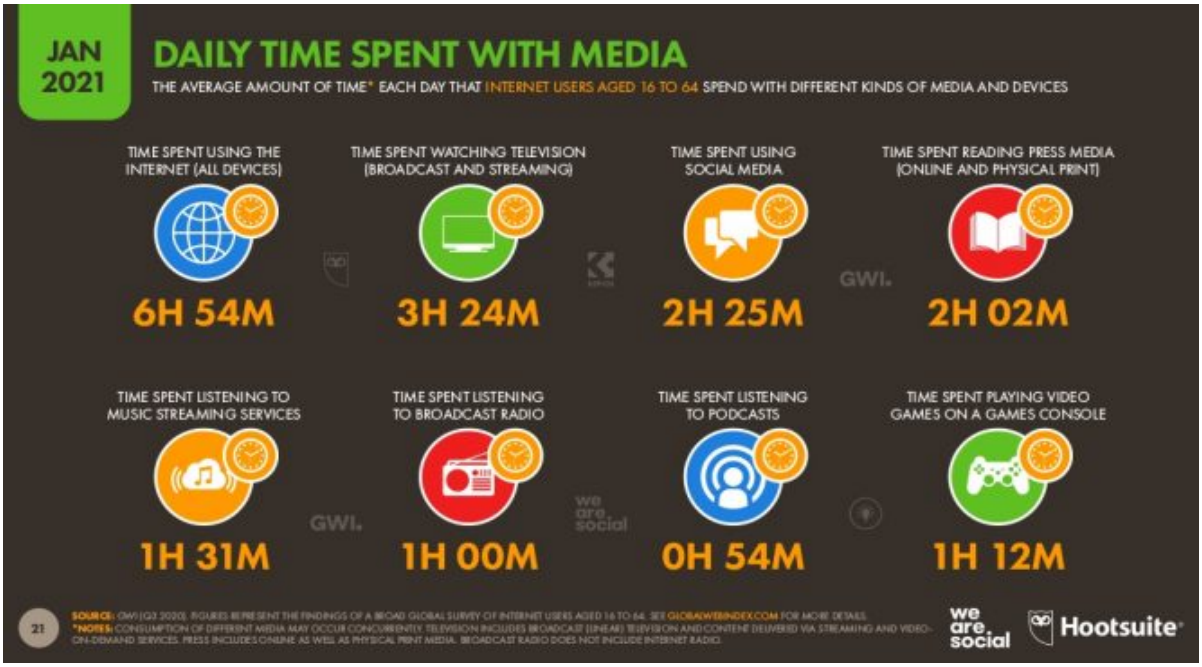
من بين العديد من إحصائيات هذه الدراسة فقد تم تسجيل الأرقام التالية فيما يخص استخدام الانترنت لسنة 2021 من بين 7.83 مليار نسمة (عدد سكان المعمورة)،5.22 مليار مستخدم للهاتف النقال بزيادة بلغت 1.8 % مقارنة بالسنة الفارطة (2020) أي بنسبة 66.60 %.وبلغت زيادة المستخدمين الحديثين 7.3%،منهم 4.2 مليار مستخدم نشط عبر مواقع التواصل الإجتماعي، سجلت فيها نسبة 63.4 %،يستخدمون محرك البحث كروم .

كما نوّهت الدراسة أن جائحة كوفيد-19 كان لها تأثير هام على عدد مستخدمي الانترنت، حيث بلغت نسبة الولوج خلال جانفي 2021 نسبة 59.5% من بين سكان العالم بمجموع 4.66 مليار مستخدم للانترنت Internautes.

وجاء في التقرير أيضا أنّ مستخدمي الانترنت يقضون وقتهم كالتالي: 3 سا و24د لمشاهدة الأفلام التلفزيونية أو السينمائية، 2سا و25د أمام شبكات الواصل الاجتماعي، 2ساو02د لقراءة الصحف، ساعة و31د للاستماع للموسيقى، ساعة و12د لألعاب الفيديو، و54 دقيقة مخصصة للاستماع للتسجيلات.وأضاف ذات المصدر أنّ اختلاف أصناف المستخدمين للشبكة يخضع إلى عدة عوامل وأسباب وتتنوع فيها الحاجات الدافعة لهذا الاستخدام سواء تعلق الأمر بوسيلة ما أو بموقع معين أو بتطبيقات محددة ،وعلى ضوء نتائج الدراسة فقد بلغت نسبة المستخدمين للانترنت 63% ممن يستخدمونها كمصدر للمعلومات، 56.30 % من يلجون إليها بغرض البقاء على اتصال مع الأصدقاء والعائلة .في حين من يهتمون بمعرفة آخر المستجدات و الأحداث بنسبة 55.60 %.وقد حظيت مشاهدة البرامج التلفزيونية والفيديوهات بالحصيلة الأقل حيث سجلت 51.70 %.

- ناهيك عن ذلك فقد حددت الدراسة المواقع الأهم و الأكثر زيارة منذ بداية 2020، تمثلت في الثلاثي Google, YouTube et Facebook ،وحسب الكثيرين فهي تعتبر من أهم المواقع والتطبيقات التي لا بديل لها .تربع فيها اليوتيوب على النسبة الأعلى للزيارة بحجم 33 دقيقة و11 ثانية. ((Patard, blogmoderateur, 2021)

المصدر : موقع Hootsuite (https://www.hootsuite.com/fr/)



ونظرا لما فرضته جائحة كورونا على الأفراد من عزلة اجتماعية، وتوقف شبه تام لمختلف الأنشطة الحياتية اليومية، بات السبيل الوحيد للبقاء على اتصال بالعالم الخارجي هو توفره تكنولوجيا الاتصال من فضاءات ومنصات لإشباع الحد الأدنى من

الحاجات، وهو ما يؤكده التقرير الرقمي السنوي، الذي جاء فيه أنّ متوسط الوقت الممضى على شبكة الانترنت عبر مختلف الأجهزة قد عرف ارتفاعا كبيرا سنة 2020، بحيث انتقل من 6سا و68 د خلال الثلاثي الأخير من سنة 2019 إلى 6سا و54د فيما بعد (+4%)، بما يعادل 48 ساعة على الخط أسبوعيا.

فعلى افتراض أن مستخدم الانترنت Internaute ينام بين 7و8 ساعات يوميا، فهذا يدل على أننا اليوم نقضي حوالي 42% من حياتنا ونحن مستيقظين على الخط، فالوقت الذي نقضيه على شبكة الانترنت أكثر مما نقضيه نائمين، وإذا استمر استخدام الانترنت بهذا المستوى طيلة سنة 2021 فإن مستخدمي الانترنت عبر أنحاء العالم سيمضون ما يقارب 12 مليار ساعة على الخط.

وكانت أهم دوافع اتصال الأفراد بشكة الانترنت حسب ذات الدراسة متمثلة فيما يلي:

- البحث عن المعلومات 63%
- البقاء على اتصال مع الأصدقاء والعائلة 56.3 %
- الاطلاع على المستجدات والأحداث 55.6%
- البحث عن البرامج التعليمية 51.9%
- التسوق على الخط 69.4%
- مشاهدة الفيديوهات، الحصص التلفزيونية والأفلام 51.7%

وبعد تحديث التقرير الرقمي شهر أفريل 2021 المقدّم من طرف Hootsuiteو Are Social We تأكّد الارتفاع الكبير لاستخدام الانترنت ومواقع التواصل الاجتماعي وهو ما يفسر تأثير الأزمة الصحية التي شهدها العالم، وقد تم تسليط الضوء على تأثير هذه المواقع والتطبيقات في سلوك الاستخدام لدى الأفراد أثناء معايشتهم للوضع الصحي المفروض بمختلف إجراءاته الاحترازية للحد من انتشار الوباء؛ حيث تبيّن أنّ عدد مستخدمي الانترنت قد ارتفع إلى 4.72 مليار أي 6 أشخاص من بين 10 في العالم بزيادة تقدر بـ 7.6% ، من بينهم 4.38 مليار شخص متصل على الانترنت باستخدام هاتفه المحمول (92.8% من مجمل مستخدمي شبكة الانترنت)، وقدر عدد المستخدمين النشطين لشبكات التواصل الاجتماعي بـ 4.33 مليار مستخدم بارتفاع يقدر بـ 13.7% اي أكثر من 1.4 مليار مستخدم لمنصات التواصل الاجتماعي يوميا. وتم تحديد أنّ تطبيق الواتساب هو المنصة المفضلة لدى الأشخاص الذين تتراوح أعمارهم بين 16 إلى 64 سنة بنسبة استخدام تقدر بـ 24.1%، يليها الفايسبوك بنسبة 21.8%، الانستغرام 18.4%، تيك توك 3.4% والسناب شات 1.5% وأخيرا بانتريست Pinterest بنسبة 2.3.%.(Patard, blogmoderateur, 2021)

وحسب ذات التقرير الرقمي لسنة 2021، فإن المستخدمين في الخمسين من أعمارهم يمثلون الفئة الأكثر نموا على أهم المنصات الاجتماعية ، وردت الأرقام فيها كما يلي:

- الفايسبوك: +25% من فئة الرجال الذين تبلغ أعمارهم 60سنة فما فوق.
- الانستغرام: +63.6% فئة الرجال الذين تتراوح أعمارهم بين 55 و 64 عاما.
- السنابشات: +33.3% رجال من عمر 50 سنة فما فوق.

2.6- واقع استخدام الانترنت في القارة الإفريقية:

لم يتوقف عدد مستخدمي الانترنت عن الارتفاع في القارة الإفريقية في السنوات الأخيرة من 2011 إلى غاية 2018، حيث تضاعف من نسبة 13.5% إلى 28%، وبالرغم من ذلك فإنّ القارة لا تزال تعرف ثغرات هامة بالنسبة للبنية التحتية التي تسمح بتقديم خدمة انترنت سريعة ومستقرة.

خلال سنة 2018 ساهمت التكنولوجيات والخدمات المحمولة بنسبة 8.6%من الناتج الإجمالي المحلي في أفريقيا شبه الصحراوية l'Afrique subsaharienne، تقابل هذه النسبة ما قيمته 144 مليار دولار إلاّ أن القارة الإفريقية تعاني من بنية تحتية قديمة وغير مستقرة، مما يصعب تقديم خدمة الانترنت في مناطق نائية ومنعزلة على الكرة الأرضية، وأغلب الأفراد الذين يعيشون في المناطق النائية ويعتبرون أنفسهم في منأى عن هذه الخدمة، يُعتبَرون اليوم فئة هامّة.

كما أنّ سعر الانترنت في دول هذه القارة مرتفع جدّا لأنّ الحكومات غير مدعّمة لهذا القطاع، ففي الثلاثي الثاني من سنة 2019 بلغ سعر الجيغا بايت الواحد 2.21 دولار في رواندا، 3.17 في البورندي، 15 دولار و15 دولار في زمبابوي، مع العلم أنّ 1جيغا بايت يستهلك بسرعة فائقة أثناء الإبحار على الويب، كما أنّ القدرة الشرائية لمجتمعات هذه الدول ضعيفة جدّا. (Université de Sherbrooke, 2021).

- ✓ **أرقام حول استخدام الانترنت في أفريقيا سنة 2020: (Kamdem, 2020)**
  - 08.1 مليار يستعملون الهاتف النقال، بنسبة ارتفاع تقدر بـ 5.6%
  - 453.2 مليون مستخدم للانترنت، مع تسجيل 42 مليون مستخدم جديد خلال سنة واحدة
  - 217.5 هم مستخدم نشط على مواقع التواصل الاجتماعي

حيث أنّ تطبيقات التّراسل الآنية Applications de messagerie instantanées، تحتل الصدارة وفي مقدمتها الواتساب يليها الفايسبوك، عدا إثيوبيا التي يغلب فيها استعمال التلغرام وتطبيق إيمو IMO.

7- واقع استخدام الانترنت بالجزائر في ظل جائحة كورونا:

كغيرها من دول العالم شهدت الجزائر ارتفاعا متناميا لاستخدام الانترنت خاصة أثناء تفشي جائحة كورونا، ففي حين بلغ عدد سكان الجزائر مع بداية جانفي 2021 44.23 مليون نسمة، يعيش أغلبهم (74%) في المناطق الحضرية، فإن الإحصائيات المقدمة ضمن تقرير البيانات المنشور خلال شهر فيفري DATA REPORTAL2021 (تقرير يقدم الإحصائيات المتعلقة بالانترنت عبر العالم باستعمال الهاتف الثابت أو المحمول) تأكّد تسجيل ارتفاع الاستعمال الرقمي والويب خلال جائحة كوفيد-9، وذلك من خلال الأرقام التالية:(Whitelineservices) :

- 26.35 مليون مستخدم للانترنت في الجزائر.
- ارتفاع عدد مستخدمي الانترنت بنسبة 16% مقارنة بسنة 2020.
- 46.82 مليون جزائري يتصلون على الانترنت باستعمال الهاتف النقال.

وحسب ذات التقرير فإنّ 25 مليون نسمة يستخدمون مواقع التواصل الاجتماعي خلال جانفي 2021، وهو ما يمثل نسبة 56.6% من إجمالي سكان الجزائر، بزيادة تقدر بـ 3.0 مليون مستخدم ما تمثله نسبة 14%+ بين سنة 2020 و 2021. (Kemp, 2021)

من جهة أخرى فقد تم تسجيل 46.82 مليون اتصال عبر الأجهزة المحمولة Connexions mobiles في جانفي 2021، بزيادة تقدر بـ 963 ألف (+2.1%) مقارنة بجانفي 2020، إنّ عدد الاتصال على الانترنت عن طريق الأجهزة المحمولة يمثل 105.8% من إجمالي عدد السكان.(Mehenni, 2021)

بالرغم من الارتفاع المسجّل في عدد مستخدمي الانترنت بالجزائر، إلّا أنّ التصدع الواقع بين الدول جد المتقدمة والدول في طور النمو واضح ولا يمكن تجاهله، ويمكن أن يظهر ذلك من خلال متوسط سرعة تدفق الانترنت، فإذا كانت بعض الدول مثل سنغافورة أو ايسلندا تسجل سرعة تدفق جد مرتفعة 190.9 و 156.2 ميغابايت في الثانية على الهاتف الثابت، 61 و 72.8 ميغابايت على المحمول، فإنّ دولا أخرى لا تزال جد متأخرة، فالجزائر وفنزويلا تعتبران من الدّول الأقل تقدّما، حيث أنّ سرعة التّدفق فيهما على الثابت (على التوالي) 3.8 و 3.7 ميغابايت، بينما التدفق على المحمول حدد بـ 5.9 و 6.6 ميغابايت، بل إن الانترنت في سنغافورة أسرع 50 مرة منها في الجزائر (Sophie Amsili، 2019).

وكما ذكرنا سابقًا حول ضعف البنية التحتية الرّقمية في القارة الإفريقية فإنّ الجزائر أيضًا تعاني من تبعات ذلك التّصدع، وهو ما ينتج عنه عدم توفّر الحماية اللّازمة لمستخدمي الانترنت خاصّة وأنّ عددهم في ارتفاع مستمر، ممّا أتاح الفرصة لانتقال الجريمة من العالم الحقيقي إلى العالم الافتراضي (الفضاء السيبراني)، لتوفر عوامل تنفيذها وسهولة وسائلها ما جعلها تنافس الجريمة التقليدية.

لقد حذرت المصالح الأمنية من ارتفاع عدد الجرائم الالكترونية بعد أن سجلت كل من مصالح الدرك والشرطة ما يربو عن 8آلاف جريمة الكترونية خلال 2020، مقابل 500 جريمة سنة 2015 (Bachouche, 2021) في حين بلغ عددها 4210 جريمة سنة 2019 وذلك حسب تصريح مدير الشرطة القضائية السيد حاج سعيد ارزقي (خلال عرض الحصيلة السنوية لنشاطات مصالح الشرطة القضائية) (APS, 2021)

حيث سجلت المديرية العامة للأمن الوطني 5200 قضية، في حين سجلت قيادة الدرك الوطني 1362 جريمة سيبرانية تورط فيها 1028 شخص خلال 2020، واحتلت جرائم القذف والسب عبر الفضاء السيبراني الصدارة بنسبة 55%، تليها الجرائم ضد الأمن العمومي، ثم الأفعال الماسة بالحياة الخاصة وإفشاء الأسرار، وأخيرا الابتزاز والنصب والاحتيال والاستغلال الجنسي والأفعال المخالفة للآداب العامة، وحسب شركة كاسبرسكي المختصة في محاربة الجريمة السيبرانية أنّ الجزائر صنفت سنة 2018 الأولى عربيا والرابعة عشر عالميا من حيث البلدان الأكثر تعرضا للهجمات الالكترونية، وقد أحبطت ذات الشركة 95 ألف هجمة الكترونية ضد الجزائر خلال سنة 2020. (Bachouche, 2021)

إن الارتفاع الملاحظ في عدد الجرائم السيبرانية سنة 2020 مقارنة بسنة 2019 أو سنة 2015، ومن جهة أخرى ارتفاع عدد مستخدمي الشبكة العنكبوتية خاصة بواسطة الأجهزة المحمولة Les connexions mobiles حيث بلغ نسبة (105.8%) من إجمالي عدد السكان خلال جانفي 2021، إنما هو راجع إلى ما فرضته جائحة كوفيد-19 -التي اجتاحت العالم بأسره- من: حجر منزلي، عزلة اجتماعية، تباعد الأفراد، والضغط النفسي الذي أصبح يعيشه الأفراد من أجل تلبية أبسط احتياجاتهم اليومية، إضافة إلى توقف أغلب النشاطات الاقتصادية والإنتاجية، ساهمت هذه العوامل مجتمعة في لجوء الأفراد إلى ممارسة سلوكات المنحرفة واللاأخلاقية متجسدة في مختلف أنواع الجرائم السيبرانية وتنفيذها في الفضاء الوحيد الذي أصبح يجمع أكبر عدد ممكن من الأفراد بعيدا عن تهديدات الجائحة اللعينة، ودون قيود.

إنّ تنوع الجرائم الالكترونية في الجزائر أثناء جائحة كورونا، بين ما هو متعلق بالأفراد، وبين ما هو متعلق بالمؤسسات خاصة الأجهزة الأمنية العمومية، إنما هو راجع إلى تزعزع النظام القيمي للأفراد المستخدمين، تلك المعايير الّتي تكوّن نظامًا صلبًا لابد من الرجوع إليه لتقييم السلوك والاختيار من بين البدائل المتاحة في مختلف المواقف التي يتعرض لها الأفراد سواء في العالم الواقعي أو الافتراضي، هذا من جهة، ومن جهة أخرى عدم تمكن مستخدمي الانترنت (سواء أفراد أو مؤسسات) بمختلف تطبيقاتها من تأمين معلوماتهم، بياناتهم، برامجهم وأجهزتهم لمجابهة تلك الجرائم، وهو ما يؤكّده رئيس النقابة الوطنية أصحاب العمل الرقميين Syndicat national du patronat citoyen du numérique حول غياب الوعي الجماعي والمؤسساتي (سواء مؤسسات عمومية أو خاصة أو إدارات عمومية) تجاه أهمية امتلاك بنية صلبة تسمح بتأمين نظم المعلومات،كما يدعمه في ذلك نائب رئيس Think Tank Care ® إذ يركز على أهمية الحماية ضد الهجمات السيبرانية، مع الأخذ بعين الاعتبار أن المؤسسات لا تزال مستمرة في التفكير بأنّ تلك الهجمات لا تأتي إلا لغيرها لأنه ليس لديها ما تخفيه ولكن على العكس من ذلك فإن كل معلومة لها قيمتها، وبالتالي فجميعها قابلة للبيع والاستعمال. (APS, aps.dz, 2021)

1.7- الإجراءات المتخذة من أجل تحقيق الأمن السيبراني والتصدي لمخاطر الجرائم الالكترونية بالجزائر :

بهدف مواجهة الجرائم السيبرانية، والحد من المخاطر التي تسببها سواء على المستوى الفردي أو المؤسساتي، قامت الدولة من خلال مختلف أجهزتها، بوضع استراتيجيات وقائية وأخرى ردعية تماشيا مع التطور الذي تشهده البلاد جراء تنامي استخدام تكنولوجيات الإعلام والاتصال خاصة خلال فترة تفشي جائحة كوفيد-19 حيث عرفت ارتفاعا محسوسا في عدد الجرائم الالكترونية التي تمس بالأفراد أو المؤسسات أو الإخلال بالأمن العام، أهمها ما يلي:

- إنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: إن إنشاء هذا القطب المتخصص في المتابعة والتحقيق بالجرائم المتعلقة بتكنولوجيات الإعلام والاتصال، يتيح حسب الخبراء ورجال القانون المواجهة الفعالة للجريمة السيبرانية للحدّ من نشر المعلومات المضلّلة بهدف تحقيق الأمن العام والمحافظة على استقرار المجتمع.

وقد تم إنشاء هذا القطب تنفيذًا تعليمات رئيس الجمهورية في اجتماع المجلس الأعلى المنعقد في 04 أوت 2021 حول الوضعية الأمنية والصحية، وتبعًا لذلك تمّ تقديم مشروع أوّلي لمرسوم رئاسي من طرف وزير العدل، ليتمّم ويعدّل الأمر الرئاسي رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجنائية.(Benrahal, 2021) .

وبعد الصدور الفعلي للأمر الرئاسي رقم 21-11 المؤرخ في 25 أوت 2021، تمّ تحديد مهام هذا القطب الجزائي، كما تم تحديد مفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، على أنّها: "كل جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال".

® Think Tank Care : مؤسسة فكرية حول الشركات والسياسة الاقتصادية، تضم مجموعة من الخبراء مستقلة عن الدولة أو أي جهة ضاغطة، مهمتها المساهمة في تحسين ظروف التطور الاقتصادي والاجتماعي للبلاد، من خلال التفكير، التواصل وترقية كل مبادرة اقصادية إيجابية(CARE)

كما تم تحديد مهام وكيل الجمهورية وقاضي التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة. (joradp.dz, 2021)

إنّ استجابة الحكومة للتغيرات الاستراتيجية الّتي فرضتها تكنولوجيات الإعلام والاتصال على المستوى المحلي والعالمي، تعد خطوة هامة رغم تأخرها مقارنة بانتشار الكبير والاستخدام الواسع لتكنولوجيات الإعلام والاتصال بالجزائر خاصة أثناء فترة تفشي جائحة كورونا التي تزامنت مع ارتفاع عدد الجرائم الالكترونية أيضا، ولكنها لا يمكن إلا أن تكون خطوة أولى للتمكن من إنشاء بنية تحتية صلبة ومتينة لمواجهة التهديدات السيبرانية التي أهم ما يميزها الانتشار الكبير والسريع، إضافة إلى اختلاف معالمها. ولذلك إضافة إلى برمجة دورات تكوينية لفائدة قضاة القطب الجزائي السبراني في هذا المجال،

- **تنظيم دورات تكوينية ومؤتمرات حول الجريمة الالكترونية طرق تحقيق الأمن السيبراني:**

إنّ اتخاذ الجراءات القانونية اللازمة لمكافحة الجريمة السيبرانية لا يعد كافيا، لأن التعامل مع هذا النوع من الجرائم يتطلب دراية تقنية كافية، وتمكنا فعليا بتكنولوجيات الإعلام والاتصال: وسائلها، برامجها، تطبيقاتها، استخداماتها.... من أجل ضمان الفهم الدقيق لأبعاد كل جريمة تفتح أمام الهيئات القضائية المعنية بالحكم فيها، ومن بين ذلك نجد:

- تسطير عدة برامج تكوينية من طرف وزارة العدل لفائدة جميع مستخدمي القطب الجزائي السابق الذكر، خاصة القضاة، حيث تم تنظيم ورشة عمل وطنية على الخط، حول "التحضير للحصيلة السنوية حول وضعية الجريمة الالكترونية والأدلة الالكترونية"، في إطار البرنامج الأوروبي لمكافحة الجريمة الالكترونية، إضافة إلى استفادة مجموعة من القضاة ومهندس إعلام آلي بالمديرية العامة لعولمة العدالة من المشاركة بسلسلة webinaires حول: " تطبيقات التشفير في مجال الجريمة الالكترونية والإجرام الرقمي"، المنظمة من طرف المنظمة العالمية للشرطة الجنائية Interpol، وبرنامج Glacy* ® لمكافحة الجريمة الالكترونية بحضور ممثلين عن المديرية العامة للأمن الوطني، ومسؤولي مصالح التكوين ومكونين على مستوى وزارة العدل.
- تنظيم الطّبعة السّابعة للمؤتمر الموسوم بـ: "الأمن السيبراني: من سرقة البيانات إلى التّلاعب بالمعلومات" "La cybersécurité: du vol des données mobiles à la manipulation de l'information", المنظم من طرف World Trade Center Algiers في 07 ديسمبر 2021 بالجزائر العاصمة، حيث أوصى على هامشه الخبراء المشاركين فيه بإنشاء مدرسة متخصّصة في الأمن السيبراني، وذلك لاكتساب الخبرات اللازمة من أجل التصدي لمختلف الهجمات الالكترونية الّتي تهدّد استقرار البلاد، والتمكّن من مواجهة تحديات المحيط الجيواستراتيجي الحالي، وحماية الجزائر من خلال وضع استراتيجية وطنية أمنية في إطار ما تقترحه المدرسة(APS, aps.dz, 2021) .

8- الإجراءات الواجب اتخاذها من أجل تحقيق الأمن السّيبراني والتصدي لمخاطر الجرائم الالكترونية:

® GLACY (Action Globale sur la Cybercriminalité): هيئة أوروبية مهمتها مساعدة جميع دول العالم ووضع اتفاقيات عالمية حول الجريمة الالكترونية، وهدفها التعاون مع الجهات القضائية في ما يخص الجريمة الالكترونية والأدلة الرقمية.(Conseildel'Europe)

إنّ الإجراءات السّابقة الذكر إنّما هي إجراءات تضمن التّحكم في تحديد تفاصيل وأبعاد الجرائم الالكترونية وتقنيات ارتكابها ومن ثَمَّ تسليط العقوبات اللّازمة على مرتكبيها، ولكن الارتفاع المستمر في عدد مستخدمي الانترنت خاصة بواسطة الأجهزة المحمولة من جهة، ومن جهة أخرى مخلفات جائحة كورونا سواء على المجال الاجتماعي، الاقتصادي أو السياسي، ودون التغاضي عن الهوة المتزايدة بين الدّول المتقدّمة والدّول النامية أو الّتي في طور النّمو (الجزائر) في مجال التكنولوجيا والمجالات الأخرى، بالموازاة مع "تفشي مفهوم العالمية والتنميط" الذي يسعى لترويجه أصحاب رؤوس الأموال وكبرى الشركات العالمية متجاوزين الخصوصية الثقافية والاجتماعية للمجتمعات، ومتجاهلين الحدود الجغرافية والسياسية للدول ممّا يؤدي بالأفراد إلى التخلي عما تنص عليه الأنظمة القيمية لمجتمعاتهم بحجة تبني العالمية واعتبارها المرجع الأساس في مختلف المواقف الحياتية اليومية، كل هذه العوامل تشكّل في مجملها البيئة المناسبة لارتكاب الجرائم الالكترونية بمختلف أنواعها.

وعليه فإنّ الإجراءات الواجب اتخاذها لمكافحة هذه الجائحة (الجرائم الالكترونية)، لابد أن تكون وقائية، توعوية، وتربوية يتحمل مسؤوليتها جميع مكونات المجتمع: أفراد، مؤسسات خاصة، مؤسسات حكومية، جهات أمنية، جهات ضاغطة...كل في مجاله حتى تتحقق المناعة الجماعية للحدّ من وباء الجريمة الالكترونية، وذلك من خلال ما يلي:

- ضرورة نشر الوعي بين الأفراد والمؤسسات بضرورة التعلم الجاد والدراية التقنية اللازمة حول الأجهزة التكنولوجية التي يمتلكونها وما تحويه من برمجيات، تطبيقات ومعلومات وكيفية الاستخدام الأمثل لها، وكيفية تأمينها.
- ضرورة اقتناع الأفراد والمؤسسات بحتمية تأمين جميع تكنولوجيات الإعلام والاتصال التي يستخدمونها من أجل ضمان تأمين المعلومات التي تحويها مهما كانت بسيطة بنظر مالكها وبغض النظر عن تكاليفها.
- عدم الاستخفاف بعالم الانترنت وعدم الخوض في روابط أو مواقع غير مؤمنة أو مشبوهة.
- توعية الأفراد والمؤسسات وتحسيسهم بوجود جهات أمنية وقضائية مختصة وفعّالة على أتم الاستعداد لحمايتهم في حال تعرضهم لهجمات سيبرانية والاقتصاص لهم بموجب ما ينص عليه القانون الخاص بذلك (كما ذكرنا سابقا).
- ضرورة سهر الجهات الحكومية بكل جدية على توفير ودعم أنظمة وبرمجيات تأمين الأجهزة والمعلومات، لتفادي تفشي وتغلغل الجريمة الالكترونية في الجزائر لأن ذلك يهدد حتما استقرارها الاجتماعي، الاقتصادي، الثقافي، الأمني والسياسي على المستوى المحلي أو العالمي، لأنها جرائم لا حدود لها.
- ضرورة حماية الأطفال من خطر تكنولوجيات الإعلام والاتصال، لأنهم الأكثر عرضة للتهديدات السيبرانية بسبب عدم قدرتهم على الاستخدام المثالي لتلك التكنولوجيات وذلك راجع لعدم اكتمال القدرات العقلية للأطفال بعد في هذه المرحلة العمرية الحساسة التي يتم فيها التشكيل العقلي و الفكري و السلوكي للطفل.
- التركيز على ضرورة التمسك بالنظام القيمي للمجتمع الجزائري العربي الإسلامي، الذي لا يمكن أن يسمح بأي شكل من الأشكال بارتكاب أي نوع من أنواع تلك الجرائم الالكترونية، لأنه يعزز قيم الاحترام، الصدق، الإخلاص، الأمانة، الوفاء، العضوية، التكامل، التعاون...وهذه المهمة موكلة إلى جميع مؤسسات التنشئة الاجتماعية بدءً بالأسرة إلى المسجد، فالمدرسة، إلى وسائل الإعلام (سواء التقليدية أو الجديدة متمثّلة في وسائل الإعلام الجديد).
- ضرورة التربية الإعلامية لمختلف شرائح المجتمع خاصة الأطفال منهم، من أجل التمكن من تطوير التفكير الناقد لديهم تجاه تكنولوجيات الإعلام والاتصال الحديثة والمعلومات التي تتضمنها، وتعريف التربية الإعلامية، حسب توصيات مؤتمر فيينا 1999، هو:" تختص التربية الإعلامية في التعامل مع كل وسائل الإعلام و الاتصال، و تشمل الكلمات، والرسوم

المطبوعة، والصوت، والصور الساكنة والمتحركة، التي يتم تقديمها عن طريق أي نوع من أنواع التقنيات، وهي تمكّن أفراد المجتمع من الوصول إلى فهم وسائل الإعلام والاتصال التي تستخدم في مجتمعهم، والطريقة التي تعمل بها هذه الوسائل، و من ثم تمكنهم من اكتساب المهارات للتفاهم مع الآخرين ". (الشميمري، 2010)

فاعتماد التربية الإعلامية في المجتمع خاصة منذ مرحلة الطفولة، من شأنه أن يقلل من الجريمة الالكترونية لأنها تضمن تكوين أفراد متمكنين سواء بالنسبة لكيفية استخدام وسائل تكنولوجيا الإعلام والاتصال، أو بالنسبة للمضامين التي تقدمها وتلقيها بتفكير ناقد، وبالتالي عدم إتاحة الفرصة لتهديدات الجرائم الالكترونية.

قائمة المصادر والمراجع:

I- باللغة العربية:

- بارة سمير ،الأمن السيبراني في الجزائر –السياسات والمؤسسات– ، المجلة الجزائرية للأمن السيبراني ، العدد04 ، جويلية 2017 ،
- جمال بوازدية ،الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية —التحديات والآفاق المستقبلية– ،مجلة العلوم القانونية والسياسية ،المجلد 10،العدد 01 ،الجزائر.2019 .
- روان بنت عطية الله الصحفي ،الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات،العدد 24 ،ماي 2020.
- فهد بن عبد الرحمن الشميمري، التربية الإعلامية، كيف نتعامل معها؟ن الرياض، 2010.
- محمد ابو القاسم الردفاني ، تحقيقات الشرطة في مواجهة الجرائم السيبرانية ، المجلة العربية للدراسات الأمنية والتدريب،المجلد 31 ،العدد 61، 2014.
- منى عبد الله السمحان ، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود ، مجلة كلية التربية ، العدد 11 ، جامعة المنصورة.المملكة العربية السعودية ،جويلية 2020.

II- باللغة الأجنبية:

- Centre International pour la prévention de la criminalité, 6e rapport international : Prévention de la criminalité et sécurité quotidienne, prévenir la cybercriminalité, Montréal, 2018.

III- المواقع الالكترونية:

- political-encyclopedia-org .
- tisri.org
- studies.aljazeera.net
- hbrarabic.com
- / attaa.sa
- ab7as.net
- www.aps.dz
- Jordp.dz
- **avocatalgerien.com**
- www.elmoudjahid.dz
- www.dgsn.dz
- perspective.usherbrooke.ca
- www.whitelineservices.dz
- **www.lesechos.fr**
- www.blogdumoderateur.com
- cmdafrique.net
- www.echoroukonline.com
- www.algerie-eco.com