مجلة العلوم القانونية والاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

الإطار القانوني للوقاية من الجرائم السّيبرانية ضدّ الأطفال ومكافحتها

The Legal Framework for Combating and Preventing Cyber Crimes against Children

بهلـول سميّـة [1]*

[1]كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين سطيف 2، (الجزائر)

s.bahloul@univ-setif2.dz

تاريخ ارسال المقال:2021/09/03	تاريخ القبول:2021/10/.25	تاريخ النشر: 2021/09/01

*المؤلف المرسل

الملخّص:

تعتبر الجرائم السيبرانية من أخطر الجرائم التي يشهدها العالم اليوم، والتي تشكل الوجه السلبي لانتشار استعمال تكنولوجيات الإعلام والاتصال والانتقال من العالم التقليدي إلى العالم الرقمي الذي يقوم على اقحام التكنولوجيا في جميع مجالات الحياة، ومع الانتشار الهائل لهذه الجرائم فقد أصبحت تشكل تهديدا ليس فقط للأفراد، بل حتى للدول ومؤسساتها، وما زاد من خطورتها أنها أصبحت موجهة بدرجة كبيرة إلى فئة **الأطفال** لما تشكله هذه الفئة من ضحية سهلة لارتكاب هذه الجرائم دون تعرض المجرم لخطر التفطن لجرمه أو حتى اكتشافه، الأمر الذي جعل العمل على حماية الأطفال من مخاطر الجرائم السيبرانية والوقاية منها يتزايد كل يوم ويفرض على الدول تسخير كافة الوسائل القانونية والمادية التي من شأنها المساهمة في الوقاية من مخاطر الجرائم السيبرانية الواقعة على الطفل بمختلف أشكالها ومكافحتها، بما يحول دون انتشارها وتطورها بصورة أكبر مما هي عليه اليوم.

الكلمات المفتاحية: الجرائم السيبرانية;الطفل;الإنترنت; الألعاب الإلكترونية; الهيئة الوطنية لحماية وترقية الطفولة; الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

Abstract:

Electronic Crime or Cyber-crime is one of the most dangerous crimes that the world is witnessing today, This crime constitute the negative side of the widespread use of Technology of Information and Communication (TIC), and with the widespread availability of this crimes, they have become a threat, not only to individuals, but even to states and their institutions. What made it more dangerous is that it has become directed to a large extent of children, because this category is an easy victim to commit these crimes without the criminal being exposed to the risk of recognizing or even discovering his crime.What made work to protect children from the dangers of cybercrime and prevent it increased, and states are required to employ every legal means that would contribute to preventing the risks of cyber-crimes against children.

Keywords:*Cyber-Crimes*; *Child*; *Internet*; *Electronic Games*; *National Authority for Childrenwood Protection and Promotion*; *National Authority for Combating Crimes related to Technology of Information and Communication.*

مقدّمة:

مع الانتشار الخطير للممارسات السلبية العنيفة ضد الأطفال أصبح تقنين جرائم العنف ضد الأطفال ووضع الآليات المناسبة لمكافحته والحماية منه يشكل أول اهتمامات ومسؤوليات الدولة الحديثة، حيث أصبحت جميع التشريعات تسعى إلى سن نصوص قانونية صارمة لفرض الحماية الجادة للأطفال من جميع صور وأشكال العنف والحد من انتشاره [1] حيث يقع على عاتق الدولة إلزامية حماية الطفل من كل ما من شأنه أن يلحق به ضررا أو إهمالا أو عنفا أو سوء معاملة أو استغلال أو إساءة بدنية أو معنوية أو جنسية، وتتخذ من أجل ذلك جميع التدابير المناسبة لوقايته وتوفير الشروط اللازمة لنموه ورعايته، والحفاظ على حياته وحماية حقوقه وحرياته في جميع الحالات، حيث ما فتئت الأمم المتحدة تدعو في إعلاناتها إلى ضرورة حماية الطفل من كل ما يسيء لحالته الصحية أو النفسية، وذهبت في اتفاقياتها ومعاهداتها إلى تجريم الأفعال التي من شأنها المساس بهذه الفئة. [2]

وفي الوقت الذي لا زالت النصوص القانونية تعالج ظاهرة الإجرام الواقعة على الطفل في صورتها التقليدية، وجد العالم نفسه أمام توجه جديد في جميع المجالات والذي ظهر تحت مسمى **التوجه الرقمي** الذي أصبحت تفرضه تكنولوجيات الإعلام والاتصال، لتظهر معها تهديدات جديدة لفئة الطفولة والمتمثلة في **الجريمة السيبرانية الإلكترونية** لتظهر أمام التشريعات الوطنية والدولية بذلك تحديات كبيرة لوضع مختلف الأطر القانونية التي من شأنها مكافحة هذه الجريمة والوقاية منها.

من هنا جاءت فكرة هذا المقال الذي سنحاول من خلاله تسليط الضوء على الجريمة السيبرانية الواقعة على الأطفال انطلاقا من إشكالية رئيسية مفادها:**ما هو الإطار القانوني الذي نظمهالمشرع في سبيل الوقاية من الجرائم السيبرانية الواقعة على الأطفال ومكافحتها؟**

ويتفرع عن هذه الإشكالية العديد من الأسئلة الجزئية أهمها:

- ✓ **ماذا يقصد بالجريمة السيبرانية وما هي أهم الخصائص التي تميزها عن الجرائم التقليدية؟**
- ✓ **كيف تم استغلال هذا الشكل من الجرائم للاعتداء على الأطفال وما هي أهم صورها؟**
- ✓ **فيم تتمثل أهم الآليات القانونية والعقابية التي بذلتها النصوص القانونية في سبيل مكافحة هذه الصورة من الجريمة، وهل هناك هيئات مكلفة بمكافحتها والوقاية منها؟**

للإجابة على الإشكالية والأسئلة المرتبطة بها اعتمدنا في دراستنا على **المنهج الوصفي التحليلي** والذي سنقوم من خلاله بتحديد الإطار العام لمكافحة الجريمة السيبرانية عامة، وتلك الواقعة على الأطفال خاصة، مع العمل على تحليل مختلف النصوص القانونية الناظمة لهذه الجزئيات، ومحاولة وضع اقتراحات في حال تسجيل أي نقص وقصور في هذا المجال.

وذلك من خلال تقسيم مقالنا وفقا لما يلي:

المبحث الأوّل: التأصيل النّظري للجرائم السيبرانية ضدّ الأطفال.

سنقوم من خلال هذا المبحث بتحديد الجانب المفاهيمي للجرائم السيبرانية عموما وتلك الواقعة على الأطفال خصوصا من خلال تحديد خصائصها وضوابطها القانونية مختلف صورها الموجهة ضد سلامة الأطفال وأمنهم، وذلك من خلال ضبط مفهوم الجرائم السيبرانية (**المطلب الأول**) ومن ثم تحديد أنواع وصور الجرائم السيبرانية المرتكبة ضد الأطفال (**المطلب الثاني**).

المطلب الأول: مفهوم الجرائم السيبرانية ضد الأطفال

تعتبر الجرائم السيبرانية من الجرائم الحديثة والمرنة والتي لا زال هناك خلاف كبير حول مفهومها خاصة وأنها تتطور بتطور تكنولوجيات الاعلام والاتصال وتتخذ كل يوم صورة ومظهرا جديدا، إلى جانب كونها جريمة واسعة النطاق توسع معها مفهوم الجريمة وبالضرورة مفهوم العقاب خاصة وأنها أصبحت تهدد إلى جانب الأفراد العديد من المؤسسات والهيئات العمومية والخاصة وتهدد استقرار الدول وأمنها. (3)

إن تحديد مفهوم الجريمة السيبرانيةيحيطه الغموض الذي تفرضه كافة جوانبه بداية بوسائل استخدامه ومرورا بمختلف المفاهيم التي تدخل في إطاره والتي لا زالت هي الأخرى محل خلاف فقهي وهو الأمر الذي جعل الأنظمة الأمنية والساحة الفقهية تتعامل معهاكجريمة مستحدثة على الجانبين المفاهيمي والتطبيقي الأمر الذي يستوجب معه العمل على استحداث أسس قانونية وأطر نظرية وتطبيقية خاصة بالجريمة السيبرانية والتي يسهل بناءا عليها ليس فقط تحديد مفهومها بل وبذل وسائل قانونية ناجعة لمكافحتها والوقاية منها، وهو الأمر الذي لا يتأتى إلا بدراسة متأنية لكافة جوانب هذه الجريمة وأسباب انتشارها لدرجة أصبحت تهدد سلامة أبنائنا. (4)

على اعتبار أن أي مفهوم يستوجب لتوضيحه بيان مختلف العناصر المتعلقة به، فإننا سنحاول ونحن بصدد العمل على ضبط مفهوم الجريمة السيبرانية ضد الطفل، توضيح الإطار النظري لهذه الجريمة وذلك من خلال، تحديد تعريفها (**الفرع الأول**) ومن ثم بيان مختلف خصائصها (**الفرع الثاني**) وذلك قبل الانتقال إلى توضيح مختلف صورها خاصة منها الموجهة ضد الأطفال وسلامتهم.

الفرع الأول: تعريف الجرائم السيبرانية

تعتبر الجرائم السيبرانية من الجرائم المستحدثة التي لم تظهر على الساحة الدولية إلا مع الانتشار الواسع لتكنولوجيات الإعلام والاتصال وتزايد استخدامها وما ترتب عنه من تجاوزات من طرف الأفراد والمؤسسات في استغلال واستعمال هذه التكنولوجيات الأمر الذي استوجب إعادة النظر في الجرائم التقليدية والعمل على بذل إجراءات وقائية، ردعية وتجريمية لهذا النوع من الجرائم والذي أصبح يثبت يوميا مدى خطورته بالنسبة للأفراد والمؤسسات والتي تطورت إلى درجة أنها أصبحت تهدد حتى الأمن القومي للدول وسيادتها واستقرارها.

وتعرف الجريمة في صورتها التقليدية بأنها "**كل عمل غير مشروع يقع على الانسان في نفسه أو ماله أو عرضه أو على المجتمع ومؤسساته ونظمه السياسية والاقتصادية**" (5)ومن زاوية قانونية تعرف بأنها "**كل عمل أو**

امتناع يعاقب عليه القانون بعقوبة جزائية" [6] وبداية من هذا الاختلاف الواضح مبدئيا بين الجريمة التقليدية والجريمة السيبرانية وغياب تعريف قانوني واضح ودقيق لمفهوم الجريمة السيبرانية خاصة مع بداية ظهورها وجد الفقهاء أنفسهم أمام ضرورة العمل على وضع تعريف دقيق لمفهوم الجريمة السيبرانية وهو الأمر الذي شهدا في البداية تداخلا وخلطا في المفاهيم خاصة مع غموض المفاهيم التي ظهرت في المجال الالكتروني ومجال استعمال تكنولوجيات الاعلام والاتصال.

ومن جهة أخرى ومع عدم تبلور مفهوم الجريمة السيبرانية ظهر على ساحة الدراسات القانونية مصطلحات جديدة أهمها "**الجرائم الإلكترونية**" و "**الجرائم المعلوماتية**" و"**جرائم الانترنت**" وهو الأمر الذي طرح تساؤلات جديدة حول العلاقة بين هذه الجرائم أهمها **هل الجريمة السيبرانية هي نفسها الجريمة المعلوماتية وجريمة الانترنت؟** وإن كانت الإجابة بالنفي **فما هو تعريف كل جريمة من هذه الجرائم وما هو الفرق بينها؟**

ومع اتساع انتشار الجريمة السيبرانية وغموض مفهومها **فما هو تعريف هذه الصورة من الجرائم وهل أدت خطورتها إلى اهتمام المشرع بها ووضع تعريف قانوني لها، أم أن التعاريف المبذولة في هذا المجال تقتصر على التعاريف الفقهية؟** هذا ما سنوضحه من خلال هذا الفرع وذلك من خلال ضبط التعريف الفقهي للجريمة الالكترونية (أولا) ومن ثم تحديد التعريف التشريعي (**ثانيا**).

أولا–التعريف الفقهي: إن غياب تعريف تشريعي واضح لمفهوم الجريمة السيبرانية وضع على عاتق الفقهاء مسؤولية ضبط تعريف لها انطلاقا من القواعد العامة لتعريف الجريمة التقليدية واستنادا إلى النقاط المستحدثة بشأن الجريمة السيبرانية، وهو الأمر الذي جعل كل باحث وفقيه يركز على زاوية معينة ما ترتب عنه ظهور العديد من التعاريف منها التي سعى من خلالها الفقهاء إلى التضييق من نطاقها والتركيز بموجبها على محل الجريمة ومنها من ذهب إلى تعريفها استنادا إلى الفاعل مرتكب الجريمة كما ذهب جانب آخر إلى التوسع في تعريف الجريمة السيبرانية وادخل ضمنها كافة العمليات والممارسات الغير مشروعة المرتبطة بتكنولوجيات الإعلام واستخدام الحاسوب الآلي والوسائل الالكترونية وشبكة الانترنت فانقسم تعريف الجريمة السيبرانية إلى:

1–التعريف الضيق للجريمة الالكترونية: ذهب جانب كبير من الفقه إلى التضييق من نطاق التعريف الموضوع لمفهوم الجريمة السيبرانية وركز بذلك كل فقيه على جانب معين في سبيل وضع هذا التعريف، فذهب البعض إلى تعريفها انطلاقا من الوسيلة التي يستخدمها المجرم في سبيل القيام بالجريمة في حين ركز جانب آخر على مدى مستوى معرفة المجرم بالتقنيات الحديثة للحاسوب وتكنولوجيات الاعلام والاتصال وذهب بدوره جانب ثالث من الفقه إلى تعريف الجريمة السيبرانية بالتركيز على محلها ألا وهو المال المعلوماتي المعنوي.

أ–تعريف الجريمة السيبرانية استنادا إلى وسيلة ارتكابها: يذهب الفقه انطلاقا من هذا المعيار إلى التركيز على الحاسب الآلي على اعتباره أساس الجريمة السيبرانية ونقطة التمييز بينها وبين الصور التقليدية وحتى الحديثة للجرائم المعروفة في مجال القانون، ويؤكدون في هذا المقام أن جهاز الحاسوب ولكونه أصبح وسيلة ضرورية تستعمل

بشكل يومي ومتكرر في عصر التكنولوجيا فإن هذا جعله يدخل في العديد من مجالات علم الإجرام ففي مقابل كونه سهل العديد من الممارسات والمعاملات والمهام والوظائف اليومية إلا أن استخدامه الدائم أدى إلى تفاقم الجريمة وتطورها وظهور صور جديدة تتعلق بهذه الوسيلة بالدرجة الأولى والأخيرة. (7)

من هذا المنطلق يعرف الفقه الجريمة السيبرانية بأنها "**الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بهدف تحقيق الربح**" (8) وعرفها البعض الآخر بأنها "**فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية**" (9)كما ذهب جانب آخر من الفقه إلى القول بأن الجريمة السيبرانية هي "**كل نشاط إجرامي تستخدم فيه التقنية الالكترونية المتمثلة في الحاسوب الآلي الرقمي وشبكة الانترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف**" (10) وهناك من ذهب إلى التفصيل نوعا ما في هذا المعيار وعرفها على أنها "**جرائم الشبكة العالمية التي يستخدم فيها الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة، كاستخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب**". (11)

وما يسجل على هذه التعاريف التي اعتمدت على معيار الوسيلة لتحديد مفهوم الجريمة السيبرانية أنها ركزت بدرجة كبيرة على وسيلة ارتكاب الجريمة في حين أغفلت في المقابل الفعل أو السلوك الإجرامي ومرتكبه رغم كونهما أهم بكثير من الوسيلة المستخدمة في تنفيذه، وهو الأمر الذي ترتب عنه غموض أغلب هذه التعاريف وقصورها عن تحديد مفهوم واضح جامع ومانع للجريمة الالكترونية. (12)

ب–تعريف الجريمة السيبرانية استنادا إلى مستوى معرفة المجرم للتقنيات الحديثة للحاسوب وتكنولوجيات الإعلام والاتصال: إلى جانب تعريفها انطلاقا من الوسيلة المستخدمة في ارتكابها ذهب جانب آخر من الفقه إلى تعريف الجريمة السيبرانية استنادا إلى مستوى معرفة المجرم للتقنيات الحديثة للحاسوب وتكنولوجيات الاعلام والاتصال على اعتبار أن هذه التقنيات والوسائل هي المحل الأساسي لارتكاب هذا النوع من الجرائم وتنفيذها يستحيل دون علم المجرم بهذه التقنيات ومعرفة طريقة استخدامها لارتكاب الفعل الاجرامي، وانطلاقا من هذا المعيار يعرف الفقه الجريمة السيبرانية بالقول أنها "**جرائم يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب**" كما أنها "**كل فعل غير مشروع تكون المعرفة بتقنية المعلوماتية أساسية لمرتكبه وللتحقيق فيه وملاحقته قضائيا**" (13) وعرفها جانب آخر بأنها **كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى**". (14)

ج–تعريف الجريمة السيبرانية استنادا إلى محلها أو موضوعها: يذهب جانب ثالث من الفقه إلى تعريف الجريمة السيبرانية بالاستناد إلى محلها أو موضوعها ويذهبون إلى القول بأن وسيلة الجريمة وفاعلها لا يؤديان أي دور في تحديد مفهوم هذا النوع من الجرائم، ويركزون من هذا المنطلق على المالي المعلوماتي المعنوي كموضوع للجريمة لوضع تعريف لها، ومن بين التعاريف الموضوعة انطلاق من هذا المعيار القول بأن "**الجرائم السيبرانية هي الجرائم التي ترتكب ضد الأنظمة الالكترونية والشبكات المعلوماتية**" أي أنها "**كل فعل غير مشروع موجه لنسخ أو**

تغيير أو حذف أو الوصـــول إلى المعلومات المخزنة داخل الحاســـب الآلي أو التي تحول عن طريقه" كما أنها **"كل غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها".** (15)

أي أنه بعبارة أخرى واستنادا إلى هذا المعيار فإن الجريمة السيبرانية **"هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الالكتروني أو التي تحول عن طريقه".** (16)

2-التعريف الموسع للجريمة السيبرانية: مع ثبات قصور التعريف الضيق على الالمام بمختلف جوانبها وإعطائها مفهوما جامعا مانعا وبالتالي عدم الإحاطة بأوجه ظاهرة الإجرام الالكتروني خاصة وأن الحاسب الآلي الذي اتخذه البعض قاعدة لتحديد تعريف الجريمة السيبرانية لا يتعدى مع ظهور وسائل حديثة كالهواتف الذكية عن كونه وسيلة تقليدية لا تستخدم إلا في بعض الجرائم السيبرانية، علاوة على أنه من المتعارف عليه في ساحة فقه القانون الجنائي أن الوسيلة المستعملة في ارتكاب الجريمة لا تدخل ضمن تكوينها ولا تعريفها. (17)

من هذا المنطلق توجه الفقه نحو توسيع المعايير المعتمدة لتعريف الجريمة السيبرانية بهدف تغطية جوانب القصور التي تشوب التعاريف السابقة فعرف البعض الجريمة السيبرانية بأنها **"كل فعل أو امتناع عن فعل يأتيه الانسان إضرارا بمكونات الحاسب الآلي المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد تحت مظلة قانون العقوبات لحمايتها".** (18)

كما عرفها البعض بأنها **"كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها"** (19) وتم تعريفها بأنها **"كل استخدام في صورة فعل أو امتناع من شأنه الاعتداء على أي مصلحة مشروعة، سواء كانت مادية أو معنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ومعاقب عليه قانونا أيا كان غرض الجاني".** (20)

وما يمكننا تسجيله أو رواد هذا الاتجاه قد وسعوا من نطاق المعايير المعتمدة لتعريف الجريمة السيبرانية لتستغرق بذلك كل فعل أو امتناعا عن فعل ويستوي في ذلك أن يكون في صورة مادية أو معنوية كما تم التركيز أيضا على تقنية المعلوماتية وتكنولوجيات الاعلام والاتصال لكونها زاوية التفرقة بين الجريمة السيبرانية وغيرها من الجرائم التقليدية. (21)

3-التعريف المختلط: تعتبر منظمة التعاون والتنمية الاقتصادية(OCDE) من السباقين لوضع تعريف للغش المعلوماتي والجريمة السيبرانية والتي ذهبت إلى القول بأنها:

« Est considéré comme crime informatique tout comportement illégale ou contraire à l'éthique, ou non autorisé qui concerne un traitement automatique de données ou de transmissions de données ». *(22)*

وانطلاقا من هذا التعريف ذهب الفقه إلى تعريف الجريمة السيبرانية بأنها "**كل سلوك غير مشروع أو يتعارض مع قواعد السلوك الأخلاقي وغير مرخص، والذي يخص المعالجة الآلية للمعطيات أو انتقال هذه المعطيات**" (23) كما عرفها البعض بأنها "**كل جريمة أو سلوك غير مشروع يستخدم بالحاسب الآلي أو محاولة نسخ أو حذف أو إتلاف لبرامج الحاسب الآلي أو أي جريمة يكون لتنفيذها صلة بالقواعد والعلوم المعلوماتية أو أي سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات**". (24)

ثانيا: التعريف التشريعي: في سبيل التصدي لهذه الجريمة التي أصبحت تمس بالأمن الوطني، تم تعديل الكثير من التشريعات الوطنية والدولية وإدخال هذه الجرائم ضمن نطاق الأفعال المجرمة التي يعاقب عليها القانون وتخصيص عقوبات تحد من انتشارها واتساعها، وعلى اعتبار أن وضع وضبط تعاريف للمفاهيم القانونية لا يدخل ضمن نطاق اختصاص المشرع فإن المشرع الجزائري وبموجب تعديل قانون العقوبات سنة 2004 (25) عمل على تجريم الجرائم السيبرانية التي أصبحت تنتشر في المجتمع الجزائري مع بداية توجهه نحو المعلوماتية والانفتاح على العالم الرقمي، واستحدث قسما خاصا بالعقوبات المطبقة على الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات.

إلا أن تطور هذه الجرائم دفع المشرع إلى استحداث قانون متخصص لمعالجة الجرائم السيبرانية وما يتعلق بها من تجاوزات تمس الأفراد والمؤسسات فصدر بذلك سنة 2009 أول نص قانوني متعلق بالجرائم السيبرانية الإلكترونية ومكافحتها والذي وضع من خلاله المشرع الجزائري تعريفا للجرائم السيبرانية الالكترونية التي اصطلح عليها بمصطلح **الجرائم المتصلة بتكنولوجيات الإعلام والاتصال** وذلك لاستبعاد الغموض والمرونة التي تتميز بها التعاريف الفقهية لهذا النوع من الجرائم وجاء تعريفها بناءا على هذا بالقول "**الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: هي 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**". (26)

ومن منطلق هذه التعاريف نجد أن التعبير عن الجريمة السيبرانية وتحديد مفهومها تغير وتنوع بحسب الزاوية التي ينطلق منها كل تعريف كما أنه تتزاحم المصطلحات في التعبير عن مدلولها فهناك من يعتمد مصطلح الجريمة السيبرانية وهناك من يصطلح عليها بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وآخر يسميها بجرائم التقنية العالية وآخر يربطها بجهاز الحاسوب أو الكمبيوتر إلى جانب جرائم الانترنت أيضا.

وبالرغم من ذهاب البعض إلى القول بأن جميع المصطلحات السابقة تحمل نفس المدلول، في حين ذهب جانب آخر إلى أنه حتى تكيف الجريمة بأنها جريمة سيبرانية الكترونية وجب اتصال جهازين الكترونيين، لأنه لا يمكن ارتكاب جريمة الكترونية من خلال جهاز منفرد مهما كان نوع الجرم المقترف، ذلك أنه يمكن استخدام الكمبيوتر في الكثير من الجرائم لكن لا تكيف على أنها جريمة الكترونية، على غرار التزوير في المستندات والوثائق أو نشر المطبوعات، فمثل هذه الأفعال إذا ما تمت باستخدام الحاسوب فهي ترد إلى أصل الفعل ويمكن أن تكون جريمة معلوماتية وهي في الوقت ذاته تشكل جريمة الكترونية بمجرد ارسالها من جهاز الكتروني إلى جهاز آخر. (27)

وبمفهوم آخر فإن الجريمة السيبرانية لا تختلف عن الجريمة المعلوماتية في كثير من الأحوال باستثناء أنها تتم عن طريق جهازين الكترونيين أو أكثر يمكن الاتصال بينهما بواسطة شبكة انترنت محلية أو دولية أو بواسطة إحدى التقنيات الإلكترونية الحديثة [28] وعليه فإنه من الصعب القول بوجود حدود فاصلة بين الجريمة المعلوماتية والجريمة السيبرانية فكلاهما مرتبط بوجود جهاز الكتروني حديث طالما أنه في الوقت الحاضر لم يعد يتم استخدام جهاز الكمبيوتر فقط، إنما اتسع نطاق الاختراعات التكنولوجية إلى العديد من الأجهزة الالكترونية التي تسمح بتخزين المعلومات والاتصال فيما بينها كالمفكرات الالكترونية وأجهزة الهواتف النقالة الذكية وغيرها من الاختراعات الالكترونية التكنولوجية التي تشهدها الساحة الدولية يوميا. [29]

الفرع الثاني: خصائص الجرائم السيبرانية

يعتبر موضوع أو محل الجريمة السيبرانية من أهم الخصائص التي جعلتها تتميز عن غيرها من الجرائم، لكون المعلومات والبرامج محل الاعتداء تشكل النبضات الالكترونية التي تعمل وفقها الجريمة السيبرانية، وهو الأمر الذي يضعنا أمام ظاهرة إجرامية مستحدثة ذات طبيعة خاصة تقوم على أركان وأسس مستقلة، فالجريمة السيبرانية هي إفراز ونتاج لتقنية المعلومات واتساع نطاق تطبيقها في المجتمع أعطاها طابعا ولونا قانونيا خاصا وميزها بمجموعة من الخصائص التي تختلف كليا عن الجرائم التقليدية لحداثة أسسها وصعوبة إثباتها واكتشافها. [30]

كما تتميز بمجموعة من الخصائص منها ما يتعلق بطبيعة الجريمة والتي يترتب عنها صعوبة اكتشافها لقيامها على أسس رقمية غير ملموسة ما يصعب اكتشاف حتى الشخص مرتكب الجريمة او تحديد الشخص أو الأشخاص الذين يشكلون طرف الضحية في الجريمة من جهة، وصعوبة إثبات الجريمة السيبرانية خاصة فيما يتعلق بتحديد أركانها وبيان وصفها الواقعي والقانوني من جهة أخرى، والأكثر من كل هذا هو الطبيعة الخاصة للحدود التي يتم في نطاقها تنفيذ الجريمة السيبرانية والتي تجعلها من الجرائم العابرة للقرات والتي يمكن تنفيذها على مستوى دولي الأمر الذي يصعب معه متابعة المجرم خاصة في إطار الحدود والقواعد التي يحكمها القانون الدولي.

وسنقوم من خلال هذا الفرع بالتفصيل في مختلف خصائص الجريمة السيبرانية وذلك بالتطرق إلى تلك التي تقوم على صعوبة اكتشافها (**أولا**) ومن ثم الخصائص المبنية على صعوبة إثباتها (**ثانيا**).

أولا–صعوبة اكتشاف الجريمة السيبرانية: يذهب كثير من الفقه إلى أن الجريمة السيبرانية ما هي إلا أداة محايدة في حين أن مصدر الانتهاك الأساسي هو الإنسان ذاته، لكونه غالبا ما يهيئ الفرصة لاستغلالها، وبناءا عليه فإن جوهر الجريمة السيبرانية يرتبط بالجاني وشخصيته ودوافعه، أما فيما يخص المجني عليهم فغالبا ما يفضلون عدم إفشاء الجرم الواقع عليهم والمرتكب ضدهم، خاصة وأنها جرائم لا تحتاج إلى العنف ولا إلى استخدام وسائل الجريمة التقليدية، كما أنها لا تترك أي آثار ملموسة في الغالب، الأمر الذي يجعل من الصعب بما كان اكتشافها مع غياب آثارها المادية الخارجية، وتنقسم صعوبات اكتشاف الجريمة السيبرانية إلى قسمين منها ما يتعلق بالجاني أو المجرم مرتكب الجريمة السيبرانية ومنها ما تنصرف أو تتعلق بالمجني عليه أو الضحية المتضرر من هذه الجريمة. [31]

1-الصعوبات المتعلقة بالجاني: ثبت أن المجرم في جميع الحالات شخص طبيعي لكن المتغير أنه يهدف من خلال قيامه بالجريمة إلى تحقيق مصلحة شخصية له أو لحساب أحد الأشخاص المعنوية العامة أو الخاصة التي تعمل في مجال المعلوماتية وتستند في عملها على التكنولوجيا بهدف التعدي على الأنظمة المعلوماتية أو الإضرار بالغير، علاوة على كون العوامل التي تدفع لارتكاب هذا النوع من الجرائم ليس الهدف منها الإضرار بالأشخاص إنما وفي العادة المساس بالمؤسسات والإضرار بالأمن العام للبلاد، خاصة وأن المتورطين في هاته الجرائم لديهم قدر كبير من الذكاء والتفوق الذي يجعلهم يباشرون جرائمهم بدقة متناهية خشية افتضاح أمرهم وضبطهم. (32)

ويجمع الفقه في هذا الإطار أن الإجرام الالكتروني هو إجرام المتخصصين والذين هم في العادة الأشخاص الذين يتقلدون مناصب مهمة خاصة في المجال الالكتروني واستعمال التكنولوجيات الحديثة، وتتميز هذه الفئة من المجرمين بالذكاء مقارنة بالمجرم التقليدي الذي يميل إلى العنف في سبيل ارتكاب جرائمه، كما أن اغلب الجرائم السيبرانية ترتكب بدافع اللهو وإظهار التفوق في مجال استخدام الحاسب الآلي والتكنولوجيات الحديثة والتحكم في البرامج المخصصة لأمن نظم المعلوماتية، كما أن أغلبهم وخاصة منهم المتخصصين في مجال القرصنة يبادرون للقيام بهذه الجرائم بهدف المساعدة أكثر من كونهم يسعون لإلحاق الضرر. (33)

2-الصعوبات المتعلقة بالمجني عليهم: مما تتميز به الجريمة السيبرانية أن الضحية يستوي أن يكون شخصا طبيعيا أو معنويا طالما أن هذا الشخص يستند على استخدام الحاسب الآلي في ممارسة أنشطته الاقتصادية والاجتماعية أو حتى السياسية والعسكرية، وتكمن خصوصية الجريمة هنا في أنه من الصعب تحديد نطاق هؤلاء الضحايا على وجه الدقة وذلك راجع إلى أن هؤلاء لا يعلمون شيئا عن الجريمة إلا بعد وقوعها بالفعل وترتيبها لمختلف آثارها، كما أن ما يجعل المجني عليهم في الجريمة السيبرانية يختلفون عنهم في الجريمة التقليدية كونهم في غالب الأحيان لا يقومون بالإبلاغ عنها خاصة وأن أغلب الضحايا يكونون مؤسسات مالية أو مصارف أو شركات ضخمة، الامر الذي يجعل مجالس الإدارة يخشون الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، الأمر الذين يجعلهم يتجنبون الإبلاغ عن هذا النوع من الجرائم مخافة الكشف عن الاختراقات والانتهاكات الواقعة ضد أنظمتهم المعلوماتية. (34)

إن عدم الإبلاغ عن الجرائم السيبرانية من طرف الضحايا يعتبر من أهم الخصائص السلبية التي تتميز بها والتي تعتبر السبب الرئيسي في انتشارها الأمر الذي جعلها حافزا مهمّا للمجرمين الالكترونيين لتكرار ارتكابها، على الرغم من أن عدم الإبلاغ قد يساهم في عدم نشرها وتكرارها ومعرفة المجرمين خاصة الهواة، الأمر الذي من شأنه الحفاظ على مواطن الضعف في البرامج الأمنية للمؤسسات والنظام المعلوماتي لها، كما أن انتشار هذا التحفظ يرتبط في حد ذاته بمجموعة من الخصائص المتعلقة بطبيعة الجريمة في حد ذاتها والمتمثلة خاصة في: (35)

- ✓ اعتماد الجريمة السيبرانية على الفكر لا على العنف.
- ✓ اتسامها بالهدوء لكونها جريمة فنية لا تترك آثارا كالآثار المادية المترتبة على الجرائم التقليدية.

- ✓ وقوعها بمجرد إصدار أوامر للحاسوب الآلي ومن مسافات بعيدة قد تتعدى إقليم الدولة الواحدة.
- ✓ الغالب أن اكتشافها يتم عن طريق الصدفة ونادرا ما يتم اكتشافها لحظة وقوعها.
- ✓ قدرة المجرم الالكتروني على تدمير جميع أدلة ادانته لما يتمتع به من قدرات فنية عالية.

ثانيا–صعوبة إثبات الجريمة السيبرانية: إلى جانب كون الجريمة السيبرانية صعبة الاكتشاف، فإنه وحتى في حال اكتشافها والإبلاغ عنها فإنه من الصعب بما كان إثباتها والتحقيق فيها، ويعتبر إثبات الجريمة من أكثر وأهم الخصائص التي تميزها عن غيرها من الجرائم التقليدية خاصة لكونها لا تترك أي آثار مادية يمكن متابعتها والاستدلال بها على مرتكبها لكونها في غالب الأحيان أرقام وبيانات تتغير وتمحى من السجلات المخزنة في ذاكرة أجهزة الإعلام الآلي الأمر الذي يجعلها لا تترك أي أثر خارجي مرئي مما يصعب إثباتها[36] كما أنها تتميز بصعوبة التعامل بها من طرف جهات التحقيق الذين قد لا يتعاملون معها باحتراف خاصة في غياب محققين متخصصين في المجال المعلوماتي، والتعامل المحترف مع الأدلة الالكترونية، كما أن مما يعرقل الاثبات التسبب بدون قصد أو عن طريق الخطأ في إتلاف الأدلة الالكترونية أو تدميرها كما في حالة محو البيانات الموجودة على الأسطوانات الصلبة أو المرنة، أو تجاهل المحققين لبعض الأدلة الالكترونية تماما ظنا منهم بعدم أهميتها أو خدمتها لمجرى التحقيق [37] وعموما يمكن حصر أهم أسباب صعوبة إثبات الجريمة السيبرانية في:

1–من حيث أركان الجريمة السيبرانية: تعتبر أركانها من أهم الأسباب المؤدية إلى صعوبة إثباتها ويمكن التفصيل في أوجه هذه الصعوبة من حيث: [38]

أ–الركن الشرعي: مع التقدم التكنولوجي الذي يشهده العالم ظهرت العديد من الجرائم السيبرانية التي لا ينطبق عليها أي وصف قانوني الأمر الذي وضع التشريعات الوطنية أمام ضرورة أخذ هذا التطور بعين الاعتبار والعمل على تطوير الوسائل اللازمة وعلى راسها قواعد التجريم لردع هذه الجرائم المستحدثة، خاصة مع ثبوت أنه وفي العديد من الدول تبقى الجهود ذات بعد فردي وتتم عن طريق التوعية ووضع بعض أنواع الحماية والشفرات الالكترونية لردع أي اختراق ومحاولة الاعتداء، الأمر الذي يستوجب العمل على التحديد الواضح لهذه الجرائم وبيان التجريم القانوني لها بصورة تميزها عن غيرها وتحد من نطاق اتساعها وانتشارها.

ب–الركن المادي: يستوجب في الفعل أو السلوك المجرم بموجب القانون أن يكون ملامسا لأرض الواقع حتى وإن كان لا يرتب أي آثار مادية ملموسة حتى يمكن التحقق منه وإثباته، وقد أكد الفقه أنه لا يمكن الحديث عن الركن المادي في الجرائم السيبرانية التي تكون وسيلة ارتكابها الكترونية، حيث لا يمكن حصرها تحت تكييف واحد، والثابت أن الأمر الذي يثير صعوبة هو الشكل المستحدث للجريمة الالكترونية والتي يكون موضوعها في الغالب المال المعلوماتي المعنوي على غرار إساءة استخدام البريد الالكتروني عن طريق الرسائل المفخخة وقرصنة حقوق الملكية الفكرية والولوج غير المشروع وتعطيل الشبكات عن طريق الفيروسات التي تقوم بتدمير المعلومات أو النظام المعلوماتي كليا أو جزئيا، أو تحريف المعطيات أو محوها بشكل كلي أو جزئي. [39]

كما ثبت أيضا أنه مما يزيد من صعوبة إثباتها هو عدم مساعدة المجني عليه للسلطات في حال اكتشاف الجريمة، خاصة وأن أغلب القواعد الجنائية غير كافية لوجود صعوبات أخرى تتبلور من صعوبة البحث عن الأدلة وجمعها ومشكلة قبولها إن وجدت ومدى مصداقيتها وحجيتها في إثبات الوقائع، ما يستوجب التحيين والتطوير الدائم والمستمر للمنظومة القانونية واستحداث نصوص جديدة بشكل دوري تتلاءم مع المستجدات التي تفرضها التكنولوجيا الحديثة، ما يجعل من الأدلة التقليدية غير ملائمة لاعتمادها في إطار الجريمة السيبرانية ولزوم البحث الدائم عن أدلة جديدة وحديثة. (40)

ج–الركن المعنوي: مع توسع وانتشار استخدام التكنولوجيات الحديثة في ارتكاب الجريمة تغيرت صورة المجرم ومستواه وأصبح المجرم الالكتروني يتمتع بقدر كبير من الذكاء والفطنة ومستوى عال من التعليم والتخصص فالجرائم السيبرانية كما سبق ووضحنا أصبحت تستوجب للقيام بها توافر قدر كبير من المعرفة في مجال تقنية المعلومات والحاسوب والتحكم في التكنولوجيات الحديثة.

ومن الأمور التي أكد الفقه الجنائي على ضرورة إعادة النظر فيها حقيقة كونها لا تقع غالبا إلا بصورة عمدية يسبقها التفكير في الحصول على المعلومة أو اختراق الشبكة المعلوماتية، فالأصل في الجرائم هو العمدية إلا ما استثني منها بنص القانون وهو الأمر الذي يستوجب على المشرع إعادة النظر في إرادة ارتكاب السلوك وتحقق النتيجة، حيث يكتفي في هذه الحالة بتوافر القصد الجنائي العام بصورتيه "العلم والإرادة" كالدخول إلى الأنظمة المعلوماتية وتدمير المعلومات التي كانت عليها من أجل طمس الأدلة، كما أن المشرع وفي هذه الصورة من الجرائم أمام حتمية إضافة قصد جنائي خاص إلى القصد الجنائي العام كضرورة توافر نية المجرم في تملك الأموال المتحصل عليها من سرقة بطاقات الائتمان وتحويلها إلى حسابه الخاص، وتجدر الإشارة في هذا المقام أن هذا الأمر لا يعني أن الجريمة السيبرانية لا تتحقق بطريقة غير عمدية عن طريق الخطأ أو الصدفة، على نحو تدمير أجهزة مؤسسة ما نتيجة إفراط الموظف في استخدام أجهزة المؤسسة في عمليات لحسابه الخاص معتمدا على قدراته ومهاراته الوظيفية في هذا المجال، ومما يثار في هذا المجال أيضا مسألة تجاوز إطار التصريح حيث أن إثبات القصد الجنائي للفاعل الذي يتمتع بتصريح محدد صعب خاصة مع حقيقة أن أنظمة الحاسبات مفتوحة على بعضها البعض. (41)

وما تجدر الإشارة إليه أن النظام المعلوماتي في الجريمة السيبرانية ولأنه لا يتكون من طبيعة واحدة بل يتكون من عدة عناصر مادية ومعنوية فإن هذا الأمر يفتح إمكانية أن يكون موضوعها ذو طبيعتين مختلفتين، كما هو الحال بالنسبة للمعلومات التي قد تكون في حالة انتقال أو موجودة في ذاكرة النظام المعلوماتي وهنا تتخذ الصورة غير المادية كما قد تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة الكترونية، وفي حالة ثالثة قد تكون مصنفا أدبيا أو علميا مخزن بصورة الكترونية وهو الأمر الذي يثير في العادة وفي إطار معالجة هذه الجرائم مشكلة تعدد الأوصاف القانونية لمحل الجريمة. (42)

2-من حيث الوصف القانوني: تشكل صعوبة معرفة المجرم الالكتروني سببا رئيسيا لصعوبة الإثبات خاصة مع حقيقة الطابع الدولي للجريمة الالكترونية وما تثيره من مشـاكل وصـعوبات في الإثبات والتحقيق، علاوة على تصـادم هذه الحقائق مع واقع صـعوبة توقيف المجرم وتنفيذ العقاب عليه في حال ما تم ثبوت عدم انتمائه لنفس الدولة التي تم ضدها أو ضد مؤسساتها تنفيذه الجريمة خاصة وأن الأضرار المترتبة عن الجرائم السيبرانية عادة ما تكون فادحة وجسيمة، ومن الخصائص التي تتميز بها الجريمة السيبرانية من حيث وصفها يمكن حصر:

أ-جريمة عابرة للحدود: من أهم خصـائص الجريمة السـيبرانية أنها عابرة للحدود فعلى الرغم من إيجابيات تكنولوجيا الاعلام والاتصال وشبكة الانترنت إلا أنها في المقابل شكلت عنصرا أساسيا لظهور وانتشار الجرائم السيبرانية في جميع دول العالم التي أصبحت تتأثر يوميا بصورهاما ساهم في زيادة السرعة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي تفصل المجرم الالكتروني عن المعلومات والأموال محل جريمته [43] كما أن طابعها الدولي يثير العديد من الإشكاليات والصعوبات لا سيما تحديد المحكمة المختصة دوليا بالمنازعات الناشئة والقانون الواجب التطبيق عليها، وأدلة الإثبات وقبولها أمام قضاء دولة أخرى، الأمر الذي ترتب عنه تأكيد ضرورة مواجهة هذه الجرائم مواجهة فعالة خاصة مع تزايد خطورتها على أمن الدول واستقرارها ما يستوجب العمل علاوة على سن نصوص تجريم وطنية والمعاقبة عليها، ضرورة فتح مجال التعاون الدولي لمواجهة المشاكل المستجدة خاصة تلك المتعلقة بمكان وقوع الجريمة واختصاص المحاكم بها وجمع المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد صورها وقواعد تسليم المجرمين وإيجاد حلول لمشكلاتها الأساسية. [44]

ب-صعوبة تنفيذ العقاب على مرتكبيها: يترتب عن كونها جريمة عابرة للحدود احتمال ارتكاب المجرم لها في دولة غير التي ينتمي لها أو التي يقيم بها، ما ينتج عنه عدم القدرة على منع حدوثها وحتى مع احتمال صـعوبة تحديد ومعرفة الجاني فإنه في حال التعرف عليه والتوصل إليه يصعب توقيع العقاب عليه لوجود العديد من المعوقات وعلى رأسها قلة التشريعات المواجهة لهذا النوع من الجرائم، إضافة إلى اختلاف صور تجريم الجرائم السيبرانية من دولة إلى أخرى فغالبا ما نجد أفعالا غير مشروعة ولا ينطبق عليها أي وصف في قانون العقوبات خصوصا إذا نظرنا إلى الأمر من زاوية القيود التي تقيد القاضي الجنائي الذي ينطلق دائما ويتقيد بقاعدة "**لا عقوبة ولا جريمة إلا بنص**" علاوة على حضر القياس في مجال الجرائم ومبدأ التفسير الضيق للنصوص. [45]

إضافة إلى ذلك فإن الأثر الرادع للقانون الجنائي نادرا ما يجد تأثيره في الجرائم السيبرانية على عكس ما هو عليه الحال في الجرائم التقليدية، خاصة وأنها نتاج حسابات عقلية يضع بموجبها المجرم في حسابه عقوبة الفعل الذي يقدم عليه جنبا إلى جنب مع ما يعود عليه من فائدة [46] وبناءا عليه يتضح بأن الفرق بين الجريمة التقليدية والجريمة السيبرانية يكمن في كون هذه الأخيرة ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي وفي معظم الحالات يدخل ارتكاب الجريمة ضمن نطاق المعالجة الالكترونية للبيانات وتجميعها وتجهيزها لإدخالها إلى الحاسب الآلي بغرض الحصول على معلومات، إلى جانب كونها تدخل ضمن مجال المعالجة الآلية، حيث يتم التعامل مع مفردات

جديدة كالبرامج والبيانات التي تشكل محلا للاعتداء أو تستخدم كوسيلة للاعتداء كما أن مجال الاثبات سابقا كان ينحصر في المستند الورقي لكن الأمر تغير مع تغير المستندات وتحولها إلى تسجيلات الكترونية. (47)

المطلب الثاني: أنواع الجرائم السيبرانية المرتكبة ضد الأطفال وصورها

من المعروف أن الغاية من وضع قواعد القانون الجنائي في إطار الأحكام العامة هو حماية المجتمع وأفراده ومصالحهم من أي اعتداء وانتهاك، الأمر الذي جعل من اختلاف الجرائم عن بعضها واختلاف تصنيفها وصورها ومظاهرها تنطلق من هذه الأهمية النابعة عن صفتها اعتداء على الفرد والمجتمع وبقدر الضرر الذي يلحق بهما أو بقدر الخطر الذي يشكله الفاعل على المجتمع والذي من شأنه تهديد كيانه ونظامه والأسس التي تقوم عليها مؤسساته وبقدر أهمية الاعتداء يتم تصنيف الجريمة وتكييف العقوبة المقررة لها.

ولما أصبح من الثابت خطورة الجريمة السيبرانية على الأفراد والمؤسسات، هذه الخطورة التي تتزايد مع تطور تكنولوجيات الإعلام والاتصال وتزايد استخداماتها ليس في الأطر القانونية بل وحتى في الأطر القانونية التي ترتب عنها ظهور صور جديدة من الانتهاكات على حياة الأفراد وأمنهم واستقرار المؤسسات وديمومتها فإن الأمر أصبح يفرض على جميع تشريعات العالم كما هو الحال عليه في إطار الجرائم التقليدية تغطية هذه الانتهاكات عن طريق تجريم أي أفعال غير قانونية يترتب عنها المساس بأمن وسلامة الأفراد والمؤسسات وهو الأمر الذي أصبح يخلق كل يوم جريمة جديدة من الجرائم السيبرانية والتي أصبحت تتخذ العديد من الصور والمظاهر أهمها وأخطرها تلك التي أصبحت تستهدف وتهدد فئة مهمة جدا في المجتمع وهي فئة الأطفال، الذين أصبحوا يشكلون قاعدة مهمة للمجرمين الإلكترونين الساعين إلى استحداث طرق إجرامية حديثة تمس هذه الفئة بطريقة مباشرة وغير مباشرة.

ولكون الجرائم السيبرانية واسعة ومتعددة وكل يوم تظهر صورة مطورة منها، فإننا سنحاول من خلال هذا المطلب التطرق إلى أكثر هذه الجرائم خطورة وانتشارا، والتي أصبحت اليوم تشكل تهديدا حقيقيا على سلامة الطفل الجسدية والعقلية والنفسية وذلك من خلال التعرض لجرائم الاستغلال الجنسي للأطفال عبر الانترنت (**الفرع الأول**) ومن ثم الحديث إلى جرائم التجنيد الرقمي للأطفال ضمن منظمات الإرهاب الإلكتروني (**الفرع الثاني**) دون أن نغفل الحديث عن الجرائم المرتكبة عن طريق الألعاب الإلكترونية على اعتبارها أخطر الجرائم التي مست ولا زالت تمس فئة كبيرة وواسعة من الأطفال.

الفرع الأول: الاستغلال الجنسي للأطفال عبر الانترنت

وهي الجرائم التي تتعلق باستغلال فئة الأطفال والشباب القاصر في أعمال جنسية، وتشمل الرسوم والصور والكتابات والأفلام والإشارات وأي أعمال اباحية يشارك فيها القاصر أو الطفل، وتتعلق إما باستغلاله في مواد اباحية، أو إنتاج مواد اباحية للقاصرين بهدف بثها بواسطة الأنظمة المعلوماتية، وتعتبر جرائم الاستغلال الجنسي للأطفال من أخطر الجرائم وأكثرها انتشارا على مستوى العالم، وقد تطورت بظهور تكنولوجيات الإعلام والاتصال

من صورتها التقليدية إلى صورة إلكترونية، جعلت النصوص القانونية والتنظيمية تعمل على مكافحتها والوقاية منها بكافة الصور والأشكال، فعلى المستوى الدولي تعتبر اتفاقية بودابست لسنة 2001 المتعلقة **بالجريمة الإلكترونية** [48]من أول النصوص القانونية الدولية التي جرمت هذا النوع من الجرائم حيث نصت في مادتها التاسعة (09) أنه فيما يتعلق بـــ **"الجرائم ذات الصلة بمواد إباحية عن الأطفال:**

1-تعتمد كل دولة طرف ما يلزم من تدابير تشريعية أو غيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير حق:

أ-إنتاج مواد اباحية عن الأطفال بغرض توزيعها عبر نظام الكمبيوتر.

ب-عرض مواد اباحية عن الأطفال أو إتاحتها عبر نظام الكمبيوتر.

ج-توزيع مواد اباحية عن الأطفال أو نقلها عبر نظام الكمبيوتر.

د-الحصول على مواد إباحية عن الأطفال عبر نظام الكمبيوتر لصالح الشخص ذاته أو لفائدة الغير.

هـ-حيازة مواد اباحية عن الأطفال داخل نظام الكمبيوتر أو على دعامة لتخزين بيانات الكمبيوتر.

2-لغرض الفقرة أعلاه، تشـــمل عبارة "مواد اباحية عن الأطفال" المواد الإباحية التي تعرض بشـــكل مرئي:

أ-قاصر وهو يمارس سلوكا جنسيا واضحا.

ب-شخص يبدو قاصرا وهو يمارس سلوكا جنسيا واضحا.

ج-صور واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا واضحا".

وتتخذ جرائم الاستغلال الجنسي للأطفال عبر الانترنت صورتين أساسيتين

****جرائم الاستغلال الجنسي الالكتروني التي يكون فيها الطفل متلقيا****

ما يميز جرائم الاستغلال الجنسي عبر الانترنت عن الصورة التقليدية للجريمة، أن هذه الأخيرة تقع عادة على جسد الضحية بهدف إشباع رغبة الجاني الجنسية أو لأي أسباب أخرى، في حين أنها في صورتها الرقمية الإلكترونية تندرج ضمن خانة الجرائم الجنسية غير المباشرة، والتي تهدف إلى استغلال جسد الضحية بتحريضه على الدعارة والفســـق بطريقة غير مباشـــرة أو مباشـــرة، وبهدف تحقيق هدف مادي، أو تحقيق أهداف أخرى غير مادية تكون

عادة مرضيّة، وهي أخطر بكثير من الجريمة في صورتها التقليدية، لأنها غالبا ما تسعى لجعل الضحية بضاعة ووسيلة للثراء، علاوة على كونها تهدف إلى النيل من الضحية الإساءة إلى سمعتها والدفع بها إلى الانحراف، وتتخذ جرائم الاستغلال الجنسي التي يكون فيها الطفل متلقيا بدورها عدة صور أهمها: (49)

- ✓ **عرض الصور والأفلام والمحادثات المخلة بالأخلاق والمنافية للآداب العامة:** وتعرف هذه الصورة من الجريمة في العالم الرقمي بتجارة الجنس الخاص بالأحداث، حيث أن نشر الصور والفيديوهات المتضمنة أفعالا منحرفة مخلة بالآداب العامة على الانترنت تعتبر جريمة قائمة مكتملة الأركان وتتحقق من خلال العديد من الأفعال المادية التي تتجسد في عرض أو نشر أو توزيع أي صور أو أقوال أو أفعال فاحشة وفاضحة، وتقوم من خلال أيضا إنشاء مواقع جنسية على شبكة الانترنت والترويج لها والعمل على استقطاب الزائرين لها، خاصة إذا كانت هذه الأفعال ممارسة على الأطفال أو موجهة لهم، وتتزايد خطورتها في كونها تعمل على استقطاب الأطفال وادخالهم إلى هذه المواقع حتى دون علمهم، من خلال عمل الكثير من المواقع الإباحية على نشر عناوين الكترونية على المواقع التي تجذب اهتمام الأطفال والتي بمجرد أن يقوم الطفل من باب الفضول بالنقر عليها حتى يجد نفسه مباشرة ضمن هذه المواقع الجنسية. (50)
- ✓ **تحريض الأطفال على ارتكاب الأعمال الإباحية عبر الانترنت:** يعتبر التحريض على ارتكاب الأعمال الإباحية الصورة الثانية من صور الاستغلال الجنسي للأطفال عبر الانترنت، وتقوم الجريمة من الناحية القانونية من خلال تنظيم شخص أو مجموعة لبرامج منظمة يتم من خلالها تقديم عروض لأفعال مخلة بالحياء وعلاقات جنسية يشارك الطفل فيها أو يطلب منه القيام بتقليدها مع تصوير نفسه وارسال الفيديو المصور للجهة التي يتواصل معها، ويتم في هذه الحالة تحميل هذه الفيديوهات على أقراص الحاسوب وتوزيعها على مواقع الانترنت وبين فئة واسعة من محترفي هذا المجال، وتعتبر هذه الصورة من أخطر صور الاستغلال الجنسي للأطفال عبر الانترنت لأنها تدار م طرف عصابات محترفة وتعتبر تجارة غير قانونية مغرية جدا للكثير من المجرمين الرقميين، لما تدره من أرباح كبيرة الأمر الذي جعل التعامل بها يتسع كثيرا وتتزايد معه الخطورة على الأطفال وعائلاتهم. (51)

جرائم الاستغلال الجنسي الالكتروني التي يكون فيها الطفل موضوع الاستغلال

تتعالى اليوم الكثير من الأصوات التي تنادي بضرورة العمل الجاد على مكافحة جرائم الاستغلال الجنسي للأطفال على الانترنت، وذلك بعد أن أصبحت العديد من الجهات الرسمية وغير الرسمية تكشف الأرقام الخطيرة للمجرمين والضحايا أطراف هذه الصورة من الجرائم السيبرانية، التي أصبحت تعمل استنادا إلى مواقع الكترونية متخصصة في نشر صور جنسية فاضحة للأطفال، كما تعمل على توفير معلومات سرية عن بيوت الدعارة المتخصصة في المتاجرة الجنسية بالأطفال، وحتى شبكات خطوط الكترونية إجرامية توفر خدمات الاستغلال

الجنسي للأطفال عبر المكالمات الصوتية المباشرة أو المسجلة، وتقوم مواد الاستغلال الجنسي للأطفال عادة على التصوير المرئي للطفل أثناء قيامه ومشاركته في أنشطة جنسية صريحة أو عرض أجزاء حساسة من جسمه بطريقة منحرفة و بإيحاءات جنسية، بغرض توزيع هذه المواد الرقمية الالكترونية أ اتاحة توزيعها ونشرها، وحتى استغلال صور عادية للأطفال وتركيبها بطريقة تحمل ايحاءات جنسية وانتهاكات لحقوق الطفل الإنسانية. (52)

الفرع الثاني: التجنيد الإلكتروني ضمن المنظمات الإرهابية

يعتبر الإرهاب الالكتروني من أحدث وأخطر صور الجرائم السيبرانية، وكانت بدايات ظهوره واستخدامه في فترة الثمانينات على يد الباحثين في مجال الأمن السيبراني حيث تم تعريفه بأنه "**هجمات الكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، ويتوجب أن تكون هذه الهجمات ذات أثر مدمر وتخريبي ومكافئ للأعمال الإرهابية التي تحصل في الواقع**" (53)ويعتبر الأطفال أكثر فئة معرضة لمخاطر التهديدات الإلكترونية عامة وللإرهاب الالكتروني خاصة لوقوعهم ضحية اختراق الحسابات الشخصية والتتبع والاحتيال وسرقة البيانات من أجهزتهم الشخصية، خاصة وأن الأطفال اليوم أصبحوا يشكلون أكثر شرائح المجتمع استخداما للإنترنت ولتكنولوجيات الإعلام والاستعمال المفرط لمواقع التواصل الاجتماعي، الأمر الذي جعلهم فريسة سهلة لمختلف المنظمات الإرهابية الناشطة في المجال الرقمي، التي يسعى قادتها إلى ضخ الأفكار والمعتقدات وتشكيل أقنعة ذات طابع ثقافي وفكري تخفي في طياتها أفكارا إرهابية تطرفية. (54)

وما يلاحظ على توجهات التجنيد الاجباري للأطفال ضمن المنظمات الإرهابية الناشطة في العالم الرقمي أن العديد من التنظيمات الإرهابية المسلحة تعمل على بناء شبكة تجنيد الأطفال من خلال السعي للاتصال بهم بطرق عديدة والعمل على تضليلهم واقناعهم بأفكارها التطرفية، وحتى محاولة غسل أدمغة الكثير من الأطفال عن طريق ألعاب الكترونية مخصصة لنشر الأفكار والقناعات الإرهابية لدى الطفل من خلال مختلف مراحل هذه الألعاب الالكترونية التحريضية، كما تعتمد المنظمات الإرهابية عدة أساليب في تجنيد الأطفال الكترونيا، كالإغواء والإغراء من خلال زرع الرغبة لدى الأطفال في التوجه نحو الأعمال العدائية، والعمل على التخطيط للإبعاد والإكراه على التجنيد، وحصرهم في المعسكرات الخاصة بما يسمونه بالأشبال بمناطق النفوذ، وغيرها من الإجراءات المتبعة في عمليات التجنيد الذي يبدأ بطريقة إلكترونية في العالم الافتراضي لينتقل إلى العالم الواقعي. (55)

الفرع الثالث: الجرائم المرتبطة بالألعاب الإلكترونية

يعتبر اللعب من الحقوق المكفولة للطفل، حيث كرست أغلب النصوص القانونية الوطنية والدولية هذا الحق وعملت على بذل كافة الوسائل اللازمة لضمان ممارسته، حيث نصت المادة 31 من اتفاقية حقوق الطفل لسنة 1989 في فقرتها الأولى أنه "**تعترف الدول الأطراف بحق الطفل في الراحة ووقت الفراغ، ومزاولة الألعاب وأنشطة الاستجمام المناسبة لسنه والمشاركة بحرية في الحياة الثقافية وفي الفنون**" إلا أن ما يسجل على هذا النص وعلى الاتفاقية بشكل عام أنها أكدت على حق الطفل في اللعب لكنها أغفلت تحديد الضوابط والأطر

القانونية التي يمارس ضـــمنها هذا الحق، الأمر الذي يطرح ســـؤالا جوهريا حول **إمكانية الطفل في التمييز بين الألعاب الضارة والمفيدة؟** خاصة وأن التطور التكنولوجي اليوم أصبح يطرح الكثير من الفرضيات المتعلقة بمخاطر هذه التطورات التكنولوجية الأمر الذي أصـــبح يفرض إلحاق تعديل بالاتفاقية أو العمل على اســـتحداث اتفاقي جديدة تعالج مشـكلة مخاطر الألعاب التكنولوجية على الطفل. (56) وتعرف الألعاب الإلكترونية بأنها "**نزاع مفتعل محكوم بقواعد محددة من طرف مخترعي هذه الألعاب، بشكل يؤدي إلى نتائج قابلة للقياس، ويطلق على لعبة صفة الإلكترونية في حال توافرها على هيئة رقمية، ويتم تشغيلها عادة عبر منصة رقمية من الحاسوب المتصل بالإنترنت أو أي جهاز رقمي آخر**" (57)وعلى الرغم من كونها في الأصـــل إيجابية لأنها تنمي القدرات الذهنية والمعرفية للطفل إلا أنها اكتسبت بعدا سلبيا وأصبحت لها آثار خطيرة يمكن حصرها في: (58)

- ✓ **المخاطر الصـــحية والبدنية:** أثبتت الدراســـات التي أقيمت على فئة كبيرة من الأطفال أن للألعاب الالكترونية الكثير من الأضـرار الصـحية التي ترتب عنها مؤخرا ظهور مجموعة جديدة من الإصـابات المتعلقة بالجهاز العظمي والعضـلي نتيجة الحركات السـريعة وغير المنتظمة التي تفرضها بعض قواعد الألعاب، علاوة على أن الجلوس أمام الحاسوب لساعات طويلة من شأنه ترتيب آثار صحية سلبية للطفل على المدى المتوسط والبعيد.
- ✓ **المخاطر النفســية والاجتماعية:** أصـبح المختصـون في مجال علم النفس يدقون ناقوس الخطر بسبب الآثار السلبية التي تخلفها الألعاب الالكترونية على المجتمع عامة وعلى الأطفال خاصة، حيث ارتبط انتشـار نوع معين من الألعاب بتزايد السـلوك المنحرف وانتشـار العنف، وارتفاع معدل جرائم خطيرة كالقتل الاغتصاب والاعتداءات العنيفة والسلوكيات العدوانية والاستمتاع بالممارســات المنحرفة كالتعذيب، ما ترتب عنه زرع روح الإجرام وانتشــار ظاهرة الانتحار التي يعود سببها تعرض الأطفال لمضامين وسائل الإعلام والألعاب الإلكترونية السلبية، والتي تقدم وتروج كنوع من أنواع التسلية والمتعة. (59)

المحور الثاني: الآليات القانونية لمكافحة الجرائم السيبرانية ضد الأطفال

إن تطور الجريمة السيبرانية ترتب عنه ظهور أوجه ضعف وقصور في وسائل مكافحة الجريمة التقليدية والوقاية منها، عن تغطية أغلب الجرائم السيبرانية والتصدي لها، خاصة وأن طبيعتها التي انتقلت من الواقع المادي الملموس إلى الواقع الافتراضـي الغير ملموس ترتب عنه حتمية العمل على اسـتحداث منظومة قانونية حديثة يتم من خلالها بذل آليات تتماشى مع طبيعتها وتعمل على مكافحتها والحد من انتشار آثارها على الأطفال.

من هذا المنطلق عملت الجزائر انطلاقا من واقع التفشي السريع والخطير للجريمة السيبرانية الالكترونية في المجتمع وفي إطار سياسات وطنية ودولية واسعة على بذل كافة الآليات القانونية لمكافحة الجريمة السيبرانية وذلك من خلال استحداث أجهزة ووحدات قانونية تم تكليفها بصورة خاصة ومباشرة بمتابعة ورصد هذه الجرائم والتي تم تقسيمها على مستوى وطني وتكليفها بمهام وإعطائها صلاحيات ذات بعد وطني، جهوي ومحلي وتزويدها بكافة الوسائل المادية، البشرية والتقنية اللازمة لتأدية مهامها وفق ما هو مسطر لها ومأمول منها، هذا وحرص المشرع على تعزيز الجانب القانوني بعقوبات صارمة تفوق بكثير العقوبات المبذولة في إطار الجرائم التقليدية وذلك إقرارا بمدى خطورة هذه الجرائم وحرصا على ضمان أكبر قدر من الوقاية ضدها، وسنقوم من خلال هذا المحور برصد مختلف الآليات القانونية التي بذلها المشرع الجزائري في إطار سياسة مكافحة الجرائم السيبرانية الواقعة على الأطفال والوقاية منها وذلك من خلال تحديد الهيئات المكلفة بمكافحة هذه الجرائم (**المطلب الأول**) ثمبيانالوحدات التابعة للجهات الأمنية المتخصصة في مكافحة الجريمة السيبرانية (**المطلب الثاني**).

المطلب الأول: الجهات المكلفة بمكافحة الجرائم السيبرانية الواقعة على الأطفال

خلقت الجريمة السيبرانية تحديات كبرى أمام الدول وعلى اعتبار أنها حديثة الظهور فإن هذا يجعلها ذات خصوصية تميزها عن الجرائم التقليدية ما جعل الأنظمة القانونية تصطدم مع حقيقة قصور الجهات الأمنية التقليدية المكلفة بمكافحة الجريمة عن التصدي للجريمة الالكترونية وعدم القدرة على تغطية مختلف جوانبها الأمر الذي جعلها تتفشى بصورة كبيرة وسريعة وترتب معه ضرورة العمل على استحداث جهات وأجهزة حديثة تتناسب مهامها والوسائل الموكلة لها مع خصوصية الجريمة السيبرانية وتساعد على التصدي لها وفق ما هو واجب ومأمول.

إن الجزائر ولحداثة توجهها الالكتروني وجدت نفسها في السنوات الأخيرة أمام تفشي كبير للجريمة الالكترونية وغياب واضح للأجهزة والجهات الأمنية القادرة على مواجهة هذا الإجرام الجديد الذي أصبح يثبت مدى خطورته خاصة مع حقيقة كون الجريمة السيبرانية جريمة عابرة للحدود وهو الأمر الذي جعل الدولة بمختلف مؤسسات تقف أمام ضرورة مواجهة مجرمين ليس على المستوى الوطني فحسب بل والعمل على بذل جهود واحتياطات من أي جرائم الكترونية ذات بعد دولي أو ممارسة من طرف مجرمين دوليين قد تتعدى خطورتهم بكثير خطورة المجرمين في إطار الجرائم التقليدية. (60)

من هذا المنطلق توجهت الدولة وفي خطى جدية نحو محاربة الجريمة السيبرانية بمختلف صورها وأبعادها على استحداث العديد من الهيئات والأجهزة القانونية المتخصصة في متابعتها والعمل على مكافحتها والوقاية منها، ليظهر دورها في مكافحة الجرائم الواقعة على الأطفال في العالم الرقمي إلى جانب هيئات مكلفة بحماية الطفل، مع ضرورة العمل بمساعدة مختلف الجهات المسؤولة في الدولة على مكافحة كل صور الخطر التي من شأنها المساس بهذه الفئة المهمة من المجتمع من كل انتهاكات ذات مصدر رقمي الكتروني، وتم في سبيل تحقيق هذه الأهداف الحرص على تزويد هذه الهيئات الوطنية بكافة الأطر والصلاحيات القانونية التي تسمح بأدائها لمهامها على الوجه

المطلوب، وذلك انطلاقا من تطوير وعصـــرنة الأجهزة الأمنية التقليدية وتزويدها بوحدات خاصـــة مكلفة بمحاربة الجريمة السـيبرانية بما يتناسـب وخصـوصـية وخطورة هذه الأخيرة إلى جانب كل من الهيئة الوطنية المتخصـصـة في مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والوقاية منها والهيئة الوطنية لحماية وترقية الطفولة، وهو الأمر الذي سـنفصـل فيه من خلال هذا المطلب وذلك بدراسـة كافة الأسـس القانونية لهذه الهيئات والجهات القانونية المكلفة بمكافحة الجريمة السيبرانية بصفة عامة وتلك الواقعة على الأطفال بصفة خاصة.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال من أهم الجهات القانونية المكلفة بمكافحة الجرائم السـيبرانية والوقاية منها والتي تم اسـتحداثها لهذا الغرض بموجب المادة الثالثة (13) من القانون 09-04 التي نصـت أنه "**تنشـأ هيئة وطنية للوقاية من الجرائم المتصـلة بتكنولوجيات الإعلام والاتصـال ومكافحته**" وأحال تحديد تشكيلتها وتنظيمها وكيفيات سيرها إلى التنظيم ليصدر بناءا على مقتضيات هذه المادة المرسـوم الرئاسـي 15-261 المحدد لتشـكيلتها ومختلف الأحكام المتعلقة بها [61] وتم منحها صـلاحيات واسـعة وهامة في هذا المجال، كما تم تحديد تشكيلتها وتنظيمها ومختلف المهام الموكلة لها في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ووضح كيفيات سيرها مختلف الأحكام المالية والقانونية المتعلقة بها.

وقد نص المشـرع أن الهيئة الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيات الإعلام والاتصـال ومكافحتها هي "**سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى الوزير المكلف بالعدل**" [62]وتم تحديد مقرها بالجزائر العاصـمة، وسـنقوم ببيان المهام الموكلة إليها في مجال مكافحة الجرائم السـيبرانية **(أولا)** وكيفيات سيرها **(ثانيا)**.

أولا–مهام الهيئة: على اعتبار أنالهيئة الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيات الاعلام والاتصـال هي هيئة متخصـصـة فقد تم تكليفها في إطار عملها على الوقاية من الجرائم السيبرانية الإلكترونية بمختلف صورها وذلك بموجب جملة من المهام الأسـاسـية التي تمارسـها تحت رقابة السـلطة القضـائية [63] ووفق ما يقتضـيه القانون والتشريع المعمول بهما وعلى الخصوص قانون الإجراءات الجزائية [64] والقانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال [65] وتتمثل هذه المهام في: [66]

- ✓ **اقتراح عناصـر السـياسـة الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيات الاعلام والاتصـال ومكافحتها.**
- ✓ **تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.**
- ✓ **مساعدة السلطات القضائية ومصالح الشرطة في مجال مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصـــال بما في ذلك من خلال جمع المعلومات والتزويد بها من خلال الخبرات القضائية.**

- ✓ **ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص.**
- ✓ **تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.**
- ✓ **السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.**
- ✓ **تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال.**
- ✓ **المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الاعلام والاتصال.**
- ✓ **المساهمة في تحديث المعايير القانونية في مجال اختصاصها.**

ثانيا–كيفيات سير الهيئة: ضمانا لقيام الهيئة بالمهام الموكلة إليها على أكمل وجه وفق ما هو مقرر محدد قانونا عمل المشرع على ضبط كيفيات سيرها وذلك ببيان مختلف الإجراءات التي تتبعها في سبيل القيام بهذه المهام ونص في هذا الإطار على أن:

- ✓ **تجتمع الهيئة المديرة بناءا على استدعاء من رئيسها أو بناءا على طلب أحد أعضائها.**
- ✓ **إعداد نظامها الداخلي والمصادقة عليه.** (67)
- ✓ **إمكانية الاستعانة بأي خبير أو أي شخص يمكن أن يعينها في أعمالها.** (68)
- ✓ **طلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضرورية لإنجاز المهام المسندة إليها قانونا.** (69)
- ✓ **مراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية وتحت سلطة قاض مختص وذلك قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، ووفقا لما تقتضيه أحكام القانون 04-09.** (70)
- ✓ **إمكانية وضع وحدة مراقبة واحدة أو أكثر وتزويدها بالوسائل والتجهيزات التقنية لتنفيذ عملية مراقبة الاتصالات الالكترونية، وتتكون الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط واحد من الشرطة القضائية أو أكثر ينتمي للهيئة، مع الزامية امتثال الوحدة في عملها لأحكام التشريع المعمول به وشروط الرخصة المسلمة من الشرطة القضائية.** (71)

✓ **إمكانية طلب مساعدة موظفين مختصين من الوزارات المعنية في مجال تكنولوجيات الاعلام والاتصال.** (72)

ولحساسية المهام الموكلة لها ومجال اختصاصها فقد أوجب المشرع وتحت طائلة العقوبات الجزائية القانونية ألا تستخدم الهيئة المعلومات والمعطيات التي تستلمها أو تجمعها لأغراض غير تلك المتعلقة بمجال مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها مع إلزام مستخدميها بالسر المهني وواجب التحفظ وإخضاعهم لإجراءات التأهيل وأداء اليمين قبل تنصيبهم.

وانطلاقا من جملة الأحكام القانونية المتعلقة بهذه الهيئة وبالعودة إلى نصوص مواد القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والمرسوم الرئاسي 15-261 يتضح لنا الدور الهام الذي تلعبه الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، وذلك لما تتمتع بها من مزايا تبدأ من تشكيلتها وتنظيمها، حيث أنه وبالعودة إلى النصوص القانونية نجد بأن المشرع الجزائري على التركيز في القاعدة الهيكلية والتشكيلة البشرية للهيئة والتي تتكون من جهات لها دور هام في مجال مكافحة الجريمة عموما والالكترونية خصوصا والتي تتنوع ما بين وزراء وقضاة إلى جانب قائد الدرك الوطني والمدير العام للأمن الوطني، وممثلين لكل من رئاسة الجمهورية ووزارة الدفاع الوطني، علاوة على إلحاق قاضيين من المحكمة العليا لتشكيلة الهيئة والذين يتم تعيينهما عن طريق المجلس الأعلى للقضاء وهو الأمر الذي يسمح لا شك باختيار القضاة الأكثر كفاءة وجدارة وخبرة في هذا المجال بما يخدم المهام والأهداف الأساسية للهيئة.

كما أننا وباستقراء المواد الناظمة لمهام الهيئة نجد بأن المشرع عمل على تركيز هذه المهام وتوسيع نطاقها وجعلها مهام متنوعة تختلف ما بين المهام الوقائية الردعية والجزائية العقابية ومنحها في هذا الإطار صلاحية هامة يعود أساسها لما تتمتع به الهيئة من تخصص وهي صلاحية اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، إلا أن دور هذه الهيئة غير مفعّل في الواقع وقد اصطدم تفعيل مهامها بجملة من العراقيل أولها التأخر الكبير في صدور النص القانوني الناظم لتشكيلتها وتنظيمها وكيفيات سيرها، ذلك أن المرسوم الرئاسي 15-261 لم يصدر إلا بعد ست (06) سنوات من النص على استحداث الهيئة بموجب القانون 09-04 هذا من جهة ومن جهة أخرى لا يزال تنصيب مقر هذه الهيئة بصورة تسمح بمباشرتها لمهامها بصورة سليمة وفق ما ينص عليه القانون ويقتضيه لا يزال لحد كتابة هذه الأسطر حبيس الورق ولم يتم تنصيبه لحد الآن ما ترتب عنه عرقلة دورها ومهامها، وهو الأمر الذي يعيدنا في كل مرة إلى طرح سؤال جوهري عن **جدوى بذل آليات قانونية واستحداث هيئات وطنية في مسار مكافحة الجرائم السيبرانية خاصة وبرامج التحول الالكتروني عامة إذا كانت أغلب هذه البرامج والمشاريع غالبا ما تظل حبيسة الورق وإن تم تجسيدها فبصورة جد متأخرة تفرغها من قيمتها وتعرقل دورها؟** خاصة وأن هذه الهيئة تعتبر لبنة جديدة هامة في مسار الإصلاحات المرتبطة بتكريس مبادئ الأمن القانوني والتي كان يفترض أن يتم التعامل مع ضرورة تجسيدها في الوقت المحدد على محمل السرعة والأولوية خاصة لما يترتب عن الجرائم السيبرانية من أضرار وخيمة.

الفرع الثاني: الهيئة الوطنية لحماية وترقية الطفولة

تعتبر هذه الهيئة من أهم الجهات المكلفة بحماية الطفل والعمل على مكافحة كل صور الانتهاكات التي من شأنها المساس بسلامته، وتم استحداثها لهذا الغرض بموجب المادة الحادية عشر (11) من القانون 15-12 التي نصت أنه "**تحدث لدى الوزير الأول هيئة وطنية لحماية وترقية الطفولة يرأسها المفوض الوطني لحماية وترقية الطفولة يرأسها المفوض الوطني لحماية الطفولة، تكلف بالسهر على حماية وترقية حقوق الطفل، وتتمتع بالشخصية المعنوية والاستقلال المالي.**" وأحال تحديد تشكيلتها وتنظيمها وكيفيات سيرها إلى التنظيم ليصدر بناءا على هذا المرسوم التنفيذي 16-334 المحدد لتشكيلتها ومختلف الأحكام المتعلقة بها [73] وتم منحها صلاحيات واسعة وهامة في هذا المجال، كما تم تحديد تشكيلتها وتنظيمها والمهام الموكلة لها، ووضح كيفيات سيرها مختلف الأحكام المالية والقانونية المتعلقة بها.وسنقوم بتحديد تشكيلة هذه الهيئة (**أولا**) ومن ثم تحديد دورها في حماية وترقية الطفولة عامة وحمايته من خطر الجرائم السيبرانية الالكترونية خاصة (**ثانيا**).

أولا-تشكيلة الهيئة الوطنية لحماية وترقية الطفولة: تتشكل حسب ما نص عليه المرسوم التنفيذي 16-334 من مجموعة من الأقسام والمديريات التي توضع تحت رئاسة وإشراف رئيس الهيئة الذي اصطلح عليه بموجب القانون **بالمفوض الوطني لحماية وترقية الطفولة**والذي يتم تعيينه بموجب مرسوم رئاسي من بين الشخصيات الوطنية ذات الخبرة والكفاءة المعروفة في مجال الاهتمام بالطفولة، وتوضع تحت رئاسة المفوض الوطني لحماية وترقية الطفولة مجموعة من الأقسام التي تساعده في القيام بالمهام الموكلة إليه بموجب القانون والمتمثلة في: [74]

- ✓ **الأمانة العامة.**
- ✓ **مديرية حماية حقوق الطفل.**
- ✓ **مديرية ترقية حقوق الطفل.**
- ✓ **لجنة التنسيق الدائمة واللجان الموضوعاتية.**

ثانيا-اختصاصات الهيئة الوطنية لحماية وترقية الطفولة: يدخل دور الهيئة في حماية الطفل من خطر الجرائم السيبرانية في مجال اختصاصها العام في حماية الطفل ويمكن حصر هذه الاختصاصات فيما يلي: [75]

1-التخطيط: تعتبر مهمة التخطيط من أهم الاختصاصات الموكلة للهيئة الوطنية لحماية وترقية الطفولة، والتي تقوم من خلالها بوضع مختلف البرامج الوطنية والمحلية التي من شأنها ترقية حقوق الطفل من خلال التنسيق بين مختلف المتعاملين مع الطفل، وتم إسناد هذه المهمة بالتحديد للمفوض الوطني لحماية وترقية الطفولة، والذي يتولى مهمة التخطيط والتنظير من خلال متابعة الأعمال المباشرة ميدانيا في مجال حماية الطفل وضمان حقوقه.

2-وضعية الطفل عبر الانترنت: من بين أهم اختصاصات الهيئة هو منحها الدور الرئيسي في تكريس حماية حقوق الطفل في العالم الرقمي عن طريق وضع نظام معلوماتي وطني حول وضعية الطفولة والطفل في الجزائر،

في جميع المجالات وعلى جميع المستويات، لاسيما منها المتعلقة بالمجال التعليمي والتربوي والصحي والاجتماعي، مع ضرورة التنسيق مع مختلف الإدارات والهيئات المعنية التي تتولى مهمة تزويد الهيئة بجميع المعلومات التي من شأنها المساهمة في حماية الطفل من صور الاعتداءات والانتهاكات التي تمس بسلامته الجسدية والنفسية. (76)

وتمارس الهيئة صلاحياتها في هذا المجال عن طريق مجموعة من الإجراءات التي تتدخل من خلالها لحماية الطفل من أي خطر، وتتمثل هذه الإجراءات خاصة فيما يلي: (77)

- ✓ **الإخطار**: يعتبر الإخطار من الإجراءات التي بذلها القانون في سبيل المتابعة الدائمة لأي فعل أو قول من شأنه المساس بحق الطفل وسلامته، ويتولى المفوض الوطني مسألة الإخطار بأي وسيلة من طرف الطفل أو ممثله الشرعي أو أي شخص طبيعي أو معنوي، كما يمكنه أن يتدخل تلقائيا لمساعدة الأطفال في خطر أو في حالات المساس بمصلحته، وتم في هذا الإطار تزويد الهيئة بقم أخضر مجاني من شأنه أن يساهم في تسهيل عملية الإخطار.
- ✓ **التحقيق**: إضافة إلى الإخطار ضمن المشرع إجراءات تحقيق مضبوطة للهيئة الوطنية لحماية وترقية الطفولة، تخول من خلالها الهيئة صلاحية التحقيق في التبليغات المتعلقة بانتهاكات حقوق الطفل عبر مصالح الوسط المفتوح التي يتوجب عليها في هذا الشأن اتخاذ جميع الإجراءات اللازمة لإنقاذ وحماية الطفل من الخطر في حال ثبوت وجوده.

المطلب الثاني: الوحدات التابعة للجهات الأمنية المتخصصة في مكافحة الجريمة السيبرانية

نظرا للدور الجوهري الذي تلعبه الجهات الأمنية ممثلة في سلك الأمن الوطني والدرك الوطني في مكافحة الجريمة والوقاية منها، فإن المشرع عمل على تعزيز دورها في مجال مكافحة الجريمة السيبرانية والوقاية منها وذلك من خلال توسيع نطاق عملها والعمل على ضبط مجال ونطاق اختصاصها بأطر قانونية واضحة ومحددة لضمان قيامها بمهامها على أكمل وجه.

وعلى اعتبار أن الجريمة السيبرانية ذات طبيعة خاصة وتتوجب إجراءات خاصة لا يمكن تفعيلها في إطار القدرات التقليدية وبواسطة الوسائل التقليدية الممنوحة للأجهزة الأمنية والتي كانت تتماشى مع طبيعة الجرائم التقليدية دون الالكترونية فإن المشرع حرص على استحداث وحدات جديدة تم تزويدها بكافة الأجهزة والامكانيات الحديثة إلى جانب اختصاصات واسعة تنطلق من القواعد العامة لقانون العقوبات وقانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والوقاية منها، وتستند إلى القوانين الخاصة بكل من سلكي الأمن الوطني والدرك الوطني وفي إطار احترام الاختصاصات الموكلة إلى الهيئة، مع الحرص على خصوصية الجرائم الواقعة على الأطفال وخصوصية التعامل مع هذه الفئة وما يستوجبه من مجهود في حمايتها قبل وقوع الجريمة والتعامل معها بعد وقوع الجريمة، وعمد إلى استحداث وحدات خاصة تابعة لكل من سلك الأمن الوطني والدرك الوطني وخصها بمهام واسعة وهامة.

وسنقوم من خلال هذا المطلب بتحديد الوحدات المستحدثة والمكلفة بمحاربة الجريمة السيبرانية والوقاية منها والتابعة للجهات الأمنية المتخصصة مع بيان صور تدخلها في هذا المجال، وذلك بالتطرق إلى الوحدات المستحدثة على مستوى سلك الأمن الوطني (**الفرع الأول**) ومن ثم تلك التابعة للدرك الوطني (**الفرع الثاني**).

الفرع الأول: الوحدات التابعة للأمن الوطني

يلعب الأمن الوطني دورا هاما في مكافحة الجريمة ويشكل أهم أجهزة مكافحة الجرائم والوقاية منها باختلاف صورها ومظاهرها، ويترتب عن الدور الجوهري المناط به في مجال الحفاظ على النظام العام والحفاظ على الأمن والاستقرار الاهتمام الدائم بتحيين مهامه وعصرنة هياكله بما يخدم المهام الموكلة له.

في سبيل مكافحة الجريمة السيبرانية عملت وزارة الداخلية والجماعات المحلية إلى إنشاء وحدات تابعة لسلك الأمن الوطني والتي تم على مستواها استحداث **مصلحة نيابة مديرية الشرطة العلمية والتقنية** [78] هذه الأخيرة التي تم تقسيمها إلى **المخبر المركزي للشرطة العلمية** والذي تم تحديد مقره بالجزائر العاصمة إلى جانب **أربع (04) مخابر جهوية** مقرها كل من قسنطينة، وهران، بشار وتمنراست وتم على مستوى هذه المخابر إنشاء **دائرة علمية ودائرة تقنية** تم تكليفها بالقيام بمهام التحري والتحقيق وتحليل الأدلة الجنائية المتحصل عيها من ارتكاب الجريمة السيبرانية [79]وتضم المخابرعدة فروع من بينها **فرع علم الأدلة الجنائية الحاسوبية** والذي يعهد إليه متابعة الجرائم السيبرانية والتحري عنها والعمل على مكافحتها والوقاية منها وذلك عن طريق دراسة وتحليل نوعية خاصة من الأدلة المسماة **الأدلة العلمية الرقمية** المتجسدة في المعلومات المخزنة أو المنقولة بشكل رقمي وذلك وفق إجراءات خاصة تتفق وخصوصية الجريمة السيبرانية. [80]

وتسعى في هذا الإطار المديرية العامة للأمن إلى العمل على مواكبة التطورات الدولية وفتح مجال التعاون الدولي وتنظيم العديد من دورات التكوين لضمان مكافحة فعالة لكافة صور ومظاهر الجريمة السيبرانية. [81]

الفرع الثاني: الوحدات التابعة للدرك الوطني

يلعب الدرك الوطني دورا هاما في مجال مكافحة الجريمة ويعمل بشكل دوري ومستمر على استحداث الإجراءات اللازمة لمواكبة التطورات في مجال الجرائم المستحدثة وطرق مكافحتها والوقاية منها، وبالاطلاع على وحدات الدرك الوطني المتخصصة في مجال مكافحة الجريمة السيبرانية فإننا نجد بأنه تم استحداث على المستوى المركزي **مديرية الأمن العمومي والاستغلال، والمصلحة المركزية للتحريات الجنائية.**

وتم في هذا الإطار استحداث هيئة وطنية جد هامة في هذا المجال ألا وهي "**المعهد الوطني للأدلة الجنائية وعلم الإجرام**" والذي نص المشرع أنه "**يحدث معهد وطني للأدلة الجنائية وعلم الإجرام للدرك الوطني**". [82]

وتم تعريفه على أنه "**مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلال المالي.**

ويوضع تحت وصاية وزير الدفاع ويمارس قائد الدرك الوطني سلطات الوصاية عليه بتفويض منه". [83]

وقد أوكل له المشـــرع صـــلاحيات واســـعة في مجال مكافحة الجريمة والوقاية منها على اختلاف صـــورها وأشكالها، وتضم إلى جانب الصور التقليدية للجريمة الجرائم المستحدثة وعلى رأسها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال [84] حيث يتولى إدارة المعهد مدير عام ويقوم بتسييره مجلس توجيه ويزود بمجلس علمي.

وقد عملت مختلف مصالح الدرك الوطني وفي إطار تكثيف إجراءات مكافحة الجرائم السيبرانية عامة والواقعة على الأطفال خاصة على استحداث مصالح جهوية للشرطة القضائية التابعة للدرك الوطني وتوزيعها على مستوى جهوي، علاوة على فصـائل ذات خبرة تسـاعد في التحري عن الجريمة السـيبرانية وخلايا للشـرطة العلمية والتقنية التابعة للدرك الوطني.

وفي إطار العمل على مكافحة الجريمة السـيبرانية والاسـتفادة من التكنولوجيات الحديثة في هذا المجال وبناءا على السياسات الوطنية والدولية التي تتجه شيئا فشيئا إلى إشراك المواطن في الحفاظ على النظام العام إلى جانب الجهات الأمنية المتخصـصـة بصـورة من شـأنها المسـاهمة في الحد من مختلف الجرائم التي تهدد النظام العام وأمن وسلامة الأفراد والمؤسسات أعلنت قيادة الدرك الوطني مع نهاية سنة 2017 عن إطلاق موقع رسمي تحت مسمى **الشـكوى المسـبقة والاسـتعلام عن بعد** [85]والذي تم فتحه لصـالح المواطنين الراغبين في إيداع الشـكاوى والتبليغ عن أي معلومات في إطار المساهمة في مكافحة الجريمة والحفاظ على الأمن.

وقد أكدت القيادة عن كون المعطيات التي تصلها عن طريق هذا الموقع مؤمنة ولا يمكن الاطلاع عليها من قبل المتعاملين مع الإعراب عن نية مصـــالح الدرك عن اســـتحداث تطبيق خاص بهذا الإجراء عبر الهواتف النقالة الذكية، ويســـمح هذا الموقع للمواطنين بالتوجه نحو خيارين يتمثلان في **خدمة الشـــكاوى المســـبقة أو خدمة المعلومات**، ولا يخفى لما لهذا الإجراء من أهمية في مجال مكافحة الجريمة السيبرانية خاصة بالنظر لطبيعتها والتي غالبا ما يكون من الصـعب الكشـف عنها رغم المتابعة المسـتمرة، حيث أشـرنا ونحن بصـدد عرض خصـائصـها إلى أن أغلب الجرائم المسـجلة في هذا الإطار يتم اكتشـافها عن طريق الصـدفة لكونها تعتمد على برامج معقدة وإجراءات وطرق غامضـة يصـعب معها متابعتها، وهو الأمر الذي يجعل من هذا الموقع المسـتحدث من طرف قيادة الدرك الوطني يسـاهم مسـاهمة فعالة في فتح المجال للأفراد للتبليغ عن أي تجاوز يسـجل في هذا المجال قد يتم إغفاله من طرف الجهات الأمنية وهو الأمر الذي يجعل من مكافحة الجريمة السيبرانية أكثر فعالية ونجاعة.

هذا وبذل المشرع إلى جانب هذه الهيئات مجموعة من الآليات القانونية التي تم تحديدها عبر نصوص قانونية مختلفة، حيث يعتبر العقاب من أقدم الأســاليب التي انتهجتها المجتمعات لمكافحة الجريمة والحد من انتشــارها، لما أثبته من دور فعال في ردع الأفراد عن القيام بالأعمال الاجرامية والتقليل من نسبة انتشارها والتمادي في القيام بها، انطلاقا من هذه الحقيقة التي جعلت النصوص العقابية تحتل قائمة الأساليب المنتهجة من طرف الدول في سياساتها لمكافحة كافة صـور ومظاهر الجريمة، عمد المشـرع الجزائري إلى جانب الجهات المسـتحدثة على المسـتوى الوطني

والإقليمي والمحلي لمكافحة الجرائم السيبرانية إلى النص على جملة من النصوص القانونية التي تضمنت عقوبات صارمة ضد مرتكبي الجرائم السيبرانية، حيث سعى المشرع من خلال هذه النصوص التشريعية إلى العمل قدر المستطاع على الحيلولة دون وقوعها وذلك من خلال تجريم مراحل متقدمة من هذه الجرائم على غرار تجريم عملية الدخول إلى الأنظمة المعلوماتية دون وجه حق، ووصولا إلى تجريم الأفعال المترتبة عن الدخول غير المشروع إلى الأنظمة المعلوماتية والتصرف فيها وفق الصور التي وضحناها عند الحديث عن مظاهر الجريمة السيبرانية.

إن التشريع الوطني وقبله العديد من الاتفاقيات والنصوص التشريعية الدولية وإدراكا لخطورة الجريمة السيبرانية على الأفراد والدول عامة وعلى فئة الأطفال خاصة عملوا على بذل آليات عقابية للعديد من الأفعال التي من شأنها أن تقود في الحالة العادية إلى ارتكاب الجريمة السيبرانية فكان الاتفاق الجنائي على التحضير والاعداد لارتكاب هذه الجرائم على رأس قائمة الأفعال المجرمة قانونا بمجرد ترجمته إلى فعل أو عدة أفعال مادية، بل إن المشرع وفي هذا الإطار ذهب إلى أبعد من هذا وذلك من خلال نصه على عقوبات مشددة تطبق على المجرمين في حال ما كان تهذه الجريمة واقعة على الأطفال، بما يوليه المشرع عامة والدولة خاصة من اهتمام بهذه الفئة المهمة جدا من المجتمع.

وفي هذا الإطار تذهب بعض التشريعات وجانب من الفقه إلى فصل الاتفاق الجنائي على ارتكاب الجريمة السيبرانية كجريمة خاصة ومنفصلة وليست مجرد عزم على ارتكاب الجريمة، الأمر الذي يستوجب خصه بعقوبات خاصة ومنفصلة لكونه يظهر العزم الجماعي الجنائي بمظهر خارجي مادي ملموس، لكون كل شخص يعلن عزمه على ارتكاب الجريمة ومن هذا المنطلق تتحدد إرادة الأفراد المتفقين على ارتكاب الجريمة وهو الأمر الذي ينشأ الاتفاق ويجعل إثباته واردا وممكنا، علاوة على كون الاتفاق الجنائي على ارتكاب الجريمة يشكل ظاهرة خطرة تهدد الأمن العام وتخل به وهو الأمر الذي يستوجب ضبطه بأحكام عقابية واضحة ومحددة.

ومن الثابت أن العقوبة وحين النص عليها من طرف المشرع فإن السبب الأول والرئيسي لها الحد من نطاق توسع الجريمة وإثباط انتشارها لكونها تشكل تهديدا للمصالح الفردية والجماعية وأمن المجتمعات واستقرارها، الأمر الذي يجعل من العقاب على الشروع في ارتكاب الجريمة مرتبطا بمدى تشكيلها لخطر يهدد الحقوق والمصالح المكفولة والمحمية بموجب القانون، ما جعل أغلب قوانين العالم تعمل على توسيع نطاق العقوبات لتستغرق ليس فقط الضرر المادي المترتب عن ارتكاب الجريمة في حد ذاتها، بل يتعدى الأمر إلى العمل على ردع ما يترتب عنها من قلق واضطراب تلحقه بالأفراد والمجتمعات، من هذا المنطلق فإن المشرع وسع من نطاق العقوبات المطبقة عليها لتستغرق بذلك الشروع في ارتكاب الجريمة ونص على المعاقبة على الاتفاق الجنائي المجسد بأعمال مادية.

أولا–العقاب المقرر للاتفاق الجنائي على ارتكاب الجريمة السيبرانية: يقوم مبدأ العقاب على الاتفاق الجنائي لارتكاب الجريمة السيبرانية على قيام شخصين أو أكثر بخطوة للبدء في نشاط إجرامي يؤدي مباشرة وفي حالة سير الأمور بوتيرة عادية إلى ارتكاب الجريمة السيبرانية، في حين استقرت أغلب التشريعات العالمية ومن بينها

المشـرع الجزائري على كون الأعمال التحضـيرية التي تسـبق عملية البدء في تنفيذ الجريمة غير معاقب عليها كقاعدة عامة إلا إذا توافر نص قانوني خاص يجرمها.

من هذا المنطلق وبالعودة إلى المادة 394 مكرر 05 من قانون العقوبات المستحدثة بموجب القانون 04-15 نجد المشرع ينص على أن يعاقب "**كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصـوص عليها في هذا القسـم وكان هذا التحضـير مجسـدا بفعل أو عدة أفعال مادية، يعاقب بنفس العقوبات المقررة للجريمة ذاتها**"، وقد تبنى المشـــرع هذا التوجه خلافا للقواعد العامة المقررة في إطار قانون العقوبات، والتي تنص على أن العقاب لا يتقرر إلا في الجرائم الواقعة فعلا والتامة المكتملة الأركان أو الجرائم التي تقف عند مرحلة الشـروع أو المحاولة، ويعود هذا الاسـتثناء في التجريم إلى خطورة الجريمة السـيبرانية التي تقتضـي التصـدي لها بكافة الوسـائل الردعية والعقابية الممكنة، وتقرير نوع من الحماية المتقدمة والوقاية لنظم المعالجة الآلية للمعلومات والمعطيات ضد المخاطر التي تنشأ على النشاط غير المشروع. (86)

من هذا المنطلق وعلى اعتبار أن الاتفاق الجنائي يعتبر جريمة كاملة معاقبا عليها بموجب القانون فإنه يستوجب لقيامها توافر الركنين المادي والمعنوي حتى تقوم الجريمة وتستوجب العقاب وفقا لما يلي:

1-الركن المادي: يقوم الركن المادي على الاتفاق ذاته والذي يترتب عن انعقاد ارادتين أو أكثر واجتماعها على موضـوع الجريمة ومحلها مع ضـرورة أن يتخذ هذا الاتفاق الطبيعة المادية الملموسـة، والذي يفترض تعبير كل طرف عن إرادته ونيته في القيام بالعمل المجرم مع إعلام أطراف الاتفاق، ويتحقق باتجاه إرادتهم نحو هدف وطريق واحد يتلاقى عند موضوع الجريمة، ويشترط أن تترجم هذه الإرادة في شيء مادي أو ملموس كالقول الشفوي أو العبارات المكتوبة ويقوم الاتفاق سواء استغرق انعقاد الارادات وقت قصيرا أو طويلا وسواء كان اتفاقا منظما أو منفصلا.

2-الركن المعنوي: على اعتبار أن جريمة الاتفاق الجنائي من الجرائم العمدية فإنه يسـتوجب لقيامها توافر كل من القصد الجنائي بعنصريه العلم والإرادة، وذلك بعلم كل عضو من أعضاء الاتفاق بماهية الفعل أو الأفعال التي يقدمون على القيام بها والتي تم الاتفاق عليها، وبما لها من خصائص مجرمة من طرف المشرع، وعليه فمن يجهل الغرض من الاتفاق لا يعد القصد الجنائي متوافرا لديه.

علاوة على العلم يجب أن تتجه إرادة كل عضـو من أعضـاء الاتفاق إلى تحقيق نشـاط إجرامي يتمثل في التحضير للقيام بالجريمة ولا يشترط في هذه الجريمة أن يكون كل أعضاء الاتفاق عالمين بنشاط بعضهم البعض إلى جانب ضـرورة أن يكون لكل أعضـاء الاتفاق إرادة الدخول إلى في هذا الاتفاق أي إرادة كل طرف في أن يكون عضوا في الاتفاق وأن تكون الإرادة جادة.

ثانيا–العقاب المقرر لعملية الشـروع في ارتكاب الجريمة السـيبرانية: يقرر العقاب على أي جريمة انطلاقا من الضرر الذي ترتبه على المصالح الفردية والجماعية محل الحماية القانونية، وعليه فإن العقاب على الشروع بوصفه جريمة لا بد أن يقوم بناءا على الخطر والضرر المقترنين به، حيث ثبت أن خطر الجريمة لا يقتصر على ما تحدثه من ضرر مادي بالفرد بل يتعدى ذلك إلى ما تحدثه من قلق واضطراب في الجماعة، ولكون مجال الشروع في الجنايات هو الأصـل بالنظر لخطورتها ولأن جرائم المسـاس بأنظمة المعالجة الآلية للمعطيات تنطوي على خطورة كبيرة حتى وإن لم تكتمل أركان قيامها وتم الشروع فقط في ارتكابها فإن المشرع قرر إخضاعها عبر قواعد قانون العقوبات إلى نظام الشروع. (87)

ويعرف الشـروع في القانون بأنه **كل محاولات لارتكاب جناية تبتدئ بالشـروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشـرة إلى ارتكابها تعتبر كالجناية نفسـها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مسـتقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصـود بسـبب ظرف مادي يجهله مرتكبها"** (88) ويعاقب المشـرع الجزائري على محاولة ارتكاب أي جريمة من جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات وهو الأمر الذي فسره الفقه برغبته في تغطية أكبر قدر ممكن منها. (89)

ونصت المادة 394 مكرر 07 من قانون العقوبات أن **"يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسـم بالعقوبات المقررة للجنحة ذاتها"** وفي هذا الإطار انقسـم الفقه بين من يذهب إلى أنه لا يوجد شـروع في الاتفاق الجنائي لكونه حالة نفسـية تتم بتلاقي الإرادات ولا تحتمل لا بداية ولا نهاية وهو لا يقع إلا كاملا ولا يحتمل البدء في التنفيذ، خاصـة وأن المشـرع لا يعتبر الدعوة إلى الاتفاق شـروعا ولكن يعاقب عليها كجريمة قائمة، في حين يرى جانب آخر أنه طالما كانت أركان الشروع قائمة ولم يكن القانون يتضمن نصا خاصا يعاقب عليه فلا داعي للأخذ بالرأي السابق لكونه غير صحيح أن الشروع في الاتفاق غير متصور. (90)

كما بذل المشرع الجزائري في سبيل الكشف عن الجرائم السيبرانية ومحاربتها جملة من القواعد الإجرائية التي تم رصـدها لمجابهة الجريمة السـيبرانية وحدد بناءا عليها جميع المراحل المتعلقة بعملية التحري والتحقيق عن الجرائم السيبرانية إلى جانب بيان وسائل الإثبات المعتد بها في هذا النوع من الجرائم، وتنقسم هذه القواعد الإجرائية على صـورتين تقليدية ومسـتحدثة (91) وهي عديدة ومتنوعة أهمها تلك المحددة بموجب القانون 09-04 المتضـمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والمتمثلة في:

1–مراقبة الاتصـالات الالكترونية: عرف المشـرع الجزائري الاتصـالات الالكترونية بأنها **"أي تراسـل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية"** (92)وحدد الحالات التي تسمح باللجوء إلى المراقبة الالكترونية والمتمثلة في أربع حالات: (93)

- ✓ **للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.**

- ✓ **في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.**
- ✓ **لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.**
- ✓ **في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.**

ولخطورة هذا الإجراء نص المشـــرع على عدم جواز إجراء عمليات المراقبة الالكترونية إلا بإذن مكتوب من السلطة القضائية المختصة، كما خص الحالة الأولى المتعلقة بالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة بإجراءات خاصة تدخل ضمن اختصاص النائب العام لدى مجلس قضاء الجزائر وضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. (94)

2-تفتيش المنظومة المعلوماتية: أجاز المشـرع للسـلطات القضـائية وضـباط الشـرطة القضـائية في إطار القواعد المنصوص عليها بموجب قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد إلى: (95)

- ✓ **منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.**
- ✓ **منظومة تخزين معلوماتية.**

وحرص في هذا المجال على فتح باب التعاون الدولي وأشـــار إلى أهمية فتح مجال المســـاعدة الدولية في مجال مكافحة الجرائم السـيبرانية وفق ما تقتضـيه الاتفاقيات الدولية ومبادئ المعاملة بالمثل، كما نص القانون 09-04 على إجراء هام في هذا المجال وهو إجراء **"التسخير"** والذي فتح بموجبه للسلطات المختصة المكلفة بالتفتيش المجال لتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدة هذه السلطات وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها. (96)

3-حجز المعطيات المعلوماتية: فتح المشـــرع الجزائري للســـلطة التي تباشـــر التفتيش عندما تكتشـــف في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم السيبرانية أو مرتكبيها المجال لنسخ المعطيات محل البحث والمعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضـــع في أحراز وفقا للقواعد المقررة قانونا في حال ما لم يكن من الضروري حجز كامل المنظومة. (97)

وأوجب على السـلطة التي تقوم بالتفتيش والحجز السـهر على سـلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، إلا أنه من جهة أخرى أجاز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصـــد جعلها قابلة للاســـتغلال لأغراض التحقيق شـــرط ألا يؤدي هذا الإجراء إلى المســـاس بمحتوى المعطيات، ونص في هذا الإطار أنه: (98)

- ✓ في حالة استحالة إجراء الحجز وفقا لما هو منصوص عليه قانونا لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.
- ✓ إمكانية أن تأمر السلطة التي تباشر التفتيش باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

ونظرا لخصوصية الجريمة السيبرانية فقد نص المشرع الجزائري حاله حال أغلب التشريعات الوطنية والدولية على جملة من الآليات في سبيل البحث والتحقيق في الجرائم السيبرانية وعمل على جعلها تتوافق والطبيعة الخاصة لهذا النوع من الجرائم لتسهيل إثبات وقوعها والعمل على معاقبة مرتكبيها وفق ما ينص عليه القانون، وذلك إلى جانب الوسائل التقليدية للتحقيق والإثبات المتعارف عليها في إطار القانون الجنائي والتي يتم استغلالها بما يخدم الطبيعة الخاصة للجريمة الالكترونية ويساعد على الكشف عنها ومتابعة مرتكبيها وفق ما يقتضيه القانون. (99)

إلا أن ما يجب الإشارة إليه أنه على الرغم من كافة الهيئات المستحدثة في هذا الإطار والنصوص القانونية التي تسعى التشريعات القانونية الوطنية والدولية لبذلها في مجال الوقاية من الجرائم السيبرانية ومكافحتها إلا أن هذه الجرائم في تطور واتساع مستمر وهو الأمر الذي يظهر جليا من خلال الإحصائيات الدولية التي تم تسجيلها في هذا الإطار والتي توضح ارتفاعا غير مسبوق لمعدل الجرائم السيبرانية عامة والممارسة ضد الأطفال خاصة، وما ساهم في ارتفاع هذه الجرائم أيضا انتشار وباء كورونا (كوفيد 19) وما دفع إليه من ضرورة الالتزام بإجراءات الحجر الصحي التي كانت سببا في انتقال فئة كبيرة من الأشخاص من التعامل الواقعي إلى التعامل الرقمي وما أنتجه من أرض خصبة للعديد من الممارسات الإجرامية لفئة واسعة من المجرمين الرقميين، الذين انتقلوا إلى العمل على الاستفادة المادية من العالم الرقمي حتى بطرق غير قانونية.

وعليه وانطلاقا ممّا سبق عرضه وتوضيحه حول مختلف الجزئيات المتعلقة بالجرائم السيبرانية الواقعة على الأطفال ونزولا عند الأطر الدولية والوطنية للوقاية من هذه الجرائم ومكافحتها، لا تزال الأصوات تعلو بضورة العمل قبل مكافحة هذه الصورة من الجرائم على الوقاية منها، وذلك من خلال بذل كافة الوسائل الممكنة التي من شأنها أن تحول دون وقوع الطفل ضحية هذه الصورة الخطيرة من الجرائم، وهو الأمر الذي لا يتأتى إلا من خلال العمل على تجسيد مبادئ الأمن الرقمي للطفل بداية من الأسرة وانطلاقا إلى كافة الفضاءات ذات الصلة بالطفل وبنشاطاته، خاصة وأننا أصبحنا اليوم نشهد حملات توعية واسعة فيما يتعلق بحماية الأطفال في هذا المجال.

هذه الوقاية التي لن تتأتى إلا بنشر الوعي الرقمي بداية من العائلة، وذلك انطلاقا من ضرورة توفير انترنت آمن للطفل من خلال توجيهه إلى البرامج المخصصة للأطفال والتي أصبحت اليوم منتشرة عبر المواقع الإلكترونية

بالآلاف وأهمها محركات البحث العلمية المخصصة للأطفال مثل محرك البحث المخصص من طرف Google المسمى بمحرك البحث Kiddle والذي صمم خصيصا لتوفير بحث آمن للطفل في مجال اطلاعه على عالم الانترنت أو استعماله في القيام بواجباته ووظائفه الدراسية. (100)

الخاتمة:

في ختام هذه الورقة البحثية التي حاولنا من خلالها تسليط الضوء على واقع حماية الأطفال من مخاطر الجرائم السيبرانية الإلكترونية انطلاقا من إشكالية رئيسية تتمحور حول **الإطار القانوني الذي نظمته التشريعات الوطنية والدولية في سبيل الوقاية من الجرائم السيبرانية الواقعة على الأطفال** خلصنا إلى أن الجريمة السيبرانية تشكل اليوم تهديدا كبيرا على سلامة الأطفال، خاصة مع الانتشار الواسع لتكنولوجيا الإعلام والاتصال وما ترتب عنه من ظهور العديد من الأوجه السلبية التي أصبحت تهدد أبناءنا، الأمر الذي اقتضى استحداث إطار قانوني يعمل على مكافحة هذه الصورة الخطيرة من الجرائم والوقاية منها، بما يساهم في تحقيق مبادئ الأمن الرقمي والحد من الانتشار الخطير لهذه الجرائم الواقعة على الأطفال بمختلف أشكالها وصورها، وقد خلصنا من خلال هذه الورقة إلى مجموعة من النتائج أهمها:

1-ترتب عن التوجه الالكتروني الذي يشهده العالم وانتقال الأفراد من العالم الواقعي إلى العالم الافتراضي خلق نوع جديد من الجريمة المسماة "**الجريمة السيبرانية الإلكترونية**" والتي أصبحت تشكل أخطر صورا الجرائم التي شهدها العالم، والتي فتحت المجال لميلاد نوع جديد من المجرمين المختلفين عن المجرمين التقليديين قاعدة وتفكيرا، حيث أصبح العالم يواجه اليوم مجرما ذو مستوى ثقافي وفكري مرتفع يهدد ليس وفقط أمن وسلامة الأفراد، بل أصبح الكثير منهم يهدد أمن وسلامة واستقرار دول بأكملها خاصة مع التوجه الحتمي نحو ضرورة الانتقال إلى نظام التعامل لمواكبة الواقع الذي فرضته التكنولوجيا الرقمية واستعمال الانترنت.

2-يعتبر مفهوم الجرائم السيبرانية لحد اليوم وعلى الرغم من اتجاه أغلب التشريعات العالمية إلى تجريمها وضبط أركان قيامها والعقوبات المقررة لها من المفاهيم التي لا تزال محل جدال فقهي كبير لم يتحدد تعريف واضح لها لما تنطوي عليه من غموض ساهم في بلورته مختلف الخصائص التي تقوم عليها والتي تتسع وتضيق من صورة إلى أخرى، علاوة على عدم استقرار الفقه والتشريع على حد سواء على تسمية موحدة لها إذ تختلف التسميات ما بين جرائم المعلوماتية، جرائم الانترنت، الجرائم الالكترونية، والجرائم المتصلة بتكنولوجيات الاعلام والاتصال كما اصطلح عليها المشرع الجزائري.

3-إدراكا منه لخطورة الجريمة السيبرانية عمل المشرع على الحرص على تجريم الجرائم الالكترونية والعمل على الحماية منها بإجراءات قانونية صارمة كانت بدايتها مع تعديل قانون العقوبات بموجب القانون 04-15 والذي تم من خلاله استحداث قسم خاص بهذه الجرائم بموجب المواد من 394 مكرر إلى 394 مكرر 07 وهو الأمر الذي عززه صدور القانون 09-04 الذي تم تخصيصه للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا

الاعلام والاتصـــال ومكافحتها والذي حملته مواده إجراءات هامة في هذا المجال عززها المشـــرع بالنص على استحداث هيئة وطنية متخصصة في الوقاية من هذه الجرائم ومكافحتها بموجب المادة 13 منه.

4-يعتبر الأطفال أكثر فئة مهددة بخطر هذه الجرائم لأنهم الأكثر استعمالا للتكنولوجيا الحديثة والانترنت، الأمر الذي يعلهم هدفا سهلا للكثير من المجرمين الرقميين الذين يستغلون سنهم ونقص خبرتهم في ارتكاب العديد من الجرائم الخطيرة وعلى رأسها، جرائم الاستغلال الجنسي للأطفال على الانترنت وجرائم التجنيد الاجباري ضمن المنظمات الإرهابية.

5-تشـكل الألعاب الالكترونية طريقا خطيرا لتنفيذ الجرائم الإلكترونية وذلك لما تسـوقه هذه الألعاب من ضرورة استعمال العنف وانتهاج المناهج الغير قانونية والتي تصل إلى حد الانتحار والقتل في الكثير من الأحيان.

6-إن التحليل الدقيق للنصـــوص القانونية المجرمة للجرائم الســـيبرانية والعقوبات المحددة بموجبها يدل على وعي المشـــرع بخطورة هذه الجرائم والخطر الكبير الذي تشـــكله على الأطفال وســـلامتهم، وهو ما تجســـد ببذل عقوبات صارمة في سبيل مكافحتها والحد من انتشارها.

7-بذل المشرع الجزائري في سبيل الوقاية من الجرائم السيبرانية ومكافحتها وانتهاجا بمنهج العديد من دول العالم الرائدة في المجال الالكتروني مجموعة من الهيئات والجهات الرسمية المكلفة بمكافحة الجريمة الســـيبرانية عامة والواقعة على الأطفال خاصة، وحرص على تزويدها بكافة الوسائل القانونية اللازمة للقيام بمهامها كما يجب.

8-شكلت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها المستحدثة بموجب المادة الثالثة عشـــر (13) من القانون 09-04 والمنظمة بموجب المرســـوم الرئاســـي 15-261 اللبنة الأساسية في برنامج الدولة لمكافحة الجريمة الالكترونية وقفزة نوعية تحسب له في هذا المجال إلا أن التأخر الملحوظ في صدور النص التنظيمي الناظم لها والذي فصلت بينه وبين النص على استحداثها ست (06) سنوات كاملة شكّل عائقا في سبيل تحقيق الأهداف الطموحة المسطرة لها والمنتظرة منها.

9-ساهمت الهيئة الوطنية لحماية وترقية الطفولة بشكل فعال في تغطية كافة أوجه الخطر التي تواجه الطفل خاصة في المجال الرقمي، ومما دعم دورها في هذا المجال مجموع الاختصاصات الواسعة التي يتمتع بها المفوض الوطني لحماية وترقية الطفولة.

10-تعتبر الوحدات المستحدثة على مستوى مراكز الشرطة والدرك الوطني والمتخصصة في الوقاية من الجرائم الالكترونية ومكافحتها دليلا على عزم الدولة على التصـــدي لهذه الجريمة بصـــورة ســـريعة وفعالة ولمختلف الانتهاكات على جميع المستويات المحلية، الإقليمية والوطنية.

وانطلاقا من جملة هذه النتائج، حاولنا وضـــع بعض التوصـــيات التي من شـــأنها المســـاهمة في خدمة الموضوع وتغطية بعض نقاط العجز والقصور التي تم تسجيلها من خلال الدراسة، والمتمثلة في:

1-أصبح من الضروري إحاطة الجرائم السيبرانية بإطار قانوني مفصل ينظم الأسس القانونية والعقابية لهذه الجرائم ومراعاة التطور الدائم والمستمر لهذه الجرائم والذي يترتب عنه في كل يوم ظهور صور ومظاهر جديدة لها، خاصة وأننا سجلنا بأن نصوص القانون 09-04 المستحدث في هذا الإطار والمواد 394 مكرر إلى 394 مكرر من قانون العقوبات أصبحت قاصرة عن تغطية العديد من الجرائم الحديثة التي لم يتم ذكرها بموجب هذه النصوص، مع ضرورة رصد عقوبات مشددة للجرائم التي تستهدف الأطفال وتمس بسلامتهم الجسدية والعقلية.

2-على اعتبار أن مكافحة الجرائم السيبرانية والوقاية منها يبدأ من الوعي وضرورة تعريف المجتمع بمختلف صور هذه الجرائم، فإنه أصبح من الضروري تنظيم دورات تكوينية في المجال الرقمي لكل الأشخاص الذين لهم علاقة بحماية الطفل بداية بالعائلة ووصولا عند مختلف الهيئات والمؤسسات والجهات الرسمية وغير الرسمية.

3-إن توجه الطفل نحو الانترنت ووقوعه فريسة المجرمين الرقميين يعود السبب الرئيسي فيه لنقص الرقابة الممارسة من طرف الأهل خاصة، إما لتهاون أو لعدم دراية بالعالم الرقمي واستخدام التكنولوجيات الحديثة، الأمر الذي أصبح يستوجب ضرورة العمل على محاربة صورة جديدة من الأمية وهي **"الأمية الرقمية"** بطريقة تساهم في فرض رقابة أوسع وأنجع من طرف الأهل على الأطفال.

4-إن الوقاية من الجرائم السيبرانية الموجهة ضد الأطفال ومكافحتها لا يمكن أن يتم بأي وجه من الأوجه من طرف جهة دون أخرى، وبالتالي يتوجب التوجه جديا نحو وضع برامج وطنية وحتى دولية لمكافحتها وذلك من خلال تظافر جهود جميع الأطراف التي من شأنها المساهمة في إيجاد حلول للجريمة قبل وقوعها وتخفيف أضرارها بعد وقوعها وضمان توقيع جزاءات صارمة على كل طرف فيها.

الهوامش:

[1]-وهو الأمر الذي بذله المشرع الجزائري باستحداث القانون 15-12 المؤرخ في 15 جويلية 2015 المتعلق بحماية الطفل، ج.ر العدد 39 الصادرة في 19 جويلية 2015.

[2]-تجسد ذلك بصدور اتفاقية حقوق الطفل التي تم **اعتمادها وعرضها للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة 25/44 المؤرخ في 20 نوفمبر 1989 ودخلت حيز النفاذ في سبتمبر 1990، وفقا للمادة 49 من نفس الاتفاقية.**

[3]-بهلول سمية، **دور الإدارة الإلكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر**، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص: إدارة محلية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، 2018/2017، ص280.

[4]-راجع في هذا الإطار: بهلول سمية، خليفي وردة، **"الآليات القانونية للحد من العنف ضد الأطفال في التشريع الجزائر –جريمة اختطاف وقتل الأطفال نموذجا"**، مداخلة مقدمة ضمن فعاليات الملتقى الوطني حول "الطفولة المعنفة... أية حماية؟ بأي ضمانات"، المنظم من طرف كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين سطيف 2، يوم 11 جانفي 2020.

[5]- احسن بوسقيعة، **الوجيز في القانون الجزائي العام**، دار هومة للنشر والتوزيع، الجزائر، الطبعة العاشرة، 2011، ص27.

[6]- **المرجع نفسه**، ص27

[7]- غنية باطلي، **الجريمة الالكترونية (دراسة مقارنة)**، منشورات الدار الجزائرية، الجزائر، 2015، ص15.

[8]- **المرجع نفسه**، ص15.

[9]- **المرجع نفسه**، ص16.

[10]– كحلوش علي، "**جرائم الحاسوب الآلي وأساليب مواجهتها**"، مجلة الشرطة، العدد 84، جويلية 2007، المديرية العامة للأمن الوطني، الجزائر، ص51.

[11]– مصطفى محمد موسى، **التحقيق الجنائي في الجرائم الالكترونية**، مطابع الشرطة، القاهرة، الطبعة الأولى، 2009، ص112.

[12]– للاطلاع على مزيد من تعاريف الجريمة السيبرانية الالكترونية الموضوعة انطلاق من معيار الوسيلة المستخدمة لارتكاب الجريمة راجع:

* عمر بن محمد العتيبي، **الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير الدولية والمحلية**، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص21 وما بعدها.

*Al Azouzi Ali, **La Cybercriminalité au Maroc**, Edition Bishops solution, Casablanca, 2010, P43.

[13]– غنية باطلي، **مرجع سابق**، ص17.

[14]– نائلة عادل محمد فريد، **جرائم الحاسب الاقتصادية**، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق، جامعة القاهرة، 2003، ص21.

[15]– غنية باطلي، **مرجع سابق**، ص17.

[16]– أشرف جمال محمود عبد العاطي، **الإدارة الإلكترونية للمرافق العامة**، دار النهضة العربية، مصر، 2016، ص359.

[17]– غنية باطلي، **المرجع السابق**، ص19.

[18]– هلالي عبد الله أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم في جرائم المعلومات (دراسة مقارنة)**، دار النهضة العربية، القاهرة، 2000، ص07.

[19]– هشام محمد فريد رستم، "**الجرائم المعلوماتية_ أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية للتدريب التخصصي**"، ورقة بحث مقدمة ضمن فعاليات مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من 01 إلى 03 ماي 2000، منشور ضمن مجلة "الشريعة والقانون"، المجلد الثاني، الطبعة الثالثة، 2004، ص407.

[20]– أسماء حسين رويعي، **الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية**، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، 2013، ص64.

[21]–بهلول سمية، دمان ذبيح عماد، "**الآليات العقابية لمكافحة الجريمة الإلكترونية في الجزائر**"، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، المجلد السابع، العدد 13، جانفي 2020، ص ص137-157.

[22] – Site officiel de L'OCDE www.oecd.org consulté le 21 Mai 2021.

[23]– غنية باطلي، **مرجع سابق**، ص21.

[24]– نايل نبيل عمر، **الحماية الجنائية للعمل الالكتروني في جرائم المعلوماتية**، دار الجامعة الجديدة، القاهرة، 2012، ص23.

[25]– القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات، ج.ر العدد 71 الصادرة في الصادرة في 10 نوفمبر 2004.

[26]– المادة الثانية (02) الفقرة الأولى من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر العدد 47 الصادرة في 16 أوت 2009.

[27]– حسينة شرون، "**فعالية التشريعات العقابية في مكافحة الجرائم الالكترونية**"، مجلة دراسات وأبحاث، جامعة زيان عاشور_الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009، ص428.

[28]– **المرجع نفسه**، ص428.

[29]– **المرجع نفسه**، ص428. ولتفاصيل حول هذه الجزئية راجع:

* أحسن رابحي، "**الجريمة الالكترونية: النقطة المظلمة بالنسبة للتكنولوجية المعلوماتية**"، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009، ص ص98-113.

* بلبالي إبراهيم، "**الجريمة الالكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق**"، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009، ص ص133-149.

[30]– غنية باطلي، **مرجع سابق**، ص33.

[31]– غنية باطلي، **مرجع سابق**، ص34.

[32]– محمد حماد مهرج الهيتي، **التكنولوجيا الحديثة والقانون الجنائي**، دار الثقافة للنشر، الأردن، الطبعة الأولى، 2004، ص124.

[33]- غنية باطلي، **المرجع السابق**، ص36. وأنظر أيضا:

-Pierre Berthelet, « **La Lutte contre la cybercriminalité à l'échelle de l'union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agenda institutionnels** »,Revue Québéquoise de droit international, Québec Journal of International Law, 2018, p p25-39.

[34]- غنية باطلي، **المرجع السابق**، ص42.

[35]- **المرجع نفسه**، ص43. ولمزيد من التفاصيل راجع: جميل عبد الباقي الصغير، **القانون الجنائي والتكنولوجيا الحديثة (الجرائم الناشئة عن استخدام الحاسب الآلي)**، دار النهضة العربية، القاهرة، د.ت.ن، ص17.

[36]- طارق إبراهيم الدسوقي، **الأمن المعلوماتي**، دار الجامعة الجديدة، مصر، 2009، ص171.

[37]- خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي، مصـــر، 2009، ص364. نقلا عن: أشـــرف جمال محمود عبد العاطي، **مرجع سابق**، ص368.

[38]- باطلي غنية، **مرجع سابق**، ص ص44-49.

[39]- غنية باطلي، **مرجع سابق**، ص45.

[40]- **المرجع نفسه**، ص46.

[41]- Jean François Casile, **Le Code pénal à l'épreuve de la délinquance informatique**, Presse Universitaire d'Aix, Marseille, 2002, p97.

[42]- سعيد عبد اللطيف حسن، **إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت**، دار النهضة العربية، القاهرة، 1999، ص42 وما بعدها.

[43]- نائلة عادل محمد فريد، **مرجع سابق**، ص48.

[44]- لتفاصيل حول هذه الجزئية راجع:

* خالد ممدوح إبراهيم، **مرجع سابق**، ص77 وما بعدها.

* غنية باطلي، **مرجع سابق**، ص50.

* أشرف جمال محمود عبد العاطي، **مرجع سابق**، ص366.

* حكيم سياب، "**السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية**"، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد الأول، العدد الأول، ص ص212-240.

[45]- غنية باطلي، **مرجع سابق**، ص50.

[46]- **المرجع نفسه**، ص51.

[47]- علاء عبد الباســط خلاف، **الحماية الجنائية لوســائل الاتصــال الحديث**، رســالة مقدمة لنيل درجة الدكتوراه في القانون، كلية الحقوق، جامعة القاهرة، 2002، ص47. نقلا عن: أشرف جمال محمود عبد العاطي، **مرجع سابق**، ص365.

[48]-موقعة في 23 نوفمبر 2001 من طرف 67 دولة، وتتعلق بالإجرام الكوني والجرائم المعلوماتية، دخلت حيز التنفيذ بداية من 01 جويلية 2004. متوفرة على الموقع الرسمي للمجلس الأوروبي باللغتين الفرنسية والإنجليزية، للاطلاع: www.coe.int

[49]-زيبري مارية، "**الدور السلبي للتطور التكنولوجي في تنامي جرائم الاستغلال الجنسي للأطفال عبر الانترنت في ظل الإشكالات الجزائية في مجال المكافحة**"، مداخلة مقدمة ضـمن فعاليات المؤتمر الدولي الافتراضـي حول "انعكاسـات التطور التكنولوجي على حق الإنسـان في السـلامة الجسـدية"، المنظم من طرف المركز الديمقراطي العربي، برلين -ألمانيا، أيام 18/17 أفريل 2021، ص ص267-277.

[50]-قيشوش رحمونة، "**الحماية القانونية للطفل ضـحية الاسـتغلال الجنسـي في ظل الفضـاء الرقمي**"، مجلة نوميروس، المجلد الأول، العدد الثاني، جوان 2020، ص218 وما بعدها.

[51]-بودبة سعيدة، "**الإستغلال الجنسي للأطفال عبر الانترنت**"، مجلة البحوث والدراسات القانونية والسياسية، العدد الثالث عشر، ص ص86-90.

[52]-راجع لتفاصيل حول مختلف التطورات التي شهدتها جريمة الاستغلال الجنسي للأطفال عبر الانترنت:

*رشا خليل، "**جرائم الاستغلال الجنسي للأطفال عبر الانترنت**"، مجلة الفتح، العدد 27، 2006.

*بن تركية نصيرة، "**استغلال الطفل في المواد الإباحية ما بين الخطر الدولي والتجريم الوطني**"، المجلة الجزائرية للحقوق والعلوم السياسية، العدد الرابع، ديسمبر 2014.

[53]- This deffinition cited by « Barry Collin » in 1986, to read the details of this article check : Desforges Alix, « **Cyber-Terrorism** : **quel Périmètre** », fiche N11 de l'institut de recherche stratégique de l'école militaire (IRSEM), Décembre 2011, Article on ligne disponible sur le site : www.defense.gov.fr consultée le : 23 Mai 2021.

[54]-عياشي فاطمة، بودفع علي، "**تأثير الإرهاب الإلكتروني على الأطفال وطرق الوقاية منه**"، مجلة الحقوق والحريات، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، المجلد التاسع، العدد الأول، 2021، ص ص127-154.

[55]-بليدي دلال، بوقرين عبد الحليم، "**الآليات القانونية لمكافحة الجرائم الإلكترونية ضـــد الأطفال**"، مجلة التمكين الاجتماعي، العدد الأول، مارس 2019، ص80.

[56]-شمامة بوترعة، "**الألعاب الالكترونية لدى الأطفال بين حق الممارسة وفقا للمادة 31 من اتفاقية حقوق الطفل وتهديد الحق في الحياة والسلامة الجســدية –لعبة الحوت الأزرق نموذجا**"، مداخلة مقدمة ضـــمن فعاليات المؤتمر الدولي الافتراضـــي حول "انعكاســـات التطور التكنولوجي على حق الإنسان في السلامة الجسدية"، المنظم من طرف المركز الديمقراطي العربي، برلين -ألمانيا، أيام 18/17 أفريل 2021، ص122.

[57]-قدي سومية، "**إدمان الألعاب الإلكترونية وعلاقتها بالتنمر في الوسط المدرسي –دراسة ميدانية على تلاميذ المرحلة الابتدائية بمستغانم**"، مجلة التنمية البشرية، العدد الأول، مارس 2018، ص165.

[58]-ترتب عن ظهور وانتشـار فيروس كورونا (كوفيد 19) اتسـاع صـور وأشـكال المخاطر المترتبة عن الألعاب الالكترونية وذلك بسـبب فرض الحجر الصـحي وما رافقه من هروب فئة واسـعة من الأطفال للعالم الرقمي، لتفاصـيل حول هذه المخاطر والجزئيات المتعلق بها راجع: نادية عبد المهدي عبد النبي، "**إدمان الألعاب الإلكترونية وانعكاسـاتها السـلبية على حق الطفل في السـلامة الجسـدية –ظاهرة النزوح الافتراضـي للطفل في زمن كورونا نموذجا**"، مداخلة مقدمة ضمن فعاليات المؤتمر الدولي الافتراضي حول "انعكاسات التطور التكنولوجي على حق الإنسان في السلامة الجسدية"، المنظم من طرف المركز الديمقراطي العربي، برلين -ألمانيا، أيام 18/17 أفريل 2021، ص163.

[59]-غياث حياة، مرباح فاطمة الزهراء، "**الجرائم الإلكترونية الحديثة وإشـــكالية التعامل معها –تحدي الحوت الأزرق وظاهرة انتحار الأطفال في الجزائر–**"، مجلة دراسات إنسانية واجتماعية، العدد العاشر، جوان 2019، ص271.

[60]-بهلول سمية، شـــوقي يعيش تمام، "**الهيئات الوطنية المكلفة بمكافحة الجرائم الإلكترونية في التشـــريع الجزائري**"، مداخلة مقدمة ضـــمن فعاليات الملتقى الدولي حول الجرائم المستحدثة بين خطورة الآثار وآليات المكافحة المنظم من طرف كلية الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، يومي 11/10 ماي 2021.

[61]- المرســوم الرئاســي رقم 15-261 المؤرخ في 08 أكتوبر 2015 يحدد تشــكيلة وتنظيم وكيفيات ســير الهيئة الوطنية للوقاية من الجرائم المتصــلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر العدد 53 الصادرة في 08 أكتوبر 2015.

[62]- المادة الثانية (02) من المرسوم الرئاسي 15-261.

[63]- المادة الرابعة (04) من المرسوم الرئاسي 15-261، **مرجع سابق**.

[64]- الأمر 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[65]- القانون 09-04، **مرجع سابق**.

[66]- تم تحديد هذه المهام والتفصيل فيها بموجب: المادة الرابعة عشر (14) من القانون 09-04، المادة الرابعة (04) من المرسوم الرئاسي 15-261.

[67]- المادة السادسة عشر (16) من المرسوم الرئاسي 15-261.

[68]- المادة التاسعة عشر (19) من المرسوم الرئاسي 15-261.

[69]- المادة 20 من المرسوم الرئاسي 15-261.

[70]- المادة 21 من المرسوم الرئاسي 15-261.

[71]- المواد 21-22 من المرسوم الرئاسي 15-261.

[72]- المادة 31 من المرسوم الرئاسي 15-261.

[73]- المرســوم التنفيذي رقم 16-334 المؤرخ في 19 ديســمبر 2016 المحدد لشــروط وكيفيات تنظيم وســير الهيئة الوطنية لحماية وترقية الطفولة، ج.ر.ج.ج العدد 75 الصادرة في 21 ديسمبر 2016.

[74]-المادة السابعة (07) من المرسوم التنفيذي 16-334.

[75]-المواد 22-23 من المرسوم التنفيذي 16-334. ولتفاصيل حول هذه الاختصاصات راجع: شرون حسينة، قفاف فاطمة، **"الدور الحمائي للهيئة الوطنية لحماية وترقية الطفولة"**، حوليات جامعة الجزائر1، العدد 32، الجزء الثاني، جوان 2018، ص ص540-551.

[76]-المادة الرابعة والعشرون (24) من المرسوم التنفيذي 16-334.

[77]- شرون حسينة، قفاف فاطمة، **مرجع سابق**، ص546.

[78]- يذهب جانب من الفقه إلى القول بأن تسمية الشرطة العلمية والتقنية ينصرف إلى أنها تطلق "**على مجموع المعارف والأساليب والوسائل العلمية والتقنية المعتمد عليها في المعاينة والبحث والاختبارات والتحاليل بهدف إقامة الدليل في الدعاوى القضائية**"، في حين يذهب جانب آخر إلى القول بأن مفهومها ينصرف إلى العنصر البشري وذلك بالاعتماد على "**فريق العمل المتخصص الذي يتكون من خبراء مدنيين وغير مدنيين يعملون كل حسب تخصصه**"، راجع في هذا الإطار: بهلول مليكة، **دور الشرطة العلمية والتقنية في الكشف عن الجريمة**، رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق، كلية الحقوق، جامعة الجزائر 1، 2013، ص181.

[79]- لتفاصيل حول هذه الجزئية راجع: حملاوي عبد الرحمن، **"دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية"**، مداخلة مقدمة ضمن فعاليات الملتقى الوطني حول "الجريمة المعلوماتية بين الوقاية والمكافحة"، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، يومي 16-17 نوفمبر 2015.

[80]- بهلول مليكة، **المرجع السابق**، ص176.

[81]- راجع للاطلاع على مختلف المناهج والإجراءات المستحدثة في هذا الإطار الموقع الرسمي للشرطة الجزائرية: www.algeriepolice.dz تاريخ الزيارة: 16 سبتمبر 2017.

[82]- المادة الأولى (01) من المرسوم الرئاسي 04-183 المؤرخ في 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر العدد 41 الصادرة في 27 جوان 2004.

[83]- المادة الثانية (02) من المرسوم الرئاسي 04-183.

[84]- للاطلاع على مهام المعهد راجع المادة الرابعة (04) من المرسوم الرئاسي 04-183.

[85]- للاطلاع على الموقع الرسمي للشكوى المسبقة والاستعلام عن بعد: https://ppgn.mdn.dz تاريخ الزيارة 03 جانفي 2018.

[86]- غنية باطلي، **مرجع سابق**، ص197.

[87]- غنية باطلي، **مرجع سابق**، ص ص201-202.

[88]- المادة الثلاثون (30) من قانون العقوبات.

[89]- غنية باطلي، **المرجع السابق**، ص204.

[90]- **المرجع نفسه**، ص205.

[91]- لتفاصيل حول مختلف هذه القواعد الإجرائية راجع:

* شيدة بوكر، **جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن**، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2012.

*حاحة عبد العالي، قلات سمية، **"المكافحة الإجرائية للجرائم الالكترونية (دراسة حالة الجزائر)"**، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد 16، ديسمبر 2017، ص ص227-243.

[92]- المادة الثانية الفقرة "و" من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **مرجع سابق**.

[93]- المادة الرابعة (04)، **المرجع نفسه**.

[94]-راجع لتفاصيل حول هذه الشروط ومختلف الإجراءات المتعلقة بها:

*حاحة عبد العالي، قلات سمية، **"المكافحة الإجرائية للجرائم الالكترونية (دراسة حالة الجزائر)"**، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد 16، ديسمبر 2017، ص ص227-243.

* مزيود سليم، **"الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"**، المجلة الجزائرية للاقتصاد والمالية، العدد الأول، أفريل 2014، ص ص94-107.

* امحمدي بوزينة آمنة، "**إجراءات التحري الخاصـــة في مجال مكافحة الجرائم المعلوماتية (دراســـة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)**، ورقة بحث مقدمة ضـمن فعاليات الملتقى الوطني حول "آليات مكافحة الجرائم الالكترونية في التشـريع الجزائري"، المنظم من طرف مركز جيل البحث العلمي، الجزائر العاصمة، 29 مارس 2017، ص ص57-82.

[95]- المادة الخامسة (05) من القانون 09-04، **مرجع سابق**.

[96]- المادة الخامسة (05) الفقرة الأخيرة من القانون 09-04، **المرجع نفسه**.

[97]- المادة السادسة (06) من القانون 09-04، **المرجع نفسه**.

[98]- المادتين السابعة (07) والثامنة (08)، **المرجع نفسه**. ولمزيد من التفاصيل حول هذه الجزئيات راجع:

* مزيود سـليم، "**الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها**"، المجلة الجزائرية للاقتصـاد والمالية، العدد الأول، أفريل 2014، ص ص94-107.

* امحمدي بوزينة آمنة، "**إجراءات التحري الخاصـــة في مجال مكافحة الجرائم المعلوماتية (دراســـة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)**، ورقة بحث مقدمة ضـمن فعاليات الملتقى الوطني حول "آليات مكافحة الجرائم الالكترونية في التشـريع الجزائري"، المنظم من طرف مركز جيل البحث العلمي، الجزائر العاصمة، 29 مارس 2017، ص ص57-82.

[99]- لتفاصيل حول هذه الجزئية راجع:

* حجازي عبد الفتاح، **الإثبات الجنائي في جرائم الكمبيوتر والانترنت**، دار الكتب القانونية، مصر، 2007.

* ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، رسالة مقدمة لنيل شهادة الدكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2016.

* محمد علي قطب، **الجرائم المعلوماتية وطرق مواجهتها (الجزء الرابع)**، الأكاديمية الملكية للشرطة، مملكة البحرين، جويلية 2010.

* عبد الناصـر محمد محمود فرغلي، محمد عبيد سـيف سـعيد المسـماري، "**الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية –دراسـة تطبيقية مقارنة**"، ورقة بحث مقدمة ضـمن فعاليات المؤتمر العربي الأول حول "علوم الأدلة الجنائية والطب الشـرعي"، جامعة نايف العربية للعلوم الأمنية، الرياض، من 12 إلى 14 نوفمبر 2007.

[100]- يتم استعماله عبر موقعه الإلكتروني التالي: www.m.kiddle.co