التعاون الدولي في مواجهة الجرائم السيبرانية: الجزائر نموذجا

International Cooperation in Confronting Cybercrimes: Algeria As A Model

آسيا لعمراني

كلية العلوم السياسية والعلاقات الدولية - جامعة الجزائر 3

ass_lamrani@yahoo.fr

تاريخ الاستلام: 2012/09/17 تاريخ القبول: 2012/12/05

ملخص: لقد ساهمت التطورات التكنولوجية والثورة المعلوماتية التي شهدها العالم منذ نهاية الحرب الباردة، في تغير طبيعة التهديدات الأمنية من تقليدية إلى غير تقليدية. الأمر الذي جعل جميع الدول في مواجهة العديد من التهديدات الجديدة، لاسيما السيبرانية منها، وما يمكن أن تطرحه هذه التهديدات من جرائم قد تمس أمن الدول والأفراد.

وفي هذا الإطار عملت الجزائر على تطوير استراتيجية أمنية متعددة الجوانب تتناسب مع طبيعة هذه الجرائم، من خلال تعزيز منظومتها القانونية ومطابقتها للاتفاقيات الإقليمية والدولية، للرد على تحديات الإجرام السيبراني في مختلف المستويات. ونظرا لحداثة هذه الجرائم، وفي ظل غياب تعريف موحد ومحدد لها بما يسمح من تحديد آليات مكافحتها، أصبح من الصعب على الدول مواجهتها بمفردها، مما يستوجب تعاون دولي حقيقي قائم على أساس التنسيق المشترك وتبادل الخبرات والمعلومات.

الكلمات المفتاحية: الجريمة الإلكترونية، تكنولوجيات الإعلام والاتصال، الجزائر، الميكانيزمات، التعاون.

Abstract: The information and communication technologies (ICT's) revolution, that the world has witnessed since the end of the Cold War, affect our perception of security. This made all countries facing many new kinds of threats, especially cybercrime, that threat which can affect both the security of states and individuals. In this context, Algeria worked on developing a multi-faceted security strategy commensurate with the nature of these crimes, by strengthening its legal system and its conformity to regional and international agreements, in order to respond to the challenges of cybercrime at various levels. Given the novelty of these crimes and the lack of a unified and specific definition allowing the adoption of mechanisms to combat them, it has become difficult for countries to combat them on their own, which requires real international cooperation based on mutual coordination and the exchange of experiences and information.

Key words

Electronic crime, legislation, social networking sites, cybercrime.

*المؤلف المرسل

مقدمة:

إن تطور الثورة المعلوماتية ودخول العالم عصر الرقمنة، لاسيما في القرن الواحد والعشرين، أدى إلى ظهور العديد من الجرائم المرتبطة بالتقنية المعلوماتية، التي تعددت صورها وأشكالها، وبات يطلق عليها الجرائم السيبرانية، الأمر الذي جعلها تشكل تهديدا أمنيا حقيقيا، مشكلة بذلك المجال الخامس للحروب.

هذه التهديدات التي باتت تمس أمن الدول من خلال التجسس والتخريب لاسيما المنشآت الحيوية، مثل الأجهزة الأمنية، والمؤسسة العسكرية، المؤسسات الحكومية، الشركات والبنوك...الخ.

وبالتالي أصبح من الصعب جدا على الدول توفير الحماية لأنظمتها المعلوماتية، وحتى أمن أفرادها، خاصة وأن التدفق الهائل الذي تعرفه عملية الاستعمال المتزايد لأجهزة الإعلام (الثورة المعلوماتية)، دفع بها إلى الدخول في مواجهة مستمرة مع فواعل ممن يمتلكون المهارة والوسيلة المعلوماتية، ولهم القدرة على توظيفها لاختراق كل الأنظمة الحساسة مهما كانت القدرات والاحتياطات الأمنية المتوفرة. كما أن عمليات الاختراق بلغت مستويات مختلفة من شأنها أن تمس بالأمن الوطني والعالمي.

ولهذا فإن أي دولة مهما كانت قدراتها ستصبح إحدى ضحايا التهديدات السيبرانية، مما يستدعي ضرورة وضع الآليات الكفيلة لحماية هذه البيئة الرقمية من التحديات التي تفرزها التطورات التكنولوجية. وفي هذا السياق سعت الجزائر لبحث تصورات واستراتيجيات لمواجهة الجرائم السيبرانية في إطار التعاون الدولي.

ومن هنا تبحث إشكالية الدراسة في مدى فعالية الاستراتيجية الجزائرية للتوفيق بين مواجهة الجرائم السيبرانية من جهة، وتحديات تحقيق التعاون الدولي في هذا المجال من جهة أخرى.

للإجابة على الإشكالية المطروحة أعلاه، تم تقسيم الدراسة إلى ثلاثة محاور أساسية:

- تحديد الإطار المفاهيمي للدراسة.
- الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية.
- التعاون الجزائري-الدولي في مواجهة الجرائم السيبرانية.

أولا: تحديد الإطار المفاهيمي للدراسة:

يعتبر "ألفين توفلر" Alvin Toffler عالم الاجتماع الأمريكي "أن الوصول والسيطرة على المعلومة تشكل سلطة جديدة، تماما مثل القوة والمال".[1] وعليه فإنه أمام التطور الهائل في المعلوماتية في أكثر من مجال، أصبح من الضروري البحث عن الإطار المناسب لضمان سلامتها حتى تؤدي غرضها. ومن هذا المنطلق سمحت الأنظمة المعلوماتية لمجموعة من الأفراد طبيعيين أو غير طبيعيين، للتواصل والتلاقي بصفة مستمرة أو مؤقتة من أجل تبادل المعلومات (صور، صوت، تقارير...إلخ)، ليس فقط عن طريق الآلة الفردية (الحاسوب الشخصي) بل تتعداه إلى مجالات عدة كمتعامل الهاتف النقال، مواقع الأنترنت أو مجالات الهيئات الرسمية (وزارة الدفاع الوطني، الوزارات السيادية...إلخ)، فيما أصبح القاسم المشترك بين الجميع احترام قواعد المعاملات. وفي هذا الإطار لابد من التفريق بين عدة مفاهيم والتي تتقاطع فيما بينها، تتمثل فيما يلي:

- **الفضاء السيبراني:**

تتفق جميع الدراسات العلمية على أن الفضاء السيبراني[2]، هو بيئة افتراضية تعتمد في بنيتها على التكنولوجية الحديثة في التعامل والتواصل بين العديد من الفواعل، سواء كانوا أشخاص أو هيئات حكومية وغير حكومية من خلال شبكة إلكترونية (الحاسوب) ، لها استقلاليتها عن وسائل الاتصال. بمعنى آخر أن كل المعلومات والمعاملات المتداولة بقدر ما تسهل عملية الاندماج بين كل أجهزة الاتصالات والأقمار الصناعية، والفضاء الإلكتروني، بقدر ما تفتح المجال لعمليات الاختراق.

---

[1] إيريك ليوبولد-سيرج لوست، **أمن المعلومات**.(ترجمة: فتحي علي زمال)، المملكة العربية السعودية، مدينة الملك عبد العزيز للعلوم والتقنية، 2014، ص 12.

[2] اشتقت كلمة "سايبر" Cyber من الفعل اليوناني "كيبرنو" Kuberno والذي يعني "يقود"، وعليه تصبح السيبرانية Cybernetics علم الاتصالات والمعلومات والتحكم، كما ترتبط هذه الكلمة مع "الملاحة" Navigation خلال فضاء من البيانات الإلكترونية، إضافة إلى التحكم الذي يتحقق عبر معالجة تلك البيانات. **أنظر:**

عادل عبد الصادق، **الفضاء الالكتروني والرأي العام: تغير المجتمع والأدوات والتأثير**. القاهرة: المركز العربي لأبحاث الفضاء الالكتروني، 2009، ص ص 7-8.

ويعد عالم الرياضيات الأمريكي "نوربير وينر" (Norbert Wiener)، أول من نسب إليه استخدام مصطلح السيبرانية من خلال دراسته لموضوع القيادة والاتصال في عالم الحيوان وحقل الهندسة الميكانيكية. حيث وضع تعريف دقيق لهذا المفهوم، بأنه "علم التحكم والتواصل عند الحيوان والآلة، لنقل الرسائل بين الإنسان والآلة، أو بين الآلة والآلة، كما يعتبره علم القيادة أو التحكم في كل منهما".[3]

لقد أحدث التطور التكنولوجي بعد الحرب العالمية الثانية خاصة مع ظهور الأنترنت، مجموعة من المفاهيم التي أصبحت تعبر على هذا الفضاء، وحل الكمبيوتر محل الآلة التي تكلم عليها "نوربير وينر". حيث تم استخدام مصطلح الفضاء السيبراني للمرة الأولى من طرف الكاتب في الخيال العلمي "وليام جيبسون "William Gibson، في قصة قصيرة عام 1982، حيث اعتبره مزيج من "علم التحكم الآلي" و"الفضاء".[4]

فالفضاء السيبراني أو الإلكتروني كما يسميه البعض، شأنه شأن ظاهرة الفضاء التقليدية التي تتألف من أربعة مكونات رئيسية هي المكان والمسافة والحجم والمسار، يعبر محتواها عن طبيعة وجود هذا المحتوى، والذي يتميز بغياب الحدود الجغرافية وغياب الحكم القاهر للزمن، ويتطلب ذلك العالم الافتراضي لوجود هيكل مادي من أجهزة الكمبيوتر وخطوط الاتصالات. وبالتالي تصبح القيمة الحقيقية له في القدرة على الاستفادة من كم المعلومات الموجودة داخله والمساهمة والتحكم بها في إطار وشكل إلكتروني.[5]

من خلال التعاريف السابقة الذكر، يبدو أن الفضاء السيبراني يرتبط بشكل كبير بشبكات الأنترنت، فبالعودة إلى تقرير الاتحاد الدولي للاتصالات، هناك أكثر من نصف سكان العالم موصولون حاليا بالأنترنت، كما سيكون عدد مستعملي الأنترنت 51.2 % من الأفراد، أي

---

[3] أصدر "نوربير وينر" كتاب بعنوان "علم التحكم الآلي، أو التحكم والاتصال في الحيوان والآلة"، الذي نشر في طبعته الأولى عام 1948، وترجم إلى عشرات اللغات، اقترح هذا المفهوم لتعزيز رؤية موحدة للمجالات الناشئة الأوتوماتيكية والإلكترونية والنظرية الرياضية للمعلومات، أنظر:

Wiener Norbert, **Cybernetics or control and communication in the Animal and the machine**. Cambridge, Massachusetts Institute of Technology, Second edition, 1961.

[4] P. W. SINGER, ALLAN FRIEDMAN, **CYBERSECURITY AND CYBERWAR WHAT EVERYONE NEEDS TO KNOW**. OXFORD UNIVERSITY PRESS, 2014, p12.

[5] عبد الصادق، الفضاء الإلكتروني والرأي العام: تغير المجتمع والأدوات والتأثير. **مرجع سابق**، ص9.

ما يساوي 3.9 مليار نسمة، حيث يمثل ذلك خطوات هامة نحو مجتمع معلومات عالمي أكثر شمولا. ففي البلدان المتقدمة، هناك أربعة أفراد من بين كل خمسة أفراد موصولون بالأنترنت. وفي البلدان النامية، تبلغ نسبة الأفراد من مستعملي الأنترنت 45 %. وفي أقل البلدان نموا البالغ عددها 47 بلدا في العالم لا يزال انتشار الأنترنت منخفضا نسبيا، وهناك أربعة أفراد من كل خمسة أفراد (80%) لا يستعملون الأنترنت.[6]

لقد دفع التقدم التكنولوجي وثورة المعلومات، بالدول الكبرى إلى توظيف الأدوات السيبرانية لتعزيز قدراتها خاصة العسكرية، فالولايات المتحدة الأمريكية تعتمد بدرجة كبيرة على الأنترنت[7] في عمليات تنظيم الجيش وزيادة قدراته في أرض المعركة (القيادة، الهجوم، والسيطرة)، وكذا تنظيم الإمدادات وشبكة الاتصالات، وأي اختراق محتمل من الممكن أن يقوض قدراتها الهجومية أو الدفاعية أو قدراتها على الإمداد من الخارج (نفس النهج سارت عليه روسيا والصين).

من خلال ما سبق ذكره، يمكن وصف الفضاء السيبراني على أنه شبكة عالمية مترابطة من المعلومات الرقمية والبنى التحتية للاتصالات، بما في ذلك الأنترنت، وشبكات الاتصالات، وأنظمة الكمبيوتر والمعلومات.

- **التهديد السيبراني:**

بقدر ما تتيح تكنولوجيا المعلومات والاتصالات إمكانات هائلة وغير مسبوقة، لإنتاجية أفضل في جميع القطاعات، للتواصل عبر القارات بالاعتماد على البنية التحتية لهذه التقنيات، التي تمثل ارتباطا بين مصالح متعددة وخدمات مختلفة وبلدان عديدة، بقدر ما تفتح المجال لتكون عرضة للتهديد المقصود (كالاختراقات والاعتداءات) أو غير المقصود (كالإهمال، وقلة الوعي والإدراك) ، مما قد يعرض أنظمتها المعلوماتية إلى خطر دائم، خاصة وأن التعقيدات

---

[6] "تقرير قياس مجتمع المعلومات لعام 2012 -ملخص تنفيذي"، الاتحاد الدولي للاتصالات، جنيف، 2012، ص2.

[7] هذه الشبكة المعلوماتية أنشأت عام 1969(ARPA: The Advanced Research Project Administration) كانت تهدف من خلالها وزارة الدفاع الأمريكية، إلى تسهيل التواصل بين الإدارة العسكرية ومتعهد بالقوات المسلحة، وعدد كبير من الجامعات، لكن الاستخدام الكثيف للشبكة من قبل الجامعات ومراكز الأبحاث، أدى إلى ازدحام حركة العمل عليها، فأنشئت شبكة جديدة في عام 1983سميت MILNET أي الشبكة العسكرية، وخصصت لخدمة المواقع العسكرية، وتم ربطها بواسطة بروتوكول الأنترنت مع ARPA.

الناشئة عما يرتبه العمل الإجرامي لا يسمح بتحديد الهوية، ومعرفة مصدر الهجوم أو الاختراق، وإمكانية الإثبات رغم القدرات والخبرات المتوفرة في مجال تقنيات المعلومات والاتصالات [8].

ويقصد بالتهديدات السيبرانية أو الإلكترونية "تلك الهجمات التي تتم باستخدام آليات وشبكات إلكترونية كالأنترنت وأجهزة الحاسب الآلي، وتهدف إلى إلحاق الضرر بأجهزة أو شبكات إلكترونية أخرى، أو سرقة المعلومات الموجودة عليها. وهو ما يعنى أن "إلكترونية" التهديدات تشير إلى كل من أداة الهجوم، أي الآليات المستخدمة في شنه، وإلكترونية الهدف المتعرض له"[9]. ولا تقتصر التهديدات السيبرانية على قضية الإرهاب الإلكتروني فقط، وإنما تشمل العديد من المخاطر والتهديدات الأخرى التي لا ترتبط بأمن الدول فقط، بل تشمل المجتمع ككل، فهي متعلقة بأمن الأفراد والمنظمات أيضا[10]. لهذا يشمل التهديد ثلاثة فئات تتمثل فيما يلي:

الفئة الأولى تخص الدول: وهي مجموعة التهديدات التي يتعرض لها الأمن القومي، في المجالات السياسية، العسكرية، الاقتصادية، والاجتماعية، ويهدد البنية التحتية والحيوية للدول، وأسواق المال والقطاعات المصرفية، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل بكل أنواعه: البري والبحري والجوي.

الفئة الثانية تخص المنظمات: هذه التهديدات تستهدف التأثير على الفضاء الإلكتروني الذي بات يشكل مكونا رئيسيا في مسار عمل المنظمات، حيث تؤثر على أسلوب عملها وتهدد استمرارها، من خلال إحداث الضرر المادي أو الوظيفي للأجهزة أو النظم والهياكل الإلكترونية سواء تعطيلها أو اختراقها.

---

[8] هناك فئات مختلفة من مهاجمي المواقع، والتي تتدخل بشكل فردي أو من خلال المنظمات، من بينها: المتسللين أو المخترقين Hackers (مصنفون في ثلاثة فئات: أصحاب القبعات البيضاء White Hat Hackers ، وأصحاب القبعات الرمادية Gray Hat Hackers ، وأصحاب القبعات السوداء Black Hat Hackers)، قراصنة الأنترنت Cyber-pirates، المخربين Crakers الذين يكسرون حماية البرمجيات، مخترقي البطاقات Carder الذين يكسرون أنظمة حماية بطاقة الرقاقة، قراصنة شبكة الهاتف Phreakers أي اختراق نظام حماية أنظمة الهاتف.

[9] نوران شفيق، "أشكال التهديدات الإلكترونية ومصادرها". المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، https://www.europarabct.com/?p=34807

[10] عنترة بن مرزوق، محي الدين حرشاوي، "الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية". (ورقة بحث قدمت في الملتقى الدولي حول سياسات الدفاع الوطني)، جامعة ورقلة (الجزائر)، 30-31 جانفي 2017، ص69.

الفئة الثالثة وتخص الجوانب الشخصية للأفراد: مثل سرقة البيانات الشخصية وتسريبها، واستخدامها دون إذن، وسرقة الأموال، والاعتداء على الملكية الفكرية، والصناعية، والعلامات التجارية، والاحتيال، والبريد غير المرغوب فيه، والجرائم ضد الأطفال، والمحتوى غير المشروع، وغيرها من المخاطر التي تعتبر جرائم سيبرانية لها علاقة مباشرة بالأشخاص وممتلكاتهم.

ومنه نستنتج، أن التهديد السيبراني هو محاولة إلحاق الضرر والأذى سواء ضد الأشخاص أو المنظمات أو الدول، من خلال استعمال مختلف الوسائل المعلوماتية والتكنولوجية، بغرض تحقيق أهداف معينة، قد تكون سياسية، اقتصادية، عسكرية، إيديولوجية، أو دينية...الخ.

- **الجريمة السيبرانية:**

تعتبر الجريمة السيبرانية من الجرائم التي واكبت التطور التكنولوجي والمعلوماتي. وبالنظر إلى عدم التحكم فيها، فإنه بات من الصعب إيجاد تعريف محدد وموحد لها، حيث توجد عدة تسميات متداخلة مثل: الجرائم الإلكترونية، جرائم الحاسوب، جرائم الأنترنت، جرائم التقنية العالية، جرائم الياقات البيضاء، وجرائم الجيل الخامس...الخ.

تعرف المفوضية الأوروبية الجريمة السيبرانية بأنها: "الأفعال الإجرامية المرتكبة باستخدام شبكات الاتصالات الإلكترونية ونظم المعلومات أو ضد هذه الشبكات والأنظمة". ولقد تم تصنيفها إلى ثلاث فئات من الأنشطة الإجرامية: **الفئة الأولى** تغطي الأشكال التقليدية للجريمة مثل الاحتيال أو التزوير (رغم أنه في سياق الجريمة السيبرانية يتعلق الأمر بتحديد الجرائم المرتكبة عبر شبكات الاتصالات الإلكترونية ونظم المعلومات). **الفئة الثانية** تتعلق بنشر محتوى غير قانوني عبر الوسائط الإلكترونية (أي مواد الاعتداء الجنسي على الأطفال أو التحريض على الكراهية العنصرية). وتشمل **الفئة الثالثة** الجرائم الفريدة للشبكات الإلكترونية (أي الهجمات ضد أنظمة المعلومات، الحرمان من الخدمة والقرصنة). ويمكن أيضا توجيه هذه الأنواع من الهجمات على البنية التحتية الحيوية في بعض الدول، والتي تؤثر على أنظمة الإنذار السريع الحالية في العديد من المجالات، مع عواقب وخيمة على المجتمع بأسره.[11]

[11] Martti Lehto, Pekka Neittaanmäki, Cyber Security: Analytics, Technology and Automation. Springer International Publishing Switzerland 2012, p11.

هذه الجرائم تعتبر حديثة وغير معروفة بين صور الإجرام البشري التقليدي، الأمر الذي جعل البعض يعرفها بأنها: "الجريمة التي لا تعرف الحدود"، منهين إلى أن شبكة الأنترنت التي ألغت الحدود الجغرافية بين الدول ذات فاعلية تفوق قدرة الأجهزة الدولية المختصة بمكافحة الجريمة[12].

كما أنها تستعمل سلاح الفيروسات، وذلك بالدخول غير الشرعي ونسخ برامج خبيثة في أجهزة المستخدمين من غير معرفتهم، لتحدث بذلك خللا بغية تدمير البيانات أو الحصول عليها أو استبدالها بملفات خاصة به من الجهاز المستهدف، مما يتسبب بعدم قدرته على الإقلاع[13]، كما تهدف إلى تعطيل الخوادم والأجهزة التابعة للمؤسسات الحكومية وحذف محتويات الأقراص الصلبة.

وحسب اتفاقية بودابست لعام 2001 تم تصنيف الجرائم السيبرانية إلى أربعة أصناف، تتمثل فيما يلي[14]:

– الجرائم التي تستهدف سرية وسلامة وتوفر المعطيات، أي الجرائم التي تستهدف معطيات الكمبيوتر سواء بالاطلاع عليها، أو إفشائها أو تصويرها أو إتلافها.

---

[12] في آخر تقرير لوكالة تطبيق القانون الأوروبية، فإن قراصنة الويندواوز سجلوا أضخم هجوم على عشرات آلاف أجهزة الكمبيوتر في أكثر من 100 دولة، من بينها: روسيا، والهند، والصين، وبريطانيا، وفرنسا، وإيطاليا، وألمانيا، والبرتغال، وفيتنام، وتايوان، بحيث استطاعت "جماعة وسطاء الظل من إطلاق برمجية الفدية الخبيثة" التي يطلق عليها (Wanna Cry)، والتي تسببت في عرقلة تعاملات وخدمات مؤسسات متعددة وتعطيل شبكاتها وأجهزتها الإلكترونية، وإلحاق الدول خسائر مالية ضخمة.

[13] في نفس الإطار، يقول الخبراء أنه مع بداية 2010 ظهر ما يعرف باسم "إعصار ويكيليكس" الذي استغل شبكة الأنترنت العالمية لتسريب وثائق سرية للغاية متداولة بين الإدارة الأمريكية وممثلياتها بالخارج. وفي مارس2014 هاجمت مجموعة "سايبر بيكوت الأوكرانية" المواقع الإلكترونية لحلف الناتو، مما أدى إلى تعطيل مواقع الحلف لعدة ساعات. كما أكدت صحيفة نيويورك تايمز في تقرير لها في26 أفريل 2015، أن قراصنة روسيين اطلعوا على رسائل إلكترونية للرئيس الأمريكي السابق "باراك أوباما"، بعدما تمكنوا من اختراق الشبكة الإلكترونية غير السرية للبيت الأبيض، واطلعوا على أرشيف الرسائل الإلكترونية لموظفين في البيت الأبيض الذين يتواصلون يوميا مع أوباما. للمزيد من التفصيل **أنظر:**

يونس عرب، **جرائم الكمبيوتر والأنترنت، المعنى والخصائص والصور وإستراتيجية المواجهة القانونية**. المركز الوطني للتوثيق، أكتوبر2006.

[14] رحيمة ندميلي، "خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة". (أعمال المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، مركز جيل البحث العلمي، طرابلس)، ص11.

– الجرائم المرتبطة بالكمبيوتر، أي الجرائم التي يلعب فيها الكمبيوتر أو الحاسب الآلي دور الوسيلة، كجرائم الاحتيال والتزوير الإلكتروني.

– الجرائم المرتبطة بالمحتوى، أي يلعب فيها الكمبيوتر دور البيئة الجرمية، كجرائم المواد اللاأخلاقية للأطفال، وجرائم القمار، وغسيل الأموال والمخدرات.

– الجرائم المتعلقة بحقوق الملكية الفكرية كحقوق المؤلف، وهو نص مكمل لما جاءت به قوانين الملكية الفكرية المقررة وطنيا ودوليا.

هذه الجرائم يمكن تنفيذها من طرف عدة فاعلين، يمكن تقسيمهم إلى أربع فئات[15]:

- قرصنة فردية، تعمل بشكل منفرد عموما من خلال القدرة على الفعل.

- الناشط، يركز على رفع مكانة إيديولوجية أو وجهة نظر سياسية، في كثير من الأحيان عن طريق خلق الخوف والاضطراب.

- الجريمة المنظمة، التي تركز فقط على المكاسب المالية من خلال مجموعة متنوعة من الآليات، من التصيد إلى بيع بيانات الشركة المسروقة.

- الحكومات، التي تركز على تحسين جيوسياسية موقفها أو مصالحها التجارية.

الجدير بالذكر، أن الهجمات المنفذة من قبل هذه الجهات المختلفة الفاعلة لديها العديد من الخصائص المتباينة، مثل نوع الهدف، طريقة الهجوم، وحجم التأثير.

- **الإرهاب السيبراني:**

يرتبط ظهور هذا المصطلح بظهور الفضاء السيبراني، وتوسع الاعتماد على تقنيات المعلومات والاتصالات، في تنفيذ الشؤون الحياتية اليومية للأفراد، والمؤسسات، والدول. ويرتبط هذا النوع من الإرهاب، بطبيعة البيئة التي يمارس فيها ومن خلالها، وانطلاقا من الوسائل التي يمارس بواسطتها، وينفذ من خلالها، أومن خلال الجهة التي يستهدفها كذلك. وعليه، يمكن تعريف الإرهاب السيبراني "بالأعمال التي تستخدم التقنيات الرقمية، والفضاء

[15] Steve Barlock, Tony Buffomante, Fred Rica , "Cyber security: it's not just about technology ".Information Protection and Business Resilience, 2012:
https://assets.kpmg/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf

السيبراني، لإخافة وإخضاع الآخرين". كما يمكن أن يعرف "بالاعتداءات على أنظمة المعلومات، بدوافع سياسية، أو دينية"[16].

من جهة أخرى، يشير هذا المصطلح إلى عنصرين أساسيين هما: الفضاء الافتراضي والإرهاب، ويتميز عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف للإرهابيين، أي استخدام السلاح الرقمي واختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى[17].

فبقدر ما فسحت العولمة الحديثة مجال للتكنولوجيا من أجل تقريب وتسهيل المعاملات بين الدول والشعوب، بقدر ما أعطت فرص للجماعات الإرهابية لتتفاعل وتنصهر مع هذا العالم الافتراضي، من خلال استخدام شبكات المعلومات والأنترنت والكمبيوتر، وتوظيف التقنيات الحديثة في مجالات الاتصال والمعلوماتية، من أجل الإطلاع على مختلف المعلومات الأساسية للدولة خاصة الأمنية منها، واختراق المواقع الإلكترونية للمؤسسات والمسؤولين.

إن الخطورة الأمنية والمجتمعية لهذا التهديد أخذت بعدا أخطر، خاصة وأن الجماعات المتطرفة كانت من أوائل الجماعات الفكرية التي دخلت العالم الإلكتروني حتى قبل أن تظهر شبكة الأنترنت بسنوات، ومما تشير إليه المصادر الغربية أن أحد أشهر المتطرفين الأمريكيين العنصريين " توم ميتزقر" Tom Metzger من اليمين المتطرف ومؤسس مجموعة المقاومة، كان من أوائل من أسس مجموعة بريد إلكترونية White Aryan Resistance "الإريانية البيضاء" ليتواصل مع أتباعه ويبث أفكاره عام 1985.[18]

---

[16] منى الأشقر جبور، **السيبرانية هاجس العصر**. بيروت: المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، 2016، ص 85.

[17] رفد عيادة الهاشمي، **الإرهاب الإلكتروني**. (د.م.ن)، (د.ت.ن)، ص 5.

[18] أيسر محمد عطية، " دور الآليات الحديثة للحد من الجرائم المستحدثة :الإرهاب الالكتروني وطرق مواجهته".(ورقة مقدمة في ملتقى علمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية). عمان (الأردن)، 02-04 ديسمبر 2014، ص ص 10-11.

تعمل هذه الجماعات على استهداف الأفراد والمؤسسات والدول من خلال استخدام العديد من المواقع، وتأجير مواقع أخرى لنشر ثقافة "التطرف الديني" في أوساط الشباب، وطمس الهوية وتجنيدهم في صفوف المنظمات الجهادية، من أجل التخويف والإرغام والبدء في تحقيق أهداف سياسية، من خلال شن هجمات على مختلف القطاعات السياسية والاقتصادية، والعسكرية. مما يحدث شرخا كبيرا في النسيج المجتمعي ويخلق نوعا من عدم الاستقرار الأمني الدولاتي.

وبالتالي، فإن الإرهاب السيبراني عبارة عن أفعال يقوم بها أفراد أو جماعات، باستخدام الوسائل التكنولوجية والمعلوماتية، وشبكات الأنترنت من خلال زرع الخوف والتهديد، الهدف منها تدمير البنى التحتية للدول وذلك لأغراض معينة، قد تكون سياسية، إيديولوجية، دينية، أو اقتصادية...الخ.

- **الحرب السيبرانية:**

أصبح الفضاء الإلكتروني مجالا للصراعات بين كل أنواع الفواعل سواء من الدول أو من غير الدول، وتبلورت الحروب السيبرانية Cyber Wars في إطار حروب غير تقليدية، مختلفة في خصائصها عن الحروب التقليدية، سواء من حيث طبيعة الأنشطة، أو الفواعل، أو التأثيرات في بنية الأمن العالمي. وتعبر تلك الحروب عن نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني، مما يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات.[19]

هذا المصطلح يشير، إلى الحرب التي تجري في الفضاء الإلكتروني من خلال الوسائل والأساليب السيبرانية، كما يشير إلى سير الأعمال العدائية العسكرية في حالات النزاع المسلح، فاختراق شبكة الكمبيوتر للخصم المحارب مع فيروس خبيث مثلا، من شأنه أن يشكل فعل الحرب السيبرانية[20].

---

[19] عادل عبد الصادق، "أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي". موقع الإمبراطور،2017.06.23: http://alimbaratur.com/?p=2850

[20] Nils Melzer, "Cyberwarfare and International Law". Unidir Resources, 2011, p4.

ويمكن التمييز بين ثلاثة أنماط من هذه الحروب[21]:

النمط الأول-الحرب السيبرانية الباردة منخفضة الشدة: يعبر هذا النمط عن صراع مستمر بين الفاعلين المتنازعين، وقد يكون ذا طبيعة ممتدة، ودائمة النشاط العدائي أو غير السلمي، بخلاف أنه عميق الجذور ومتداخل، وله نواحي متعددة: ثقافية، أو اقتصادية، أو اجتماعية. وعادة ما يتم اللجوء إلى القوة الناعمة للحروب السيبرانية في مثل صراعات كهذه، وإن كانت لا تتطور بالضرورة إلى استخدام القوة المسلحة بشكلها التقليدي، أو شن حرب إلكترونية واسعة النطاق.

ويتم ممارسة هذا النمط عبر القيام بعدة وسائل لعل أهمها، شن الحروب النفسية، والاختراقات المتنوعة، والتجسس، وسرقة المعلومات، وشن حرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية. ويظهر هذا النمط من حالات الحروب في الصراعات السياسية، ذات البعد الاجتماعي – الديني الممتد، مثل الصراع العربي – الإسرائيلي، أو الصراع الهندي – الباكستاني، أو الصراع بين الكوريتين الشمالية والجنوبية، أو الصراع بين إيران وإسرائيل مثل شن الأخيرة هجمات فيروس "ستاكسنت" ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة عام 2010، إلى جانب حالة التوتر بين إستونيا وروسيا عام 2007، والاختراقات المتبادلة التي تتم بين الصين والولايات المتحدة، أو ما بين الأخيرة وروسيا، أو ما بين طهران وواشنطن. ويدخل في هذا النمط التجسس وجمع المعلومات الاستخباراتية، وشن حملات مؤثرة في الرأي العام الداخلي كحالة التدخل الروسي في الانتخابات الرئاسية الأمريكية.

ولقد تعرض العالم لعدد من الهجمات مثل هجمات فيروس "شمعون 2" خاصة بالشرق الأوسط، وهجوم فيروس "ويناكراي"، والذي اتهمت به كوريا الشمالية.

النمط الثاني-نمط الحرب السيبرانية متوسطة الشدة: حيث يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة على الأرض. ويكون ذلك تعبيرا عن حدة

---

[21] عادل عبد الصادق، "الهجمات السيبرانية:أنماط وتحديات جديدة للأمن العالمي".الموسوعة الجزائرية للدراسات السياسية والاستراتيجية،2019/11/27:

https://www.politics-dz.com

الصراع القائم بين الأطراف، كما قد يمهد لعمل عسكري. وتدار حروب الفضاء الإلكتروني عن طريق اختراق المواقع الإلكترونية وتخريبها، وشن حرب نفسية ضد الخصوم وغيرها.

يستمد هذا النوع من الحروب السيبرانية شدته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي، خاصة في ظل بعض التقديرات التي تشير إلى أن تكلفة هذه الحروب قد تشكل أربع مرات من إنفاق نظيراتها التقليدية، بما يمكن من تمويل حملة حربية كاملة عبر الأنترنت بتكلفة دبابة.

تاريخيا، تم استخدام الحروب السيبرانية متوسطة الشدة في هجمات حلف الناتو عام 1999 على يوغوسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم أيضا، وبرزت خلال الحرب بين حزب الله وإسرائيل عام 2006، وكذلك بين روسيا وجورجيا عام 2008، والمواجهات بين حماس وإسرائيل عامي 2008 و2012.

النمط الثالث-الحرب السيبرانية "الساخنة" مرتفعة الشدة: حيث يعبر هذا النمط عن نشوء حروب في الفضاء الإلكتروني منفردة، وغير متوازية مع الأعمال العسكرية التقليدية. لكن لم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل مع تطور القدرات التكنولوجية، واتساع الاعتماد بين الدول والفواعل من غير الدول على الفضاء الإلكتروني.

ينطوي هذا النمط من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار وإدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم الإلكتروني، والاستحواذ على القوة الإلكترونية.

رغم التهديدات الحقيقية بالحرب السيبرانية، ورغم كل التحذيرات الشديدة من خطورة حدوث "سايبر بيرل هاربور"[22]، إلا أن قلة الاهتمام بمثل هذه التحذيرات، اعتبره الخبراء من بين التبريرات التي تفسر ما حدث في الانتخابات الأمريكية التي تتهم روسيا بالتدخل فيها عن

[22]Daniel Ventre, « **La cyber paix, un thème stratégique marginal** », Revue internationale et stratégique,2012/3 n° 87, 2012, p89.

طريق حملات ممنهجة عبر الفضاء السيبراني، هذا النموذج يعتبر بمثابة الدليل القاطع لما قد يؤدي إليه تجاهل التحذيرات بشأن خطورة ما قد يحدث سيبرانيا[23].

من خلال هذا، بات مفهوما أن الحرب السيبرانية تمثل نمطا جديدا من التنافسية، والمتمثل في قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد. لهذا تعتبر هذه الحرب كأداة من أدوات "الجيل الخامس للحروب"، التي سترسم ملامح القرن القادم.

- **الأمن السيبراني:**

ما تضمنه الفضاء السيبراني من عمليات الدخول والخروج، لمختلف مواقع تداول وتخزين المعلومات والبيانات، يستوجب بالضرورة خلق قواعد وآليات تثبيت أصول الأمن لحماية هذه المواقع وأنظمتها المعلوماتية.

في هذا الإطار، يعرف كل من "بيكا نيتنماكي" Neittaanmäki Pekka و "مارتي لهتو" Lehto Martti الأمن السيبراني:" على أنه مجموعة من الإجراءات المتخذة في الدفاع ضد الهجمات الإلكترونية وعواقبها وتشمل تنفيذ التدابير المضادة المطلوبة"[24]. أي أن الأمن السيبراني مبني على تحليل التهديدات، من خلال استراتيجية أمنية وبرنامج تنفيذها على حسب تقدير التهديدات وتحليل المخاطر، ففي كثير من الحالات يصبح من الضروري تحضير العديد من الإستراتيجيات وإرشادات أمان الأنترنت المستهدفة للمؤسسة.

وفقا للاتحاد الدولي للاتصالات لعام 2011، فإن الأمن السيبراني في النهاية يؤدي هدفا معينا، ويجب أن يكون الهدف منه هو بناء الثقة. هذه الأخيرة من شأنها أن تجعل البنية

---

[23] تشير بعض المعلومات إلى أن البريد الإلكتروني للجنة الوطنية الديمقراطية، وواحدة من كبار مساعدي "هيلاري كلينتون"، تم اختراقه ليس فقط لجمع المعلومات الاستخبارية، ولكن أيضا للعثور على معلومات محرجة للدعاية. وقد شارك المخترقون رسائل البريد الإلكتروني المسروقة مع ويكيليكس، والتي أفرجت عنها للجمهور، ما أدى إلى التغطية الإعلامية السلبية للمرشحة الديمقراطية في الفترة التي سبقت يوم الاقتراع. ففي الأشهر التي سبقت الانتخابات، بدأت الشركات الروسية المرتبطة بالكرملين في شراء الإعلانات على فيسبوك، وأنشأت جيشا من حسابات تويتر تدعم "دونالد ترامب"، المرشح الجمهوري. كما أعطت شبكة الأنترنت أجهزة الأمن الروسية القدرة غير المسبوقة للوصول إلى ملايين الناخبين الأمريكيين بالدعاية.

[24] Martti Lehto , Pekka Neittaanmäki, **Cyber Security: Analytics, Technology and Automation**. Springer International Publishing Switzerland 2015, p25

التحتية للمعلومات تعمل بشكل موثوق، وستواصل دعمها للمصالح على المستوى الوطني حتى عندما تتعرض للهجوم. لذلك فإن الأمن السيبراني الوطني يجب أن يركز على بناء استراتيجيات لمواجهة التهديدات التي من المرجح أن تؤدي إلى تعطيل الوظائف الحيوية للمجتمع[25].

لهذا، عرف الأمن السيبراني من زاويتين، أولا، من حيث الأهداف يعتبره النشاط الذي يؤمن حماية الموارد البشرية والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار إلى خسائر دائمة. ثانيا، من حيث المهمة يشير مصطلح "الأمن السيبراني" إلى "مختلف الأنشطة مثل مجموعة الأدوات والسياسات والإجراءات الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والتدريب وأفضل الممارسات والتقنيات، التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمات والمستخدمين".[26]

إضافة إلى ما سبق ذكره، يطال الأمن السيبراني جميع المسائل الاقتصادية، والاجتماعية والسياسية، والإنسانية، وذلك انطلاقا من التعريف المقدم له، على أنه قدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم، بأمان من جهة، ومن كونه يرتبط ارتباطا وثيقا بسلامة مصادر الثروة في العصر الحالي، والتي تعني البيانات، والمعلومات، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكون حوله الإنتاج، والإبداع، والقدرة على المنافسة من جهة أخرى.[27]

فالأمن السيبراني والذي يشار إليه أيضا باسم أمن تكنولوجيا المعلومات، هو مجموعة الوسائل والإجراءات والقوانين والسياسات والتقنيات وكل التدابير التي يمكن استخدامها لحماية البيئة السيبرانية، بما في ذلك حماية المستخدمين، سواء الدول أو المؤسسات أو الأشخاص، ومواجهة التهديدات السيبرانية سواء كانت مقصودة أو غير مقصودة (الأخطاء).

المحور الثاني: الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية:

---

[25] *Idem.*

[26] أنظر التقرير الصادر عن الاتحاد الدولي للاتصالات، حول "اتجاهات الإصلاح في الاتصالات لعام 2010-2011".

[27] للمزيد من التفصيل أنظر: منى الأشقر جبور، **السيبرانية هاجس العصر**. مرجع سابق، ص ص 28-31.

يعتبر الأمن السيبراني حسب المشرع الجزائري مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم اعتمادها لمنع الاستخدام غير المصرح به، وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة، لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

وتجدر الإشارة، إلى أن الجزائر احتلت المرتبة 23 عالميا من أصل 29 مرتبة في مستوى التأهب في مجال الأمن السيبراني، وذلك في تصنيف الترتيب العالمي حسب الرقم القياسي العالمي للأمن السيبراني GCI [28] لعام 2015. بمؤشر 0.1765 مقارنة بالولايات المتحدة الأمريكية صاحبة المرتبة الأولى بمؤشر0.824 ، والمرتبة العاشرة (10) عربيا بمجموع 0.1765 مقارنة بسلطنة عمان بمجموع 0.7647[29]. (وحسب تقييم المؤشر العالمي للأمن السيبراني لعام 2018، احتلت الجزائر المرتبة 108 عالميا و14 عربيا من أصل 173 دولة شملها التقييم).

1-الجرائم السيبرانية في التشريع الجزائري:

اعتمد المشرع الجزائري في سن الأحكام القانونية لمحاصرة الجريمة الإلكترونية على ثلاثة معايير متفق عليها إلى حد ما لدى الفقهاء والتشريعات المقارنة، **أولا:** وسيلة الجريمة المتمثلة في استخدام تكنولوجيات الاتصال، **ثانيا:** موضوع الجريمة المتمثل في المساس بالأنظمة المعلوماتية، **ثالثا:** الجانب الشرعي والمتمثل في العقوبات المحددة في القانون. ويهدف المشرع من هذه الخطوة إلى تحديد النطاق الذي تنشط فيه الجريمة الإلكترونية حتى يتسنى للفاعلين التحكم في الموضوع[30].

[28] الرقم القياسي يندرج ضمن البرنامج العالمي للأمن السيبراني للاتحاد الدولي للاتصالات يتناول مستوى الالتزام في خمسة مجالات :التدابير القانونية، التدابير التقنية، التدابير التنظيمية، بناء القدرات، والتعاون الدولي.

[29] "تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية". جنيف: الاتحاد الدولي للاتصالات، مكتب تنمية الاتصالات، أفريل2015.

[30] جمال بوازدية، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية". مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، أفريل 2019، ص 1278.

تركزت الجهود الجزائرية أساسا في مجال اتخاذ التدابير القانونية دون غيرها من التدابير الأخرى، ويتضح ذلك من خلال صدور القانون رقم 09-04 المؤرخ في 5 أوت 2009[31]، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تم فيه تحديد الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الإلكترونية، بناءا على ما ورد في المادة 4 من الفصل الثاني، والتي نصت على ما يلي[32]:

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
ج- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

لقد أحدث المشرع الجزائري قسم في قانون العقوبات في القسم الرابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات (المواد: 394 مكرر، 399 مكرر، 394 مكرر1، 394 مكرر2، 394 مكرر3، 394 مكرر4، 394 مكرر5، 394 مكرر6، 394 مكرر7). وباستقراء هذه المواد يتضح أن المشرع الجزائري قسم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو الجرائم الإلكترونية إلى أربعة أنواع[33]:

---

[31] يتضمن القانون 19 مادة موزعة على 6 فصول، أعده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاما خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية وعددت الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية.

[32] قانون رقم 09- 04 مؤرّخ في 14 شعبان عام 1430هـ الموافق 5 أوت سنة 2009 م، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرّسميّة للجمهوريّة الجزائريّة /العدد 47، 25شعبان عام 1430 هـ 16أوت سنة 2009 م.

[33] نمديلي، "خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة". مرجع سابق، ص ص 11-12.

النوع الأول: طبقا للمادة 390 مكرر من قانون العقوبات وهي جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير، وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات، ويعاقب الجاني بعقوبة 3 أشهر إلى سنة وبغرامة من خمسين إلى مئة ألف دينار. وتضاعف العقوبة إذا ترتب عن الفعل الإجرامي حذف أو تغيير المعطيات، كما يعاقب الجاني بستة أشهر إلى سنتين وغرامة من خمسين ألف إلى مئة وخمسين ألف دينار وفي حالة تخريب النظام المعلوماتي.

النوع الثاني: الجرائم الإلكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي، كجرائم التحويل الإلكتروني والسطو والنصب والاحتيال والسلب وغيرها، وهذا ما نصت عليه المادة 394 مكرر2، وعقوبتها من شهرين إلى ثلاث سنوات وبغرامة مليون دينار إلى خمسة مليون دينار.

النوع الثالث: الجرائم الإلكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب، وعقوبتها تضاعف عقوبة النوع الثاني لخطورتها طبقا للمادة 394 مكرر3.

النوع الرابع: الجرائم الإلكترونية للشخص المعنوي، حيث نص المشرع الجزائري على خلاف التشريعات المقارنة الأشخاص المعنوية بنص خاص، وعقوبتها تعادل خمس مرات الجرائم المرتكبة من طرف الشخص الطبيعي طبقا للمادة 394 مكرر4 من قانون العقوبات الجزائري.

بالإضافة إلى ذلك، تدعمت الإجراءات القانونية بآلية تقنية جديدة تتمثل في صدور القانون المتضمن البصمات الجنائية في الإجراءات الجزائية لتحديد هوية الأشخاص، كما تم تعزيز الجهات القضائية على المستوى الوطني بأربعة محاكم خاصة pôles de magistrats spécialisés (الجزائر، قسنطينة، وهران، ورقلة)، لتسهيل عمليات البحث والتحري لذوي الاختصاص من الأجهزة الأمنية، والبث في القضايا المعروضة دون الرجوع إلى الوصاية، كما شمل التشريع بعض المجالات التي يحتمل أن تشملها الجريمة والتي لها صلة بمجال الحريات الخاصة على غرار قانون الملكية الفكرية، الثقافية، حقوق المؤلف (قانون 05.03 و03-06

الصادرين بتاريخ 2003.07.19)، وقانون مكافحة تبييض الأموال (01-05 الصادر بتاريخ 2005.02.05)، وقانون الوقاية ومكافحة المخدرات (04-18 الصادر بتاريخ 2004.12.25)[34].

بالرغم من المجهودات المبذولة من طرف الدولة الجزائرية، إلا أن المختصون يرون أن البنية التنظيمية والتشريعية مازالت في طور التشكيل، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها، واقتصرت العقوبات في أغلب الأحيان على الغرامة المالية. كما أن هناك العديد من الجوانب لم يتم تطويرها بما يتوافق مع البيئة الوطنية (كالمقاييس الدولية للحماية، المواصفات التقنية للمعلومات، البيانات، الأنظمة، البرامج والأجهزة). الأمر الذي دفع السلطات الجزائرية إلى استحداث هيئات مختصة تعمل على التطبيق الصارم للتشريع الجزائري المتعلق بمكافحة الجرائم السيبرانية.

2-الهيئات الجزائرية المتخصصة في مجال مكافحة الجرائم السيبرانية:

لتفادي الوقوع في تداخل الصلاحيات بين مختلف الأجهزة الفاعلة في مسائل الأمن والدفاع الوطني، حرص المشرع الجزائري على وضع ضوابط لاحترام الإطار الإداري المنظم لصلاحيات الهيئات المدنية والعسكرية والتقنية في إدارة الإستراتيجية الجزائرية للأمن السيبراني، والتي يمكن ذكرها فيما يلي:

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

نص عليها قانون 09-04 لسنة 2009 في الفصل الخامس – المادة 14، وتمارس الهيئة مهامها تحت رقابة السلطة القضائية، وفق ما ورد في المادة 4 من المرسوم، حيث تكلف بما يلي[35]:

-اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

---

[34] بوازدية،"الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية". مرجع سابق، ص 1278.

[35] مرسوم رئاسي رقم 15- 261 مؤرّخ في 24 ذي الحجة عام 1436هـ الموافق 8 أكتوبر سنة 2015 م ، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرّسميّة للجمهوريّة الجزائريّة /العدد 53، 24 ذي الحجة عام 1436هـ الموافق 8 أكتوبر سنة 2015 م.

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

-ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

-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 الإعلام والاتصال.

- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

-المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

تتكفل هذه الهيئة أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الإلكترونية وتحديد مكان تواجدهم، إضافة إلى التأكيد على التعاون والمساعدة القضائية الدولية في إطار مبدأ المعاملة بالمثل.

ب- مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:

بالنظر لحساسية قطاع الدفاع الوطني، استحدثت هذه المصلحة، على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، وأوكلت لها مهمة حماية المنظومات

والمنشآت الحيوية للجزائر ضد كل أنواع التهديدات السيبرانية[36]، حيث تتمحور إستراتيجية الدفاع السيبراني للجيش حول سبعة محاور، يمكن ذكرها فيما يلي[37]:

- جانب وظيفي وتنظيمي، حيث تكون أعمال الدفاع السيبراني ضمن الجيش الوطني الشعبي موجهة ومنفذة في إطار سلسلة وظيفية أو تنظيمية مكرسة لضمان تجانس وفعالية هذه الأعمال.
- جانب قانوني، مكلف بتحيين وتعزيز باستمرار الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال عموما، وتأمين منظومات الإعلام خصوصا.
- جانب الموارد البشرية، تعتبر جاهزية مورد بشري تقني معتبر وذي كفاءة عالية في مجال الدفاع السيبراني هدفا أساسيا لكي تضمن نجاح إدخال هذا المجال في النشاطات العملياتية والتسيير للجيش الوطني الشعبي.
- جانب تقني، يتعلق بتقوية وتكييف القدرات التقنية للحماية والكشف والرد على الهجمات السيبرانية باستمرار، مع ضمان يقظة دائمة فيما يخص الطرق والوسائل المستعملة من طرف المهاجمين.
- جانب الوقاية والتحسيس، يرتبط بوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنجر عن استعمال تكنولوجيات الإعلام والاتصال في الإطار المهني أو الشخصي بطريقة مستمرة.
- جانب البحث والتطوير، باستعمال وسائل تقنية خاصة ومشخصة من طرف هياكل البحث والتطوير للجيش الوطني الشعبي، لاسيما تلك المستعملة للحماية ضد التهديدات السيبرانية عنصرا حاسما في إستراتيجية الدفاع السيبراني.

---

[36] تحبط وزارة الدفاع الوطني يوميا 3500 محاولة اختراق لمواقع قيادات قواتها ومديرياتها المركزية، بمعدل 130 ألف محاولة اختراق في السنة، من قبل عصابات "الهاكرز" من مختلف دول العالم، في إطار ما يعرف بـ "الحرب الإلكترونية". **أنظر:** نوارة باشوش، "استحدث مصلحة للدفاع السيبراني ومراقبة أمن الأنظمة. الجيش يدخل حرب "الفضاء الإلكتروني" ومكافحة الجوسسة". موقع الشروق أون لاين، 12-10-2017:

https://www.echoroukonline.com

[37] محمد بوكبشة، "الأمن والدفاع السيبراني أولوية قصوى". **الجيش**، العدد 651، أكتوبر 2017، ص 35.

- جانب التعاون، من خلال تعزيز التعاون في مجال الدفاع السيبراني مع جيوش الدول الشريكة من أجل السماح للجيش الوطني الشعبي بالاستفادة من الخبرات والوسائل التكنولوجية المتقدمة جدا.

ج-المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني (SCLC) :

تعتمد هذه المصلحة على موارد بشرية لها من الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال التعامل مع المصالح المختصة (أنتربول، أفريكوم) أو مصالح الشرطة لكبرى الدول، وعلى المستوى الوطني تتواصل مع الشرطة العلمية والمكاتب اللامركزية المختصة في الإجرام(الشرطة القضائية.)

د-مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية التابعة للقيادة العامة للدرك الوطني(CPLCIC):

لا يختلف كثيرا في مهام التحقيق والتحريات في هذا المجال عن نظيرته للأمن الوطني سواء محليا أو وطنيا، بل بالعكس يتم التنسيق بينهما تحت المسؤولية المباشرة للنائب العام على مستوى دائرة الاختصاص.

هـ-المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني التابع للقيادة العامة للدرك الوطني(INCC):

يعتمد المعهد في أداء مهامه على الخبرة العلمية والتجارب المخبرية الدقيقة لكل الأدلة المتحصل عليها من مكان ارتكاب الجريمة عامة، من أجل تنوير العدالة وتوجيه الجهات الأمنية كلما تعلق الأمر باستكمال التحقيق، ومن بين النتائج المتوصل إليها من طرف هذه المصالح، اتضح أن الجرائم الإلكترونية بالجزائر تتضاعف بطريقة سريعة جدا، وهذا ما كشفت عنه الأرقام المسجلة التي تم البث فيها 2500 جريمة، ويتعلق أبرزها (70%) بانتهاك الحريات الشخصية، والتهديد عبر الأنترنت، ونشر صور فاضحة، والابتزاز، والقرصنة الإلكترونية، وغيرها.[38]

بصفة عامة، حاولت الجزائر مواجهة مختلف أشكال الجرائم السيبرانية من خلال استغلال إمكانياتها المتوفرة، لاسيما تخصيص هيئات ومصالح تسهر على أداء هذه المهام، إلا

[38] بوازدية ،"الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية". مرجع سابق، ص1280.

أن خطورة هذه الجرائم وتزايد معدلاتها أصبحت تشكل تهديدا كبيرا سواء على مستوى الأمن الوطني أو العالمي، الأمر الذي يستدعي تطوير جهودها في إطار التعاون الدولي المشترك لمكافحة هذه الجرائم.

ثالثا: التعاون الجزائري-الدولي في مكافحة الجرائم السيبرانية:

تعتبر الجريمة السيبرانية ذات أبعاد عالمية، كونها تتجاوز بمفعولها ومداها، أشخاصا أو دولا في مناطق مختلفة، والتي تقع تحت اختصاصات قانونية متباينة في عدد من الدول، هدفها الوصول إلى نتيجة سواء على مستوى المتابعة والملاحقة وجمع الأدلة، أو على مستوى إنزال العقوبة. وفي هذا الإطار انخرطت الجزائر في العديد من الاتفاقيات الإقليمية والدولية التي نصت على ضرورة التعاون الدولي من أجل مواجهة مثل هذه الجرائم، بما فيه التعاون القضائي والأمني.

1- الاتفاقيات الإقليمية:

تعتبر الاتفاقيات الإقليمية ترجمة لمساعي التعاون بين العديد من الدول، سواء على المستوى الأوروبي أو على المستوى العربي، وذلك من أجل ضمان الإجراءات الخاصة بمكافحة الجرائم السيبرانية. تتمثل أهم هذه الاتفاقيات فيما يلي:

أ- على المستوى الأوروبي:

من بين أهم الاتفاقيات الأوروبية التي جاءت بشأن الجرائم الإلكترونية، هناك **"اتفاقية بودابست"** التي أبرمت بتاريخ 23 نوفمبر 2001 بعاصمة المجر بودابست، ودخلت حيز التنفيذ عام 2004. تتضمن أربعة فصول تتمثل في: تعريف المصطلحات الأساسية، التدابير الواجب اتخاذها على الصعيد المحلي (القانون الموضوعي والقانون الإجرائي)، التعاون الدولي، والأحكام الختامية. تهدف هذه الاتفاقية بشكل أساسي إلى ما يلي[39]:

- مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية.

[39] للمزيد من التفصيل أنظر:"التقرير التفسيري لاتفاقية الجريمة الإلكترونية " من سلسلة المعاهدات الأوروبية رقم185. بودابست، في 23 نوفمبر 2001.

- التنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم ومتابعتها قضائيا، علاوة على الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر، أو التي تكون الأدلة المتصلة بها في شكل إلكتروني.
- إنشاء نظام سريع وفعال للتعاون الدولي.

يتطرق القسم الأول من الفصل الثاني (مسائل القانون الموضوعي) إلى أحكام التجريم والأحكام الأخرى ذات الصلة في مجال الجريمة الإلكترونية أو الجريمة المتصلة بالكمبيوتر، حيث صنفت تسعة جرائم في أربع فئات مختلفة، ثم تناولت المسؤولية الفرعية والعقوبات. وتتمثل هذه الجرائم فيما يلي: النفاذ أو الولوج غير القانوني، والاعتراض غير القانوني، وتداخل البيانات، وتداخل النظام، وإساءة استخدام الأجهزة، والتزوير المتصل بالكمبيوتر، والاحتيال المتصل بالكمبيوتر، والجرائم المتصلة باستغلال الأطفال في المواد الإباحية، والجرائم المتصلة بحق التأليف والنشر والحقوق المجاورة[40].

تجدر الإشارة، إلى أن هذه الاتفاقية تعتبر أول أداة إقليمية ملزمة لمكافحة الجريمة السيبرانية، عبر تحقيق الانسجام بين القوانين الوطنية، حيث ألزمت الاتفاقية الدول الأطراف بأن تتخذ التدابير اللازمة كتشريع قوانين على المستوى الداخلي، تجرم سلوكيات محددة تمس خصوصية وتجانس وتوافر بيانات الكومبيوتر ومنظوماته. أتبعت هذه الاتفاقية بروتوكول دخل حيز التنفيذ عام 2006، يهدف إلى تجريم المحتوى العنصري وكراهية الأجانب على الأنترنت وتجريم التهديدات والشتائم المبنية عليهما.

إضافة إلى ما سبق ذكره، أكدت الاتفاقية على الحاجة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء لمكافحة الجريمة المعلوماتية، واعتبرت مرجعا لا يستهان به في ميدان محاربة الإجرام السيبراني، سواء بالنسبة لبعض الاتفاقيات اللاحقة ذات الصلة أو بالنسبة للتشريعات الداخلية لبعض الدول.

[40] نفس المرجع.

وعليه، تم مطابقة التشريع الجزائري الداخلي مع ما جاء في التشريعات الإقليمية الأوروبية لاسيما اتفاقية بودابست، التي تعتبر بمثابة المرجعية القانونية لكل التشريعات الوطنية والدولية الصادرة في هذا المجال، حيث يتضمن الفصل الثالث الأحكام المتعلقة بالمساعدة المتبادلة التقليدية والمتصلة بالجريمة الإلكترونية، فضلا عن قواعد تسليم المجرمين. ومن بين النقاط التي شملتها المطابقة ما يلي[41]:

-استعمال المصطلحات المعمول بها في مجال الإعلام الآلي وتكنولوجيات الاتصال: معطيات الإعلام، معطيات متعلقة بالاختراق، ممول الخدمات (أنظر المادة الأولى من الاتفاقية ومقدمة القانون 04.09 الجزائري)، ليبقى الهدف تسهيل عمل المختصين في الإعلام الآلي من قراءة صحيحة للعمل المطلوب أو الملف المطروح.

-الدخول غير الشرعي للأنظمة المعلوماتية، (أنظر المادة الثانية من الاتفاقية والمادة 394 مكرر قانون العقوبات الجزائري) ، أهمية تجريم هذا العمل هو تحديد نقاط الضعف للنظام المستهدف مع إمكانية تحديد هوية الجاني.

-الاعتراض غير الشرعي للمكالمات والمعطيات المتبادلة سواء في إطار خاص أو مهني (أنظر المادة الثالثة من الاتفاقية والمادة 303 من قانون العقوبات الجزائري) .

-المساس بنزاهة أو استماتة المعطيات (أنظر المادة الرابعة من الاتفاقية والمادة 394 مكرر من قانون العقوبات الجزائري) ، لأن الحصول على المعطيات بطريقة غير شرعية من شأنه أن يحول من مسار المعلومة في جانبها المهني أو الشخصي، وهذه الخطوة من أخطر التهديدات الإلكترونية.

-المسؤولية المعنوية للجهات المكلفة بتسيير مجالات تكنولوجيا الإعلام تبقى قائمة، لأنهم في نظر القانون الضامن الوحيد على حسن وسلامة الأنظمة المعلوماتية (أنظر المادة 12 من الاتفاقية والمادة 394 مكرر من قانون العقوبات الجزائري) .

-التعاون الدولي من أجل سلامة الإجراءات القانونية (الإنابة القضائية، وتسليم المجرمين).

انطلاقا من هذا، فإن الجزائر عملت على تعزيز منظومتها القانونية ومطابقتها للتشريعات الإقليمية، للرد على تحديات الإجرام السيبراني سواء على المستوى الوطني، أو الإقليمي أو الدولي، مع التأكيد على احترام مبدأ السيادة الوطنية وحقوق الإنسان.

---

[41] بوازدية ،"الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية". مرجع سابق،ص ص1278-1279.

ب- على المستوى العربي:

وقعت الدول العربية على **"الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"** وذلك بتاريخ 21 ديسمبر2010، والتي تعد نقطة تحول في التعاون العربي لمكافحة هذه الجرائم. حيث تهدف وفق المادة الأولى من الفصل الأول، إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[42].

كما نصت هذه الاتفاقية على التعاون العربي في مكافحة الجرائم المعلوماتية في العديد من المجالات منها: التعاون القضائي، تبادل المعلومات، تبادل الخبرات، الاختصاص القضائي، تسليم المجرمين، المساعدة القضائية...الخ. وأصبحت الاتفاقية سارية المفعول بعد تصديق مصر عليها عام 2015، ليكتمل نصاب الدول السبع المطلوبة لسريانها[43].

ومن الجرائم المعلوماتية المدرجة ضمن القانون العربي النموذجي، هناك: جريمة غسل الأموال عبر الوسائط الإلكترونية، جريمة التزوير الإلكتروني، جريمة اختراق النظم المعلوماتية كالسرقة المعلوماتية، الاعتداء على سلامة البيانات، جريمة استخدام وسائل تقنية المعلومات، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، والجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات...الخ

ورغم أن هذه الاتفاقية أدت إلى ظهور قوانين عديدة لمكافحة ما يسمى بالجرائم المعلوماتية في بعض الدول العربية مثل السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان، إلا أن البيئة التنظيمية والتشريعية العربية، ما زالت بعيدة نوعا ما لمكافحة مثل هذه الجرائم، خاصة في ظل حداثة طبيعة الفضاء السيبراني. ما يعني أن الإطار القانوني لوحده لا يكفي، ما لم تتضافر الجهود الإقليمية والدولية.

---

[42] وثيقة "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات". جامعة الدول العربية، الأمانة العامة، 21 ديسمبر 2010.

[43] لورنس سعيد الحوامدة، " الجرائم المعلوماتية أركانها وآلية مكافحتها: دراسة تحليلية مقارنة". المملكة العربية السعودية: جامعة طيبة، كلية الحقوق، 2017/2016، ص 29.

2- الاتفاقيات الدولية:

يتقاسم العالم اليوم تهديدات أمنية مشتركة، لاسيما الجرائم السيبرانية. الأمر الذي يجعل من التعاون الدولي النموذج الأمني الأمثل في عصرنا الحالي، حيث أصبح الأمن متشابكا بوتيرة متزايدة، وأصبح تحقيق الأمن السيبراني يتطلب مزيدا من العمل مع الدول والمؤسسات والمنظمات الدولية.

إن اهتمام الدول بالتعاون يبدو واضحا، من خلال مشاركتها في أعمال الجمعية العامة للأمم المتحدة، والتي أصدرت عددا من القرارات، التي يمكن اعتبارها قاعدة لانطلاق الجهود المشتركة في مكافحة الجريمة السيبرانية. وفي هذا الإطار يمكن ذكر القرار الصادر عام 1990، حول قانون جرائم المعلوماتية، ثم قرارا آخرا في العام اللاحق، حول مكافحة الاستخدام الجرمي لتقنيات المعلومات والاتصالات. كما أصدرت الأمم المتحدة، قرارا خاصا حول الأمن السيبراني عام2003، ركز على القدرة على مكافحة الجريمة السيبرانية، ومن ثم أصدرت قرارا حول الموضوع نفسه عام 2010، وملحقا حول ضرورة أن تلجأ الدول إلى إجراء تقييم ذاتي بمحض إرادتها، لمعرفة مدى تناسب أطرها التشريعية، وقدرتها على مكافحة الجريمة السيبرانية، على ضوء التطورات السريعة الحاصلة، في مجال تقنيات المعلومات والاتصالات. كذلك بذلت جهود عدة من قبل مجموعات عمل متخصصة، بدعم من الاتحاد الدولي للاتصالات، حيث برزت الحاجة إلى تعاون الدول فيما بينها، لإقرار مجموعة من المعايير والقواعد، التي تضمن الاستخدام الآمن للمجال السيبراني[44].

من هنا، يبدو ضروريا أن تلعب الأمم المتحدة، دورا إيجابيا في تحقيق السلام السيبراني، لاسيما وأنها المعنية الأولى بتحقيق السلم والأمن الدوليين. وفي هذا الإطار عين "بان كيمون" الأمين العام للأمم المتحدة سابقا في 2012، فريقا من الخبراء تألف من 15 دولة، من بينها الأعضاء الدائمون في مجلس الأمن، لدراسة إجراءات التعاون الممكنة لمواجهة المخاطر السيبرانية . وفي التقرير الذي رفعه الخبراء عام2013 ، والذي جاء تحت ثلاث عناوين أساسية، برزت عدة مبادئ حول[45]:

---

[44] الأشقر جبور، السيبرانية هاجس العصر. مرجع سابق، ص 107.

[45] نفس المرجع، ص 100.

• تطبيق القانون الدولي على سلوك الدول في الفضاء السيبراني.
• توسيع مدى تطبيق القواعد التقليدية حول الشفافية وبناء الثقة.
• توصية بالتعاون الدولي وبناء القدرات لجعل البنية التحتية للمعلومات والاتصالات حول العالم أكثر أمنا.

لقد أبرز هذا التقرير، المخاطر الناتجة عن انتشار الاعتماد على تقنيات المعلومات والاتصالات في البنية التحتية، لاسيما في مجال أنظمة إدارة ومراقبة المفاعلات النووية. وتبقى أهمية التقرير، فيما يمثله من سابقة في مجال التوافق بين الدول على مجموعة من التوصيات حول المعايير والقواعد، ومبادئ مسؤولية الدول في المجال السيبراني، ما يؤسس لنواة قانون دولي في هذا المجال، ويسمح بالتوجه نحو الإقرار بتطبيق القوانين الدولية، في غياب الإطار القانوني الخاص، وبتطبيق شرعية الأمم المتحدة على الدول الأعضاء، وبإتاحة المجال أمام الدول التي تتعرض لاعتداءات، لمراجعة الأمم المتحدة وأجهزتها المختصة[46].

ورغم أهمية هذه الاتفاقيات، إلا أنها تبقى غير ملزمة لاسيما في ظل ازدياد الهوة الرقمية بين الدول والتباين في التحكم الرقمي. إذ تواجه المعاهدات المتعلقة بالحظر لاستخدام الفضاء الإلكتروني لأغراض حربية عائقين على الأقل[47]:
أولا، الدول ليست هي الوحيدة التي تستخدم البعد السيبراني (تعدد الجهات الفاعلة وبعضهم غير مدركين للحق في الاستخدام).
ثانيا، لن يكون الحظر فعالا إلا إذا كان لدى ضامني السلام الوسائل اللازمة لمعاقبة المخالفين (وهذا يعني التعرف عليهم).

وبهذا، فإن تأخر الدول في إبرام اتفاقيات متعلقة بالجرائم السيبرانية، ترجع إلى عدم رغبة الدول الكبرى المعروفة بصناعتها العسكرية والتقنية المتطورة، للدخول إلى اتفاقيات دولية قد تحضر عليها وسائل تساعد في حفظ أمنها، تحت مسميات الضرورة العسكرية مثل الولايات المتحدة الأمريكية. هذه الأخيرة وبعد موافقتها على الاتفاقية وبروتوكولاتها اللاحقة، اعترضت عام 2002 على تعديل أدان نشر مواد عنصرية، أو محرضة على كراهية الأجانب،

[46] نفس المرجع ونفس الصفحة.

[47] Ventre, « La cyber paix, un thème stratégique marginal », Op.Cit, pp 88.89.

بواسطة الأنظمة المعلوماتية، إضافة إلى تأييد المجازر والجرائم ضد الإنسانية، متذرعة بتعارض هذا التعديل، مع حرية التعبير المكرسة في الدستور الأمريكي.

3- التعاون الدولي في المجالين القضائي والأمني:

نتيجة للتحول في مجال الاتصالات وتقنية المعلومات، لم تعد الحدود الموجودة بين الدول تشكل حاجزا أمام مرتكبي الجرائم الإلكترونية، لهذا بات التعاون الدولي أكثر من ضروري سواء تعلق الأمر بالتعاون القضائي أو الأمني أو التقني. ولقد تفاعلت الجزائر مع كل صور التعاون الدولي بمختلف مظاهره خاصة وأن معدل الاختراقات على الشبكة العالمية للمعلومات، وعلى الأنظمة المعلوماتية الوطنية بلغ درجات من الخطورة المهددة للأمن الوطني والعالمي.

أ- التعاون القضائي:

يتمثل التعاون القضائي في كل الإجراءات التي تقوم بها الدول، والتي من شأنها تسهيل المهام في بقية الدول لمواجهة الجرائم المعلوماتية، من خلال بعض الاتفاقيات الإقليمية والدولية. أمام هذه التحديات لجأت الجزائر إلى التعامل مع هذه الجريمة من خلال تفعيل المبادئ العامة المتعارف عليها عالميا في مجال مكافحة الجريمة. ويشمل هذا التعاون عدة أشكال تتمثل فيما يلي[48]:

- **تبادل المعلومات:** يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية، وهي بصدد النظر في جريمة ما عن الاتهامات التي وجهت ضد أحد رعاياها في الخارج، والإجراءات التي اتخذت ضدهم. وقد يشمل تبادل السوابق القضائية للمتابعين في مثل هذه الجرائم. وهو ما نصت عليه الفقرة الثانية من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية.

نفس الأمر ما قضت به المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية. والمادة

---

[48] حسين بن سعيد بن سيف الغافري، **الجهود الدولية في مواجهة جرائم الإنترنت**. موقع المنشاوي للدراسات والبحوث، 2007، ص ص 12-14.

الأولى والثانية من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي. وفي نفس الإطار صاغ اتفاق شنجن للاتحاد الأوروبي نظاما متكاملا لتبادل المعلومات.

- **نقل الإجراءات:** قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية، وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت شروط معينة، من أهمها التجريم المزدوج الذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها.

ولقد أقرت العديد من الاتفاقيات الدولية والإقليمية هذه الصور كإحدى صور المساعدة القضائية الدولية، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، والمؤتمر الإسلامي لمكافحة الإرهاب الدولي عام 1999، والمادة 16 من النموذج الاسترشادي لاتفاقية التعاون القضائي والقانوني الصادر عن مجلس التعاون الخليجي عام 2003.

- **الإنابة القضائية:** والتي تعني طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، من أجل الفصل في مسألة معروضة على السلطة القضائية تعذر على الدولة الطالبة القيام به بنفسها. وتهدف الإنابة القضائية إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، وعادة ما يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية.

في نفس الإطار، وسعت الدولة الجزائرية من دائرة التقارب لتشمل: تبادل الزيارات الميدانية والدورات التكوينية واللقاءات التشاورية، في المجالات التي شملتها السياسة الجنائية لمكافحة الإجرام عامة، والاستفادة من خبرات بعض الدول العربية والتعرف على قوانينها التشريعية، وكذا الآليات التقنية المستعملة في مواجهة الجرائم السيبرانية.

وبالحديث عن العمل الميداني المتضمن المساعدة التقنية الثنائية والمتعددة الأطراف التي تخص الإنابة القضائية وتسليم المجرمين، ورغم أهمية التعاون والتنسيق القضائي إلا أن

هناك العديد من الصعوبات التي تواجهها الدول في تحقيق التسليم نظرا لارتباط إجراءاته بالسيادة الوطنية من جهة، وعدم التزام بعض الدول المطالبة بالتسليم لتنفيذه بحجة حقوق الإنسان من جهة ثانية.

ب-التعاون الأمني:

سعت الجزائر في إطار مكافحة الجرائم السيبرانية، إلى توطيد التعاون الأمني مع العديد من المنظمات الإقليمية والدولية، والتي يمكن ذكرها فيما يلي:

- **المنظمة الدولية للشرطة الجنائية "الأنتربول":**

تهدف هذه المنظمة إلى تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية، في إطار القوانين القائمة في مختلف الدول وبروح الإعلان العالمي لحقوق الإنسان. مع التأكيد على إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام ومكافحتها.[49]

انضمت الجزائر إلى هذه المنظمة أثناء انعقاد الجمعية العامة للأنتربول في هلسنكي بفنلندا، خلال شهر أوت 1963، بمشاركة 53 دولة، ممثلة بالمكتب المركزي الوطني، حيث يعمل هذا الأخير تحت الوصاية المباشرة لمديرية الشرطة القضائية-المديرية العامة للأمن الوطني، ويباشر مهامه وفقا لنصوص التشريعات الوطنية، ملتزما بالأطر القانونية المسيرة للمنظمة الدولية للشرطة الجنائية (أنتربول). من ناحية أخرى يجب على المكتب المركزي الوطني تسيير نشاطاته ضمن استراتيجية واضحة ومحددة المعالم وفقا لما تقتضيه الاحتياجات الأمنية المسجلة على الصعيد الوطني، وضرورة أن تكون في سياق الوظائف الأساسية المقررة من طرف المنظمة الدولية للشرطة الجنائية خدمات اتصالات شرطية عالمية مأمونة، وخدمات بيانات ميدانية وقواعد بيانات شرطية، وخدمات إسناد شرطي، والتدريب وإنماء القدرات.[50]

---

[49] تم إنشاء المنظمة الدولية للشرطة الجنائية-أنتربول في 07 سبتمبر 1923، حيث تعد من بين أهم المنظمات الدولية الناشطة في مجال مكافحة الجريمة نظرا لما تقدمه من إمكانية تعقب وضبط لمرتكبي الجرائم على اختلاف أنواعها (الإجرام المالي والمرتبط بالتكنولوجيا المتقدمة، الإخلال بالأمن العام والإرهاب، الاتجار بالبشر، إسناد التحقيقات بشأن المجرمين الفارين) أينما وجدوا وتسليمهم إلى الهيئات المختصة بغية محاكمتهم وتوقيع العقوبة المناسبة عليهم.

[50] "المنظمة الدولية للشرطة الجنائية – أنتربول". الجمهورية الجزائرية الديمقراطية الشعبية، المديرية العامة للأمن الوطني: https://www.algeriepolice.dz

ويظهر التعاون الجزائري في المجال الأمني من خلال زيادة الترابط وتبادل المعلومات أكثر بين الأنتربول والجزائر منذ ظهور ما يعرف بتنظيم "الدولة الإسلامية في العراق والشام" (داعش)، حيث تلقت الجزائر في الفترة الأخيرة مذكرة أمنية تحت عنوان "تنامي الجريمة العابرة للأوطان"، تخص تطبيق القوانين الخاصة بمكافحة الإرهاب والمقاتلين الأجانب والجريمة الإلكترونية والهجرة غير الشرعية و الجريمة المالية. وتدعو التوصية الأولى الواردة في المذكرة الجزائر إلى "الرفع من توزيع المعلومات حول المقاتلين الأجانب، وعرقلة سفرياتهم، واستغلال القواعد البيانية الخاصة بمراقبة الحدود"، ونبهت الشرطة الدولية في توصيتها الثانية الجزائر إلى تقوية تدابير مكافحة الجريمة الإلكترونية عن طريق تدعيم تبادل المعلومات، واستعمال آليات منظمة الأنتربول من أجل دعم التحقيقات والتحسيس بالمخاطر المترتبة عن هذا النوع من الجريمة[51].

- **مركز الشرطة الأوروبية (الأوروبول):**

يساهم "الأوروبول" بدور فعال في مكافحة الجرائم الإلكترونية[52]، من خلال تعزيز التنسيق الأمني وتبادل المعلومات بين الشرطة في البلدان الأعضاء بالاتحاد الأوروبي ومع الدول المجاورة له.

ففي إطار التعاون الأمني الجزائري-الأوروبي، صادقت الجزائر على البيان الختامي الذي خرج به مؤتمر "يوروميد" للشرطة[53]، المنعقد بالعاصمة الإسبانية مدريد عام 2012، حول مكافحة تهريب المخدرات وغسل الأموال في إطار مشروع "يوروميد" الثالث الممول من طرف الاتحاد الأوروبي، لتعزز شراكتها أكثر مع الدول الأوروبية والأنتربول والأوروبول في العمل

---

[51] مراد مقعاش، "التهديدات الأمنية في المتوسط وأثرها في علاقات الأمن والتعاون الأورو – جزائري".المركز الديمقراطي العربي .4يناير 2017:

https://democraticac.de/?p=42040

[52] الأوروبول اختصار للتسمية التي تطلق على "المكتب الأوروبي للشرطة"، فهي وكالة تعمل على تطبيق القانون الأوروبي، وظيفتها حفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوروبي في مجالات مكافحة الجرائم الدولية الكبيرة والإرهاب. وتعمل بشكل وثيق مع أجهزة أمن دول الاتحاد الأوربي ودول من خارج الاتحاد.

[53] مشروع يوروميد للشرطة يهدف إلى توفير أمن المواطنين عبر المنطقة الأورومتوسطية، من خلال دفع التعاون حول المسائل الأمنية ضمن البلدان الشريكة في جنوب المتوسط (البلدان المعنية: الجزائر، مصر، الأردن، لبنان، ليبيا، المغرب، تونس، فلسطين، إسرائيل، وسوريا عضويتها معلقة).

الإستخباراتي المتعلق بهاتين الظاهرتين. ويهدف هذا المشروع الأمني إلى تطوير القدرات المهنية لخدمات الشرطة و قوات الأمن لدول جنوب المتوسط، إلى جانب تطوير التعاون الدولي للشرطة بين الدول الأعضاء في الاتحاد الأوروبي ودول جنوب البحر الأبيض المتوسط، وكذلك بين دول جنوب البحر الأبيض المتوسط في حد ذاتها، في مجال مكافحة الجوانب الرئيسية للجريمة المنظمة بدءا بالإرهاب، ثم تهريب المخدرات، الاتجار بالبشر، الجريمة المالية، جرائم الأنترنت، الإتجار بالأسلحة، التهريب والتزوير، والمخاطر الناجمة عن الأحداث الكبرى[54].

كما أنشأ جهاز الشرطة الأوروبية (أوروبول) في 2015 وحدة لمحاربة جرائم المعلوماتية تغطي القارة الأوروبية بأكملها، مهمتها التصدي لأنشطة الجماعات الجهادية الدعائية خصوصا تنظيم "الدولة الإسلامية" على مواقع التواصل الاجتماعي على الأنترنت. وفور رصد أي أنشطة للمتطرفين سيتم إبلاغ الشركات المشغلة للمواقع ومن ثم إغلاق تلك الحسابات[55]. كما شاركت إدارة "فيسبوك" في جانفي 2018 في محادثات رئيسية مع أجهزة الشرطة الأوروبية حول كيفية وقف واستئصال منشورات المتطرفين على الأنترنت المرتبطة بالإرهاب والعنف[56].

في سياق آخر، تم إقرار التعاون الأمني في جوان 2018 بين وكالة الشرطة الأوروبية "أوروبول" ودول عربية وإسلامية مثل الجزائر ومصر والأردن ولبنان والمغرب وتونس وتركيا، لتعزيز سبل التعاون في مجال تبادل المعلومات والبيانات الشخصية للأفراد. كما جرى الاتفاق بين ممثلي حكومات دول الاتحاد الأوروبي على تعزيز مشروع ميزانية عام 2018 للوكالات التي لها مهام تتعلق بالأمن مثل "أوروبول" ووكالة العدل الأوروبية (أوروجست)[57]. هذه الأخيرة تعتبر

---

[54] "الجزائر تعزز شراكتها الإستخباراتية مع الأنتربول واليوروبول بمصادقتها على نتائج مؤتمر يوروميد للشرطة". الفجر 18 - 07 - 2012: https://www.djazairess.com/alfadjr/219938

[55] "الشرطة الأوروبية تنشئ وحدة لمحاربة تنظيم "الدولة الإسلامية" على الإنترنت". موقع فرانس24، 2015/06/22: https://www.france24.com/ar.

[56] "صرح "فنسنت سيمستر" رئيس وحدة الأنترنت في الأوروبول، بأن وكالة الشرطة الأوروبية تتعاون مع إدارة "فيسبوك" منذ عامين من أجل "الحد من الوصول للدعاية على الأنترنت"، فيما أعلنت الشرطة الأوروبية "أوروبول" في أفريل 2018 عن شن عملية إلكترونية منسقة، أدت إلى عملية تعطيل متزامنة للوكالات الدعائية لتنظيم "داعش" على الأنترنت، وأضاف أوروبول أن العملية الإلكترونية نفذتها الشرطة الأوروبية والأمريكية، وأتاحت شل المواقع الإلكترونية للتنظيم المتطرف لوقت غير محدد. أنظر: "مكافحة الارهاب...مهام وصلاحيات اليوروبول". المركز الأوروبي لدراسات مكافحة الإرهاب والإستخبارات. 04-07-2019: https://www.europarabct.com

[57] نفس المرجع.

الدعامة الفعالة في مجال التحقيقات والملاحقات التي تقوم بها السلطات القضائية الوطنية، خاصة فيما يتعلق بالإجرام الإلكتروني، إضافة إلى اتفاقية "شنغن" التي تعمل على مراقبة المشتبه بهم عبر الحدود وملاحقة المجرمين المتورطين في الجرائم الإلكترونية.

- **منظمة الشرطة الجنائية الإفريقية (الأفريبول):**

تعتبر هذه المنظمة أكبر منظمة شرطة في القارة الإفريقية، وهي مكونة من قوات الشرطة لواحد وأربعين دولة، مقرها الرئيسي في الجزائر العاصمة. تهتم بتسهيل تبادل المعلومات بين قوات الشرطة الوطنية بخصوص الجريمة الدولية والإرهاب والمخدرات والاتجار بالأسلحة في إفريقيا. ومن أهم أهدافها، التزام المؤسسات الشرطية الإفريقية على إيجاد حلول إفريقية خالصة، كفيلة بمعالجة كل قضاياها وانشغالاتها الأمنية، لاسيما تلك المتعلقة بمكافحة الجريمة المنظمة العابرة للأوطان والإرهاب. مع التجسيد الفعلي لمكاتب الاتصال الوطنية للأفريبول التي تمثل "ركيزة أساسية" في تبادل المعلومات والخبرات بين الدول، وإعداد التحاليل الجنائية والإستراتيجية والعملياتية[58].

أولت الجزائر أهمية بالغة لآلية التعاون الشرطي الإفريقي، كونها أداة تعاون إقليمية في غاية الأهمية لمجابهة المخاطر الجديدة التي باتت تهدد الأمن والسلم الدوليين، في إطار مواصلة السعي مع جميع الأطراف والشركاء للرقي بها وبأدائها، قصد رفع مستوى التنسيق والتعاون بين دول القارة، بما يخدم مصلحة الدول الأعضاء والمجتمع الدولي. كما أشادت الجزائر بقرارات الاتحاد الإفريقي التي تتعلق بتعزيز منظومة الأمن والسلم في المنطقة و"الارتقاء بالعمل الأمني للتكيف مع معطيات السياق الدولي الذي تتنامى فيه تهديدات الجريمة المنظمة العابرة للأوطان والجرائم السيبرانية". إضافة إلى هذا، تعزيز القدرات العملياتية والتقنية لمصالح الشرطة الإفريقية، من خلال تطوير مناهج العمل واستحداث مراكز الامتياز في التكوين والبحث والتحليل الجنائي الشرطي[59].

---

[58] "الجزائر تولي أهمية لـ"أفريبول" لمجابهة المخاطر الجديدة". جريدة المساء، 2019/10/03:
https://www.el-massa.com/dz

[59] نفس المرجع

ورغم أن هذه المنظمة حديثة النشأة، إلا أن الجزائر تسعى للمساهمة بدور كبير في مكافحة الجريمة المنظمة، وفي التنسيق والتشاور بين آلية التعاون الشرطي الإفريقي "أفريبول"، خاصة وأن استفحال الجريمة المنظمة والإرهاب وتعقيداته يؤكد أهمية التعاون، لاسيما ما تعلق بتبادل الخبرات وتعزيز القدرات والتنسيق الأمني من أجل مكافحة الجريمة العابرة للحدود والوقاية منها.

- **مجلس وزراء الداخلية العرب:**

ظهرت فكرة إنشاء المجلس خلال المؤتمر الأول لوزراء الداخلية العرب الذي عقد بالقاهرة عام 1977، وتقرر إنشاؤه في المؤتمر الثالث الذي عقد بمدينة الطائف عام 1980. وقد صادق المؤتمر الاستثنائي لوزراء الداخلية العرب الذي عقد بالرياض عام 1982، على النظام الأساسي للمجلس والذي تم عرضه على مجلس جامعة الدول العربية في شهر سبتمبر من نفس العام، والموافقة عليه[60]. يهدف المجلس إلى تنمية وتوثيق التعاون، وتنسيق الجهود بين الدول العربية في مجال الأمن الداخلي ومكافحة الجريمة، ويمارس الاختصاصات التي تمكنه من تحقيق أهدافه، بما في ذلك ما يلي:[61]

- رسم السياسة العامة التي من شأنها تطوير العمل العربي المشترك في مجال الأمن الداخلي، وإقرار الخطط الأمنية العربية المشتركة لتنفيذ هذه السياسة.
- إنشاء الهيئات والأجهزة اللازمة لتنفيذ أهدافه، وتشكيل لجان خاصة ممن يرى الاستعانة بهم من الخبراء والمستشارين، لتقديم اقتراحات وتوصيات في المواضيع المكلفة بدراستها، وإقرار المقترحات والتوصيات الصادرة عنها، وعن مختلف الهيئات المشتركة العاملة في المجالات الأمنية والإصلاحية.
- دراسة وإقرار جدول أعمال دورة انعقاد المجلس، ومناقشة وإقرار التقرير السنوي الذي تضعه الأمانة العامة عن نشاطات المجلس خلال الدورة، وما يتعلق منها بتنفيذ قراراته،

---

[60] "عقد مجلس وزراء الداخلية العرب 34 دورة حتى الآن، كان أولها في الدار البيضاء بالمملكة المغربية في شهر ديسمبر عام 1982، وآخرها بتونس في شهر أبريل عام 2017، على أن تكون طبعته الـ 35 بالجزائر.

[61] مجلس وزراء الداخلية العرب". الجمهورية الجزائرية الديمقراطية الشعبية الجزائرية، وزارة الداخلية والجماعات المحلية والتهيئة العمرانية:
http://www.interieur.gov.dz

والتقرير السنوي الذي يضعه رئيس مجلس إدارة جامعة نايف العربية للعلوم الأمنية عن أعمال الجامعة.

- إقرار برامج العمل السنوية للمجلس، المقدمة من الأمانة العامة، والميزانية المقترحة لها.
- إقرار وتعديل النظام الداخلي للمجلس، وأنظمته الإدارية والمالية، بما يتفق مع الأنظمة الإدارية والمالية النافذة في جامعة الدول العربية.
- دعم الأجهزة الأمنية العربية ذات الإمكانيات المحدودة.
- تعزيز وسائل التعاون مع الهيئات الدولية المعنية باختصاصه.

شاركت الجزائر في جميع دورات مجلس وزراء الداخلية العرب منذ نشأته، كما سبق لها وأن احتضنت أشغال الدورة السابعة عشر (17) للمجلس خلال الفترة الممتدة من 29 إلى31 جانفي 2000، والدورة الثانية والثلاثين (32) للمجلس المنعقدة، وهو ما يبرز عزم الجزائر على المضي قدما في تفعيل العمل الأمني العربي المشترك، ونقل تجربتها والممارسات التي استخلصتها في مجال مكافحة الإرهاب والتطرف العنيف المفضي إلى الإرهاب، واقتراح حلول نوعية وعمليّة على الصعيد العربي ومداره الإقليمي[62].

وبهدف تطوير التعاون بين أجهزة الشرطة العربية في مجال مكافحة الجريمة، أنشأ مجلس وزراء الداخلية العرب، "المكتب العربي للشرطة الجنائية"، حيث تجسدت مجهودات الدول العربية في النتائج التي انتهى إليها المؤتمر السادس والثلاثين لقادة الشرطة العرب المنعقد يومي 09 و 10 ديسمبر 2012 بالجزائر، من خلال تأكيد الحاضرون وعلى رأسهم وزير الداخلية الجزائري آنذاك "دحو ولد قابلية" الذي طلب من قادة أجهزة الشرطة العرب العمل على تجفيف منابع الإجرام، وإعطاء أهمية لمحاربة الجريمة الإلكترونية، التي تتفاقم في العالم العربي وتتيح للمجرمين استغلال تقنيات المعلومات في نشاطاتهم[63].

هذا الطرح تم تعزيزه ومساندته رسميا من طرف منظمة الشرطة الدولية "أنتربول"، وهو ما تضمنته كلمة السيدة "ميراي باليستارازي" رئيسة المنظمة التي ثمنت مشاركتها في مؤتمر

---

[62] نفس المرجع.

[63] عمر شابي، "المؤتمر 36 لقادة الشرطة العرب بالجزائر...وزير الداخلية يدعو العرب إلى تنسيق مكافحة الجريمة المنظمة". جريدة النصر، 09 -12-2012:

https://www.djazairess.com/annasr/43653

قادة الشرطة العرب بالجزائر، واعتبرتها بالخطوة الإيجابية في التعاون بين الهيئتين العربية والدولية للشرطة، وأوضحت أن جهاز "أنتربول" يوفر للمتعاملين معه قواعد بيانات مفتوحة طول الوقت، حيث بلغت عمليات البحث في قوائمه وبياناته عن الأشخاص حجم 15 مليون عملية بحث منذ توقيع إتفاقية التعاون بين "الأنتربول" ومجلس وزراء الداخلية العرب عام 1999، كما تم استغلال بيانات "أنتربول" للبحث عن الوثائق في 80 مليون عملية[64].

وفي أشغال المؤتمر الثالث والأربعين لقادة الشرطة والأمن العرب، بمشاركة ممثلين من مختلف الدول العربية، فضلا عن ممثلين عن جامعة الدول العربية، والمنظمة الدولية للشرطة الجنائية (الأنتربول)، وجامعة نايف العربية للعلوم الأمنية والاتحاد الرياضي العربي للشرطة، تم عرض تجربة الشرطة الجزائرية في مجال "نظام إرسال الفيديو في الزمن الآني عبر حوامات الأمن الوطني إلى مختلف المصالح الأمنية المختصة باستعمال شبكة 4.G ." [65]

هذا اللقاء يعتبر من بين أرقى الفضاءات المخصصة للبحث والتشاور بين أجهزة الشرطة العربية لدراسة أنجع السبل وأفضل الوسائل الكفيلة بمواجهة التحديات الأمنية، وتسمح أيضا بتوحيد الجهود وتسخير كل الطاقات للتصدي لمختلف التهديدات الإجرامية، بما فيها الاتجار غير الشرعي بالمخدرات والجريمة السيبرانية.

لابد من التذكير بأن الشرطة الجزائرية اتخذت كل ما يلزم من إجراءات وقائية وردعية لمكافحة الجريمة الإلكترونية، من خلال عصرنة الأجهزة واعتماد الحلول التقنية المبتكرة، واستحداث مصالح مركزية وفرق متخصصة، لفك العديد من القضايا، إلى جانب العمل الإتصالي والتوعوي لفائدة مختلف شرائح المجتمع، خاصة على مستوى المؤسسات التربوية، مشيدة بالمبادرة التي أطلقتها الأمانة العامة لمجلس وزراء الداخلية العرب بشأن إنشاء وحدة متخصصة في الأمن الإلكتروني. كما عملت الجزائر على تعزيز ودعم القدرات في مجال مكافحة الجريمة وتحديث أساليب العمل، وتوطيد علاقة الثقة مع المواطن، بالإضافة إلى تطوير التعاون الثنائي والمتعدد الأطراف على الصعيدين الإقليمي والدولي، والتأكيد على أن

---

[64] نفس المرجع.

[65] "المديرية العامة للأمن الوطني تشارك في أشغال المؤتمر الـ43 لقادة الشرطة والأمن العرب بتونس". المديرية العامة للأمن الوطني: https://www.algeriepolice.dz

الجزائر مستعدة لتبادل خبرتها وتجربتها في مجال مكافحة الجريمة المنظمة العابرة للحدود الوطنية والجرائم السيبرانية والإرهاب، خدمة وتعزيزا للتعاون الشرطي العربي[66].

من خلال ما سبق ذكره، يمكن القول أن الجزائر رغم اتخاذها مختلف الإجراءات القانونية والأمنية الممكنة لمواجهة الجرائم السيبرانية في إطار تعاونها الدولي، إلا أن المعالجة الأمنية لوحدها لا تكفي لتحقيق هذه الغاية، ما لم تكن مقرونة بالتكفل الأمثل بالقضايا الاجتماعية والاقتصادية والثقافية، وذلك من خلال القضاء على الظروف المؤدية للإجرام، ودعم التنمية والحكم الراشد، لبناء علاقات متينة مع المواطن وجعله شريكا فعالا في المعادلة الأمنية.

الخاتمة:

تعتبر الجرائم السيبرانية من أخطر التحديات الأمنية التي يشهدها القرن الحادي والعشرين سواء على المستوى الوطني أو الإقليمي أو الدولي، لهذا بات من الضروري على جميع الدول العمل المشترك من أجل تعزيز التعاون، القائم على التنسيق وتبادل الخبرات والممارسات، لمواجهة المخاطر المختلفة التي يمكن أن تطرحها هذه الجرائم في جميع المجالات.

وفي هذا الإطار، عملت الجزائر على تطوير استراتيجية أمنية متعددة الجوانب(التشريعية، التنظيمية، البشرية، المالية، التقنية، والمعلوماتية)، تتناسب مع طبيعة هذه الجرائم، من خلال تدعيم منظومتها القانونية ومطابقتها للاتفاقيات الإقليمية والدولية، للرد على تحديات الإجرام السيبراني على مختلف المستويات.

ورغم ذلك مازالت الدولة الجزائرية في حاجة إلى استثمارات فكرية ومادية هائلة لتصميم وتطوير هذه الاستراتيجية، حتى تضمن تأمين الثورة الرقمية للأفراد والمؤسسات، وبالتالي التصدي لخطر تشتكي منه اليوم كل الدول.

---

[66] نفس المرجع.

من جهة أخرى، فإن حداثة هذه الجرائم تعيق إلى درجة كبيرة استراتيجيات المواجهة ما لم يتفق المجتمع الدولي على تعريفها بما يسمح من تحديد آليات مكافحتها، ويؤسس لتعاون دولي حقيقي في إطار الثقة المتبادلة.

بعد الدراسة والتحليل لكل المعطيات المتعلقة بهذا الموضوع، يمكن اقتراح التوصيات التالية :

– تنظيم حملات توعية لمستعملي الوسائط الإلكترونية (الحاسوب، الأنترنت، الهواتف الذكية وغيرها)، وتعريف المواطنين بحجم الخطورة التي تترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة عند استعمالهم لهذه الوسائط، مع ضرورة التحديث المستمر لبرامج الحماية.

– تنمية وتطوير على نطاق أوسع وبصفة مستمرة من الناحية المادية، والبشرية والتنظيمية للمراكز العملياتية المتخصصة لمعرفة كل الصعوبات والعوامل التي تؤثر، أو تحول دون الالتزام بتنفيذ وإنجاح الخطط والبرامج المسطرة، وإدخال التعديلات التي تسمح برفع مستوى الجاهزية للإسهام بفاعلية في الوقاية وردع انتهاكات القوانين المشتركة في مختلف المجالات.

– إنشاء بنك معلوماتي رئيسي لجمع المعلومات وتوثيقها وتصنيفها وتوزيعها بين المراكز المختلفة، تسند إدارته إلى أشخاص من ذوي الكفاءة العالية في المجال، لأن قاعدة البيانات المدققة المتاحة للمختصين تسهل تعاون سلطات تنفيذ القانون في إطار تبادل المعطيات لتيسير الكشف عن مواطن العطب، هذا بالإضافة إلى ضرورة كشف الأساليب والوسائل التي تلجا إليها المنظمات الإجرامية، وبالتالي ضمان التحري والملاحقة القضائية.

– فتح جسور تواصل قضائية وأمنية مع جميع الدول وكذا المنظمات الدولية المتخصصة الحكومية وغير الحكومية في مجال تبادل المعلومات المختلفة، للاستفادة من التطور العلمي وثورة المعلومات والاتصالات والتوجهات العالمية في هذا الصدد، والسياسات والتدابير المتخذة لمنع الجريمة السيبرانية، ومن هنا يمكن انتهاج خطة موحدة على نحو أكثر شمولية ومرونة لاستيعاب خصوصية هذه الجريمة وتحدياتها.

قائمة المراجع:

- قانون رقم 09- 04 مؤرّخ في 14 شعبان عام 1430هـ الموافق 5 أوت سنة 2009 م ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرّسميّة للجمهوريّة الجزائريّة /العدد 47، 25شعبان عام 1430 هـ 16أوت سنة 2009 م.

- "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات". جامعة الدول العربية، الأمانة العامة، 21 ديسمبر 2010.

-"التقرير التفسيري لاتفاقية الجريمة الإلكترونية "، من سلسلة المعاهدات الأوروبية رقم185. بودابست، في 23 نوفمبر 2001.

- الغافري حسين بن سعيد بن سيف، **الجهود الدولية في مواجهة جرائم الإنترنت**. موقع المنشاوي للدراسات والبحوث، 2007.

-الهاشمي رفد عيادة ، **الإرهاب الإلكتروني**. (د.م.ن)، (د.ت.ن).

-ليوبولد إيريك- سيرج لوست، (ترجمة: فتحي علي زمال)، **أمن المعلومات**. المملكة العربية السعودية، مدينة الملك عبد العزيز للعلوم والتقنية، 2012.

-عبد الصادق عادل، **الفضاء الالكتروني والرأي العام : تغير المجتمع والأدوات والتأثير**. القاهرة: المركز العربي لأبحاث الفضاء الالكتروني، 2009.

- عرب يونس، **جرائم الكمبيوتر والأنترنت، المعنى والخصائص والصور وإستراتيجية المواجهة القانونية**. المركز الوطني للتوثيق، أكتوبر2006.

- الحوامدة لورنس سعيد، " الجرائم المعلوماتية أركانها وآلية مكافحتها: دراسة تحليلية مقارنة". المملكة العربية السعودية: جامعة طيبة، كلية الحقوق،

-- "المنظمة الدولية للشرطة الجنائية – أنتربول". الجمهورية الجزائرية الديمقراطية الشعبية، المديرية العامة للأمن الوطني:

https://www.algeriepolice.dz

- "المديرية العامة للأمن الوطني تشارك في أشغال المؤتمر الـ43 لقادة الشرطة والأمن العرب بتونس". الجمهورية الجزائرية الديمقراطية الشعبية،المديرية العامة للأمن الوطني:

https://www.algeriepolice.dz

- "مجلس وزراء الداخلية العرب". الجمهورية الجزائرية الديمقراطية الشعبية الجزائرية، وزارة الداخلية والجماعات المحلية والتهيئة العمرانية:

http://www.interieur.gov.dz

- باشوش نوارة، "استحدث مصلحة للدفاع السيبراني ومراقبة أمن الأنظمة. الجيش يدخل حرب "الفضاء الإلكتروني" ومكافحة الجوسسة". موقع الشروق أون لاين، 12-10-2017:

https://www.echoroukonline.com

http://alimbaratur.com/?p=2850

-عبد الصادق عادل، "الهجمات السيبرانية:أنماط وتحديات جديدة للأمن العالمي".الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، 27-11-2019:

https://www.politics-dz.com

-

https://democraticac.de/?p=42040

- شابي عمر ، "المؤتمر 36 لقادة الشرطة العرب بالجزائر. وزير الداخلية يدعو العرب إلى تنسيق مكافحة الجريمة المنظمة ". جريدة النصر، 09 - 12 -2012:

https://www.djazairess.com/annasr/43653

https://www.europarabct.com/?p=34807

-"الجزائر تعزز شراكتها الإستخباراتية مع الأنتربول واليوروبول بمصادقتها على نتائج مؤتمر يوروميد للشرطة".الفجر 18 - 07 – 2012:

https://www.djazairess.com/alfadjr/219938

- "الجزائر تولي أهمية لـ"أفريبول" لمجابهة المخاطر الجديدة". جريدة المساء، 03-10-2019:

https://www.el-massa.com/dz

https://www.europarabct.com

- Lehto Martti, Neittaanmäki Pekka, **Cyber Security: Analytics, Technology and Automation**. Springer International Publishing Switzerland 2015.

- Melzer Nils, **Cyberwarfare and International Law**. Unidir Resources,2011.

-Norbert Wiener, **Cybernetics or control and communication in the Animal and the machine**. Cambridge, Massachusetts Institute of Technology, Second Edition ,1961.

- Ventre Daniel, « La cyber paix, un thème stratégique marginal », **Revue internationale et stratégique**, 2012/3 n° 87, 2012.

- Barlock Steve, Buffomante Tony, Rica Fred , «Cyber Security: it's not just about technology » .Information Protection and Business Resilience, 2014:

https://assets.kpmg/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf