

وزارة التعليم العالي والبحث العلمي
جامعة مولود معمري - تيزي وزو
كلية الحقوق والعلوم السياسية
قسم الحقوق

مكافحة الإرهاب الإلكتروني في القانون الدولي

رسالة لنيل شهادة دكتوراه في العلوم
تخصص: قانون

• تحت اشراف:
الأستاذ الدكتور خلفان كريم

• من اعداد الطالبة الباحثة:
نجاري بن حاج علي فايزة

﴿لجنة المناقشة﴾

أ/د. تاجر محمد، أستاذ جامعة مولود معمري، تيزي وزو..... رئيسا
أ/د. خلفان كريم، أستاذ جامعة مولود معمري، تيزي وزو..... مشرفا ومقررا
أ/د. البريقات عبد القادر، أستاذ جامعة بن عكنون، الجزائر..... ممتحنا
د/ علي احمد رشيدة، أستاذة محاضرة صنف(أ)، جامعة مولود معمري، تيزي وزو..... ممتحنة
د/ لوني نصيرة، أستاذة محاضرة صنف(أ)، جامعة أكلي محمد اولحاج، البويرة..... ممتحنة
د/ بركاني اعمر، أستاذ محاضر صنف(أ)، جامعة عبد الرحمن ميرة، بجاية..... ممتحنا

تاريخ المناقشة...../.....

﴿ كلمة شكر وتقدير ﴾

أول الشكر هو شكر الله سبحانه وتعالى على فضله أن يسّر لي إتمام هذه الأطروحة.

اعترافاً بالفضل والجميل أتوجّه بخالص شكري ووامتناني مع كل احترامي إلى **الأستاذ الدكتور خلفان كريم** الذي تفضّل بالأشراف على هذا العمل وتابعه بالتصويب في جميع مراحل إنجازه ، فجزاه الله عني كلّ الخير.

كما لا يفوتني ان اتشكر أعضاء لجنة المناقشة على رأسهم الأستاذ الدكتور تاجر محمد، لقبولهم تقييم وتصويب هذا العمل واثراءه بملاحظاتهم التي تزيد من قيمة العمل وترقى به من حسن لأحسن.

وأخيرا اتشكر كل اساتذتي من الطور الابتدائي الى الجامعي ، واطمئن بالذكر المعلم نجاري بن حاج علي بالعربي.

نجاري بن حاج علي فائزة

إهداء



إليك يا **أبي الفضيل**.... ذات يوم كنت زعيم الجزائر بعملك وكفاحك في سبيل الرقي بهذا الوطن، واليوم انت زعيم الزعماء بعطاء خير خلفك.

إليك يا **أبي**.... يا قرّة العين ورفيقة الفؤاد وساترة العيوب.

إليك اخوتي.... والله ما حلت الدنيا في عيني يوما إلا لوجودكم فيها: عثمان، خالد، حمزة، عمر، خليل، يونس، يوسف.

إليك يا **أختي آمنة الرائعة**.... وما عساها تقول الروح فيك وانت القلب النابض لهذه الروح، وما زادك حلاوة سندك الذي احبه حبا اخويا عزالدين متبوعا بفراشتان ولا أروع، صغيرتي ماريا ورتال.

اليكن يا اشباه الملائكة **زوجات اخوتي** شياء ورزيقة وأطفالكن هارون، آية، زكريا ريح من رياح الجنة.

إليك يا **أصحاب المشوار الدراسي**.... وجودكم جلع للمنافسة العلمية مذاق عسل جبلي حر، كلما أكلت منه زدت رغبة فيه.

إليك يا **أصدقائي**.... وهل تحلوا الحياة من دون صداقة يتبعها وفاء واحترام.

الى كل فرد من عائلات: نجاري بن حاج علي، عيفون، سعدي، رايب، بنجاوي، سي أحمد، اوشبوك، توجي، تعزيت، عوانة محمد عربي.

وأخيرا:

إليك انت **زوجي وحيبي**.... أراك طفلي عند الحب، وابي عند ضعفني، واخي عند شجاري بمزاح، وكل البشر عندما اشعر بأني وحيدة... **احبك** وكفاني بهذه الكلمة اختم

اهداي. كصفافيزة نجاري بن حاج علي

فايزة نجاري بن حاج علي

المختصرات:

باللغة العربية:

ج.ر: الجريدة الرسمية.

En français:

ANSSI: Agence nationale de la sécurité des systèmes d'information.

IRM: Imagerie par résonance magnétique.

J.O.U.O: Journal officiel de l'Union européenne.

OCDE: Organisation de coopération et de développement économiques.

VPN: Réseau privé virtuel.

In English :

ACARS: Aircraft Communication Addressing and Reporting System.

AMPS: Advanced Mobile Phone System.

CD-ROM: Compact Disc -Read Only Memory.

C-Netz: Radio Telephone Network C.

CSDP: Common Security and Defence Policy.

DES: Data Encryption Standard.

FBI: Federal Bureau of Investigation.

FECT: Financial and Economic Crime Team.

FSB: Federalnaïa Sloujba Bezopasnosti.

FTP: File Transfer Protocol.

GPS: Global Positioning System.

GSM: Global System for Mobile Communications.

IBM: International Business Machines Corporation.

IDEA: International Data Encryption Algorithm.

IOCTA: Internet Organised Crime Threat Assessment.

IP: Internet Protocol

IPES: Imprived Proposed Encryption Standard.

LAN: Local Area Network.

MBR: master boot record.

NIJ: National Institute of Justice.

NMT: Nordic Mobile Telephone.

NSF: National Science Foundation.

PES: Proposed Encryption Standard.

POP3: Post Office Protocol

PSTN: Public Switched Telephone Network.

PVC: Poly Vinyl Chloride.

RSA: Rivest Shamiret Adleman

SMTP: Simple Mail Transfer Protocol

SOCTA: Serious and Organised Crime Threat Assessment.

SWGDE: Scientific Working Group on Digital Evidence.

SWIFT: Society for Worldwide Interbank Financial Telecommunication.

TCP: Transmission Control Protocol

TELNET: terminal network ou telecommunication network.

UDP: User Datagram Protocol

USB: Universal Serial Bus

WAIS: Wechsler Adult Intelligence Scale.

WAN: Wide Area Network.

WIPO: World Intellectual Property Organization.

www: World Wide Web.

مقدمة

تعد الظاهرة الإرهابية ظاهرة قديمة قدم الإنسانية، فقد مثلت لعقود من الزمن آلية يتم استغلالها، وأسلوبا يتم انتهاجه لإثبات وجهات النظر وفرضها، وتمير الأفكار والسياسات والإيديولوجيات وتثبيتها، وإحداث تغييرات أو مقاومتها، فهو آلية متاحة لكل الأطراف الفاعلة على الصعيدين الداخلي والدولي، رغم تفاوتهم في شكل توظيفها، والتبعات التي تتجر عنها.

لكن هذه الظاهرة لم تتشكل في شكلها الأكثر عنفا ودموية إلا مع بداية القرن التاسع عشر، فمنذ تلك الحقبة أصبحت الظاهرة الإرهابية توظف بشكل مخيف، وبصورة أكثر راديكالية، وقد خلفت وراءها مآسي أصمت أذن التاريخ، وتركت خلفها رعبا ممتد الآثار، ورهبة ثقيلة الوطأة، وقد حفظت لنا ذاكرة التاريخ وأخبار الرواة وشهود العيان صورا قبيحة للإرهاب العنصري الذي مارسته القوى النازية في أوروبا الغربية قبل وإبان الحرب العالمية الثانية، وعلى رأسها مجازر الهولوكوست، وقد عايشنا أيضا بعضها في أواخر القرن المنصرم كأحداث الحادي عشر من سبتمبر 2001، والعنف الدامي الذي شهدته الجزائر فيما يعرف بالعشرية السوداء.

فالظاهرة الإرهابية هي الهاجس الأكبر الذي يورق البشرية جمعاء، إذ انه يمثل التهديد الأكبر للدول في وجودها وبنيتها ومقوماتها واستقرارها، وهي من أبرز الظواهر التي تزعزع وتهدد الأفراد في أمنهم المادية والنفسي، وهي في الوقت ذاته خطر داهم يعصف بالعلاقات الدولية والاستقرار والأمن الدوليين، فهي إذا ظاهرة تضع العالم أجمع أمام تحديات حقيقية يتعين عليه رفعها والتعامل معها بقدر كبير من المسؤولية.

يعترف الواقع أن ظهور الثورة الصناعية والتطور التكنولوجي والتقني، والذي شهدته حقبة القرن الثامن عشر، والذي لم يفتر من ذلكم الحين، قد ساهم وبشكل أساسي ورئيسي في خلق صور ومظاهر متطورة للظاهرة الإرهابية، والمميز لهذه الصور أنها تشكل تهديدا خطيرا بالحياة البشرية مقارنة بالصور التقليدية له، حيث ظهر إرهاب بيولوجي وآخر نووي، وإرهاب إشعاعي وآخر كيميائي، وهذه الأشكال بالغة الخطورة وعظيمة الأثر وشديدة الفتك، غير أنه وبعد ظهور عصر مجتمع المعلومات، وتزايد انصراف البشر إلى فضاء المعلومات والاتصالات، بانث صورة حديثة من الإرهاب لا تقل خطورة عن سابقتها، حيث تعتبر كمهدد جدي للأمن والسلام العالميين، والمتمثلة في الإرهاب الإلكتروني.

لقد تكيف الفكر الإرهابي والفاعلين الذين يتبنونه مع التدامج والتداخل الحاصل بين تكنولوجيات المعلومات وتكنولوجيات الاتصال، والذي خلق فضاءً إلكترونيا رحبا يجمع بين ثنياه حاضره البشرية ومستقبلها، والذي أصبح ساحة من ساحة خوض الحروب الناعمة والصلبة على حد سواء، وفضاء للصراعات بين القوى الفاعلة من الدول وغير الدول على قدم المساواة، ويتم ذلك من خلال توظيف جملة من الأسلحة الإلكترونية الفتاكة التي يمكن أن تخلف وراءها دمارا وخرابا مهولا يمكن أن يتسبب في انهيار الدول، لما لأمنها القومي من ارتباط وثيق بهذا الفضاء الذي يعد حيويا في الكثير من المجالات الاستراتيجية.

فبظهور هذا الفضاء الإلكتروني أصبح العالم أمام أمر واقع، وهو وجود تحولات كبرى تأثر بشكل كبير وحرص على جميع مجالات الحياة الإنسانية من سياسة واقتصاد وتجارة وأعمال وإدارة وغيرها وقد أجبر هذا الوضع الدول على إعادة النظر في مفاهيم أمنية وسياسية وقانونية كثيرة، وأصبحت الضرورات والاعتبارات التي يفرضها هذا الفضاء دافعا للدول نحو تبني مفاهيم جديدة وعلى رأسها المعضلة الأمنية الناتجة عن النشاطات الإرهابية والتخريبية على الفضاء الإلكتروني.

و هذه المفاهيم الجديدة التي بدأت بالتشكل مع تشكل الفضاء الإلكتروني وذيوع توظيفه واستعماله في الكثير من مجالات الحياة، إنما أتت من واقع هذا الفضاء الإلكتروني نفسه، والذي يعتبر فريدا في بنيته التكوينية، شاملا لمباني الحياة الإنسانية كلها، لذلك فإنها مفاهيم متأقلمة مع طبيعة هذا الفضاء، مبنية على جوهره وخصائصه، وهذا ما يجعل منها مفاهيم معقدة أيضا، وغير واضحة المعالم، مما فتح مجالا لنشوب خلافات كثيرة حول سبل التعامل معها، وإنزالها منزل التطبيق والتوظيف.

و من بين هذه المفاهيم الجوهرية التي تمخضت عن هذا الفضاء الإلكتروني، مفهوم الإرهاب الإلكتروني، والذي حاول الباحثون والدارسون الوصول إلى تعريف جامع ومانع له، مستبصرين في ذلك بما يمكن أن يشتمل عليه من خصائص وما يمكن أن يميزه من مميزات، وما قد يكون عاملا منشأ له فكان أن أخذ كل منهم في ذلك مسلكه، فتعددت نحلهم وتوجهاتهم، وتناقضت آراؤهم وأفكارهم، وتضاربت تصوراتهم ومداركهم، وجرى على مفهوم هذا النوع من أنواع الإرهاب ما جرى على الظاهرة الإرهابية بشكل عام من اضطراب في المفهوم.

و يمكن أن نعتبر هذا الاضطراب الحاصل في مفهومه أكثر تعقيدا من ذاك الذي ساد الإرهاب التقليدي، إذ أنه يحمل في جوهره نفس المعضلات المفهومية التي تشوب مفهوم الإرهاب التقليدي، وتقوم على نفس أسس الخلاف في تعريفه وطبيعته، وتزيد عليها بكونها متعلقة بفضاء

إلكتروني فسيح لم يحسم فيه الباحثون رأيا، فكون الإرهاب الإلكتروني ضمن صور الظاهرة الإرهابية، وكونه واقع على فضاء إلكتروني غامض المفهوم، يعد من بين أبرز وأكثر الأسباب التي تضيف على مفهومه الغموض، وعلى تعاريفه وطبيعته عدم الدقة والوضوح.

بالإضافة أيضا إلى إمكانية تلاقي الإرهاب التقليدي مع الإرهاب الإلكتروني، وتكوين إرهاب إلكتروني هجين، وهذا حينما لا يكون الهدف منه إحداث دمار في الفضاء الإلكتروني نفسه أو في البنى التحتية الحرجة المتصلة به، بل يكون عندما يتم توظيفه من أجل دعم ومساندة نشاطات إرهابية تقليدية، إذ أنه من الممكن جدا أن يكون الفضاء الإلكتروني آلية ووسيلة في أقصى درجات الخطورة حينما يتم استغلالها لتنشيط عملية تجنيد الإرهابيين أو تمويل الإرهاب.

كما يلتقي أيضا الإرهاب الإلكتروني مع الإرهاب التقليدي في الكثير من الأسباب التي تقف وراءه، والعوامل التي تؤثر في حجمه وشيوعه، ومع ذلك نجده ينفرد عن الإرهاب التقليدي في جانبه التقني والفني، وهذا ما يجعله إرهابا فريدا، وتهديدا معقدا.

و مع ذلك يجمع الباحثون والدارسون على خطورة هذه الظاهرة، ومساسها الكبير بالأمن والسلامة على الصعيدين الوطني والدولي، واجمعوا على ضرورة العمل على توحيد الجهود وتوجيهها نحو التصدي لمظاهرها ومنعها، أو الحيلولة دون تفاقمها وتفاقم الأضرار التي قد تترتب عنها، ودق ناقوس الخطر الذي بانته معالمه في أفق عصر المعلومات من خلال توالي الهجمات على أهداف تتسم بالحرج وتضع الأمن والسلامة الوطنية والدولية على المحك، وبشكل خاص، بالنسبة لتلك الدول التي يعتبر فيها الفضاء الإلكتروني عصب قطاعات حيوية كبرى، والتي لا يتوقف التوجه نحو رقمنة كل مجالات الحياة فيها.

ولعل هذا التزايد المستمر لتوظيف الفضاء الإلكتروني في قطاعات حساسة وفي إنشاء بنى تحتية حرجة وإدارتها، والتنامي الكبير في التوجه نحو الحوكمة الإلكترونية للكثير من الأجهزة والمنظمات السيادية في الدولة كقطاع العدالة والدفاع، هو الذي جعل من الإرهاب الإلكتروني مصدر قلق كبير للدول لما قدر ينجر عنه من تداعيات لا تختلف في قوتها التدميرية عن الإرهاب النووي أو البيولوجي على سبيل المثال، ويعود هذا الأمر لما يتميز به هذا الإرهاب من يسر في التنفيذ وسيطرة الغموض والإبهام عن آليات الحسم والمواجهة الأمنية والتقنية والقانونية لعدم قدرة الدول على فرض سيطرة كاملة على الفضاء الذي يمارس فيه أو عليه، وهذا ما دفع بالدور إلى التوافق على ضرورة التصدي له ومواجهته.

ساهم هذا الاتفاق على ضرورة قيام الدول بدفع سياساتها الداخلية للمزيد من التوسع لتشمل موضوع الإرهاب الإلكتروني، والوقوف في مواجهتها والتصدي لها، وتفعيل كل الآليات القانونية والتقنية الممكنة.

ولا ريب أن الطبيعة العالمية لظاهرة الإرهاب الإلكتروني وتجاوزها للحدود السيادية للدول لا تكفي ولا تفي معها المواجهة الداخلية أو حتى الإقليمية بمفردها، لذلك فإن هناك ضرورة ملحة إلى تكاثر الجهود الدولية، وبناء نظام دولي متكامل الأركان في التصدي له، وفق نهج شامل وكامل.

ويجب على النهج الذي تعتمد عليه هذه المواجهة ألا يخلو من عنصرين جوهريين، ونمطين أساسيين، أولهما هو الحسم الأمني والوقائي أين تتهيكّل المواجهة وتتخذ بعدا تنظيميا وتقنيا موائما لجوهر الظاهرة، مسائرا لطبيعتها التقنية المعقدة، وشاملا لكل النطاقات التي يمكن أن يستهدفها، والآليات التي يمكن أن يستغلها ويوظفها، فضلا عن دعم الطب الشرعي وتطويره، وتكوين التخصصات والهياكل والكوادر المعنية بالتحقيق في مثل هذه الجريمة.

وأما ثانيهما فهو الحسم التشريعي والذي مفاده بناء واستحداث نصوص التشريعية، وطنية وإقليمية ودولية، تنص صراحة على تجريم هذه الظاهرة، وتقمعها بنصوص عقابية رادعة تتناسب مع خطورتها الإجرامية.

ولا شك أيضا أن على عاتق الدول مسؤولية فتح منافذ وسبل التعاون فيما بينها للسيطرة على هذه الظاهرة التي تتفاقم يوما بعد يوم وتوفير المواد والإمكانية اللازمة للتصدي لتداعياتها العالمية، ولذلك تلجأ الدول إلى استغلال كل آليات التعاون القانوني والقضائي المعمول بها في مواجهة صور الإجرام المنظم، وصور الإرهاب التقليدي، بالإضافة أيضا إلى محاولاتها المستمرة لخلق منافذ تعاون جديدة وأساليب متطورة تتوافق مع الطبيعة الاستثنائية لهذه الظاهرة، وإعادة تشكيل هيكل التعاون الدولي بما يضمن الأمن والسلم العالميين.

وبناء على ما تقدم ذكره، فإن الإشكالية التي تقوم عليها الدراسة كلها، هي البحث في:

ما هي الآليات التقنية التي يمكن التصدي بها لظاهرة الإرهاب الإلكتروني؟ وما هي السبل القانونية التي يمكن أن تحقق ضمانا شاملا لأمن الفضاء الإلكتروني من تهديدات وهجمات الإرهاب الإلكتروني؟

أهمية الموضوع:

يعد موضوع الإرهاب الإلكتروني من المواضيع التي أصبحت تكتسي أهمية خاصة، وهذه الأهمية إنما أكتسبها لكونه من المسائل أو القضايا المستجدة التي أصبحت تتسارع في تفشيها وانتشارها، ولكونه أيضا من الجرائم التي أصبحت تأخذ بعدا دوليا ومنظما، فالإرهاب الإلكتروني وبقطع النظر عن الطبيعة العالمية للفضاء التي يوظف فيه أصبح يهدد بشكل كبير أمن واستقرار المجتمع الدولي ككل، كما أن الإرهابيين الإلكترونيين أصبحوا يشكلون جماعات الإجرام المنظم العابر للأوطان.

يكتسي موضوع الإرهاب الإلكتروني أيضا أهمية كبيرة، ويشغل حيزا واسعا في الدراسات الأكاديمية، لكونه إرهاب معقد، فهو على خلاف الإرهاب التقليدي يتضمن جانبا فيه يتأسس على التقنية، إذ أنه إرهاب يقوم على ما جادت به عقول العلماء من ابتكارات واختراعات تكنولوجية مركبة، حيث يعمل على توظيفها لأغراض إجرامية وإرهابية، ولتهديد الأمن والسلم العالميين.

يعتبر موضوع الإرهاب الإلكتروني موضوعا ذو أهمية بالغة أيضا لما قد ينجر عنه من كوارث وطامت جسام، فالتداعيات والمخاطر التي قد تتمخض عن الهجمات الإلكترونية والسيبرانية بأي سلاح من أسلحتها قد يكون لها أثر تدميري خطير، خاصة مع ارتباط الكثير من القطاعات والبنى التحتية الحرجة بالفضاء الإلكتروني محل تنفيذ الهجمات، فالإرهاب الإلكتروني يعد من أكبر التهديدات المعاصرة للأمن القومي للدول من جهة، وسلامة العلاقات الدولية من جهة ثانية، والتكامل الفردي من جهة ثالثة.

يمكن أن يكون الإرهاب الإلكتروني وسيلة من الوسائل التي يتم استخدامها لخدمة أهداف الإرهاب التقليدي، فتجنيد الإرهابيين وتمويل الإرهاب، وتيسير عمليات الاتصال الآمن بين أفراد التنظيمات الإرهابية، والتدريب على استعمال أشكال مختلفة من الأسلحة أو صناعتها وما إلى ذلك يعد مظهر من مظاهر الإرهاب التقليدي وفي الوقت نفسه يطغى عليه الجانب التقني في ممارسته، ولذلك فإن أهمية موضوع الإرهاب الإلكتروني إنما أتت في المقام الأول من خطورة الظاهرة الإرهابية بشكل عام.

أسباب اختيار الموضوع:

دعت الأهمية الكبرى التي يمتاز بها موضوع الإرهاب الإلكتروني، والتزايد المستمر للمجتمع الدولي على العناية به وجمع جوانبه إلى اختياره كموضوع للدراسة، ذلك أنه موضوع الساعة وفيه

من الجدة والحادثة ما يجعله موضع اجتهادات فقهية مختلفة، وساحة خصبة للبحث القانوني، وبحرا متلاظما من الآراء والتوجهات المتباينة، فكان اختياره بغرض جمع شتات الأبحاث المتناثرة، والتوفيق بين الآراء المتناقضة، والوصول إلى تكوين نظرة شاملة، تتضح لنا فيها معالم هذه الظاهرة، والآليات التي نصرف بها خطرهما، ونجتث بها جذورها.

إن افتقار المكتبة العربية إلى دراسات مستفيضة وأبحاث متقدمة في موضوع الإرهاب الإلكتروني كان له الدور المهم في اختيارنا لهذا الموضوع خدمة منا لمجتمعنا، وإثراء لمكتبتنا، وإسهاما ولو بجزء بسيط في خدمة المنظمة القانونية في بلادنا، ولا شك أيضا أن للدوافع النفسية دورا في اختياره، فالميل الشخصي إلى دراسة المواضيع التي تجمع بين صنوف مختلفة ومباحث متعددة من المباحث العلمية كان من بين أسباب هذا الاختيار الذي نراه موقعا.

منهج الدراسة:

لا يختلف باحثان على أن موضوع كموضوع الإرهاب الإلكتروني من غير الممكن على الإطلاق انتهاج نهج بحثي واحد من مطلعه إلى خاتمته في عملية دراسته، فقد انتهجنا لاعتبارات خاصة متعلقة بالصعوبات التي واجهتنا في بحثنا إلى عدة ألوان ونهج البحث العلمي، إذا أننا، سلكنا مسلك الاستنباط والظاهر جليا في الكثير من مواضع وفروع هذه الدراسة، ولاسيما في بيان خطورة تداعيات الظاهرة، حيث ننقل من كليات الإرهاب التقليدي إلى جزئيات الإرهاب الإلكتروني لتفصيل مباحث هذه الدراسة، كما ننقل أيضا بشكل تصاعدي في إطار نهج استقرائي حال دراسة النصوص القانونية المتعلقة بهذا المجال، وذلك من أجل تكوين نظرة شاملة عن أسس التجريم وأساليب العقاب وإجراءات المتابعة.

ونظرا لكون ظاهرة الإرهاب الإلكتروني من بين أهم الظواهر الإجرامية الحديثة، فإن الضرورة تقتضي أن يكون للوصف مقاما كبير في دراستها، لذلك فقد ارتأينا أن يكون للمنهج الوصفي والتحليلي مكانة مهمة في هذه الدراسة، وهذا لبيان وبشكل شاف وكاف لحقيقة هذه الظاهرة وعرضها على صفحات بيضاء، كما أننا لجأنا إلى نهج النقد العلمي البناء في بعض المسائل المرتبطة بموضوع الدراسة، وليس ذلك إلا بالنظر الياسير وبما تمليه علينا دوافع الحرص على خدمة هذا الموضوع وإثراءه خاصة وأن الموضوع موضوع خصب.

تقسيم البحث:

تم تقسيم هذه الدراسة إلى بابين اثنين، فأما الباب الأول فقط تطرقنا فيه إلى الإرهاب الإلكتروني في ظل العولمة الافتراضية، أين عالجنا في فصله الأول الإطار المفهومي للفضاء الإلكتروني وتركيبته وأثرها على العديد من المفاهيم المختلفة، وظاهرة الإرهاب الإلكتروني بمفهومها وأسبابها وأساليبها وما ينجر عنها من تبعات وتداعيات وهذا في فصله الثاني، أما الباب الثاني فكان مضمونه التصدي الدولي لجريمة الإرهاب الإلكتروني، فتناولنا في الفصل الأول الجهود الأمنية الدولية في مواجهة الإرهاب الإلكتروني، أما الفصل الثاني منه فكان موضوعه الجهود القانونية الدولية في مواجهة ظاهرة الإرهاب الإلكتروني، وختمنا الدراسة بجملة من الاستنتاجات وبصفوة من التوصيات والمقترحات التي رأينا أهميتها وضرورة الإشارة إليها.

الباب الأول:

الإرهاب الإلكتروني في ظل عولمة الفضاء
الإلكتروني

لقد خطى الإنسان مع بداية القرن التاسع عشر خطوات كبرى لا نضير لها إلى عالم التطور التكنولوجي في جميع المجالات واليادين، واستطاع هذا التطور والازدهار أن يشمل مجالات مهمة وحساسة تبرز المعلومات والاتصال في مقدمتها، فقد تمكن الإنسان المعاصر من إحداث تغيرات فعلية في البنية الأساسية للعمليات المتعلقة بمعالجة وتخزين المعلومات كما أحدث على الصعيد نفسه تغيرات أسطورية في آليات الاتصال ووسائله، وتمكن بعد ذلك من خلق بيئة تقنية تمازجت فيها تكنولوجيا المعلومات مع تكنولوجيا الاتصال لتخلق فضاء عاما تتلاقى فيه البشرية كلها بتراتها وعلومها وإرثها الحضاري ومخزونها المعلوماتي دون أن يكون للفوارق العرقية والثقافية والدينية والهوياتية والحدود الجغرافية والسياسية أي اعتبار.

وأصبح هذا الفضاء الذي يطلق عليه الدارسون اسم الفضاء الإلكتروني أو الفضاء السيبراني صورة جديدة أو بالأحرى بعدا عصريا من الأبعاد الكونية، وأصبح يكتسي أهمية كبيرة في مفهومه وفي التغيرات الجذرية التي تمكن بكل براعة وفاعلية وكفاءة من إحداثها في مدة زمنية مختصرة وعلى كافة المستويات وكل الأصعدة بما في ذلك تأثيراته على الكثير من المفاهيم ذات الطبيعة الاستراتيجية، كما وأنه قد فتح آفاقا جديدة أمام إنسان مجتمع المعلومات ووضعه أيضا في نفس الوقت أمام تحديات معقدة لم يعهدها من ذي قبل، الأمر الذي دعا إلى ضرورة تكوين تصورات ومنظمات معرفية جديدة تتناول مفاهيم قديمة نسبيا من زاوية يكون فيها الفضاء الإلكتروني محورا أساسيا وعنصرا رئيسيا (الفصل الأول).

يبرز الأمن كمفهوم أساسي من المفاهيم التي أثر فيها الفضاء الإلكتروني تأثيرا مباشرا وسلبيا، فقد تمكن من وضع البشرية جمعاء، مؤسسات ودول وأفراد على محك تحديات وتهديدات حديثة في آلياتها وفريدة في طبيعتها وشاملة في أبعادها وكثيرة في عددها وشديدة في قوتها، والأكثر من ذلك كله أنها تحديات على قدر كبير من المرونة والتعقيد بحيث تستطيع إعادة تشكيل الخرائط السياسية والتأثير على مسار توازن القوى على المستوى الدولي، ويشكل الإرهاب الإلكتروني أهم هذه التحديات والتهديدات الأمنية بحيث أصبحت بعدا جديدا يهدف إلى تهديد أمن المجتمعات وتفكيك بنيتها بالإضافة إلى أهدافها في تقويض السلم والأمن العالميين.

وأمام ظهور وتطوير أسلحة إلكترونية حديثة وأساليب جديدة مبتكرة في توظيفها والغياب شبه الكامل للآليات التي يمكن بها التصدي لهذه الآفة أو الظاهرة ذات الصبغة العالمية ولاسيما غياب الجانب التشريعي والرقابي جعل منها من أبرز المظاهر التي تهدد الأمن وتزعزع الاستقرار، ولما

كان الفضاء الإلكتروني ذو أهمية استراتيجية وبعداً حيوياً في حياة المجتمعات المعاصرة وتعلق الكثير من مجالات الحياة به والتزايد الكبير في الاعتماد عليه في إنشاء وبناء وتسيير البنى التحتية الحرجة، كان من الضروري فهم جوهر الإرهاب الإلكتروني وماهيته من خلال العمل على كشف الأسباب التي تقف وراءه، وتحديد طبيعة الهجمات المحتملة والأسلحة التي يتم توظيفها، والمظاهر التي تتشكل فيها، بالإضافة إلى معرفة متقنة بكل ما يتدعى عن تلك الهجمات الإرهابية على الساحة السيبرانية من أضرار على الأمن القومي للدول وتأثيراته على العلاقات والتفاعلات الدولية، وهذا من أجل تحقيق الكفاءة والفعالية في تحديد الآليات والوسائل والتقنيات التي يمكن بها قمع هذه الظاهرة أو الحد من حجم تداعياتها بما يكفل ويضمن المساعي الدولية في تحقيق الأمن والسلامة (الفصل الثاني).

الفصل الأول:

الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

لقد شهد العالم منذ مطلع القرن التاسع عشر موجة كبرى من التطور المتسارع في الميدان التكنولوجي والتقني ولاسيما ذاك التطور الذي شهدته تقنيات وتكنولوجيا المعلومات والاتصال التي أفرجت عن فضاء إلكتروني مترامي الأطراف ومتعدد الوظائف، وأصبح النقاش عن مفهومه وتحديد جوهره يتصدر أحدث الدراسات القانونية والسياسة نظرا لعمق جوهره وأصالة الميادين التي يبسط عليها أثره، وتعدد خصائصه وسماته، وأهمية خدماته التي يتم توظيفها وتسخيرها في مجالات متعددة حتى لا يكاد يخلو منها مجال.

فالفضاء الإلكتروني الذي تحول إلى عالم متكامل بالمعنى الواسع للكلمة حريٌّ بأن يشغل هذا الاهتمام في محاولة لفهمه وفهم ماهيته وهذا من خلال الإحاطة بمفهومه وبالدور الاستراتيجي الذي يلعبه من جهة، ومن خلال فهم عناصر البنية التكوينية الأساسية له من جهة أخرى (المبحث الأول).

ولعل الداعي الأكثر إلحاحا في إنشاء منظمة متكاملة من المعارف التي تهتم بدراسة الفضاء الإلكتروني وخاصة في الميادين السياسية والقانونية والأمنية هو الوقع الذي ترتب عنه، والذي يتمثل بصفة أساسية في التغيرات الكبرى التي طالت الكثير من المفاهيم الأساسية والاستراتيجية في العلوم السياسية والقانونية والأبحاث الأمنية المتقدمة، فقد استطاع الفضاء الإلكتروني إجراء تحويلات كبرى في مفهوم السيادة والعلاقات الدولية والدبلوماسية العامة، حيث تمكن من إحداث تغيرات حقيقية ومحسوسة في البنية التشكيلية للنظام الدولي الجديد وتبدلات كبيرة في مراكز القوى العالمية والأسس السياسية والقانونية والتنظيمية.

كما أن الطبيعة التي يتميز بها الفضاء الإلكتروني والتوظيف الدولي له في مجالات حيوية كالمجال العسكري والاقتصادي والسياسي والاجتماعي قد ترتب عنه تغيرات كبيرة في المفاهيم الأمنية من خلال نشوء أشكال وأنماط غير معهودة من التهديدات والتحديات الأمنية على الصعيدين الوطني والدولي وعلى المستوى الفردي والمؤسسي، الأمر الذي فرض مفهوم الأمن السيبراني كحقل جديد من حقول الدراسات والاستراتيجيات الأمنية، التي تتطلب توفير رؤية أمنية متكاملة على الفضاء السيبراني من خلال توفير جملة من المكونات التي من شأنها أن تشمل جميع الأبعاد الأمنية التي من المحتمل أن تطالها التهديدات الأمنية الجديدة (المبحث الثاني).

المبحث الأول:

ماهية الفضاء الإلكتروني

يعتبر الفضاء الإلكتروني شأنه شأن الكثير من الظواهر والمفاهيم السياسية والقانونية الحديثة التي لم يتوصل الفقهاء والدارسون إلى وضعها في إطار مفهومي موحد ومحدد نظرا لتباين الرؤى وتعدد الزوايا والإيديولوجيات التي تسطوا غالبا على الرؤية الموضوعية والدراسة التحليلية الأكاديمية، ولعل اتساع مجال استغلال الفضاء الإلكتروني والأهمية التي تكتسي أهدافه ووظائفه وكذلك تنوع سماته وتعدد خائصه جعله مفهوما قابلا لتحوير مضمونه بالشكل الذي يتناسب مع الغايات والأهداف، وخدمة للمنافع والمصالح الاستراتيجية المراد نيلها وتحقيقها (المطلب الأول).

كما تعود أيضا زبئية مفهوم الفضاء الإلكتروني إلى التشكيلية البنيوية الأساسية للفضاء الإلكتروني، إذ تعتبر بنية متنوعة ومتفرعة يختلط فيها الجانب المادي مع الجانب المعنوي، وتترابط فيه العناصر الإعلامية مع العناصر البشرية بروابط تقنية وشبكية عالمية النطاق، فهذا الترابط بين الكثير من الطبقات التكوينية القاعدية والعناصر الجوهرية الأساسية التي يقوم عليها الفضاء الإلكتروني ككيان افتراضي ذو انعكاسات كبرى على العالم الواقعي بشكل عظيم التعقيد وفي نفس الوقت بالغ التنظيم هو الذي يشكل عقبة أخرى في فهم ماهية الفضاء الإلكتروني (المطلب الثاني).

المطلب الأول:

مفهوم الفضاء الإلكتروني:

يعد مفهوم الفضاء الإلكتروني من بين المفاهيم التي ظهرت مع ظهور التقانة والثورة الرقمية التي يشهدها العصر الحديث، وليس من السهل الوصول إلى تعريف موحد لهذا الكيان المستجد نظرا لعوامل كثيرة تحتل المصالح والرؤى الاستراتيجية سدتها ومقدمتها (الفرع الأول)، ومع هذا تجدر الإشارة إلى أن الخصائص والسمات التي يتميز بها الفضاء الإلكتروني فريدة من نوعها ومتميزة في طبيعتها (الفرع الثاني)، وهذا ما يبرز الأهمية الكبيرة التي يحتلها الفضاء الإلكتروني في التسيير والإدارة الجيدة لقطاعات ومرافق حساسة بالإضافة إلى أهميته في إدارة شؤون مؤسسات القطاع الخاص وأهميته أيضا بالنسبة للأفراد، فالفضاء الإلكتروني على وجه العموم قد أصبح ضرورة عصرية لا يمكن الاستغناء عليها (الفرع الثالث).

الفرع الأول: تعريف الفضاء الإلكتروني:

يعد الفضاء الإلكتروني مفهوما حديثا نسبيا وقد تبلورت أهمية التوصل إلى تعريف له مع الإقبال المتزايد على الخدمات التي يقدمها، والاعتماد عليه في العمل المؤسسي والمرفقي، حتى أصبح هذا الفضاء من بين أهم المتطلبات التي تبني عليها قطاعات البنية التحتية في البلاد بما في ذلك القطاع العسكري حتى تم اعتباره إقليما جديدا للدولة (أولا) الأمر الذي أثار إشكالية الحدود التي تأطر هذا الإقليم وحدود سيادة الدولة فيه (ثانيا).

أولا/ تعريف الفضاء الإلكتروني:

لقد عرفت البشرية منذ بدايتها وإلى أوائل القرن المنصرم نوعين فقط من المجالات المادية التي تعمل في ساحتها، وهما الأرض والبحر، ثم حدث بعد ذلك تطور كبير عند إضافة المجال الثالث وهو المجال الجوي، حيث مكنت التكنولوجيا المتطورة من استغلاله، ثم ظهر بعد ذلك المجال الرابع وهو مجال الفضاء الخارجي، وهو مجال مسخر أيضا بفعل التطور التكنولوجي، وتتميز هذه المجالات الأربع بخصائص فيزيائية مختلفة جذريا ولا يمكن استخدام ولا استغلال هذه الخصائص إلا من خلال التكنولوجيا، وفي العصر الحديث ظهر مجال خامس، وهو المجال أو الفضاء الإلكتروني⁽¹⁾، الذي يعتبر من أهم المجالات في العصر الحاضر لما له من أدوار استراتيجية تنعكس بشكل مباشر على حياة الأفراد وتوازن القوى بين الدول.

1- تعريف القواميس للفضاء الإلكتروني:

يعرف القاموس الفرنسي لاروس الفضاء الإلكتروني على أنه فضاء افتراضي جمع بين ثنائيته متصفح الإنترنت (الذين يمثلون مجتمع المعلومات) وموارد المعلومات الرقمية التي يمكن الوصول إليها من خلال شبكات أجهزة الكمبيوتر⁽²⁾، وعرفه القاموس الإنجليزي أكسford أنه: (يعتبر الإنترنت مساحة وهمية دون وجود موقع فعلي لها يتم فيه الاتصال عبر شبكات الكمبيوتر)⁽³⁾.

وتذهب الموسوعة العربية في تعريف الفضاء السيبراني على أنه (الفضاء التخلي الذي خلقتة أنظمة الكمبيوتر وأحد تعريفاته هو امتداد ثلاثي الأبعاد ليس له حدود تتم فيه الأحداث وتتخالف فيه الكيانات وله موقع واتجاه نسبي وهو يأخذ شكل عوالم واقعية تخيلية أو قد يكون

⁽¹⁾ Daniel T. KUEHT, *From Cyberspace to Cynerpower : (Defining the Problem)*, cyber and national Security, first Edition, centre for technology and national security, national defense university press, fotomac books inc, washington, 2009, pp 24-42.

⁽²⁾ cyber monde, dictionnaire Larousse :

<https://www.larousse.fr/dictionnaires/francais/cybermonde/21258>

⁽³⁾ cyberspace, oxford dictionary :

<https://www.oxfordlearnersdictionaries.com/definition/english/cyberspace?q=cyberspace>

في منتهي البساطة هو البريد الإلكتروني، فمستخدميه يقولون بأن مجرد إمكانية التخاطب مع أفراد منتشرين في العالم أجمع يكسر الحدود الاجتماعية والحدود المكانية⁽¹⁾.

2- تعريف الدارسين للفضاء الإلكتروني:

لم يرد أي اتفاق أو إجماع فقهي حتى الآن بشأن قضية التعريف النظري للفضاء الإلكتروني، إذ لا تكاد تجد تعريفا واحدا يتفق مع آخر، فالدارسون قد أحصوا ما يعادل 28 تعريفا على الأقل لهذا الفضاء، وهذا ما يجعل من عملية اصطفاء تعريف شامل ودقيق أمر بالغ التعقيد والصعوبة، فهناك من الدارسين من يعرف الفضاء السيبرنيطيقي على أنه وسط افتراضية تولد بفعل استعمال أجهزة الكمبيوتر والاعتماد عليها كآلية للتواصل في ظل دائرة حقل شبكي عالمي الامتداد⁽²⁾.

كما يذهب آخرون في تعريفه على أنه مجال أو فضاء عالمي يتميز بالتفاعلية والحركية من جهة، وبالاستخدام المشترك للأجهزة الإلكترونية والأطراف الكهرومغناطيسية من جهة أخرى، الأمر الذي أتاح عملية كثيرة كإعداد وحفظ وتسوية واسترجاع المعلومات في ظل شبكة منظمة غاية في الرقي والازدهار، كما يرى البعض الآخر أنه مجال حاصل لما تمخض عن التطور التكنولوجي الكبير وعلى رأسها الطفرة العلمية الكبرى في مجال الشبكات الرقمية، كما يمكن اعتباره أيضا على أنه بيئة معاصرة ومستجدة الاتصال لما يحمله من خدمات مكنت المجتمع الإنساني من تبادل المعلومات وآلية من آليات توليد وتكوين المعلومات ونشرها، وتشبيد الروابط الاجتماعية وتوطيدها⁽³⁾.

وثمة زاوية أخرى عرفه من خلالها بعض الدارسين، وهي زاوية الاستغلال لمجال يتسم بالاستقلال الداخلي للأنظمة الشبكية التكوينية لبنيتها التحتية، إذ تم تعرفه على أنه: (التعامل مع العالم من خلال شبكة إلكترونية لها استقلاليتها من الداخل وتقوم بنيتها الأساسية على التقنيات الحديثة وهو أيضا أنظمة التعامل مع الحاسوب)⁽⁴⁾، كما ذهب دارسون آخرون إلى النظر إليه كنطاق مجازي تتلاقى في بنائه أنظمة الحاسوب والشبكات الإلكترونية وتعمل جميعها معا من أجل تحقيق أهداف تتمحور أساسا في حفظ المعلومات على تخزين المعلومات والتواصل بين الأفراد ومختلف الجهات بشكل فوري وسريع عن طريق استغلال نظم الشبكات⁽⁵⁾.

(1) سيد حسب الله، أحمد محمد الشامي، الموسوعة العربية، المجلد الأول، المكتبة الأكاديمية، مصر، 2001، ص 733.

(2) بلباسم أمين بن عمرة، دور الوسائط الاتصالية في تشكيل الفضاءات العمومية الهامشية النسائية داخل الحيز الافتراضي، أطروحة دكتوراه في الطور الثالث في علوم الإعلام والاتصال، كلية العلوم الاجتماعية، جامعة عبد الحميد بن باديس، السنة الجامعية 2017-2018، ص ص: 177-178.

(3) المرجع نفسه، ص 178.

(4) نجوى السوداء، بحث الفضاء السيبراني، 15 مايو 2015، تم الاطلاع عليه 12 فيفري 2020 على الساعة 12:42 سا، في الموقع:

<https://seconf.wordpress.com/2015/05/15/بحث-الفضاء-السيبراني/>

(5) المرجع نفسه.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وعرفته الموسوعة الحرة على أنه: (الوسط الذي تتواجد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني وبمفهوم أشمل يعرف بأنه مجال مركب مادي وغير مادي يشمل مجموعة من العناصر هي أجهزة الكمبيوتر، أنظمة الشبكات وبرمجيات حوسبة المعلومات، نقل وتخزين البيانات ومستخدومي كل هذه العناصر)⁽¹⁾.

كما عرفه فريدريك مايور بأنه: (بيئة إنسانية وتكنولوجية جديدة للتعبير والعلوم والتبادل وهو يكون أساسا من الأشخاص الذين ينتمون لكل الأقطار والثقافات واللغات والأعمار والمهن المترابطة بعضها ببعض عن طريق البنية التحتية الاتصالية التي تسمح بتبادل المعلومات ونقلها بطريقة رقمية)⁽²⁾.

وتم تعريف الفضاء السيبراني أيضا على أنه: (مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الإنترنت وكم هائل من البيانات والمعلومات والأجهزة) وعرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) بأنه: (فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية) وتم تعريفه أيضا بأنه: (بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين)⁽³⁾.

وقد لاحظنا في هذه التعاريف المعروضة وغيرها مما لم نورد في بحثنا، تصورا للفضاء الإلكتروني على أنه مجال أو فضاء افتراضي، فكثيرا ما يعبر عنه بمصطلح "الفضاء الافتراضي"، غير أن الدكتور عادل عبد الصادق قد أشار إلى جزئية مهمة حول هذا المصطلح، إذ أن التعبير عن الفضاء الإلكتروني بالفضاء الافتراضي يوحي إلى أن الفضاء الإلكتروني احتمالي الوجود، في حين أن الفضاء الإلكتروني هو واقع ملموس وليس افتراض، ولذلك يحبذا الدكتور استعمال الفضاء الإلكتروني أو الرقمي⁽⁴⁾، ونوافقه هذا على هذا الطرح.

(1) ويكيبيديا: فضاء إلكتروني، الموسوعة الحرة: https://ar.m.wikipedia.org/wiki/فضاء_إلكتروني

(2) وداد سميحي، الحوار الإلكتروني والفضاء العام الافتراضي: (منتديات النقاش الإلكتروني نموذجاً)، مجلة العلوم الإنسانية، العدد 2 المجلد 25، جامعة منتوري، قسنطينة، جوان 2014، ص ص 563-578:

<https://www.asjp.cerist.dz/en/article/90088>

(3) إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، جامعة الشهيد حمزة لخضر، الوادي، الجزائر، أفريل 2019، ص ص 1016-1031: <https://www.asjp.cerist.dz/en/article/91423>

(4) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسلة أوراق، العدد 23، وحدة الدراسات المستقبلية، مكتبة الإسكندرية، الإسكندرية، مصر، 2016، هامش الصفحة 21.

و قد يتكرر منا أيضا استعمال الفضاء السيبراني بدلا من الفضاء الإلكتروني، كما سيتكرر منا أيضا التناوب في استعمال مصطلحات مثل الأمن السيبراني والإرهاب السيبراني للدلالة على الأمن والإرهاب الإلكترونيين، وسيكون ذلك على سبيل المرافقة، وذلك توفيقا منا بين الفكر الغربي الذي يسود فيه استعمال مصطلح السايبر، والفكر العربي الذي يغلب فيه استعمال مصطلح إلكتروني أو رقمي.

3- تعريف المؤسسات الحكومية للفضاء الإلكتروني:

تعود أول محاولة لتعريف الفضاء الإلكتروني لسنة 2000 حيث تم تعريفه فيها على أنه (البيئة الافتراضية التي يتم فيها نقل المعلومات الرقمية)، لكن هذا التعريف صادف رفضا من الكافة وذلك لاعتباره تعريفا غير كافٍ لبلورة المفهوم الحقيقي للفضاء الإلكتروني وجوهره، لكن في عام 2006 تم تقديم النواة الأولى لتعريف أكثر دقة ووضوحا حين طرحت فكرة من زاوية ومنظور مهم وهذا من خلال الاستراتيجية الوطنية لتأمين الفضاء الإلكتروني التابعة للولايات المتحدة الأمريكية حيث قامت بمحاولة لتعريف الفضاء الإلكتروني على أنها: (الجهاز العصبي، وهو نظام التحكم في البلاد، ويتكون من مئات الآلاف من أجهزة الكمبيوتر المرتبطة والخوادم وأجهزة التحويلية والمحولات والألياف البصرية)⁽¹⁾.

وبعد ذلك، عرفة هيئة الأركان في 2006 بأنه: (مجال يتميز باستخدام الإلكترونيات والطيف المغناطيسي لتخزين وتعديل وتبادل المعلومات عبر شبكات نظم المعلومات والبنية التحتية المادية)⁽²⁾.

ويعرفه البيت الأبيض على أنه: (شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات وتشمل الإنترنت وشبكات الاتصال السلكية واللاسلكية وأنظمة الكمبيوتر والمعالجات المدمجة والضوابط في الصناعات الحرجة)، ثم عرفت وزارة الدفاع الأميركي أنه: (مجال عالمي داخل بيئة المعلومات التي تتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات بما في ذلك الإنترنت، شبكات الاتصالات وأنظمة الكمبيوتر والمعالجات المدمجة ووحدات التحكم)⁽³⁾.

تنظر كندا إلى الفضاء السيبراني من بعد إنساني ومنظور مصلي ومنفعي بحث، وهذا واضح من خلال التعريف المعتمد لهذا الفضاء والذي يقضي بأن: (الفضاء السيبراني هو العالم

⁽¹⁾ Daniel T. KUEHT, Op.Cit.

⁽²⁾ ibid.

⁽³⁾ ibid.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

الإلكتروني الذي تم إنشاؤه بواسطة شبكات مترابطة من أنظمة تكنولوجيا المعلومات والمعلومات الموجودة على شبكاتها، ويعد الفضاء الإلكتروني منفعة عامة تربط أكثر من 1.7 مليار شخص يتبادلون الأفكار والخدمات ويقيمون الصداقات⁽¹⁾، فالفضاء الإلكتروني من المنظور الكندي هو ساحة دولية مشاعة جدير بها أن تكون وسطا للنمو الإنساني عبر تبادل الأفكار والخدمات، وبناء جسور المودة والصداقة بين كافة أبناء البشرية بتعدد أعراقهم وثقافتهم.

ومع هذا فإن كندا لم تغفل البعد العسكري للفضاء الإلكتروني رغم أن قواتها العسكرية لا تزال إلى حد الآن تسير على النمط التقليدي الذي لا ينظر إلى المجالات العسكرية إلا وفق النظرة التقليدية، ويظهر البعد العسكري للفضاء الإلكتروني في المنظور الكندي من خلال اعتماد قواتها على الفضاء الإلكتروني، فالقوات العسكرية الكندية لا تنزل إلى الساحة إلا وهي مجهزة بأحد التقنيات المعلوماتية والاتصالية⁽²⁾.

وبدل أيضا على أن كندا لم تغفل البعد العسكري للفضاء الإلكتروني ذاك التفويض الذي منحه الاستراتيجية الوطنية للأمني السيبراني الكندية للأجهزة العسكرية أو القطاع العسكري والذي يتضمن موضوع حماية شبكاتها الإلكترونية، ومع أن هذا التفويض لم يتحدث عن أي موقف هجومي على الفضاء الإلكتروني، إلا أن هناك من المنشورات التي صدرت من كلا المؤسساتين تأكد أن هناك فعلا عمليات عسكرية على الفضاء الإلكتروني⁽³⁾.

إن تعريفات متعددة ومتفرعة والمتباينة للفضاء السيبراني تسمح لنا بأن نؤكد على أن الوصول إلى تعريف شامل ودقيق تعتبر من القضايا الشائكة والعصية، وتمتاز بنوع من العسر والصعوبة، لأنها بكل بساطة قضية على قدر كبير من النسبية، فهي مقيدة ومرتبطة ارتباطا شديدا ببعض الحثثيات والمفاهيم المعقدة من جهة، وبالأهداف والاستراتيجيات والرؤى من جهة أخرى، فتأثير الدولة، والرؤية الاستراتيجية لها، وأبعاد تمكنها من على تقييم كفاءتها وإمكانياتها في التوظيف الأمثل لهذا الفضاء مع قدرتها على انتقاء مخاطره ومواجهتها، يؤثر بشكل مباشر على العناصر الجوهرية التي سيتضمنها التعريف الذين يطرح لهذا الفضاء⁽⁴⁾.

⁽¹⁾ gouvernement de canada, Stratégie de cybersécurité du Canada:(renforcer le canada et accroître sa prospérité), canada, 2010, P.02.

⁽²⁾ LCol J.M.F. Robichaud, le cyberspace et les forces armées canadiennes, collègues des forces canadiennes, défense nationale, canada, 2016, P.03.

⁽³⁾ LCol J.M.F. Robichaud, Op.cit. P.07.

⁽⁴⁾ ربيع محمد يحيى، إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط، مجلة رؤية استراتيجية، المجلد الأول، العدد 03، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبوظبي، الإمارات العربية المتحدة، يونيو 2013، ص ص: 65-89.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

فعدم وجود استراتيجية مشتركة ورؤى دولية متطابقة يؤدي إلى تعدد التعاريف وتأثرها بالرؤى والمصالح، فالصين مثلا يمكن أن نقول أنها على خلاف ما تقدم، نادرا ما تستعمل مصطلح الفضاء السيبراني، خاصة في الخطابات الرسمية إذ تفضل الحديث عن الإنترنت أو تأمين المعلومات⁽¹⁾، وهي في حقيقتها ترى من الفضاء الإلكتروني ساحة من ساحات الصراع بدليل ما سيتقدم في بحثنا من أشكال الهجمات التي تنفذها الصين ضد العديد من الدول، وهي تحاول بإصرار شديد أن تثبت للعالم بأنها تحتل مكانة في الفضاء الإلكتروني⁽²⁾.

والتعريف الذي نراه موفقا في تعريف الفضاء الإلكتروني هو: (التعامل مع العالم من خلال شبكة إلكترونية لها استقلاليتها من الداخل وتقوم بنيتها الأساسية على التقنيات الحديثة وهو أيضا أنظمة التعامل مع الحاسوب)⁽³⁾، لان هذا التعريف يطرح لنا فكرة الفضاء الإلكتروني ككيان يتمتع بالاستقلالية، ويجلي لنا طبيعته البنيوية، وأهم من ذلك كله، يطرح الفضاء الإلكتروني ككيان واقعي له وكمجال خامس يتم التعامل من خلاله مع العالم.

ثانيا: حدود الفضاء الإلكتروني:

اعتبارا لما سبق من التعريفات والرؤى المختلفة للفضاء الإلكتروني يمكن القول أن الكثير من الدول تعتبر الفضاء السيبراني كمجال خامس للحروب، ومنها من يرى أنه على الدول القيام برسم حدوده لإخضاع هذا الفضاء لسيادة القانون. ولكن مثل هذا الطرح وهذه الوجهة في النظر إلى مفهوم الفضاء الإلكتروني تثير إشكاليتين، أولهما تتعلق باعتبار الفضاء الإلكتروني إقليم، وثانيهما في حدوده السيادية⁽⁴⁾.

قبل أن نحاول الإجابة على هذه الإشكاليات يجب أن نفهم جيدا أن مسألة عرض الفضاء الإلكتروني كإقليم أو كمجال خامس كان حديث المنشأ من الناحية التاريخية، حيث أن الفكرة قد ظهرت وتطورت على أيدي رواد الإنترنت في أعقاب عام 1990، وكان الفكرة قائمة على وجود إقليم مستقل غير خاضع لأي شكل من أشكال السلطان ولاسيما سلطان الحكومات والدول، ومحاولة الدفاع على بقاء هذه الاستقلالية على حالها، والمناداة بوجوب التزام الدول عدم التدخل

⁽¹⁾ Frederick DOUZET, *la géopolitique pour compadre le cyberspace*, La Découverte « Hérodote », 1 n° 152-153, 2eme trimestre, 2014, pp 3-21: <https://www.cairn.info/revue-herodote-2014-1-page-3.htm>

⁽²⁾ Frédéric DOUZET, *Géopolitique du cyberspace* : (La cyberstratégie de l'administration Obama Geopolitics of cyberspace: the Obama administration's cyberstrategy), Bulletin de l'association de géographes français, 91-2 | 2014, PP. 138-149: <https://journals.openedition.org/bagf/1837>

⁽³⁾ نجوى السودة، المرجع السابق.

⁽⁴⁾ Frédéric DOUZET, *la géopolitique pour compadre le cyberspace*, Op.cit.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

في تنظيم هذا الفضاء وقد صرح أبرز روادها بهذه الاستقلالية حيث أكد أن الدول لا تملك أي سيادة على مستوى الفضاء الإلكتروني⁽¹⁾.

فقبل ذلك لم يكن الفضاء السيبراني يحمل هذا المعنى، إذ كان منشأ استعمال مصطلح سايبير نفسه يعود في أصوله إلى الخيال العلمي، حيث تم استعماله في رواية (cyberpunk) لصاحبها وليام جيبسون (William Gibson)⁽²⁾، ومن المعروف عن جيبسون جنوحه في غالبية قصصه إلى التصورات المستقبلية المتأثرة بتكنولوجيا الفضاء السيبراني⁽³⁾، ويعرف جيبسون الفضاء السيبراني على أنه: (عبارة عن شبكات الكمبيوتر خيالية تحتوى على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة)⁽⁴⁾ وتم طرحها بعد ذلك من قبل المتخصص في مجال الاتصالات الإلكترونية والعلوم المتعلقة بالسيطرة نوربرت وينز (Norbert Wiener)⁽⁵⁾، وكان أول استخدام له للتعبير عن الإنترنت⁽⁶⁾.

ثم بعد ذلك عان هذا المصطلح من الهجران وقلة الاستعمال ولاسيما في الدوائر الحكومية وعلى هذا فإنه لم ينل قسطا من الدراسات الأكاديمية والعلمية، وبقي على هذا الحال إلى غاية احتدام الصراع السيبراني وتكاثر الهجمات الإلكترونية، وحينها عاد الفكرة مرة أخرى إلى الساحة في عام 2000 كما سبق وأن أشرنا، لكن هذه المرة بطريقة جديدة وبثوب آخر، إذ تم العمل على تحويل مفهومه وتغيره بحيث أصبح مناقضا تماما للأطروحات السابقة التي أشرنا إليها، فقد سعت الدول التي تعاني من تلك الهجمات السيبرانية والتي تخشى من إطابة ملكها وسلطتها إلى إعادة طرح موضوع الفضاء السيبراني من وجهة نظر تمكنهم من شرعة الإجراءات التي تمكنهم من فرض سيادتهم وهيمنتهم على الفضاء الإلكتروني محاولين رسم حدود له خلافا لما كان يسير عليه

(¹) Frederick DOUZET, Alix DESFORGES, Kevin LIMONIER, *Géopolitique du cyberspace : ("territoire", frontières et confits)*, Fronts et frontières des sciences du territoire, Paris, France, Mar 2014, pp.173-178 <https://hal.archives-ouvertes.fr/hal-01353455>

(²) محمد الجندي، متاهة الإرهاب: (الشرق الأوسط من الخلافة إلى الإرهاب في الفضاء الإلكتروني)، الطبعة الأولى، مجموعة النيل العربية، القاهرة، 2020، ص 70.

(³) كيث بوكرو وأن ماري توماس، المرجع في روايات الخيال العلمي، ترجمة (عاطف يوسف محمود)، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2010، ص 279.

(⁴) مولود بلقاسمي وإبراهيم حادي، تحولات مفهوم القوة في الفضاء الإلكتروني: (مقاربة سياسية)، مجلة القانون والعلوم السياسية، المجلد 02، العدد 01، معهد الحقوق والعلوم السياسية، المركز الجامعي صالح أحمد نعام، الجزائر، جانفي 2016، ص ص: 525-539: <https://www.asjp.cerist.dz/en/article/86822>

(⁵) محمد طرابلسية، أيديولوجية الفضاء الرقمي: (دراسة في الخلفيات المرجعية)، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 11، العدد 01، جامعة حسينية بن بوعلي، شلف، الجزائر، جانفي 2019، ص ص: 47-58: <https://www.asjp.cerist.dz/en/article/74664>

(⁶) مولود بلقاسمي وإبراهيم حادي، المرجع نفسه.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

رواد الإنترنت وما يتصورنه عليه، إذ تم تمثله وتشكله بالقدر الكافي ليكون إقليما أو أرضا يمكن العمل على إخضاعها للرقابة بسط السيطرة وحتى ممارسة أنواع الغزو المختلفة عليها، وهذا كله من أجل رسم نطاق محدد المعالم من أجل تطبيق قوانينهم الدفاع عن مبادئهم، فبغرضي الأمن والدفاع أخذت الدول تعمل على البحث عن طريقة تحديد المساحة الوطنية للفضاء الإلكتروني⁽¹⁾.

ويطرح دانيال لامباش الفضاء السيبراني من وجهة نظر الخواص الكلاسيكية لمفهوم الإقليم، فالفضاء السيبراني هو ثلة كبيرة من الإقليم التي ليس لها حدود معينة بفعل تمازجها واشتباكها ببعضها البعض والتي يتم النقاش والتداول حول مسألة ترسيم حدودها والتصريح عنها⁽²⁾.

وتجدر الإشارة هاهنا أن هناك الكثير من الدول التي لا تستخدم هذا المصطلح كثيرا وهذا نظرا لاعتبارات ثقافية وهوياتية كثيرة، وعلى أي فإن هذه الأطروحة التي تجعل من الفضاء الإلكتروني كإقليم يقوم على مفهومين أساسيين متناقضين بشكل شديد، المفهوم الأول يرى أن الفضاء الإلكتروني يجب أن يبقى كنطاق مستقل غير محدد بحدود سيادية ويجب أن يضل فضاء حر دون أن تفرض عليه الرقابة ومن جهة أخرى نرى مفهوما آخر مناقضا له وهو التي تري فيه الدول بأن الفضاء الإلكتروني هو إقليم أو قطر يمكن غزوه وفرض الرقابة عليه كما يجب أن يكون خاضعا لمبدأ السيادة وعلى هذا إن الفضاء الإلكتروني قد تحول ليكون هدفا للتنافس السلطوي بين الجهات الفاعلة من أجل بسط سيطرتها وهيمنتها والعمل على تنظيم نشاطاته⁽³⁾.

ومع هذا فإنه من غير الممكن أن نفهم الفضاء الإلكتروني كإقليم مرسوم الحدود بعيدا أن الإطار النظري أو الإطار المفهومي الجيوسياسي، فرغم إن هناك اعتبارات تدعو إلى النظر إلى الفضاء الإلكتروني كفكرة تترتب عنها تحديات كثيرة بالنسبة للدول وبالنسبة للباحثين على حد سواء إلا أنه من غير الممكن أن نعتبره نطاقا جغرافيا أو عالما منفصلا، ففي نهاية المطاف وجوده كان بفعل العامل البشري وعلى هذا فإن كل الصراعات والأزمات المتعلقة به لا يمكن النظر إليها إلا في سياق جيوسياسي بحث⁽⁴⁾.

⁽¹⁾ Frederick DOUZET, Alix DESFORGES, Kevin LIMONIER, Op.cit.

⁽²⁾ نقلا عن: هدير أبو زيد، السيادة الإلكترونية: (اتجاهات تشكيل مناطق سيبرانية تحت سيطرة الدول والشركات)، مركز المستقبل للأبحاث والدراسات المتقدمة، 23 سبتمبر 2020، تم الاطلاع عليه بتاريخ 12 فيفري 2021، على الساعة 22:57، مختصر الرابط:

<https://cutt.us/qC4B4>

⁽³⁾ Frederick DOUZET, Alix DESFORGES, Kevin LIMONIER, Op.cit.

⁽⁴⁾ Ibid.

الفرع الثاني: خصائص الفضاء الإلكتروني:

لقد عمل الفضاء الإلكتروني على توفير خدمات كبرى من شأنها أن تحدث تغيرات جوهرية في نمط حياة البشرية سواء على مستوى الأفراد والمؤسسات، فخصائصه الخدماتية قد منحت جانبا كبيرا من السهولة واليسر للكثير من جوانب حياة الأفراد (أولا) كما أن للفضاء الإلكتروني ميزات وخصائص تنظيمية ميزته عن الكثير من الأدوار التي كانت تلعبها آليات تقليدية وغيرت من نطاقها ونظامها ونمط استغلالها (ثانيا).

أولا: خصائص خدمات الفضاء الإلكتروني:

1/ التفاعلية:

على خلاف وسائل الاتصال التقليدية، يعتبر الفضاء الإلكتروني ساحة تأخذ المعلومات في حركتها فيها مسلكين اثنين بدلا من المسلك الأحادي الذي تكون فيه جهة من الجهات مصدرا لتكوين وصياغة المعلومات وجهة ثانية تتلقاها دون أن يكون لها أي دور ولا إسهام فيها، فالساحة الإلكترونية إذا هي ساحة تفاعلية فتحت مجالا واسعا لتبادل الأدوار⁽¹⁾، بحيث تمكن المشاركين في هذا المسار أو هذه العملية في كل مراحلها من التأثير في أدوار الآخرين والقدرة على تبادلها من خلال سلسلة من النشاطات الديناميكية للمسار الاتصالي والتي من خلالها يمكن لأي فرد أو أي جهة أن تكون مرسله ومستقبله في آن واحد مشكلة بذلك كله بيئة تعاضدية تتشارك فيها الجهود وتتحول فيها الوظائف والمهام⁽²⁾.

فالتفاعلية إذا هي: (الدرجة التي تستطيع تكنولوجيا الاتصال بواسطتها خلق بيئة للمشاركين التواصل من خلالها سواء بشكل متزامن أو غير متزامن وتبادل الرسائل من أجل إدراك الخبرة ومحاكاة الاتصال بين الأشخاص وزيادة وعيهم رغم الحضور عن بعد)⁽³⁾.

إن خاصية التفاعلية التي يتمتع بها الفضاء الإلكتروني تتعكس بصفة مباشرة على أنماط وأساليب ممارسة الوظائف والأعمال المختلفة، كما له أثر كبير ومباشر على الروابط المختلفة

⁽¹⁾ مشري محمد الناصر، سبل تفعيل دور تكنولوجيا المعلومات والاتصال في دعم التنمية المستدامة في المؤسسات الصناعية الجزائرية: (دراسة عدد من المؤسسات في الشرق الجزائري)، رسالة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والعلوم الاجتماعية وعلم التسيير، جامعة فرحات عباس، سطيف 01، الجزائر، السنة الجامعية 2016-2017، ص 30.

⁽²⁾ فضيلة تومي، تكنولوجيا الاتصال: (التفاعلية وعلاقتها بالبحث العلمي في الجامعة الجزائرية)، مجلة الباحث في العلوم الإنسانية والاجتماعية، ورقلة، عدد خاص، المجلد 03، العدد 6، جامعة قسدي مبراح، مارس 2011، ص ص: 486-521.

<https://www.asjp.cerist.dz/en/article/19268>

⁽³⁾ حسن فراج حسن، تكنولوجيا الإقناع في تصميم مواقع الصحف الإلكترونية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر، ص 154.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

ضمن إطار منظمة العمل، حيث تقلص تركز عملية اتخاذ القرارات في جهة واحدة، فأصبح مبدأ المشاركة هو الذي حل محله في سير عملية اتخاذ القرارات، وأصبح تضافر الجهود داخل المنظومة هو المظهر الداخلي السائد⁽¹⁾.

ليس هذا فحسب، بل إن التفاعلية التي تتميز بها خدمات الفضاء الإلكتروني قد عملت أيضا على إزاحة الدولة كفاعل وحيد -باعتبار دورها التقليدي- في إصدار المعلومات ومختلف الأنباء، مفسحة المجال بذلك للأفراد لانتقاء معلوماته بناء على توجهاتهم المختلفة وبما يسمح لهم به وعيه، وبما تتيحهم لهم طاقاتهم وإمكاناتهم الاستيعابية، متحملين بذلك كله أعباءها بشكل مطلق⁽²⁾، فالدولة لم يعد لها مع هذا الفضاء الرحب، أي وصاية على انتقاء الأفراد لمعلوماتهم، ولا أي دخل في أنواقهم واختياراتهم، فضلا عن عدكم إمكانية الدولة في حصر مصادر ذلك فيها، فالفضاء الإلكتروني قد فتح أفقا يكون فيه وعي الفرد وحده هو الوصي على انتقاء المعلومات.

ومع أن خاصية التفاعلية قد نتج عنها انكماش دور الدولة في وصايتها على مصادر المعلومات، إلا أنها في المقابل قد أتاحت لنوع من التقارب بين الأفراد والدولة، وذلك من خلال ما يعرف بالديمقراطية الرقمية، التي يرى أنصارها ومؤيدوها بأن الهام المنشأ لها وهو الفضاء الإلكتروني يعبر عن أهمية بالغة في تكريس المشاركة السياسية، وتوطيد العلاقة الاتصالية بين الأفراد والدولة بما يسمح لهذه الأخيرة من تحقيق مطالب الأفراد، فالتفاعلات على هذا الفضاء ذات دور محوري في تنامي ووفرة المصالح المرفقية التي تمنح للأفراد إمكانية الاطلاع على المعلومات بما يضمن الشفافية والتفاعل في اتصال الدولة بمواطنيها⁽³⁾.

على أن التفاعلية التي يمتاز بها الفضاء الإلكتروني قد انجرت عنها الكثير من الآثار الأخرى، وبشكل خاص تلك الآثار ذات الصلة بعلاقة الفرد بينه وبين وسطه وبيئته من جهة، وبينه وبين الدولة من جهة أخرى، فالعمليات التفاعلية على الفضاء السيبراني أحدثت في الأفراد نوعا من التفوق على الذات وحصر التفاعل الإتصالي في البيئة الإلكترونية وتجاهل الروابط الاجتماعية الفعلية، فالتورط والسقوط في هذا التجاهل ضمن وسط لا يسرى عليه قيد ولا هيمنة فيه

(1) مشري محمد الناصر، المرجع السابق، ص 30 .

(2) حرية بولعويات، استخدام تكنولوجيا الاتصال في المؤسسات الاقتصادية الجزائرية: (دراسة ميدانية بمؤسسة سونلغاز فرع تسبير شبكة نقل الغاز بالشرق "GRTG" قسنطينة)، مذكرة ماجستير في الاتصال والعلاقات العامة، كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة منتوري، قسنطينة، السنة الجامعية 2007-2008، ص 82.

(3) برامود كيه نابار، مقدمة إلى وسائل الإعلام الجديدة والثقافات الإلكترونية، ترجمة (جلال الدين عز الدين علي)، مؤسسة هنداي سي آي سي، المملكة المتحدة، 2017، ص 25.

على مسارات الحوار قد أفضي أيضا إلى فصل الفرد عن السلطة وضوابطها، الأمر الذي أنتج فكرا متحررا وملتزمدا سواء أكان التمرد في ذلك على السلطة السياسية أو على السلطة الاجتماعية⁽¹⁾.

2/ اللاماهرية:

لقد أصبحت أطروحة بعض المفكرين الذين يرون مع بداية التطور التكنولوجي الموهول أن العالم يتحول مع الزمن إلى قرية صغيرة بفضل نهضة وسائل الاتصال الجماهيرية، غير أن هذه الأطروحة تحتاج لأن تكون محل فحص ومعاينة، وإعادة التفكير في الرؤية التي تقدمها على الدور الذي يلعبه الفضاء الإلكتروني في البنية العامة للمجتمع، وهذا الأمر يعود بشكل خاص إلى التحولات الاستراتيجية التي استجبت وطرأت على الفضاء الإلكتروني من أواخر التسعينات إلى يومنا هذا، بحيث أصبحت الرسالة على الفضاء الإلكتروني غير موجهة إلى الجمهور كما كان الأمر عليه في الماضي، فقد تحول الميل إلى تحديد الرسائل وتصنيفها لتكون على شكل يتأقلم ويتلاءم مع نوعية معينة من الجماهير، فيتم استهدافهم أفرادا وجماعات من خلال رسائل مصاغة بشكل انفرادي وخاص⁽²⁾.

ولا تقتصر اللاماهرية على إمكانية التحكم في الرسائل الاتصالية فحسب، بل تتخطى ذلك إلى القدرة الكاملة على تسخير هذا النظام الاتصالي بشكل يكون الفرد محوراً الأساسي، بمعنى أن العملية الاتصالية ضمن الفضاء الإلكتروني يمكن أن تتخذ شكلا خصوصيا، فتكون العمليات الاتصالية وما إلى ذلك بصفة مباشرة، فترسل الرسائل بشكل مباشر من مصدر توليدها إلى المستخدم الذي ينتفع بها دون غيره من الأفراد⁽³⁾، فاللاجوهريّة هي خاصية تحمل في معناها مدلول انفرادية التعامل، وتظفي على العمليات على الفضاء الإلكتروني طابعا شخصيا، فيكون التعامل الاتصالي بين الصانع والمستهلك.

(1) فريدة صغير عباس ورضوان رياح، التفاعل الافتراضي نحو مقاربة المفهوم في ظل المجتمعات الافتراضية، مجلة الصورة والاتصال، المجلد 07، العدد 02، جامعة وهران السانانية، وهران، الجزائر، ديسمبر 2018، ص ص 119-127:

<https://www.asjp.cerist.dz/en/article/75913>

(2) جميلة سالم عطية، الثورة المعلوماتية وإشكالية بناء وتداول الخطاب اللغوي البصر: (دراسة تحليلية سيميولوجية على عينة من الخطابات اللغوية والبصرية في مواقع شبكات التواصل الاجتماعي - الفيسبوك نموذجا-)، مذكرة ماجستير في علوم الإعلام والاتصال، كلية الإعلام والاتصال، جامعة الجزائر، 2013-2014، ص 62.

(3) مشري محمد الناصر، المرجع السابق، ص 30.

3/ السرعة وضمان انتشار المعلومات:

لقد مرت المراسلات بعدد كبير من التحولات المختلفة، وأهم ميزة تتغير في كل مرحلة من مراحل هذا التحول تتمثل في الوقت الذي تستغرقه هذه المراسلات بين أطرافها، فبعد أن كانت تقدر بالأيام أصبحت تقدر بالدقائق واللحظات، ومع ذلك فإن لكل تطور عيوبه الخاصة، لكن مع ظهور الكمبيوتر والنظام الشبكي الذين كونوا فضاء إلكتروني كونيا أصبحت المعلومات تنتشر دون عناء وبسرعة خارقة، فلا يتطلب إرسالها إلا ثواني قليلة جدا لتصل إلى المرسل إليه، سواء أكان شخصا مفردا أو جماعة من الأفراد، كما أن أي وثيقة يمكن حفظها بصيغتها الرقمية ويمكن إرسالها في أقصر الأوقات عبر فضاء فسيح، كما يمكن استقبال مثله على جهازك الذي تدخل من خلاله هذا الفضاء الإلكتروني⁽¹⁾.

4/ الفورية:

تمكن الفضاء الإلكتروني من تسخير آليته بما يزيح به أي حاجز زمني ومكاني، فلا عبء بالزمان والمكان في العملية الاتصالية التي تقع بشكل آني على الفضاء الإلكتروني، ولا عبء أيضا بزمان ذلك ولا بمكانه، فأطراف العلاقة التواصلية يتعاملون فيما بينهم بحركات بسيطة على أجهزة الحاسب أو الهاتف، ونفس هذه الحركات تحيطك علما بكل ما ترجو معرفته أو الاطلاع عليه مختزلة لك الزمان والمكان، اللذين نسخا أمام ما يتيح هذا الفضاء الذي لا يتوقف لا بليل ولا بنهار، ولا يعرف عطلة على مدار العام⁽²⁾.

ولا يتوقف التحرر من قيود الزمان عند هذه النقطة، بل إن الفضاء الإلكتروني يفتح مجالا لتلقي البعثات والرسائل في الوقت الذي يكون فيه الشخص جاهزا لاستقبالها، فلا يشترط في خدمات الفضاء الإلكتروني أن يكون المستخدمين الذين يتبادلون مختلف الرسائل والبعثات متواجدين في نفس اللحظة على الفضاء الإلكتروني، فخدمات هذا الفضاء توفر عبر آلياتها ونظمها للأفراد آليات يمكن من خلالها أن يسلموا ما بدى لهم من رسائل وملفات وأن يستلمها أيضا

(¹) محمد بري، وسائل الاتصال الحديثة وأثرها على التغير الاجتماعي في المجتمع الجزائري: (دراسة ميدانية على أساتذة التعليم الثانوي بئر العاتر (ولاية تبسة)، مذكرة ماجستير في علم اجتماع الاتصال والعلاقات العامة، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خضير، السنة الجامعية 2011-2012، ص ص: 79-80.

(²) علي بن عبد الله عسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص ص: 23-24.

دون أن يكون للوقت أي معنى في ذلك، فيمكن لأي مستخدم أن يقوم بهذه الأعمال في الوقت الذي يراه ملائما لذلك⁽¹⁾.

ثانيا: الخصائص التنظيمية للفضاء الإلكتروني:

1- العالمية:

يعتبر الفضاء الإلكتروني فضاءً عالمياً وكونياً، إذ أنه فضاء لا يعرف الحدود ولا يجد المبحر فيه أي حاجر، لقد أتاح هذا الفضاء للأفراد إمكانية الوصول إلى أي بقعة من بقع هذا العالم دون أن يكابد نفسه وعناء السفر، ودون أن تغبّر رجليه من الترحال، فحركات بسيطة على جهاز الحاسب أو الهاتف المحمول تحمله من قارة لأخرى وهو قابع في مكانه لا يتحرك، مغنية له عن تقديم وثائق السفر وإجراءات الجمارك، كما تمنح له فرصة الحصول على كل ما يريد من معلومات واستئصالها على جهازه، الأمر الذي أثر سلباً على الرقابة الأمنية، حيث جعلت من عملها أكثر عسراً وتعقيداً، وأصبح هذا الفضاء في الوقت ذاته آلية من آليات العولمة في العصر الحديث⁽²⁾.

ولذلك وصف البعض هذا الفضاء الإلكتروني بأنه "عالم متكامل"، أو "قرية كونية" تقطنها مجموعات بشرية مهولة، تعيش حياتها فيها متحدة زمانياً، -رغم انقطاعها مكانياً-، ويقضون أوقاتهم فيها بممارسة شتى النشاطات، وعدداً من الفعاليات، وصوراً متعددة من التصرفات، ويعملون فيها على تبادل مختلف الخدمات والمصالح⁽³⁾.

لقد تحول الفضاء الإلكتروني إلى عالم مترابط تنتقل فيه المعلومات بكل حرية، إذ لم تعد الآراء والمعلومات حبيسة الحدود دخولاً أو خروجاً، وليس لأياً كان إمكانية الانزواء أو النأي بنفسه عن بقية العالم في ظل هذا الفضاء متصل الأركان⁽⁴⁾.

فالفضاء الإلكتروني لا يعترف بالحدود، ولا يمكن تحديد مواقع سكانه أو قاطنيه، وقد قررت إحدى المحاكم أن الإنترنت: (لا يميز بين الحدود الجغرافية وفي جميع الحالات تقريباً لا يعرف مستخدمو الأنترنت أو يعبئون بالموقع الحقيقي للمصادر المتوافرة على الشبكة التي يطلعون

(1) مشري محمد الناصر، المرجع السابق، ص 31.

(2) علي بن عبد الله عسيري، المرجع السابق، ص 23.

(3) بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة دكتوراه في العلوم القانونية، كلية العلوم الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2014-2015، ص 9.

(4) صالح ليبيد، إشكالية سيادة الدولة في ظل العولمة، رسالة ماجستير في العلوم السياسية، كلية العلوم السياسية والإعلام، جامعة بن يوسف بن خدة، الجزائر، 2008-2009، ص 99.

عليها، لقد وصعت بروتوكولات الإنترنت بحيث تتجاهل لا أن تحدد المواقع الجغرافي، فبينما يكون هناك عناوين لأجهزة الكمبيوتر المتصلة بالشبكة فهي عناوين منطقية على الشبكة أكثر منها عناوين حقيقية في الفضاء الواقعي حيث لا يوجد في أغلب الأحيان أي علامة تشير إلى الموقع الجغرافي وحتى وإن وجدت يمكن أن تكون مضللة⁽¹⁾.

2- ديناميكية الفضاء الإلكتروني:

يعد الفضاء الإلكتروني وسطا ديناميكيا ونشطا، فهو وسط يكون فيه التغير والتبدل المستمرين والثابتين سمة بارزة فيه، والمتأمل في الإحصائيات المتعلقة بما يستحدث على الفضاء الإلكتروني من المواقع المختلفة والصفحات الإلكترونية المتنوعة يدرك أبعاد هذا النشاط وهذه الديناميكية التي يتميز بها هذا الفضاء، وهذه الأعداد التي تعبر هذه الإحصائيات عنها قد منحت للأفراد والمستخدمين إمكانية السباحة في فلك مترامي الأطراف متسع الأرجاء، الأمر الذي أثار وأقلق المهتمين بالجوانب الأمنية لما في ذلك من عدم القدرة على حصر أبواب الخطر ومصادره ولا يمكن الهيمنة والسيطرة عليه بحال من الأحوال⁽²⁾.

وسعة الفضاء الإلكتروني لا تقف فقط عند اتساع أعداد المواقع وصفحات الإنترنت، لأن الفضاء الإلكتروني لا يرادف الإنترنت حتى وإن كان هذا الأخير الوجه الأكثر تعبيرا عن هذا الفضاء، فسعة الفضاء الإلكتروني تمتد أيضا إلى ديناميكية طبقاته المادية والبرمجية، ففي كل مرة تبرز لنا معدات جديدة وبرامج مختلفة وتطبيقات متنوعة، كما تمتد أيضا إلى حجم المعلومات نفسها، والتي لا تكاد تتوقف لحظة على الفضاء السيبراني، مما يضيف عليها فعلا هذه الصفة.

3- نهج استغلال استثنائي:

إن الفضاء الإلكتروني فضاء فريد من حيث تعدد الفئات المستغلة له من جهة، وتعدد أشكال الاستغلال من جهة أخرى، فالفضاء الإلكتروني يلجأ إلى خدماته كل أفراد المجتمع، أيا كان جنسهم، وأيا كانت أعمارهم ووظائفهم، وأيا كان مستواهم ومقامهم التعليمي والثقافي والاجتماعي وحتى القانوني، وهو أيضا فضاء يفتح من مجالات الاستغلال ما لا يكاد يخلو من أثرها ميدان من ميادين الحياة⁽³⁾.

⁽¹⁾ نقلا عن: لورنس لسيج، الكود المنظم للفضاء الإلكتروني، الإصدار الثاني، مؤسسة هندواي للتعليم والثقافة، القاهرة، مصر، 2014، ص 96.

⁽²⁾ علي بن عبد الله عسيري، المرجع السابق، ص ص: 25-26.

⁽³⁾ المرجع نفسه، ص 26.

ولذلك فإنك تجد مصطلحات جديدة تواكب هذا التوظيف وتساييره، مثل التسويق الإلكتروني، الإدارة الإلكترونية، التعليم الإلكتروني، الدبلوماسية الإلكترونية، الاقتصاد الإلكتروني، وما إلى ذلك، وتجد أيضا مصطلحات تواكب حتى أنماط وأشكال المستخدمين، كمصطلح المجرم السيبراني، الخبير السيبراني.

الفرع الثالث: أهمية الفضاء الإلكتروني:

يجب الإقرار بأن الفضاء الإلكتروني قد أحدث تغيرات جذرية في أداء العمل المرفقي الحكومي وقد بلغت أهميته درجة كبيرة حين اعتمد مرفق القضاء على الخدمات التي يوفرها والإمكانيات التي يتيحها (أولا) كما أصبح أيضا عمدة في الاستغلال الاقتصادي حين تم توظيفه في البناء التكنوني للمؤسسات الاقتصادية والتجارية (ثانيا) وامتد أيضا هذا الفضاء ليعزز أهميته ودوره الفعال في دعم ورعاية المجال الثقافي والعلمي والعمل على إثرائهما وتعزيز آليات تطورهما وازدهارهما (ثالثا).

أولا: أهمية الفضاء الإلكتروني لعمل الحكومة ومرفق القضاء:

1- الحكومة الإلكترونية:

إن أهمية الفضاء الإلكتروني تتجلى بصورة واضحة من خلال نشوء الحكومة الإلكترونية التي أصبحت في عصرنا الحاضر من بين أهم وأبرز الوسائل المثلى للتمكن من الإدارة والتسيير بفعالية تامة لجميع المصالح المتعلقة بالمواطنين وذلك من خلال إرضاء جميع طموحاتهم وتحقيق كل مطالبهم المختلفة عن طريق خدمات إلكترونية دون الحاجة إلى دول التنقل إلى بين مختلف الهياكل الحكومية والمرفقية⁽¹⁾.

وقد أصبح نظام الحكومة الإلكترونية في العديد من دول العالم واقعا فعلية تمت صياغة هياكلها ونظمها وآليات عملها في أرض الواقع رغم عدم كمال مظهرها ونموذجها بشكل تام لها لارتباط ذلك بالحاجة إلى الاستمرارية في بذل المزيد من المساعي المبذولة والمعدات المتطورة والأنظمة الذكية بالإضافة إلى أنها تتعرض في وسط غير عامر، وتسير في طريق مهجور، غير أنه طريق يخفي في طياته آمال وطموحات كثيرة، ولهذا تعتبر محط أنظار الدول، التي لمحت بجلاء ووضوح ما توفره هذه الحكومة للمواطنين من خدمات وما يمكنها أن توفره للدولة من سبل

(¹) ليلي عصماني، نظام التقاضي الإلكتروني آلية لإنجاح الخطط التنموية، مجلة الفكر، العدد 13، كلية الحقوق والعلوم السياسية، جامعة محمد

خيضر، بسكرة، الجزائر، فيفري 2016، ص ص: 215-225:

<https://www.asjp.cerist.dz/en/article/62437>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

لتعزيز نفوذها على النشاطات التي تمارس على الفضاء الإلكتروني، فالدولة التي تريد لنفسها مواكبة العصر وضمان عدم أقول شمسها، لا بد عليها أن صنع لنفسها مقاما أو مكانة في هذا الفضاء الإلكتروني، فهو بما له من خواص وسمات ندر ما تجدها في غيره لا يدع أمام الدول التي ترمي إلى الحكم الرشيد وبلوغ السدة إلا الاتجاه نحو هذا المجتمع المعلوماتي بخدماته الرقمية⁽¹⁾.

تعد الحكومة الإلكترونية ذات أهمية بالغة في إرساء الشفافية التي تعتبر من مستلزمات ومتطلبات الحكم الرشيد، حيث تؤدي آلياتها التقنية والبرمجية إلى تمكين المواطنين من بلوغ المعلومات وحيازتها الأمر الذي سيفضي تبعاً إلى إزاحة الغموض ورفع الالتباس، مما يتيح المجال لهم في مشاركة الحكومة صناعة القرار والمطالبة بتحقيق كافة حقوقهم المدنية، وهذه الشفافية التي تحققها الحكومة الإلكترونية تعتبر آلية فعالة في مكافحة الفساد أو الحد منه عن طريق فرض سلطة القانون بشكل واسع وكبير، أو عن طريق الحوسبة الإدارية وتحديد مستويات بلوغ المعلومات والحد من الفوضوية في المعاملات الوظيفية، وتعزيز المساءلة والمحاسبة وتوسيع دائرة المشاركة بين القطاع العام والقطاع الخاص وتوطيد دعائم الديمقراطية الفعالة⁽²⁾ التي تعبر عن وجود حركة تغير فريدة في الصلات التي تربط الدولة بمواطنيها وبموظفيها، ففي ظل الديمقراطية الرقمية تتغير النظرة إلى العديد من المفاهيم ولاسيما تلك المفاهيم المتعلقة بالانتخابات وصياغة القرارات، والرقابة عليها، وعلى آليات تنفيذها، فالديمقراطية بهذا الشكل تمكن بالفعل المواطنين من مباشرة العمل السياسي والمشاركة فيه في كل مراحله التكوينية⁽³⁾.

ومن بين المتطلبات الأساسية التي يجدر بنا الإشارة إليها في خضم الحديث عن اكتمال المظهر النهائي للحكومة الإلكترونية، نجد وجوب خلق هيكلية تشريعية وقانونية متكاملة تعمل على إحاطة هذه الحكومة بمجموعة من القوانين التي تتناسب مع أدوارها الحيوية من جهة، ومع طبيعتها من جهة ثانية، كما يتطلب تطبيق الحكومة الإلكترونية أيضاً تشكيل نهج إدارية جديدة ومبتكرة، تسعى إلى القضاء على ما يخنق روح الابتكار الإداري وطغيان النمط البيروقراطي في التعاملات الإدارية، فمن الضروري إذا بناء نظام إداري، روحه وجوهره هو اختزال التعاملات الإدارية لتتمكن من مسايرة التطور الكبير الذي تعلق بكل مجالات الحياة المعاصرة، والعمل أيضاً

(1) سمية بو مروان، الحكومة الإلكترونية ودورها في تحسين أداء الإدارات الحكومية: (دراسة مقارنة)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2014، ص 15 و 23.

(2) محمد الشايب، الحكومة الإلكترونية كآلية لتوطيد الحكم الجيد: (دراسة في تطبيقات العالم المتقدم والنامي)، مذكرة ماجستير في العلوم السياسية والعلاقات الدولية، كلية الحقوق، جامعة الحاج لخضر، باتنة، السنة الجامعية 2008-2009، ص ص: 89-94.

(3) المرجع نفسه، ص 101.

على ضمان عصرة إدارة وتسيير المرافق والمؤسسات داخل الدولة، مع العمل على تكوين قيادات إدارية تتمتع بروح العصر وتسعى حثيثاً لمواكبته⁽¹⁾.

2- المحكمة الإلكترونية:

لقد تجاوزت الدولة في نظرتها إلى الفضاء الإلكتروني حد التوظيف له كآلية لإدارة وتسيير المجالات ذات الطابع الاقتصادي، وبدأت في النظر إليه كآلية وأسلوب تماشي مع مقتضيات وخدمات الأجهزة القضائية، وذلك عن طريق اللجوء إلى توظيف تقنيات ونظم يوفرها الفضاء الإلكتروني في تسيير إجراءات التقاضي، وهذا ما ترتب عنه ما يعرف بالتقاضي الإلكتروني، والذي يمكن اعتباره كنظام تقني حديث يمكن من خلاله لأطراف الدعوى مباشرة إجراءات التقاضي أمام الجهات القضائية المختصة والسير فيها، من بدايتها إلى غاية صدور الحكم النهائي فيها، دون أن يتكبدوا عناء الانتقال إلى مقر الجهة القضائية⁽²⁾.

وعلى هذا الأساس تم إنشاء المحاكم الإلكترونية والتي يمكن أن تعرف على أنها: (حيز تقني معلوماتي ثنائي الوجود، يسمح ببرمجة الدعوى الإلكترونية، ويتألف من شبكة الربط الدولية، إضافة إلى مبنى المحكمة، بحيث يتيح الظهور المكاني الإلكتروني لوحدات قضائية وإدارية، ويباشر من خلاله مجموعة من القضاة مهمة النظر في الدعوى والفصل فيها، بموجب تشريعات تخولهم مباشرة الإجراءات القضائية، مع اعتماد آليات تقنية فائقة الحداثة لتدوين الإجراءات القضائية وحفظ وتداول ملفات الدعوى) ويمكن تعريفها أيضاً على أنها: (تنظيم تقني معلوماتي تفاعلي مؤمن على الشبكة العالمية، يتيح للمتقاضين تحريك دعواهم وتقديم البيانات والإطلاع على مجريات الجلسات، وللقضاة وأعوانهم النظر في الدعوى وتدوينها وحفظها والفصل فيها، عبر الرسائل التقنية الحديثة)⁽³⁾.

وقد عرف المشرع الإماراتي التقاضي الإلكتروني أو التقاضي عن بعد في القضاء المدني على أنه: (إجراءات التقاضي المدنية - غير الجزائية - التي تباشر باستخدام وسائل الاتصال عن بعد، أو عبر الوسائط الإلكترونية، لتحقيق الحضور عن بعد، وتبادل المستندات والمذكرات،

(1) عباس زبون عبيد العبودي، الإطار القانوني للحكومة الإلكترونية، مجلة العلوم القانونية والسياسية، مجلة العلوم القانونية والسياسية، العدد 01،

كلية القانون والعلوم السياسية، جامعة ديالى، العراق، 2012، ص ص 84-102:

<https://www.iasj.net/iasj?func=issueTOC&isId=6634&uiLanguage=ar>

(2) ليلي عصماني، المرجع السابق.

(3) عبد العزيز بن سعد الغانم، المحكمة الإلكترونية: (دراسة تأصيلية مقارنة)، دار جامعة نايف للنشر، الرياض المملكة العربية السعودية، 2017،

ص ص: 37-38

الفصل الأول الفضاء الإلكتروني والتحول الرقمي في المفاهيم الاستراتيجية

وتشمل - في هذا القرار - قيد الدعوى وإجراءات الإعلان، وإجراءات المحاكمة أمام المكتب وأمام المحكمة المختصة، وإصدار الأحكام⁽¹⁾.

وعرفها المشرع الإماراتي أيضا في مجال القضاء الجنائي على أنه: (الإجراءات الجزائية التي تباشر باستخدام تقنية الاتصال عن بعد، لتحقيق الحضور والعلانية وسرية التحقيقات وإبداء المرافعات وتقديم المستندات والمذكرات وإصدار الأحكام، سواء تمت بشأن استقصاء الجرائم وجمع الأدلة، أو عند التحقيق والمحاكمة)⁽²⁾.

لقد أحدث الفضاء الإلكتروني فوارق كبيرة في النظام القضائي ومتطلباته القانونية، وقد ظهرت دراسات جادة وعميقة تعرض بشكل فقهي ممنهج الأثر الذي أنتجه الفضاء الإلكتروني على إجراءات التقاضي المعروفة، كمسألة حضور الخصوم في المرافعات والجلسات، ومحاضر الدعاوى الإلكترونية وتسجيلها وإصدار الحكم فيها، وطرق الإثبات القانونية من شهادة ومحررات توقيعات إلكترونية⁽³⁾.

ثانيا: الاقتصاد الرقمي:

يمكن تعريف الاقتصاد الرقمي على أنه: (التفاعل والتكامل والتنسيق بين تكنولوجيا المعلومات وتكنولوجيا الاتصال من جهة، وبين الاقتصاد القومي والقطاعي والدولي من جهة أخرى، بما يحقق الشفافية والفورية والإتاحة لجميع المؤشرات الاقتصادية المساندة لجميع القرارات الاقتصادية والتجارية والمالية في الدولة خلال فترة ما)⁽⁴⁾.

وينبني الاقتصاد الإلكتروني في ممارسة نشاطه على ما يوفره الفضاء الإلكتروني من معلومات، ويستفيد بشكل أساسي في جميع مراحله وخطواته من الاستعانة بتكنولوجيا المعلومات والاتصال التي مكنت من تدفق المعلومات والسلع والخدمات وحركة رؤوس الأموال متخفية كل الفواصل والحدود وفي سرعة كبيرة، وهذا التوظيف الواسع للفضاء الإلكتروني في مجالات الاقتصاد قد سمح بإنعاش الحركة الاقتصادية من خلال سلسلة انتقال الأموال زمانيا ومكانيا،

⁽¹⁾ أنظر المادة الأولى من القرار الوزاري رقم 260 لسنة 2019 الصادر بتاريخ 27 مارس 2019 في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات المدنية، المنشور الجريدة الرسمية رقم 651، ص 121.

⁽²⁾ أنظر المادة الأولى من القرار الوزاري رقم 259 لسنة 2019 الصادر بتاريخ 27 مارس 2019 في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات الجزائية، المنشور الجريدة الرسمية رقم 651، ص 107.

⁽³⁾ يمكن الاطلاع على دراسة عبد العزيز بن سعد الغانم، المرجع السابق، فهي أحسن نموذج للدراسة الوافية لهذا الموضوع.

⁽⁴⁾ كنزة تتيو ومحمد دهان، دور الاقتصاد الرقمي في تحقيق جودة الحياة: (دراسة مقارنة بين الجزائر والإمارات)، مجلة الاستراتيجية والتنمية، العدد 03 مكرر (الجزء الأول)، المجلد 09، كلية العلوم الاقتصادية، التجارية وعلوم التسيير، جامعة عبد الحميد بن باديس، مستغانم، 2019، ص

ص: 364-385: <https://www.asjp.cerist.dz/en/article/98416>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وبناء اقتصاد إلكتروني يعزز الشفافية ويكرس الحياد في ما يتعلق بتوظيف العلمية الإلكترونية، ويتكون الاقتصاد الإلكتروني من مكونين أساسيين هما⁽¹⁾:

أ- الأعمال الإلكترونية:

يمكن تعريفها على أنها التحول من "الأداء التقليدي إلى الأداء الإلكتروني"، وتتكون الأعمال الإلكترونية بدورها من عدة عناصر مهمة وتتمثل في⁽²⁾:

1. الإدارة الإلكترونية:

تعرف الإدارة الإلكترونية على أنها: (منظمة وظيفية وتقنية متكاملة لإدارة وتوجيه وتنفيذ الأعمال الإدارية إلكترونيا سواء فيما يخص الأعمال المتعلقة بين الموظفين أو بينهم وبين المواطنين)⁽³⁾.

وتعرف أيضا على أنها: (العملية الإدارية القائمة على الإمكانيات المتميزة للإنترنت وشبكات الأعمال في التخطيط والتنظيم والتوجيه والرقابة على الموارد، والقدرات الجوهرية للشركة والآخرين بدون حدد من أجل تحقيق أهداف الشركة)⁽⁴⁾.

فهي إذا تعبر عن تغيرات في البنية التنظيمية للإدارة من خلال انتقالها من النمط التقليدي الجامد بإدراج الفضاء الإلكتروني النشاط والدقيق كبعد جديد أو كآلية وأسلوب في تسيير المرافق الإدارية بما تقدمه من خدمات، وبما تلعبه من أدوار، وقد أطلق عليها بعض الدارسين " إدارة بلا أوراق " إذ تقوم على الفضاء الإلكتروني -بما يتمتع به من خواص- في أداء ما أنيط بها من مهام خدمانية أو تنظيمية أو رقابية⁽⁵⁾.

(1) عدنان مصطفى البار، خالد علي المرحبي، الاقتصاد الرقمي، 21 جانفي 2019، تم الاطلاع عليه بتاريخ 3 فيفري 2020 على الساعة 21:22 سا، في الموقع:

<https://www.awforum.org/index.php/en/component/k2/item/208-الإقتصاد-الرقمي>

(2) المرجع نفسه.

(3) صفاء فتوح جمعة، مسؤولية الموظف العام في إطار تطبيق نظام الإدارة الإلكترونية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2014، ص ص: 08-09.

(4) مصطفى يوسف كافي، الإدارة الإلكترونية: (إدارة بلا أوراق-إدارة بلا مكان-إدارة بلا زمان-إدارة بلا تنظيمات جامدة)، دار ومؤسسة رسلان للطباعة والنشر والتوزيع، دمشق، سوريا، 2011، ص 41.

(5) أحلام محمد شواي، الإدارة الإلكترونية وتأثيرها في تطوير الأداء الوظيفي وتحسينية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 24، العدد 4، جامعة بابل، العراق، سنة 2016، ص ص: 2388-2411: <https://www.iasj.net/iasj/article/120141>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وتتقسم هذه الإدارة إلى نوعين؛ أولهما هي الإدارة الإلكترونية الداخلية، وهي التي تعنى بكل ما له علاقة بالأشغال والمهام والممارسات الإدارية على المستوى الداخلي للجهة المعنية، وثانيهما هي الإدارة الإلكترونية الخارجية والتي إدارة تعنى بشكل خاص بكافة الممارسة ذات الطابع الإداري أو التنظيمي خارج نطاق الجهة أو المنظمة المعنية⁽¹⁾.

أ.2: الأرشفة الإلكترونية:

هي من بين العناصر المكونة للأعمال الإلكترونية⁽²⁾، ويغلب في معناها الدلالة على الترتيبات والإجراءات التي يكون محلها اختزان المستندات التي لا يؤلف استعمالها، أيًا كان نوعها وشكلها، في وسائط إلكترونية، للرجوع إليها عند تحقق الغرض من ذلك⁽³⁾.

ب/ التجارة الإلكترونية:

تعتبر التجارة الإلكترونية من بين أهم المظاهر التي تبرز أهمية الفضاء الإلكتروني باعتبارها من بين المفردات الأساسية المنبثقة من بنية الفضاء الإلكتروني التكوينية من تكنولوجيا المعلومات وآليات الاتصال، وتحتوى التجارة الإلكترونية على العديد من النشاطات المتعلقة بالصفقات التبادلية، ومن بين أبرزها البيوع الإلكترونية بمختلف أشكالها، وآليات الدفع والتسويق الإلكتروني، وحركة المعاملات بين الموردين والعملاء⁽⁴⁾.

وقد عرفت المنظمة العالمية للتجارة بأنها: (مجموعة متكاملة من عمليات إنتاج وتوزيع وترويج وبيع المنتجات من خلال شبكات الاتصالات، ومن الأمثلة الشائعة للسلع الموزعة إلكترونياً: الكتب، القطع الموسيقية)، وعرفت منظمة التعاون والتنمية الاقتصادية كونها: (تشمل جميع أشكال المعاملات والصفقات التجارية التي تتم من قبل الأفراد والهيئات، وتقوم على أساس معالجة ونقل البيانات الرقمية على اختلاف أشكالها سواء كانت مكتوبة أم مرئية أو مسموعة) وعرفت أيضاً المنظمة العالمية للملكية الفكرية في شكلها الواسع على أنها كل آلية إلكترونية توظف في بلوغ أهداف تجارية⁽⁵⁾.

⁽¹⁾ عدنان مصطفى البار، خالد علي المرحبي، المرجع السابق.

⁽²⁾ المرجع نفسه.

⁽³⁾ عامر قنديلجي، التوثيق الإعلامي والأرشيف الصحفي، دار البازوري للنشر والتوزيع، الأردن، 2014، ص 40.

⁽⁴⁾ هشام بن عبد الله العباس، تسويق خدمات المعلومات عبر الإنترنت، مكتبة الملك فهد الوطنية، الرياض، المملكة العربية السعودية، 2009، ص 99.

⁽⁵⁾ سميرة ديمش، التجارة الإلكترونية: حقيقتها وواقعها في الجزائر، مذكرة ماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، السنة الجامعية 2010-2011، ص ص: 36-37.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وذهب المشرع الجزائري في تعريفها على أنها: (النشاط الذي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك إلكتروني عن طريق الاتصالات الإلكترونية)⁽¹⁾.

والتجارة الإلكترونية يمكن النظر إليها من منحين إثنين، أو بالأحرى يمكن تقسيما إلى صنفين، تجارة الأعمال مع الأعمال، وتتخلص في تلك المعاملات الكبرى التي تتعلق بالشركة ومورديها ومبار عملائها، وتجارة الأعمال مع المستهلكين، والتي يعتبر عنها في الغالب بالتسويقي الإلكتروني أو تجارة التجزئة الإلكترونية⁽²⁾.

إن أهمية الفضاء الإلكتروني في إنعاش وتطوير التجارة تظهر بكل وضوح من خلال المزايا التي توفرها التجارة الإلكترونية والتي تتجلى بصفة خاصة في تلك المساحة الواسعة من الحرية وانخفاض التكاليف خاصة تلك التي تتعلق بالتسويق والترويج والتخزين، كما أنها تجارة متحررة من كل القيود الزمانية والمكانية وفتحت الأسواق أمام المشروعات الصغيرة، ووسعت من دائرة الاختيار بالنسبة للمستهلكين، لأمر الذي ساهم بشكل كبير جدا في توسع النشاطات التجارية حيث بلغ حجمها 25 تريليون دولار على أقل تقدير، وأصبح للأفراد مجالا يمكنهم من إجراء عملية التسوق والتسويق من أي مكان في العالم وفي أي وقت وحين⁽³⁾.

فأصبح الفضاء الإلكتروني بذلك كله أساسا للعمليات التسويقية في العصر الحديث وأصبح الزبون يعامل معاملة الملك الذي يسعى الكل إلى نيل رضاه من خلال تقديم ضمانات عدة وامتيازات كثيرة، حيث يتم استقطابه من خلال عمليات الترويج الإلكترونية والتي أصبحت أكثر تفاعلية حيث يتم توظيف منصات وخدمات الفضاء الإلكتروني للتقرب من الزبائن وتكوين علاقات تفاعلية وشفافة من خلال القيام بحوارات مباشرة على المواقع الإلكترونية والمننديات التابعة للمؤسسات أو عن طريق البريد الإلكتروني⁽⁴⁾.

(¹) المادة 06 من قانون رقم 18-05 المؤرخ في 10 مايو 2018 والمتعلق بالتجارة الإلكترونية، المنشورة ب16 مايو 2018، ، الجريدة الرسمية رقم 28.

(²) حسين مصطفى هلاي، إيمان صالح حسن عبد الفتاح، ريم الألفي، غريب جبر غنام، محمد محمد الألفي، الإدارة الإلكترونية، الطبعة الأولى، دار السحاب للنشر والتوزيع، مصر، 2010، ص ص: 10-11.

(³) أشرف دوابة، التجارة الإلكترونية بين الفرص والتحديات، 07 ديسمبر 2019، تم الإطلاع عليه بتاريخ 8 فيفري 2020 على الساعة 18:30 سا، في الموقع: <https://mugtama.com/articles/item/95962-2019-12-07-14-30-38.html>

(⁴) أمينة قدايفة، أثر تكنولوجيا المعلومات على المزيج التسويقي: (دراسة حالة عينة من المؤسسات الاقتصادية الجزائرية)، أطروحة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير. جامعة أمحمد بوقرة، بومرداس، السنة الجامعية 2013-2014، ص ص:

ج/ ظهور الشركات الرقمية:

تعتبر الشركات الإلكترونية من بين الثمار البارزة التي أفرزها التطور التقني والتكنولوجي الذي ساد المرحلة المتأخرة من عصرنا الحاضر، وقد كان لها الأثر الكبير في إحداث تغيرات كبيرة على صعيد علاقات الأعمال في البيئة التجارية، كما أحدث تحولات كبرى في أنظمة الشركات والمنظمات، إذ تمت رقمنتها وتحولت جل أعمالها بما فيها الأكثر أهمية إلى ساحة الفضاء الإلكتروني الذي أصبح الركيزة الأساسية التي تركز عليها أعمال المؤسسات والشركات التي يجمع بينها الفضاء الإلكتروني⁽¹⁾.

صفوة الكلام وخلاصته أن القرارات الاقتصادية في مجملها ولاسيما في قطاع التجارة لم يعد لها أي علاقة تربطها بالموقع الجغرافي لأطراف العلاقة التجارية، فالتجار عموما يعملون على تحقيق مصالحهم التجارية في أقصر الآجال الممكنة طبقا للمعطيات التقنية والبرمجية التي يتم الاعتماد عليها⁽²⁾، والمنظومات والكيانات الاقتصادية، أيا كان مقامها والجهات التي تشرف عليها، إن لم تكن قادرة على السير وفق هذه القواعد الجديدة للعبة فإن إلى الزوال مآلها، والبقاء في خضم هذه الظروف يكون فقد للكيانات التي تتمتع بقدر من المرونة لمسايرة هذا النمط الجديد للاقتصاد العالمي⁽³⁾.

ثالثا: الثقافة والتعليم الإلكترونيين:

إن الآليات والتقنيات التي كانت في الماض القريب تحتل الأفضلية التقنية والشيوع الكبير قد أصبحت في الوقت الراهن مع هذا التسارع في التقنيات ذو أداء يتسم بالمحدودية إن لم يكن أقرب إلى فقدان الجدوى، فتأثير الفضاء الإلكتروني الكبير هو الذي نستقبله في الأيام القادمة وليس فيما استدبرنا من تقنيات، فالدور الذي سيلعبه الفضاء الإلكتروني في تغيير المناهج والتقنيات في المجال التعليمي والتدريبي سيكون ذو أهمية كبرى في مستقبل أيا منّا، فليس من الضروري أن يلتقي المدرب والمعلم مع طلبته في حيز مكاني واحد، إذ بالإمكان إلقاء الدروس والمحاضرات أمام الجموع عن طريق خدمات الفضاء الإلكتروني، فالتعليم الإلكتروني حقق جملة من الأهداف لم تكن لتتحقق لولاه، ولعل من أبرزها نجد؛ المرونة في التعامل مع الحيز المكاني والتوقيت الزمني،

(1) بلقيثوم صباح، أثر تكنولوجيا المعلومات والاتصالات الحديثة على التسيير الاستراتيجي للمؤسسات الاقتصادية، رسالة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة قسنطينة 2، الجزائر، السنة الجامعية 2012-2013، ص 138.

(2) جويل كرتزمن، موت النقود، ترجمة (محمد بن سعود بن محمد العصيمي)، الطبعة الأولى، دار الميمان للنشر والتوزيع وبنك البلاد، الرياض، المملكة العربية السعودية، 2010، ص 140.

(3) المرجع نفسه، ص 152.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

والوصول إلى أعداد كبيرة من الجماهير والمتابعين في مختلف أنحاء العالم بحيث يصبح التدريب ذو صبغة عالمية وثرء في المحتوى مع قلة التكاليف وتنوع الأساليب والمناهج⁽¹⁾

إضافة أيضا إلى ما توفره من أسباب الراحة للإنسان، والاقتصاد في موارده الورقية، فلا يسرف فيها، خصوصا مع ظهور أسولب رقمة مختلف المصنفات، فثلا عن إمكانية توظيفها في إذاعة مختلف البرامج المعرفية والتعليمية بحيث تمكن أجهزة التعليم من بلوغ مقاصد تعليمية كبرى والمساهمة في تدارك السليبات والمساوئ التي تشوب الأنظمة التعليمية الكلاسيكية⁽²⁾ وذلك من خلال تضمين مختلف الخدمات والتقنيات التي يوفرها الفضاء الإلكتروني في التدريس الحضوري للطلبة في بداياتها، وإلى غاية بلوغ اعتماد التعليم الهجين الذي يكون الفضاء الإلكتروني حاضرا بخدماته وذلك باعتماد نمطي التعليم الحضوري والتعليم عن بعد، وفي النهاية بلوغ التعليم الإلكتروني كامل العناصر أين يكون هناك انفصال مكاني تام بين الأستاذ والطالب⁽³⁾.

المطلب الثاني:

البنية التكوينية للفضاء الإلكتروني

يتكون الفضاء الإلكتروني من مجموعة من العناصر المادية التي تمثل القاعدة الأساسية التي يقوم عليها الفضاء الإلكتروني (أولا)، بالإضافة إلى طبقة من البرمجيات التي تعمل على استغلال هذه الطبقة المادية وهي بطبعة حال الطبقة المنطقية التي تمنح الصبغة الخدماتية للفضاء الإلكتروني وتسخره للعب أدوار حيوية في حياة الأفراد والدول (ثانيا)، كما يدخل أيضا في البنية التكوينية الأساسية للفضاء الإلكتروني هذا الوسيط الحيوي الذي يربط بين كافة عناصر المعلوماتية في كل منطقة من مناطق العالم من خلال نظام شبكي يسهم بشكل أساسي في بلورة ماهية الفضاء الإلكتروني وكيونته (ثالثا)، والذي يربط من خلاله الأفراد سواء أكانوا مستغلين أو مبرمجين بين مختلف المعلومات التي تعمل على خلق نموذج متكامل من البناء المعلوماتي العالمي (رابعا).

⁽¹⁾ علي عماري، مساهمة تكنولوجيا المعلومات في تنمية الكفاءات: (دراسة حالة مطاحن الأوراس باتنة)، أطروحة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد خيضر، بسكرة، السنة الجامعية 2017-2018، ص: 124-125

⁽²⁾ حورية بولعويذات، مرجع سابق، ص 87.

⁽³⁾ نسيمه ضيف الله، استخدام تكنولوجيا المعلومات والاتصال وأثره على تحسين الجودة العملية التعليمية: (دراسة عينية من الجامعات الجزائرية)، أطروحة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الحاج لخضر، باتنة 1، السنة الجامعية 2016-2017، ص 174.

الفرع الأول: الطبقة المادية للفضاء الإلكتروني:

تعد مرحلة ظهور أجهزة الكمبيوتر هي المرحلة الأساسية التي بدأ فيها تشكل مفهوم الفضاء الإلكتروني إذ تعد هذه الأجهزة النواة الأساسية والعمود الفقري الذي يقوم عليه مفهوم الفضاء الإلكتروني (أولا) ثم بعد ذلك تأتي الهواتف النقال التي أصبحت النموذج المنقول للفضاء الإلكتروني والذي أحدث تغيرات جذرية في حياة الأفراد (ثانيا) وترتبط بين مختلف هذه الأجهزة سواء أكانت حواسيب أو هواتف ذكية مجموعة من الألياف البصرية التي تشكل نظام شبكي معقد هو نفسه ثمرة الفضاء الإلكتروني في شكله المتكامل (ثالثا).

أولا: الحاسوب:

1- تعريف الحاسوب وتطوره:

أصبحت أجهزة الحاسب الآلي في العصر الحاضر منتشرة بشكل كبير بين الأفراد فضلا عن كل المؤسسات، إذ أصبح تشغيلها وصيانتها أمر غاية في السهولة واليسر ، إذ أصبح أمر تشغيلها واستغلالها في متناول الأفراد كلهم الأفراد، حتى الذين لا يمتلكون أي معارف أو مؤهلات تقنية، كما أصبحت الحواسيب من الصغر ما يمكن معه نقلها من مكان إلى آخر دون عناء، وهذا ما لم يكن متاحا في الماضي، وأصبح الحاسب الآلي ذو دور مهم في ظهور مجتمع المعلومات وو أشكال النظم الإلكترونية المتطورة، فهو يوفر سمات عدة أبرزها السرعة والدقة والثقة، الأمر الذي ينتج عنه الكفاءة والفعالية في العمل والدقة في الأداء مع قدرة هائلة على إجراء العمليات المعقدة والحفظ الأمثل للمعلومات واستدعتها عند الحاجة وفي أوقات مختصرة جدا⁽¹⁾.

لقد تعددت التعاريف المقدمة للحاسب الآلي إلا أنها معظمها ينصب في فكرة واحدة وهي المميزات والسمات الأساسية التي تمتاز وتتسم بها وظائفه وأدائه، فعرفه البعض على أنه: (آلة تقوم بمعالجة البيانات، تخزينها، استرجاعها بدقة وسرعة فائقة، فنحن نقوم بالتعامل مع تلك الآلة عن طريق برمجتها لكي تقوم بأعمال المعالجة والتخزين والاسترجاع)⁽²⁾، كما عرفه آخرون على أنه: (جهاز إلكتروني يقوم بتلقي البيانات ومعالجتها وتخزينها واسترجاعها بدقة متناهية وسرعة فائقة وذلك وفقا لمجموعة من التعليمات وصولا إلى المعلومات المطلوبة)⁽³⁾.

(1) حسين عماد مكاي، تكنولوجيا الاتصال الحديثة في عصر المعلومات، الثانية، الدار المصرية اللبنانية، القاهرة، 1997، ص ص: 59-60

(2) نسيمه ضيف الله، المرجع السابق، ص 99.

(3) سعاد شحات، استخدامات تكنولوجيا المعلومات والاتصال والفعالية التنظيمية للمؤسسات الاقتصادية: دراسة للمؤسسات الصغيرة والمتوسطة بالجزائر، مذكرة ماجستير في علم الاجتماع والاتصال، كلية الآداب والعلوم الاجتماعية، جامعة 08 ماي 1945، السنة الجامعية 2009، ص 128.

وهناك تعريف آخر نعتبره أكثر شمولاً وتوصيفاً لهذا الجهاز حيث تم تعريفه بالاستناد إلى التفاعل بين عنصر هذا الجهاز، إذ عرف على أنه جهاز يتركب من مجموعة من الآلات أو القطع التي تتفاعل فيما بينها للقيام بمعالجة وتشغيل البيانات بالسرعة والدقة، حيث يمتلك هذا الجهاز قابلية استقبال البيانات وتخزينها بطريقة آلية، ثم يقوم بمعالجتها عن طريق خوارزميات أو حسابات منطقية توجيهية تم برمجتها الحاسب الآلي عليها سلفاً من أجل الحصول على مخرجات أو استنتاجات لتلك العمليات⁽¹⁾، وقد مر جهاز الحاسب بعدة مراحل أو أجيال ليصل إلى الحالة التي نراه عليه الآن، وهذه الأجيال هي:

أ- الجيل الأول:

يعد جهاز "UNTVAC" عام 1951 كأول جهاز حاسوب يتم إدخاله في الخدمة العمومية، ثم بعد سنتين أعلنت شركة "IBM" على أول حاسوب تنتجه، والذي كان يعتمد بشكل أساسي على الصمامات المفرغة، الأمر الذي جعل درجة حرارته مرتفعة، مما كان يتطلب تغيير هذه الصمامات بمعدل صمام كل يوم، وهذا يستوجب القيام بعمليات التبريد الكبيرة، ونظراً للاعتماد على مثل تلك الصمامات فإن حجمها كان يأخذ حيزاً كبيراً، كما أن لغة البرمجة لهذا الحاسب كانت لغة الآلية، الأمر الذي انعكس على سرعته فقد كان جهازاً بطيء الأداء قليل الكفاءة⁽²⁾.

استعملت شركة "IBM" في حاسوبها الذي كان أشهر حاسبات الجيل الأول كذاكرة للجهاز "الأسطوانة الممغنطة" كما استخدمت البطاقات المثقوبة كوسيلة إدخال وإخراج⁽³⁾.

ب- الجيل الثاني:

أخذت الحواسيب مع هذا الجيل في استخدام الترانزستور محل الصمامات المفرغة، الأمر الذي انعكس على حجم حواسيب الجيل الثاني، حيث بدأ حجمها في التصاغر مع تزايد ملحوظ في سرعة التنفيذ وبدأ استبدال الأقراص الممغنطة بالقلوب الممغنطة كذاكرة للحاسب، وبدأ استخدام أنظمة التحكم في الإدخال والإخراج بدل استخدام البطاقات المثقوبة، وبدأ هذا الجيل من الحواسيب

⁽¹⁾ مرابط عياش عزوز، دور تكنولوجيا المعلومات في تنمية كفاءات المهنية للعامل، أطروحة دكتوراه في علم الاجتماع، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، السنة الجامعية 2016-2017، ص 32.

⁽²⁾ علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، الطبعة الثانية، دار المناهج للنشر والتوزيع، 2002، سلطنة عمان، ص: 114-115.

⁽³⁾ عبد الله بن عبد العزيز الموسى، مقدمة في الحاسب الآلي، الطبعة الأولى، مكتبة الملك فهد الوطنية، الرياض، 2010، ص 10.

في الاعتماد على لغات عالية المستوى، مثل لغة الفورتران، ولغة كويول⁽¹⁾، فأصبح العمليات تقاس بالميكرو ثانية وكذلك تقليل استعمال الطاقة الكهربائية وانخفاض الحرارة الصادرة عن تشغيلها⁽²⁾.

ج- الجيل الثالث:

لقد سم استخدام الدوائر المتكاملة في تصميم وتصنيع هذه الحواسيب، وهي أقل حجما من الترانزستور وأعلى قدرة على التنفيذ حيث تقاس سرعتها بالنانو ثانية⁽³⁾.

فهو بذلك يتمتع بسرعة كبيرة ودقة عالية مع قدرته أيضا على استيعاب في يحفظ ويخزن بداخله بشكل واسع، كما أن قدرة على التنفيذ حيث تقاس سرعتها بالنانو ثانية، كما أن إنشاء نظم الشبكات للحواسيب الآلية يتم بموجبها الربط بين الدوائر بفروعها على مسافات بعيدة عن طريق اللجوء إلى استخدام النهايات الطرفية⁽⁴⁾.

د - الجيل الرابع:

يتم تصنيع حواسيب هذا الجيل من مادة السيليكون، وأجريت على هذا الجيل تعديلات محورية وهامة غيرت تماما من طبيعته وقوة أدائه، حيث تم صياغة نظم تشغيل مستحدثة وتم إجراء تعديلات على أداء نقل البيانات ووحدات الإدخال والإخراج، وازدادت معها إمكانياتها التخزينية، وسرعة معالجة المعلومات واستردادها، وظهرت وحدات اتصال طرفية بصفة كبيرة حيث يتم الوصول الفوري للبيانات واسترجعها ومعالجتها في نفس الوقت، كما ظهرت حواسيب صغيرة الحجم حيث يتم تجميع دوائر صغيرة على لوحة تدعى باللوحة الأم لتتخذ بعها شكلا مبسطا خفيف الوزن صغير الحجم فائق الدقة وسريع التنفيذ⁽⁵⁾.

2- أنواع الحواسيب الآلي:

هناك عدة أنواع من الحواسيب الآلية وهي عادة ما تصنف وقف معايير مختلفة، إذ يمكن تصنيفها على أساس الحجم أو القوة التنفيذية لها، أو على أساس العمل الذي تؤديه، كما يمكن تقسيمها على حسب الجهات التي تقوم بتوظيفها، والتقسيم الأنسب لهذه الدراسة هو التقسيم الذي ارتضته بلقيدوم صباح، وهو على النحو الآتي ذكره⁽⁶⁾:

أ- الحواسيب الشخصية: تنقسم الحواسيب الشخصية إلى عدة فئات هي:

(1) علاء عبد الرزاق السالمي، المرجع نفسه، ص 115.

(2) عبد الله بن عبد العزيز الموسى، المرجع السابق، ص 11.

(3) المرجع نفسه، ص 11.

(4) علاء عبد الرزاق السالمي، المرجع نفسه، ص 115.

(5) عبد الله بن عبد العزيز الموسى، المرجع السابق، ص 11.

(6) أنظر فيه: بلقيدوم صباح، المرجع السابق، ص 141.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

أ-1- حاسبات المكاتب: هي حاسبات شخصية تم تصميمها للاستغلال الفردي وتعمل على تشغيل بعض الأنظمة والبرامج التي من شأنها أن تعين الأفراد على رفع إنتاجية الأعمال التي يقومون بها.

أ-2- حواسيب محمولة: وهي نوع من الحواسيب الآلية التي تسمح طبيعتها وحجمها بحملها من مكان لآخر وهي تمتاز كونها مطابقة للحواسيب المكتبية في قدراتها على المعالجة وفي إمكانياتها ومكوناتها.

ب- حواسيب المنظمات: وحواسيب المنظمات تنقسم بدورها إلى ثلاث أقسام رئيسية هي:

ب-1- الحواسيب العملاقة: هي حاسبات آلية تمتلك قدرة كبيرة جدا في معالجة البيانات والأوامر والتعليمات حيث تملك سرعة تفوق فيها الحاسبات الشخصية.

ب-2- الحواسيب المركزية: هي حواسيب تمتلك القدرة العالية على بعدد كبير من المعالجات الآلية للبيانات وتنفيذ أعداد هائلة من الأوامر والتعليمات وبسرعة خارقة كما أنها تحوى على ذاكرة مركزية واسعة جدا.

ب-3- الحواسيب المتوسطة: هي حواسيب لا تتمتع بالقدرة العالية على معالجة وتخزين المعلومات مقارنة بالحواسيب التي تقدم ذكرها.

ثانيا: الهاتف النقال:

الهاتف النقال هو شكل من أشكال التطور التي طرأت على الهاتف الكلاسيكي الذي يرتبط بمجموعة من الكابلات والأسلاك التي تجعله غير قابلا للحركة، فقام المختصون بإزالة عنصر الثبات عن الهواتف باختراع وتطوير الأنظمة الخلوية التي تعتمد على موجات الراديو التي تسمح بإجراء اتصالات عن طريق وسيط محطة التحويل⁽¹⁾.

ومع تقدم الزمن وظهور أشكال جديدة ومتطورة من أجهزة الهاتف المحمول أصبحت هذه الأخيرة آلية يتم استخدامها للاتصالات الصوتية، فالتطورات التي أجريت عليه استحدثت فيه عددا كبيرا من الخدمات المهمة ومنها خدمة التواصل بالرسائل، وخدمة متابعة القوات الفضائية، والإبحار في عالم الإنترنت، وإجراء محادثات بالوسائط المتعددة من صوت وصورة، كما أصبح

⁽¹⁾ مريم ماضي، تأثيرات الهاتف النقال على أنماط الاتصال الاجتماعي لدى الطالب الجامعي: (طلبة جامعة قسنطينة نموذجاً)، مذكرة ماجستير في الإعلام وتكنولوجيا الاتصال الحديثة، كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012-2013، ص 37.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

الهاتف النقال في العصر الحديث بالكاد يكون بنفس الإمكانيات التي تتمتع بها الحواسيب، إذ أنه يملك ميزة القدرة على معالجة كمية كبيرة من البيانات والمعطيات، ويمكن تعرف الهاتف النقال على أنه: (عبارة عن جهاز اتصال صغير الحجم، مرتبط بشبكة للاتصالات اللاسلكية، وتسمح ببث واستقبال الرسائل الصوتية والنصية والصور عن بعد وبسرعة فائقة، نظرا لطبيعة مكوناته الإلكترونية واستقلاليته العملية فهو يوصف بالخلوي أو النقال أو الجوال أو المحمول)⁽¹⁾.

لقد مر تطور الهاتف الخلوي بعدة أطوار قبل أن يصل إلى الحال التي نراه عليه الآن في عصرنا الحالي، فكان أول ظهور له عام 1979 في اليابان والقائم على النظام التماثلي حيث كان الهاتف لا يدعم إلا خدمة الاتصال الصوتي وكان من صنع شركة " NIPPON " اليابانية، أما في الولايات المتحدة فقد ظهر نظام " AMPS " سنة 1983، وفي أوروبا ظهرت أنظمة غير متوافقة ففي الدول الإسكندنافية ظهر النظام " NMT " سنة 1981، وفي ألمانيا ظهر " C-NETZ"، ويدعى هذا النوع من الهواتف بالجيل الأول، ثم ظهر بعد ذلك الجيل الثاني عام 1990 حيث تميز بتوفير أفضلية في نقل الصوت ودعم تحويل البيانات، وتطور الأمر إلى أن ظهر نظام الجيل الثالث الذي يدعم الوسائط المتعددة وتأمين الوصول السريع إلى الإنترنت، وأخيرا ظهر الجيل الرابع الذي يتمتع بخصائص فريدة من نوعها من سرعة و ذكاء⁽²⁾.

ويعرف الهاتف الذكي على أنه: (هاتف محمول متنقل يتضمن وظائف متقدمة تتعدى إجراء المكالمات الهاتفية وإرسال الرسائل النصية والكثير من هذه الهواتف الذكية لها القدرة على عرض الصور وتشغيل ملفات الفيديو وتفقد وإرسال البريد الإلكتروني وتصفح الإنترنت)⁽³⁾.

ثالثا: الكوابل البحرية:

تعتبر الكوابل أو الكابلات البحرية البنية التحتية الأساسية التي تقوم عليها جميع أشكال الاتصالات عبر كامل الكوكب وهي العماد الرئيس الذي تتبني عليه اقتصاديات الدول، وسميت بالكوابل البحرية لأنها تصل بين مختلف البلدان والقارات من خلال تنصيبها في قاع البحار والمحيطات، ومن خلالها يتم نقل الكم المهول من مختلف البيانات والمعطيات، فالكوابل هي

⁽¹⁾ وسام كامل ياسين العقاد، مدى إمكانية استخدام تطبيقات الهاتف النقال في تطوير العمل (دراسة حالة عيادات وكالة الغوث في قطاع غزة)، رسالة ماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية، غزة، 2013، ص 29.

⁽²⁾ مريم ماضي، المرجع السابق، ص ص: 92-97.

⁽³⁾ علي بن عبد الله بن زيد الشيماني، أهمية استخدام الهواتف الذكية والحواسيب اللوحية في دعم تعلم اللغة الإنجليزية لدى طلاب المرحلة الثانوية، رسالة ماجستير في المناهج وطرق تدريس اللغة الإنجليزية، كلية التربية، جامعة أم القرى، المملكة العربية السعودية، الفصل الدراسي الثاني، 2013، ص 27.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

العمدة التي يستند إليها الفضاء الإلكتروني بكل مشتقاته، وهو الآلية الأكثر انتشار وتوظيفا في الاتصالات الدولية إذ بلغت نسبة الاعتماد عليها في ذلك إلى ما يجاوز 95 بالمائة من مجمل الاتصالات، وهذه النسبة في حقيقة الأمر تعود إلى ما لهذا الطريق وهذه الآلية من مزايا مقارنة بالأقمار الصناعية، فهي غير مكلفة وأكثر سرعة⁽¹⁾، وهناك العديد من أصناف الكوابل ويمكن تقسيمها على النحو الآتي:

1- الكابلات المزدوجة والمجدولة:

لقد بدأ استخدام هذا النوع من الكابلات من بداية عام 1852 في اطار الاتصالات التلغرافية البحرية، وهي كابلات تتكون من مجموعات ثنائية من الاسلاك النحاسية المغطاة ببلاستيك عازل وواقي وهي أسلاك ناقلة وملتوية ويبلغ سمكها ما بين 0.3 و 03 ملم، كما يوجد كابلات متعددة الأزواج أي أن هناك عدة أزواج تكوينية للكابل الواحد وسمكها عادة ما يكون من مضاعفات 25 مم، وتستخدم هذه الكابلات في القيام بعمليات الإتصال الهاتفية أو في أنظمة البيانات، مثل الأنظمة الشبكية المحلية محدودة النطاق والتي قد نجد انها مكونة أيضا من أزواج النحاس الملتوية سواء أكانت محمية أو غير محمية معدنيا وتكون حمايتها من أجل ضمان العزل الكهرومغناطيسي وتقادي الصخب أو غير ذلك من التفاعلات سواء من الوسط الذي تتواجد فيه إلى الكابل أو العكس⁽²⁾.

2- الكابلات المحورية:

هي كابلات تم استخدامها منذ ثلاثينيات القرن المنصرم، وهي كابلات تتكون من ناقل نحاسي مركزي يمثل النواة وسلك معدني آخر ذو الوظيفة التحصينية إذ يعمل كعازل كهربائي مع الغطاء المطاطي الذي يعمل بدوره على عزل المجموعة كاملة، كما يمكن العزل باستعمال البوليفينيل " PVC " والتفلون " Teflon "، وهذا من أجل العمل على نقل الإشارات الكهربائية التي تتكون من مجال عالي التردد وبصفة خاصة في اتصالات الهاتف والتلفاز الكابلي، وتتراوح سرعة نقل هذه الكابلات للبيانات ما بين 65 ألف كيلو بت و 200 مليون ميغا بت في الثانية⁽³⁾.

⁽¹⁾ هيئة تنظيم الاتصال، مسودة لائحة الكوابل البحرية، سلطنة عمان، مقدمة المسودة:

https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tra.gov.om/pdf/submarine-cables-regulation-ar.pdf&ved=2ahUKEwi04da1ppboAhV5AWMBHdJEAwUQFjAAegQIAhAB&usq__=AOvVaw0ANiCzMuhHrTbm4PPV2tMB

⁽²⁾ كمال عايد، تكنولوجيا الإعلام والاتصال وتأثيرها على قيم المجتمع الجزائري - الشباب الجامعي لتلمسان نموذجا - أطروحة دكتوراه ل.م.د، كلية العلوم الإنسانية والاجتماعية، جامعة أبي بكر بلقايد، تلمسان، السنة الجامعية 2016-2017، ص ص: 52-53.

⁽³⁾ المرجع نفسه، ص 53.

وتتسم الكابلات المحورية بالعديد من الخصائص، فهي تعمل على عزل (Gross talk)، أي تمنع من انتقال الإشارات غير المرغوبة عبر القنوات بشكل شبه كامل بحيث لا يكاد تذكر، كما أنه يعمل على حصر وتقليل التشوهات التي تصيب الإشارات والتي تترتب عن 03 تشوهات أساسية، أولهما هي تشوه الإتساع، وثانيهما هي تشوه في أطوار الموجات، وثالثهما هو تشوه التأخر، كما أن الكوابل المحورية يمكن حين إستغلالها أن نستغنى بها عن الأجهزة والمعدات التي تعمل على تقليل من تأثير الصدى⁽¹⁾.

3- الألياف الضوئية:

تعتبر تقنية الألياف البصرية أو الألياف الضوئية من أكثر التقنيات حداثة في مجال تكنولوجيا الإتصال، وو يتم توظيفها من أجل نقل البيانات والصوت وكذلك نقل الصورة، وهذا عن طريق اعتماد مسار متواصل ذو سعة كبيرة⁽²⁾، والألياف الضوئية هي عبارة عن حفنة من الشعيرات الزجاجية الدقيقة التي تسمح لأشعة الليزر بتجاوزها حاملة معها أشكال البيانات المختلفة بجودة عالية الدقة وبتزداد عالي⁽³⁾.

لقد كان أول استخدام للألياف الضوئية في المجال الطبي فقد كان على السبيل المثال تستعمل هذه الألياف لتوجيه نقطة ضوء نحو المعدة وتقوم بعدها ألياف أخرى بالنقاط الضوء المنعكس الذي يمكن الطبيب من إجراء فحوصات لأنسجة المعدة، ويتم استعمالها أيضا في إطار أشعة المنظار ويمكن تعريف الألياف الضوئية على أنها: (فن الإرشاد الفعال للضوء في مناطق فوق بنفسجية والضوء المرئي وتحت الحمراء للطف عبر ألياف شفافة خلال مسارات محددة مسبقا والألياف الضوئية عبارة عن قوائم (Stands) من الخيوط الزجاجية التي مير الضوء من خلالها عبر ترددات عالية جدا ويمكن لهذه الألياف أن تحمل الإشارات الصوتية والمرئية والبيانات)⁽⁴⁾.

الفرع الثاني: الطبقة المنطقية للفضاء الإلكتروني:

تعتبر الطبقة المادية للفضاء الإلكتروني غير ذات جدوى في غياب الجانب البرمجاتي الذي يجعل منها قابلة للاستغلال، وقد تعرض الدراسون والفقهاء والمختصون في البرمجة إلى محاولة

(1) محمد عبد الرحمن الحيدر، اتصالات الألياف البصرية، الطبعة الأولى، مكتبة العبيكان، الرياض، 1995، ص 20.

(2) كمال عايد، المرجع السابق، ص 53.

(3) وديع محمد العززي، التقنيات الحديثة للإنتاج التلفزيوني والعمل في القنوات الفضائية، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2021، ص 103.

(4) حسن عماد مكاوي، المرجع السابق، ص 133.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

لإيجاد تعريف ملائم لبرامج الحاسب الآلي فتعددت التعاريف بتعدد التخصصات ومجالات الدراسة (أولاً)، غير أنهم قد أجموا على ضرورة برامج الحاسب الآلي وبيئو في معرض ذلك كله التصنيفات الأساسية التي تندرج تحتها (ثانياً).

أولاً: تعريف برامج الحاسب الآلي:

تعتبر البرمجيات العماد الثاني الذي تقوم عليه البنية الإعلامية التكوينية لتكنولوجيا المعلومات والاتصال. وهي القاعدة الوظيفية المحورية واللبنة الأساسية التي يقوم عليها عمل الحاسب الآلي، حتى ذهب بعض الباحثين إلى التشكيك في قيمة الحاسب الآلي الذي يفتر إلى برمجيات، إذ تعتبره دون أي قيمة تذكر، وقد مثل البعض الآخر لأهمية البرمجيات بالنسبة للحاسب الآلي بالدور الذي يلعبه العقل بالنسبة للكائن البشري⁽¹⁾.

وتعرف البرمجيات على أنها: (مجموعة من الإيعازات والتعليمات التفصيلية المنظمة التي تسيطر على المكونات المادية للحاسوب في نظم المعلومات وتشتمل على برمجيات نظم التشغيل وبرمجيات التطبيق حيث يساهم في معالجة المعلومات تسجيلها وتقديمها كمخرجات مفيدة لأعداد العمل وإدارة التعليمات)⁽²⁾.

وتم تعريفها أيضاً على أنها: (مجموعة من التعليمات المعبر عنها بمفردات أو بدلائل أو بمخطوطات أو بأي شكل آخر والتي تمكن من القيام بنشاط علمي أو نوع آخر، أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم فاندفاعات إلكترونية أو أي أسلوب إلكتروني آخر أو ما يشبه ذلك شرط أن يكون صالحاً لمعالجة الإعلام)⁽³⁾.

كما تم تعريفه أيضاً بهذا النسق الموسع على أنه: (كافة العناصر غير المادية اللازمة للتعامل مع الجهاز ومجموعة البرامج والمناهج والقواعد وكافة الوثائق المتعلقة بتشغيله وبالتعامل مع المعطيات الموجودة بهدف المعالجة الآلية للمعطيات والبيانات)⁽⁴⁾.

أما من الناحية التشريعية، فقد تبني المشرع الأمريكي التعريف الضيق لبرامج الحاسب الآلي ويبرز ذلك من خلال إلقاء نظرة إلى الجانب الإصطلاحي الذي يعتمد عليه المشرع الأمريكي،

(1) أسامة بن بطو، حماية برامج الحاسب الآلي بين نظامي حقوق المؤلف وبراءة الاختراع، مذكرة ماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 (الحاج لخضر سابقاً)، السنة الجامعية 2014-2015، ص 07.

(2) نسيمه ضيف الله، المرجع السابق، ص 101.

(3) أسامة بن بطو، المرجع نفسه، ص 7.

(4) أكسوم عيلام رشيدة، المركز القانوني للمستهلك الإلكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص 105.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

فمصطلح " Computer Programs " المستعمل من قبل المشرع الأمريكي هو مصطلح محدد وضيق إذ حصر البرامج وحدها دون الملحقات والمستندات والوثائق وبرامج الدعم⁽¹⁾.

وعرفه المشرع الإماراتي على أنه: (مجموعة من البيانات والتعليمات والأوامر، القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة معينة)⁽²⁾، وقد عرفه أيضا القرار الوزاري المصري رقم 82 لعام 1993 على أنه: (مجموعة تعليمات يعبر عنها بأي لغة أو رمز متخذة في أي شكل من الأشكال يمكن استخدامها بطريقة مباشرة أو غير مباشرة في الحاسب لأداء وظيفة أو الوصول لنتيجة، سواء أكانت هذه التعليمات في شكلها الأصلي أو في أي شكل آخر تتحول إليه بواسطة الحاسب)⁽³⁾.

وعرفته اللائحة التنفيذية للكتاب الثالث من قانون الملكية الفكرية المصري رقم 82 لعام 2002، حقوق المؤلف والحقوق المجاورة لتاريخ 28 مارس 2005 على أنه: (مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة والتي تتخذ ضد أي شسكل من الاشكال ويمكن استخدامها بطريق مباشر أو غير مباشر في شكل آخر تظهر فيه من خلال الحاسب الآلي) وعرفه قانون حماية حق المؤلف العماني الصادر بموجب المرسوم السلطاني رقم 37/2000 بأنه: (مجموعة العبارات والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة والمعدة للاستعمال في الحاسب بطريقة مباشرة أو غير مباشرة بهدف التوصل إلى نتائج محددة) كما عرفه أيضا قانون المعاملات الإلكترونية العماني الصادر بموجب المرسوم السلطاني رقم 69 الصادر بتاريخ 17 مايو 2008 بأنه: (مجموعة معلومات إلكترونية أو تعليمات تستعمل بطريقة مباشرة أو غير مباشرة في نظم معالجة معلومات إلكترونية بغرض الوصول إلى نتائج محددة)⁽⁴⁾.

(1) أسامة بن يطو، المرجع السابق، ص 08.

(2) المادة الأولى من مرسوم بقانون اتحادي رقم 5 الصادر بتاريخ 13 أوت 2012 في شأن مكافحة جرائم تقنية المعلومات المعدل بموجب القانون الاتحادي رقم 12 الصادر بتاريخ 23 ماي 2016، الجريدة الرسمية رقم 540 ملحق ص 19، الإمارات العربية المتحدة.

(3) شامل سليمان عسله، الإشكالية القانونية للمحل في عقود إعداد البرامج الإلكترونية في التشريع المدني المصري والتشريعات المدنية المقارنة، حولية كلية الدراسات الإسلامية والعربية للبنات، المجلد الثاني، العدد 33، جامعة الأزهر، الإسكندرية، ص ص 259-296;

https://www.google.com/url?sa=t&source=web&rct=j&url=https://journals.ekb.eg/article_16901_d6876da755630c59ca01414470c26e27.pdf&ved=2ahUKEwj33_6NhsfoAhWnl-AKHTDmB80QFjAAegQIARAB&usq=AOvVaw0o30iPug75Ru0uPRZnLtl

(4) أحمد عبد الكريم موسى الصرايرة، الطبيعة القانونية لبرامج الحاسب الآلي في التشريع العماني: (دراسة مقارنة)، مجلة جامعة تكريت للحقوق، السنة 8، المجلد 3، العدد 29، كلية الحقوق، جامعة تكريت، العراق، آذار 2016، ص ص 308-326;

<https://www.iasj.net/iasj?func=issueTOC&isId=7073&uiLanguage=ar>

ويرى المشرع المغربي أن برامج الحاسب الآلي عبارة عن: (كل مجموعة من التعليمات المعبر عنها بكلمات، أو برموز أو برسوم أو أي طريقة أخرى - حينما تدمج في دعامة قابلة لفك رموزها بواسطة آلة - أن تنجز أو تحقق مهمة محددة أو تحصل على نتيجة بواسطة حاسوب أو بأي طريقة إلكترونية قادرة على معالجة المعلومات)⁽¹⁾.

وتم تعريفه من قبل المنظمة العالمية للملكية الفكرية " WIPO " على أنه: (مجموعة تعليمات يمكنها إذا نقلت على ركيزة بحسب نوعها أن تساعد في الوصول إلى نتيجة معينة عن طريق آلة يمكنها القيام بالتعامل مع المعلومة محل المراجعة) وذهب المشرع الفرنسي في تعريفها من خلال القرار الوزاري الفرنسي الصادر في 22 ديسمبر 1981 بأنها: (مجموعة من الخطوات والإجراءات التي تهدف إلى تشغيل نظام متكامل لأنظمة معالجة معلوماتية وتوظيفها وفقا للغرض الذي تم من أجله وضع نظام هذا البرنامج)⁽²⁾.

كما ذهب الكثير من الفقهاء في تعريفها مذهبين إثنين: أحدهما يضيق من دائرة التعريف بينما نجد ثانيهما يوسع فيها، فأصحاب المذهب الأول أجرو تعريف برامج الحاسب الآلي مجرى التقنيين والمختصين في مجال البرمجيات، وهذا حينما عرفوه على أنه: (تمثل بهذا ما يمكن أن نسميه بفكر الحاسب - تجاوز - فهي التي تحدد له العمليات المطلوب إنجازها وترتيب وكيفية الأداء، وبدورها لا يعدو الحاسب أن يكون مجموعة معدات إلكترونية وإلكتروميكانيكية عاطلة مثله مثل سيارة يعوزها من يقودها)، ويذهب الإتجاه الموسع في تعريفها إلى إلحاق وصف البرامج والمستندات الملحقة به إلى الوصف الضيق لبرنامج الحاسب، فجانبا من الفقه يرى أن الترجمة التي تعكس المعنى الدقيق والصحيح للكلمة الإنجليزية " Software " هي " الكيان المنطقي " للحاسب الآلي، وهذا الأخير يشتمل على مركبات عدة هي التي تبنيه وتهيكله والتي تتمثل بصفة أساسية في البرنامج بوصفه الجوهر الأساسي للطبقة المنطقية والوثائق اللازمة والمصاحبة للبرنامج، بالإضافة إلى البرامج المساعدة أو الداعمة، وباختصار فإن الحاسب الآلي في منظور المذهب الموسع في تعريفه يتكون من مجموع العناصر غير المادية⁽³⁾.

ونحن نميل بدورنا إلى الأخذ بالإتجاه الموسع في تعريف برامج الحاسب الآلي، ويعود ترجيحنا لهذا التعريف إلى كونه ذو أهمية كبيرة وبالغة في بسط الحماية على ملحقات وتوابع

(1) أكسوم عيلام رشيدة، المرجع السابق، ص 106

(2) شامل سليمان عسله، المرجع السابق.

(3) المرجع نفسه.

الحاسب الآلي، الامر الذي دعى إلى تبنيه في أغلبية التشريعات المرتبطة لحقوق الملكية الفكرية⁽¹⁾، وهو الأمر الذي يفترض أن يكون عليه في مجال حمايته في التشريعات المتعلقة بمكافحة الجريمة السيبرانية والإرهاب السيبراني.

ثانيا: أنواع برامج الحاسب الآلي:

تتقسم برامج الحاسب الآلي وفقا لوظيفتها على ساحة الفضاء الإلكتروني إلى 03 أقسام وهي:

1- برامج النظام:

تختص برامج النظم في الإدارة الكاملة لنظم الحاسب الآلي والأجهزة المحيطة به أيا كانت، فهو يعمل على قراءة ما يتم إدخاله إلى الجهاز ثم يقوم بترجمته وتأويله، كما يقوم أيضا بعملية إدارة الملفات والفهارس، ومن بين أشهر برامج التشغيل نجد برنامج " IBM " " International Bussiness Machine " وما يتوافق من برامج مع نظامها، وقد تجد الكثير من أنظمة التشغيل مبرجمة داخل الذاكرة الداخلية للحاسب الآلي وقد تجد أخرى منفصلة عنه تقتني بصفة منفردة على أقراص ممغنطة⁽²⁾.

فنظم التشغيل إذا هي عبارة عن مجموعة من التعليمات التي بموجبها يمكن للمستخدم أن يتحكم في كل ما ذكر آنفا بالإضافة إلى أنه يمكن التوفيق بين بقية برامج نظم المعلومات الأخرى، وعليه يجب أن تتوافق مع خصائص الجهاز الذي تنصب عليه والغرض من استخدامه، وفي كثير من الأحيان يثبت في الجهاز أكثر من نظام تشغيل واحد ليمنح لمستخدمه الخيار في نوع البرنامج المستخدم حسب ما يتطلبه عمله والمهام المرجوة من الجهاز⁽³⁾.

فبرنامج الحاسب الآلي هو الذي يعطي للحاسب تعليمات من أجل الأداء الأمثل لمهمته وليتم هذا المراد يجب على المستخدم أن يلتزم إختيار البرنامج الذي يتوافق مع نظام تشغيل جهازه إذ أن البرامج التطبيقية كثيرا ما تكون مصممة على أسس نظم التشغيل المختلفة ولا يمكن أن تؤدي

(1) أنظر في ذلك: عزة علي محمد الحسن، الحماية القانونية لبرامج الحاسب الآلي، الطبعة العربية الأولى، دار الجنان للنشر والتوزيع، الأردن، 2011، ص 26.

(2) سهيلة خطابي، مقاهي الإنترنت بقسنطينة ودورها في التنمية العلمية والثقافية للمجتمع، مذكرة ماجستير في علم المكتبات، كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة منتوري، قسنطينة، السنة الجامعية 2008-2009، ص 44.

(3) أنظر في ذلك: علاء عبد الرزاق السالمي، المرجع السابق، ص 70.

مهمتها إلا على ذلك النظام الذي برمجت عليه، فهي تكتب بلغات برمجية عديدة، ولكل لغة منها ما يميزها عن غيرها من لغات البرمجة والتي تجعلها تؤدي أنواع معينة دون سواها⁽¹⁾.

2- البرامج التطبيقية:

يتمتع هذا النوع من البرامج بالاستقلالية عن أنظمة تشغيل الأجهزة، ويتم إقتاؤها من الشركات بعزل عن الحواسيب والأجهزة، أو قد ترد معها، وفي كل الأحوال، لا يمكن لهذه البرامج إلا أن تعمل على الجاهز، فاستقلاليتهما تكون نسبية، -إذا لا مناص من اقترانها بجهاز أو نظام-⁽²⁾ فبرامج التطبيقات في حقيقتها هي برامج تحقق لمستخدمها نوعا من الاستفادة عند قيامه بأي عمل، إذ تعمل على تحقيق بعض المهام التي برمجت على أدائها⁽³⁾، ويتم برمجتها بوحدة من اللغات ذات الرتبة والمقام العالي⁽⁴⁾.

4- برامج الاتصال وبرامج تشغيل الشبكة:

هي برامج تُعنى بالتحكم في شبكات الكمبيوتر وتقوم بترتيب المعلومات عن طريق وحدات متخصصة يتم بوجها التعرف على كل عناوين الأجهزة على الشبكة، بما في ذلك عناوين الوحدات الطرفية المتصلة مثل الطابعات ووحدات التخزين عالية القدرة، كما ترسل وتستقبل الإشارات المختلفة، ولها قدرة إدراكية للمشاكل والأعطال الموجودة حيث لا تقوم بإرسال أي إشارة لجهاز لا يستقبلها كما تنظم أيضا مسارات الأوامر في الأسلاك بطريقة تجعلها غير قابلة للاختلاط ولا لتضيق المعلومات المرسل، إليها من أجهزة أخرى، ومن أشهر هذه البرامج نجد برنامج " windows " ⁽⁵⁾.

⁽¹⁾ علاء عبد الرزاق السالمي، المرجع السابق، ص: 70-71.

⁽²⁾ أسامة سمير حسين، ثورة الحاسوب والاتصالات، الطبعة الأولى، الجنادرية للنشر والتوزيع، الأردن، 2012، ص 132.

⁽³⁾ عمر أحمد أبو هاشم الشريف، أسامة محمد عبد العليم، هشام محمد بيومي، الإدارة الإلكترونية: (مدخل إلى الإدارة التعليمية الحديثة)، الطبعة الأولى، دار المناهج للنشر والتوزيع، الأردن، 2013، ص 96.

⁽⁴⁾ أيمن عبد الله فكري، الجرائم المعلوماتية: (دراسة مقارنة في التشريعات العربية والأجنبية)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2014، ص 65.

⁽⁵⁾ سهيلة خطابي، المرجع السابق، ص 45.

الفرع الثالث: شبكات الحاسب الآلي:

إن أول بوادر ظهور الفضاء الإلكتروني قد بدأت مع بداية ظهور التلاقي والترابط بين تكنولوجيا المعلومات وتكنولوجيا الاتصال عبر نظام شبكي يصل بين مختلف الأجهزة المعلوماتية ليكون وحدات تربط بينها بروتوكولات متخصصة من خلالها يمكن لأي شخص في أي مكان التواصل ونشر وتلقي المعلومات والموارد(أولاً)، وقد تمكنت هذه الهيكلية من توفير خدمات وأنشطة كثيفة تلبي جانباً كبيراً من إنتاجيات الأفراد والمؤسسات كما فتحت بوابات تواصل وبحث منخفضة التكلفة وعالية الكفاءة والدقة والسرعة(ثانياً).

أولاً: الشبكات المعلوماتية:

يمكن أن نعرف الشبكة المعلوماتية على أنها: (ارتباط بين مجموعتين أو أكثر من البرامج ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات)⁽¹⁾، وهي تنقسم إلى نوعين أساسيين هما:

1- الشبكة المحلية: « LAN » Local Area Network:

الشبكة المحلية هي الشبكة التي تتربط فيها الحواسيب بكوابل وأسلاك خاصة ضمن نطاق مكاني ضيق، عادة ما تكون في مبنا واحد، أو بين الحواسيب في مباني متقاربة جغرافياً، إذ يتم تركيبها بحيث تسمح للمشاركين في هذا الترابط مشاطرة مختلف الوازم والمعدات مثل تلك المتعلقة بالأعمال الإحصائية وبرامج المعالجة المختلفة، والبرامج التطبيقية، ومشاركة قواعد البيانات والطابعات عالية الجودة⁽²⁾.

ويتميز هذا النوع من الشبكات بالتشاركية حيث يمكن لأي حاسب أو جاهر مرتبط بهذه الشبكة الإطلاع على مضامين القرص الصلب لجهاز آخر ضمن دائرتها، كما يمكن ضمن هذه الشبكة إطلاق عملية الطباعة من جهاز العمل إلى جهاز آخر، وتعتمد الأجهزة في هذه الشبكة على نظام تشغيل موحد⁽³⁾.

(1) المادة الأولى من مرسوم بقانون اتحادي رقم 5 الصادر بتاريخ 13 أوت 2012 في شأن مكافحة جرائم تقنية المعلومات المعدل بموجب القانون الاتحادي رقم 12 الصادر بتاريخ 23 ماي 2016، الجريدة الرسمية رقم 540 ملحق ص 19، الإمارات العربية المتحدة.

(2) بدر الدين بلمولاي، استعمال تكنولوجيا الإعلام والاتصال الحديثة في العلاقات الإجتماعية: دراسة ميدانية بجامعة بسكرة حلو استخدام الانترنت والهاتف النقال في اختيار الزوج -، مذكرة ماجستير في علوم الاعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، السنة الجامعية 2011-2012، ص 50.

(3) محمد نبهان سويلم، مدخل إلى علوم الحاسب، الطبعة الأولى، المكتبة الأكاديمية، مصر، 2001، ص 94.

2- الشبكة الواسعة: « WAN » Wide Area Network:

هي شبكات تعمل على الوصل بين مختلف الشبكات المحلية المتباعدة فيما بينها عن طريق الإستعانة بأجهزة التوجيه والروابط المتخصصة في نقل البيانات المرقمنة، ولذلك تعتبر هذه الشبكات ذات طابع عالمي فهي تتفرع لتربط بين البلدان والقارات، وتعتبر شبكة الإنترنت أحسن مثال لمثل هذا الترابط الشبكي العالمي⁽¹⁾.

ثانيا: الشبكة العالمية للإنترنت:

يجب الإقرار أن الإنترنت قد أصبح في العصر الحاضر الظاهرة الأكثر إنتشارا على نطاق غاية في الإتساع والوسيلة الإعلامية والإتصالية الأكثر حداثة وتأثيرا في هذا التنامي الكبير والطفرة الإتصالية الكبرى التي يشهدها هذا القرن، لقد إستطاع الإنترنت أن يجمع شتات البشرية ويصنع آليات تمكنهم من الترابط في ما بينهم، مع ضمان السرعة الفائقة وسدة الضخامة وقمتها مع الشمولية التامة لجميع فروع حياتنا ومناحيها، وقد إستطاع بكل جدارة أن يغير من طرق تفكيرنا وتواصلنا مع الآخرين وأحدث تحولات كبرى في مناهجنا الأمر الذي يوضح التأثيرات الكبرى التي يحدثها رواده من صناعي الشبكات ومطورها في قيادة النظام الدولي الجديد وصياغة ثقافته وتوجيه سياساته والتحكم في إقتصادياته، كما أنهم يملكون القدرة الكافية للتأصر على وسائل الإعلام التقليدية ومناهجها وطرق تحليلها⁽²⁾.

يعرف الإنترنت على أنه: (شبكة ضخمة من الكومبيوترات المتصلة في ما بينها وهي الأكبر في العالم كما أنها مفتوحة للجميع وكل شخص مساعد لدفع مبلغ شهري ثمنا للاتصال بالشبكة عن طريق مزودي الخدمات الهاتفية يمكنه أن ينظم إلى ملايين المستخدمين على الإنترنت)، ويعرف أيضا على أنه شبكة معلوماتية عالمية تتصل فيها مجموعات كبيرة من الشبكات المحلية بالإستعانة بآليات وصل خاصة بحيث تفتح المجال لتبادل المعلومات فيما بينها من خلال مجموعة من الأجهزة الحاسوبية المركزية التي تملك قدرة عالية على حفظ المعلومات والتحكم في الشبكات والتي يطلق عليها اسم الخوادم، وهناك من عرفها من الدارسين على أنه: (عبارة عن حاسب آلي يتحدث إلى حاسب آلي آخر يرتبطان بواسطة سلك التلفون العادي أو أي نوع آخر من الكوابل، وإذا كانت الحواسيب موجودة في أماكن بعيدة ومتفرقة فيمكن إستخدام الأقمار

(1) بدر الدين بلمولاي، المرجع نفسه، ص 51.

(2) كمال عايد، المرجع السابق، ص ص: 72-73.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

الصناعية للربط بينها لتحقيق بذلك الاتصال الدولي عبر الإنترنت وحتى داخل الدولة ذاتها تعتمد شبكة الإنترنت على الوصلات الوسيطة بين نقطتين⁽¹⁾.

ويذهب برنامج التنمية التابع للأمم المتحدة الصادر بتاريخ 1994 في تعريفه بأنه: (شبكة اتصال دولية تتألف من مجموعة من شبكات المومبيوتر تربط بين الآلاف من مختلف شبكات الكومبيوتر في العالم، وتؤمن الاشتراك لملايين المستخدمين من مختلف دول العالم وتتيح إمكانية الارتباط والوصول إلى الشبكة)⁽²⁾.

ويعرف أيضا على أنه: (أشهر وسيلة معلوماتية تفاعلية، وهي عبارة عن شبكة تواصل ضخمة تضم بداخلها مجموعة كبيرة من الشبكات الفرعية المعلوماتية العمومية والخاصة التي تتصل ببعضها وهي تتكون من من معدات تقنية تتمثل في خطوط الاتصال الهاتفي وخطوط الكوابل والألياف الضوئية وكذلك الأقمار الصناعية دون أن ننسى البرمجيات التواصلية من ويب وبريد إلكتروني بالإضافة إلى العامل البشري الذي يتمثل في مديري الشبكات ومنتجي الخدمات الإلكترونية)⁽³⁾.

ويعود هذا الاختلاف والتعدد والتباين في تعريف الإنترنت إلى تبني هذه التعاريف للنسق الوظيفي لصاحبها، فالتعريف يكون قائما في أساسه على الوظيفة التي يقوم بها مقدمه أو مقترحه، فالتعريف الذي يقدمه متخصص في مجال مهني معين يختلف عن التعريف الذي يقدمه مهندس متخصص⁽⁴⁾.

تتكون شبكة الإنترنت العالمية من حوالي خمسين ألف شبكة ممتدة التأثير على نحو 60 مليون مستخدم حسب إحصائية قديمة تعود إلى شهر ديسمبر 1995، وهذه الشبكة تستطيع أن تجمع آليات المعرفة ما يغني به المستفيد عن غيرها، كونها تقدم له كل ما تقدمه الوسائل التقليدية مجتمعة، كما تخول له فرصة وضع يده على معلومات لم يكن قطعا من الممكن له أن يصل إليها نظرا لعوامل جغرافية وسياسية واجتماعية، وهي رغم ترابطها إلا أنها تعتبر شبكة منفصلة في جانب الإدارة، فالشبكات تدار بشكل إنفرادي بعيدا عن المركزية، فالشبكات تعتمد في تشغيلها

⁽¹⁾ صافية أمينة، آثار استعمال التكنولوجيا الحديثة على أفراد الأسرة الجزائرية، دراسة للتأثيرات النفسية والاجتماعية والأخلاقية والصحية لاستعمال الإنترنت على أبناء الأسرة الجزائرية نموذجا (دراسة على عينة مراقبين مستخدمة للإنترنت بمدينة أم البواقي، أطروحة دكتوراه في علم النفس الأسري، كلية العلوم الاجتماعية، جامعة وهران 02، محمد بن أحمد، السنة الجامعية 2015-2016، ص 26.

⁽²⁾ نقلا عن: رابح عمار، الصحافة الإلكترونية وتحديات الفضاء الإلكتروني، دراسة ميدانية للصحافة الإلكترونية الجزائرية، أطروحة دكتوراه في

علوم الإعلام والاتصال، كلية العلوم الانسانية والعلوم الإسلامية، جامعة أحمد بن بلة، وهران 01، السنة الجامعية 2016-2017، ص 73

⁽³⁾ كمال عابد، المرجع سابق، ص ص: 73-74.

⁽⁴⁾ أنظر: صافية أمينة، المرجع السابق، ص 27.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وإدارتها على شكل إنفرادي يصل إلى عدم تطابق المناهج والتقنيات والآليات المستعملة من شبكة إلى أخرى، فالعلاقة الوحيدة بين الشبكة العالمية للإنترنت والشبكات الأخرى هي كون هذه الأخيرة تتصل فيما بينها وتترابط من خلال بوابات إلكترونية تدعى البروتوكولات⁽¹⁾.

لقد ظهر الإنترنت خلال خمسينيات القرن المنصرم حيث تم اختراعه من أجل تقديم التعزيزات إلى جيش الولايات المتحدة الأمريكية من خلال خلق نظام معلوماتي يلبي حاجياتها الخاصة مع ضمان الحماية والأمن، فتم تأسيس وكالة مشاريع البحث المتطورة سنة 1958 من قبل الحكومة الأمريكية لتقديم إسهامات كبرى في مجال البحوث والدراسات المتقدمة المتعلقة بالحاسب الآلي والعلوم المتعلقة به بالإضافة إلى دراسات في مجال الاتصالات عن بعد، وكان هدفها الأساسي هو تطويع تقنيات الحاسوب وأجهزته لخدمة الأنشطة العسكرية التابعة للجيش الأمريكي⁽²⁾.

ثم بعد ذلك تم إنشاء أول شبكة توزيع عرفت باسم " أربانت " وذلك سنة 1969 وتشمل جملة من الأنظمة التي تعمل عن طريق التحكم عن بعد، ويتحكم كل نظام من تلك الأنظمة في شيء من المعلومات الأساسية⁽³⁾، و " أربا نيت " أو " أربا " هو إختصار للعبارة الواردة باللغة الإنجليزية (The Advanced Research Prohct Administatuion) وصممت بطريقة أطلق عليها اسم طريقة إعادة التوجيه الديناميكي (Dynamic Rerouting) حيث يتم تشغيل الشبكة تشغيلاً مستمراً في "حالة انقطاع إحدى الوصلات أو تعطلها عن العمل، حيث تقوم الشبكة بتحويل الحركة إلى وصلات أخرى" وكان الغرض الأساسي من هذا كله هو لوصول بين الإدارة ومتعهدي القوات المسلحة وعدد كبير من المعاهد والجامعات التي تقوم بأبحاث ممولة من قبل القطاع العسكري الأمريكي⁽⁴⁾.

ثم عام 1987 قامت وزارة الدفاع بحويل أمر تسيير هذا المجال إلى المؤسسة العلمية الوطنية " NSF " وذلك بسبب التكلفة المالية للإنترنت فحل بذلك محل وكالة " أربانيت "، وفي عام 1990 شهد العالم تهاافتاً كبيراً من قبل المتخصصين وذوى المهارات والخبرات في مجال برامج الكمبيوتر وقد ساعدت التكلفة المنخفضة للحواسيب الشخصية على إنتشار الإنترنت على نطاق واسع وأصبح يستخدم في منازل الأفراد والمؤسسات التجارية والمداري والمعاهد التعليمية

(1) صافية أمينة، المرجع السابق، ص ص: 25-26.

(2) كمال عايد، المرجع السابق، ص 74.

(3) المرجع نفسه، ص 74.

(4) رايح عمار، المرجع السابق، ص 75.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

ومن حينها غدت هذه الآلية الإتصالية شبكة ذات طابع عالمي، إذ تحول إلى آلية أساسية لصناعة الخبر ونقله حيث أصبح نظاما إتصاليا جماهريا منقطع النظير، فصلا عما تقدمه من خدمات إستراتيجية في ميادين مختلفة⁽¹⁾، ويقوم الإنترنت بإسداء الكثير من الخدمات المتنوعة التي من بينها:

1- خدمة البريد الإلكتروني:

يعتبر البريد الإلكتروني من أهم الخدمات التي يتقدمها شبكة الإنترنت وأكثرها شهرة واستعمالا، وقد تم إنشائه عام 1971 من أجل تناقل الرسائل على الشبكة الإلكترونية من شخص إلى آخر، ولعل ما نال به شهرته سرعته الفائقة في نقل الرسائل بين أطرافها في مختلف أنحاء العالم مع ضمان عدم تعرضها للضياع بالإضافة إلى تمتعه بجملة من المزايا الأخرى كإمكانية حفظ الرسائل في مجلدات خاصة بها كما يمكن إعادة إرسالها ومعاينتها، كما يتسم أيضا بجانبه التفاعلي⁽²⁾.

2- خدمة بروتوكول نقل الملفات:

يمكن تعريف هذه الخدمة على أنها: (برنامج متخصص بنقل الملفات والوثائق ذات الحجم الكبير بسرعة وكفاءة أكبر مما يوجد على صفحات (الويب) العادية)⁽³⁾.

يتم استخدام هذه الخدمة عند القيام بتبادل أشكال الملفات المختلفة بين الحواسيب، إذ يمكن من خلاله الإتصال بأي جهاز من الأجهزة الآخر إذ يسمح هذا البرتوكول بالإتصال بأي جهاز آخر متصل بشبكة الإنترنت ونقل الملفات إنطلاقا منه إلى الحواسيب الشخصية، وهو بذلك يمنح للمستخدم إمكانية طبع المعلومات من حواسيب أجنبية⁽⁴⁾.

3- خدمة الإتصال المباشر:

توفر شبكة الإنترنت لعملائه آليات ونوافذ تمكنهم من الإستفادة منه كوسيلة للإتصال مباشرة بين بينهم وبين غيرهم من العملاء سواء أكانوا أفرادا أو مؤسسات مع قلة التكاليف خاصة في

(1) كمال عابد، المرجع السابق، ص 74.

(2) أحمد ضيف، تكنولوجيا المعلومات والاتصال كمدخل لتفعيل إدارة التغيير بالمؤسسة الاقتصادية: حالة المؤسسة الجزائرية (مجمع اتصالات الجزائر نموذجا)، أطروحة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة أبي بكر بلقايد، تلمسان، السنة الجامعية 2012-2013، ص 91.

(3) أبو بكر محمود الهوش، أدوات البحث عن المعلومات في البيئة الرقمية، الطبعة الأولى، دار حميثرا للنشر، مصر، 2018، ص 122.

(4) أحمد ضيف، المرجع نفسه، ص 92.

الاتصالات التي تخرج عن إطار المنطقة الهاتفية، وتتخذ هذه النواذ التي يوفرها الإنترنت عدة أشكال منها ما هي نصية كخدمة الشات " CHAT " أو صوتية أو المحاورات المدعومة بالوسائط المتعددة أين تكون العملية الإتصالية صوت وصورة⁽¹⁾.

4- خدمة Ghopher:

هي آلية كان قائمة قبل ظهور الويب حيث تم وضعها في جامعة " مينيسونا " ثم توسعت بعد ذلك، وتعتبر هذه الخدمة ذات أهمية كبيرة في الوصول إلى المعلومات وبلوغ خدمة الإنترنت حيث يعرض قائمة رئيسية لاختيار مزودا من بين المزودين، وكذلك من أجل البحث والتصفح وتحميل الملفات والمعلومات وهو في الأصل عبارة عن برنامج بروتوكول يجمع بين العديد من الخدمات منها " WAIS , TELNET, FTP " ⁽²⁾.

الفرع الرابع: الطبقة الإعلامية للفضاء الإلكتروني:

يعد الفضاء الإلكتروني الثمر الأكثر تقدما وتطورا وتنظيما التي تمكن الإنسان المعاصر من التوصل إليها في ميدان تقنية المعلومات والاتصال وهي دائمة في حركة دؤوبة وتطور مستمر من أجل خلق أفق جديد في خدمة البشرية وتحقيق الرفاهية وتمكين إنسان القرن العشرين من استغلال كافة القدرات والموارد التي يمتلكها (أولا) حتى غدى المجتمع المعاصر مجتمعا معلوماتيا من الدرجة الأولى فالمعلومات في هذا القرن أصبحت المورد الأكثر حيوية والأبلغ أثرا في حركة التنمية والتقدم الحضاري والرقى الإنساني^(ثاني).

أولا: مجتمع المعلومات كطبقة بشرية في تكوين الفضاء الإلكتروني:

يعود إصطلاح "مجتمع المعلومات إلى فترة الثمانتنيات من القرن العشرين ويحمل بين طياته مدلولاً جديد للتعبير عن الحالة التي آل إليها المجتمع المعاصر في ظل بروز مفهوم الفضاء الإلكتروني⁽³⁾، فمجتمع المعلومات يحمل في مضمونه واقع العلاقة بين الإنسان

(1) أحمد ضيف، المرجع السابق، ص 92.

(2) خيرة روابحي، البحث الوثائقي ولغات الوثائق في البنية الرقمية (دراسة ميدانية حول استخدام ادوات البحث ونماذجه في الواب من لدن اساتذة جامعة تيارت: مقارنة وصفية تحليلية)، أطروحة دكتوراه في علم المكتبات والعلوم الوثائقية، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة أحمد بن بلة، وهران 01، السنة الجامعية 2018-2019، ص 42.

(3) محمد العوض محمد وداعة الله، مواقع التواصل الاجتماعي وقضايا الشباب الجامعي، الطبعة الأولى، دار الخليج للنشر والتوزيع، الأردن، 2020، ص 77.

المعاصر وأساليب تعاطيه مع المواضيع والنشاطات المختلفة لحياته وبين التكنولوجيات المعلوماتية المعاصر⁽¹⁾.

وجدير بالذكر أن تعريف مجتمع المعلومات لم يتوفق عليه الفقهاء والدارسين ونحن قد إرتأينا أن نورد هذه التعاريف نظرا لكونه مطابقة لأغراض هذه الدراسة. فيعرف على أنه: (المجتمع الذي ينشغل معظم أفرادها بانتاج المعلومات أو جمعها أو تخزينها أو معالجتها أو توزيعها) أو هو: (المجتمع الذي يعتمد في تطوره بصفة رئيسية على المعلومات والحاسبات الآلية وشبكات الإتصال، أي أنه يعتمد على التقنية الفكرية، تلك التي تضم سلعاً وخدمات جديدة مع التزايد المستمر للقوة العاملة بالمعلومات التي تقوم بانتاج هذه السلع والخدمات وتجهيزها ومعالجتها ونشرها وتوزيعها وتسويقها)⁽²⁾.

فالطبقة البشرية إنما هي جزء من الطبقة الإعلامية أو المعلوماتية لأنها ببساطة هي الطبقة التي تنتج المعلومات، وهي في نفس الوقت المستفيدة منها، وحتى الفضاء الإلكتروني كله، بجميع طبقاته السابقة واللاحقة إنما هي نتاج العقل البشري، فلولاً الطبقة البشرية لما كان هناك فضاء إلكتروني أصلاً، فضلاً عن كون العنصر البشري هو المستفيد في النهاية من هذا الفضاء.

لذلك يمكن تقسيم العنصر البشري كطبقة تكوينية للفضاء الإلكتروني إلى قسمين إثنين، أولهما القسم المنتج أو المشرف، فهذا القسم إنما يعمل على بناء هذا الفضاء الإلكتروني في طبقاته، ويديره ويشرف عليه، ويعنى بجانبه التنظيمي، ويشمل هذا القسم كل من منتجي العتاد، والمبرمجون، وصانعي المادة الإعلامية، ومقدمي الخدمات وما إلى ذلك من الأمثلة.

أما القسم الثاني فهو قسم يمثل الشريحة الكبيرة في مجتمع المعلومات، ألا وهم المستهلكون، أو المستفيديون، الذين يستفيدون من الخدمات والمزايا التي يقدمها الفضاء الإلكتروني، ويستوى في ذلك الأشخاص الطبيعية، أو حتى الأشخاص المعنوية.

ثانياً: البنية المعلوماتية:

1- تعريف المعلومات:

يختلف تعريف المعلومات تبعاً لتصور كل باحث أو مفكر، ففي الحين الذي يرى فيه بعض الباحثين أن المعلومات هي في أصلها بيانات أخذت شكلاً مفهوماً بعد أن تمت تسويتها والتعامل

⁽¹⁾ أنظر: نور الدين بن سولة، مجتمع المعلومات في الوطن العربي، مجلة جيل العلوم الإنسانية والإجتماعية، العدد 39، مركز جيل البحث العلمي، الجزائر، فبراير 2018، ص: 55-62: <https://jilrc.com/>مجتمع-المعلومات-في-الوطن-العربي-بن-سول/

⁽²⁾ منال محمود كريم حموري، أثر الثورة المعلوماتية وثورة الاتصالات على التحولات السياسية والأمنية في المنطقة العربية 2010-2017: (الأردن حالة دراسة)، رسالة ماجستير في العلوم السياسية، كلية الآداب والعلوم، جامعة الشرق الأوسط، أيار 2018، ص 42.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

معها بتقنيات المعلومات، بحيث يكون للمتعاطي معها والوقت الذي تتناسب معه، والمكان الذي تعرض فيه، والوضائف التي تشغل فيها والازمات التي قد تواجهه، دورا مهما واعتبارا خاصا، يرى البعض الآخر أنها بأنها تلك البيانات التي تتخذ شكلا يمكن من خلاله للشخص إسياعها فيه، وتتعكس على القدرة الإستيعابية للمستفيد منها، كما يراها البعض الآخر أيضا على أنها: (مجموعة بيانات منظمة بهدف إصدار أو إيصال رسالة غالبا ما تكون في شكل ملموس (مصورة، مكتوبة) أو شفوية، طريقة تنظيم هذه المعطيات تكون طبقا لرغبة المستقبل لها، فالمعلومة إذن تحدث نظرة جديدة تجاه الأحداث والأشياء الملموسة وغير الملموسة)⁽¹⁾.

وعرفها ديفيس وأولسون بطريق أكثر إتساعا حين قال بأنها: (بيانات تمت معالجتها وتحويلها إلى صيغة مفيدة ذات معنى بالنسبة إلى المتلقي، ولها قيمة حقيقية أو متصورة في الأفعال أو القرارات الحالية أو المحتملة)⁽²⁾.

وعرفت أيضا على أنها: (الخبرة المشاهدة، المساعدة على اتخاذ القرارات، وهي في الأصل المعرفة المدركة بواسطة أشخاص، وتملك اليوم أهمية كبيرة في مراقبة التسيير)⁽³⁾.

فالمعلومات رغم اختلاف الباحثين وتباينهم في تعريفها إلا أنها تحمل مدلول واحدا في نظرنا، وهو القدرة إلى إفادة المتلقي أو المستفيد بواقعة أو نبأ أو حقيقة أو حادث بشكل يمكن معه أن يدركه ويستعييه ويتأقلم معه ضمن مقتضيات وملبسات واقعه وزمانه ومكانه ومجال تخصصه، فالمعلومة الكمائية مثلا تكون معلومة عندما يلتقها المتخصص فيها، لكن عندما يتلقها رجل القانون مثلا فهي بالنسبة له دون أي معنى، فالمعلومات متعلقة بالمدرجات، وبانتقاء الإدراك ينتفي العلم وتتنتفي معه صفة المعلوماتية.

2- خصائص المعلومات:

تمتلك المعلومات خصائص متعددة تميزها عن غيرها من المفاهيم والمسائل المشابهة لها كالبيانات والمعرفة، وبالنظر إلى الطبيعة التركيبية وإلى وقع المعلومات وأثرها في المجتمعات يمكن أن نحدد أكثر من هذه الخصائص، ويمكن جمعها وترتيبها وفق ثلاث مجموعات هي:

(¹) أنظر: ياسع ياسمينه، دراسة إقتصادية قياسية لأثر تكنولوجيا المعلومات والاتصالات على الأداء الاقتصادي للمنظمة - دراسة حالة شركة القطن الممتص " SOCOTHYD "، مذكرة ماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية، جامعة أحمد بوقرة، بومرداس، السنة الجامعية 2010-2011، ص 49.

(²) ميكيل هيل، أثر المعلومات في المجتمع: دراسة لطبيعتها وقيمتها واستعمالها، مركز الإمارات للدراسات والبحوث الإستراتيجية، الإمارات العربية المتحدة، الطبعة الأولى، 2004، ص 25.

(³) جودي سامية، مساهمة نظم المعلومات الحديثة في إعادة الهندسة بالمؤسسة الاقتصادية الجزائرية: (دراسة حالة مؤسسة اتصالات الجزائر)، أطروحة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد خيضر، بسكرة، السنة الجامعية 2016-2017، ص 86.

أ- القيمة التصاعدية:

إن قيمة المعلومات ليست جامدة، فهي تتصاعد بتصاعد وإزدياد بعض العوامل، ومن أهم تلك العوامل زادة الإستخدام، فالمعلومات تكتسب قيمتها من كثرة مستخدميها، فكلما زاد استخدامها زادت معه قيمتها، كما أن قيمة المعلومات مرهونة أيضا بدقتها، فكلما كانت المعلومات دقيقة كلما كانت قيمتها ونفعها أكثر إزديادا، وتتصاعد أيضا قيمتها عندما تضم إلى غيرها من المعلومات، وهذه الخاصة إنما هي تجسيد لخاصة قابلية المعلومات للمشاركة، فلما كانت مشاركتها أوسع، كلما كانت قيمتها أكثر، ومع ذلك تبقى المعلومات قابلة للتلف والإندثار، وهذا مرهون بالقيمة التي تحملها مفردتها، وفي مدى صياغتها في قالب عملي، كما أن معظم المعلومات لا تتسم باليقين التام، إلا أنه ذلك لا يشكل قرينة على عدم كفايتها وصحتها ودقة أجهزة جمعها ونقاء مسارات تبادلها⁽¹⁾.

ب- خاصية المرونة:

تتجلى لنا مرونة المعلومات من خلال قابليتها للتميع والتشكل في العديد من القوالب، فهي قادرة على أن تتخذ العديد من الأشكال والصور، كما تظهر لنا أيضا مرونتها من خلال قابليتها للنقل عبر العديد من المسارات المختلفة والآليات والطرق المتنوعة، بالإضافة أيضا إلى سهولة ويسر عملية نسخها بالعديد من الوسائل والوسائط السهلة والميسرة⁽²⁾.

ج- سعة تقنيات المعلومات ووفرتها:

لقد غدت المعلومات وتقنياتها أساسا تقوم عليه التنمية والإزدهار في العديد من المجالات الحيوية، وهي تتميز بالوفرة والفيض، لذلك يعمل أصحابها على تقييدها وضبطها بقانون العرض والطلب⁽³⁾.

(1) أنظر في ذلك:

- ليث عبد الله القهوي، زياد كامل اللالا، بلال محمود الوادي، جودة المعلومات والذكاء الاستراتيجي في بناء المنظمات المعاصرة، الطبعة الأولى، دار ومكتبة الحامد للنشر والتوزيع، الأردن، 2013، ص: 85-88.

- أنظر كذلك: السعيد مبروك إبراهيم، المعلومات: (ودورها في دعم واتخاذ القرار الاستراتيجي)، الطبعة الأولى، المجموعة العربية للتدريب والنشر، مصر، 2012، ص: 23-26.

- أنظر أيضا: عبد الله حسن، إدارة المعرفة وتكنولوجيا المعلومات، الطبعة الأولى، دار المعتر للنشر والتوزيع، الأردن، 2015، ص: 108-111.

(2) أنظر في ذلك المراجع السابق بنفس الصفحات لـ:

- ليث عبد الله القهوي، زياد كامل اللالا، بلال محمود الوادي، المرجع السابق.

- أنظر كذلك: السعيد مبروك إبراهيم، المرجع السابق.

- عبد الله حسن، المرجع السابق.

(3) المراجع نفسها، نفس الصفحات.

2- أنواع المعلومات:

يرتبط تقسيم المعلومات وتصنيفها بالمجال الدراسي أو الوظيفي الذي تنتمي إليه، فليس هناك تقسيم واحد لأنواع المعلومات، وقد أحصينا عشرات التقسيمات في خضم بحثنا، وارتضينا تقسيمها لأغراض هذه الدراسة على النحو الآتي:

أ- المعلومات باعتبار أصحابها:

و هي المعلومات الشخصية والموضوعية التي يطلق عليها اسم المعلومات الإسمية، وهي التي ترتبط بالأفراد والتي أشار إليها القانون الفرنسي رقم 17 المتعلق بالمعلوماتية والحريات الصادر بتاريخ 6 يناير 1978 في نص مادة الرابعة بأن: (المعلومات تكون إسمية إذا كانت تسمح مباشرة أو غير مباشرة، وتحت أي شكل بالتعرف على الشخص محل هذه المعلومات، أو تجعله قابلاً للتعرف عليه)، فالمعلومات الإسمية إذا تتكون من نموذجين من المعلومات والذي يمثل أولهما المعلومات الشخصية وهي تلك المرتبطة بالجانب الخصوصي للفرد، وثانيهما هي المعلومات الموضوعية وهي المعلومات التي تعبر عن الفرد بكونه كائناً عاقلاً له توجهات وآراء يمكن له أن يبديها للناس⁽¹⁾.

3- المعلومات باعتبار حمايتها:

أ- معلومات محمية:

يتم حماية المعلومات في الغالب بالملكية الفكرية، والملكية الفكرية تعتبر ثمرة العقل البشري ونتاجاً لإبداعه الفني وغيره من الإبداعات التي تتمخض عن قريحة عقله، وبمعنى آخر هي: (كل أعمال الفكر الإبداعية من اختراعات ومصنفات أدبية وفنية ورموز وأسماء وصور ونماذج ورسوم صناعية)، وهي على قسمين، حقوق متصلة بالإبداع الصناعي، وأخرى متصلة بالإبداع الأدبي والفني⁽²⁾، وهي معلومات يملك أصحابها عليها حقوقاً أدبية ومالية وعلى هذا فهي محمية بموجب بقوانين حماية حقوق الملكية الفكرية بكل أصنافها سواء أكانت أدبية أو فنية أو صناعية بحيث تمنع هذه التشريعات القيام بأي تصرف من شأنه أن ينتهك هذه الحقوق⁽³⁾.

(1) فتحة رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، السنة الجامعية 2011-2012، ص ص: 28-29.

(2) بهاء المري، موسوعة الميري الجنائية، الجرائم الاقتصادية الشائعة، الجزء الأول، الطبعة الثانية، العربية للنشر والتوزيع، (د.ب.ن)، 2019، ص 364.

(3) فتحة رصاع، المرجع نفسه، ص 29.

ويمكن للمعلومات أيضا أن تكون موضع حماية جنائية بنصوص غير نصوص الملكية الفكرية، كالمعلومات السرية المتعلقة بالمجال العسكري أو التي ترتبط ارتباطا وثيقا بالاقتصاد الوطني والتي تصل التهم فيها إلى الخيانة العظمى التي يعاقب عليها المشرع الجزائري بالإعدام⁽¹⁾.

ب- معلومات الملك العام:

وهي معلومات يجوز لمكافحة الناس الاطلاع والحصول عليها دون الحاجة إلى الحصول على إذن كونها غير مملوكة لأي مالك معين، فهي تقتضي بالاستغلال الأول لها غير أنها قد تستظل بحماية تشريعية في حالة ما إذا بذل في جمعها وصياغتها جهد فكري⁽²⁾.

4- أهمية المعلومات:

تتجلى لنا أهمية المعلومات من خلال 03 محاور أساسية تفضل لها الباحث مراد كريم وهي⁽³⁾:

أ- إتخاذ القرار:

تعتبر المعلومات الركيزة الأساسية التي تدفع الغموض وتزيل الالتباسات في المسائل كلها، وهي آلية أساسية في عملية إتخاذ القرارات، و نظرا لأن الغموض الذي يكتنف المسائل غير ثابت المكان ولا محدد المجال فإن هذا الوضع يؤثر بشكل كبير على حجم المعلومات التي يجب أن يحصل عليها متخذ القرار تبعا للوضع المحيط بالقرار موضع الإيتخاذ⁽⁴⁾.

والقرارات تتوقف في أبعاد صحتها على صحة المعلومات وأساليب تأمينها، فكلما كانت المعلومات ذات جودة وكفاءة ودقة في التعامل معها بالعرض والشرح لمضامينها المرتبطة بمحل الدراسة، كلما كان هناك قدرة كبيرة على بناء قرار رشد ومناسب، فوفر المعلومات بالقدر والنوع والوقت المناسبة يعد بمثابة العمود الفقري الذي يقوم وينبني عليه القرار⁽⁵⁾.

ب- تنشيط البحث العلمي:

يتمحور البحث العلمي في ما يقوم به الإنسان من مساعي وجوهر منظمة قائمة على الأسلوب والنهج العلمي وطرقه، سعيا منه إلى رفع قدرته في إخضاعه وسيطره على بيئته والإطلاع على ظواهرها، ثم إيجاد المحددات التي تربط هذه الظواهر المكتشفة بالموضوع محل

(1) أنظر: المادة 63، الأمر رقم 66-156، المعدل والمتمم.

(2) فتية رصاع، المرجع السابق، ص: 29-30.

(3) مراد كريم، مجتمع المعلومات وأثره في المكتبات الجامعية: مدينة قسنطينة نودجا، أطروحة دكتوراه في علم المكتبات، كلية العلوم الإنسانية والاجتماعية، جامعة منتوري، قسنطينة، فيفري 2008، ص: 13-15.

(4) المرجع نفسه، ص: 13-14.

(5) عثمان مداحي، أهمية ودور المعلومات في إتخاذ القرارات، مجلة الإدارة والتنمية والدراسات، المجلد 07، العدد 01، جامعة علي لونيبي البليدة

02، الجزائر، جوان 2018، ص: 234-244:

<https://www.asjp.cerist.dz/en/article/52097>

النظر من أجل بيان الحقائق وبناء وصياغة نظرية معينة أو تعديلها، أو من أجل تطوير نهج من نهج العمل بناء على ما تم إكتشافه من حقائق⁽¹⁾.

ويأتي الارتباط الوثيق بين المعلومات والبحث العلمي من نفس الارتباط الذي كان قائما بين المعلومات واتخاذ القرارات والمساهمة في حل مشكلة معينة، وليس هناك من اختلاف بين الوضعين إلا في جزئية بسيطة تتمثل في عنصر الوقت إذ أن متخذ القرار يحتاج إلى معلومات جاهزة ليبنى عليه قناعته لإصدار القرار بينما الباحث العلمي هو نفسه من يقدم ويصنع المعلومات على الأسس المنهجية المعترف بها في مجال تخصصه، ومع هذا فإن الباحث العلمي يبقى مرتبطا أيضا بالإفادة وموارد معلومات غيره لتجنب تكرار الجهود السابقة من جهة، ولتحقق بحثا متكاملا من مرحلة التخطيط مروراً بتحليل النتائج وبلوغا إلى مرحلة الفحص والمقارنة والتفسير⁽²⁾.

ج- المعلومات والتنمية:

تتجلى أهمية المعلومات في مجال التنمية كونها مصدرا من المصادر التي يعتمد عليها البشر أفرادا أو مؤسسات في بسط إستغلالها للموارد الطبيعية والشرية المختلفة، فالمعلومات هي التي تملك القدرة على توجيه الطاقة الإنسانية إلى توظيف الموارد الأخرى واستغلالها بالشكل الأمثل فلولاها لما عرف الإنسان سبل الإنتفاع مما تتيحه له الطبيعة، وبما من القدرات البشرية⁽³⁾. وتلعب المعلومات دورا هاما في الحياة الاقتصادية التي هي عصب التنمية، فهي ذات أهمية قصوى كمورد من الموارد الاقتصادية، فهي بذلك تشكل قيمة مالية ومورد خصب للإقتصاد الوطني، ومناطاً للتنافس بين مختلف الفواعل الاقتصادية في السوق، فالاقتصاد المعرفة هي القاعدة الأساسية الذي ينبني عليه الهيكل الاقتصادي العالمي في العصر الحديث⁽⁴⁾ وهذا يعود لكونه إقتصادا قائما على عنصر الابتكار، فهي تضمن الكفاءة اللازمة في إدارة نشاط الإنتاج والتوزيع، فضلا عن الإرتقاء ودعم الجودة، والزيادة الكمية للإنتاج، ومنح المزيد من التنوع الذي يسمح بوجود خيارات متعددة للسلع والخدمات التي توضع في متناول المستهلكين والمنتجين على حد سواء⁽⁵⁾.

(1) أحمد حشاني، دور تكنولوجيا المعلومات والاتصال في ترقية البحث العلمي، مجلة روافد للبحوث والدراسات، المجلد 04، العدد 01، مخبر الجنوب الجزائري للبحث في التاريخ والحضارة الإسلامية، جامعة غرداية، 2019، ص ص: 39-57: <https://rawafid.univ-ghardaia.dz/article/view/167/131>

(2) مراد كريم، المرجع السابق، ص ص: 14-15.

(3) المرجع نفسه، ص 15.

(4) محمد عبد الله شاهين محمد، الاقتصاد المعرفي وأثره على التنمية الاقتصادية للدول العربية، الطبعة الأولى، دار حميثرا للنشر، مصر، 2018، ص 135.

(5) خالد أحمد علي محمود، إقتصاد المعرفة وإدارة الأزمات المالية في إطار المؤسسات الاقتصادية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2019، المقدمة: ص 06.

المبحث الثاني:

الآثار المترتبة عن عولمة الفضاء الإلكتروني

لقد تمكن التطور الكبير الحاصل في تكنولوجيا المعلومات والاتصال من خلق هذا الفضاء الإلكتروني الذي تعتبر العالمية أبرز الصفات التي يتميز بها، فهو عالم بحد ذاته، حيث تتلاشي فيه الحدود وتثوب فيه الفوارق مهما كان نوعها وأيا كان مصدرها، فقد تمكن هذا الهيكل التنظيمي الجديد من إحداث تغيرات وتبديلات جوهرية أين تشكل فيه العولمة عنصرا أساسيا، وأصبحت العلاقات الدولية في ظل عولمة هذا الفضاء تكتسي طبيعة معقدة تبدأ نواتها الأولى من التحولات التي طرأت على مفهوم السيادة والمخاطر التي تحقق بها وصولا إلى التغيرات الجذرية التي ظهرت على مفهوم القوة والهيمنة في العلاقات الدولية، مع أخذت تظهر على الساحة الدولية مفاهيم استراتيجية تغير بشكل أساسي من النظام الدولي وشكل التفاعلات بين الدول وأخذت الدبلوماسية تأخذ بعدا إلكترونيا ودورا أكثر فاعلية وهدفا أكثر اتساعا وشمولا (المطلب الأول).

كما تجدر الإشارة أيضا إلى ما ترتب عن التزايد المستمر في حجم الاعتماد على توظيف الفضاء الإلكتروني في الكثير من مجالات الحياة من تغيرات كبيرة في مفهوم الأمن وظهور نماذج إجرامية حديثة في آلياتها وأهدافها وأصبحت الدول تواجه أنماط جديدة من التهديدات والتحديات الأمنية (المطلب الثاني).

المطلب الأول:

أثر الفضاء الإلكتروني في إعادة تشكيل العلاقات الدولية

تشكل الدولة طرفا أساسيا في مجال العلاقات الدولية وأهم شخص من أشخاص القانون الدولي العام، ولكي تكون طرفا معترفا به في التشكيلة الدولية وقادرا على إبرام التصرفات القانونية وتحمل الإلتزامات الدولية يجب أن يكون طرفا كامل السيادة حر الإرادة، غير أن ظهور الفضاء الإلكتروني قد أحدث تغيرات كبيرة في مفهوم السيادة وأثر بشكل سلبي على شكل الدولة المعاصرة (الفرع الأول)، كما أصبحت العلاقات الدولية نحن منحنيا جديدا أين تكون فيه القوة والهيمنة الإلكترونية عنصر جوهريا وفاعلا في إعادة توزيع القوى وتشكيلها (الفرع الثاني) وتحولت الدول من التعامل في سياستها الخارجية مع الدول أصبحت تتعامل مع الأفراد أيضا من خلال ما يعرف بالدبلوماسية الرقمية (الفرع الثالث).

الفرع الأول: أثر الفضاء الإلكتروني على سيادة الدولة:

تعتبر السيادة من المفاهيم الأساسية التي تبلور الشكل الحديث للدولة رغم أنه كان مفهوما سائد في العصور القديمة، والسيادة هي المناط الذي تحوم حوله العلاقات بين الدول وهي عماد من أعمدة القانون الدولي العام وأساس من أسس التعامل بين أشخاص القانون الدولي العام (أولا)، غير إن ظهور الفضاء الإلكتروني وعولمته وما ترتب عنه من إختراق كبير للحدود السيادية أصبحت السادة في حالة من التآكل والضمور (ثانيا).

أولا: الإطار العام للسيادة:

1- تعريف السيادة:

تبرز السيادة كمدلول من المدلولات الاساسية التي اعتنى بدراستها فقهاء القانون والمختصون في المباحث السياسية المختلفة على حد سواء، فأهميتها كعماد من أعمدة البناء التكويني لهيكل القانون الدولي يوجب عليهم أن يولوا لها كل هذا الاهتمام بالبسط والتحليل والدراسة⁽¹⁾، فالسيادة هي الأساس الذي تقوم عليه الدول وتنشأ، ولا اعتبار لدولة دون سيادة حتى ولو توفرت فيها جميع العناصر الأخرى المكونة لهيكل الدولة⁽²⁾.

مفهوم الدولة لم يكن وليد الصدف لكنه وليد التوكيد الضمني التاريخي الذي بواسطته فرض نفسه على واقع مسيرة الدولة الحديثة، فرغم أن مفهوم السيادة لم يكن معروفا اصطلاحيا لكنه كان واقعا معاشا في ظل التطورات الحاصلة في أشكال الدول وأنماطها وفي المطالبة القديمة والمستمرة بالحرية والمشاركة في إدارة شؤون الحكم، وهذا الحاصل التاريخي هو الذي فرض على المجتمع المعاصر مفهوم السيادة كواقع معاش⁽³⁾.

وعلى رغم أن فكرة السيادة بتعدد واختلاف مستوياتها كانت سائدة منذ العصور الغابرة ومرت بمراحل وأطور من التحديث والتطور على مر التاريخ إلا أن الاهتمام بها تزايد منذ مجيء المفكر الفرنسي " جان بودان " سنة 1576 في كتابه " الستة عن الدولة " ⁽⁴⁾.

(1) سفيان العاقب، الدولة والعولمة: نهاية السيادة (فرانسيس فوكوياما نموذجاً)، مذكرة ماجستير في الفلسفة، كلية العلوم الاجتماعية، جامعة وهران 02، السنة الجامعية 2015-2016، ص 19.

(2) رحيمة لدغش، سيادة الدولية وحققها في مباشرة التمثيل الدبلوماسي، أطروحة دكتوراه في القانون العام، كلية الحقوق، جماعة أبي بكر بلقايد، تلمسان، السنة الجامعية 2013-2014، ص 26.

(3) المرجع نفسه، ص 26.

(4) سفيان العاقب، المرجع نفسه، ص 19.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

إن طرح السيادة تحت هذا التوصيف التاريخي يقضي بعدم إمكانية تقديم تعريف يتناسب مع كل مراحل تطور السيادة، فالصواب أن يكون لكل مرحلة من تلك المراحل تعريفها الذي يتناسب مع الوضع السائد فيه، والسيادة (مصطلح قانوني يعبر عن صفة من له سلطة ولا يستمد هذه السلطة إلا من ذاته، ولا يشاركه فيها غيره، والسيادة أشمل من السلطة إذ أن السلطة هي ممارسة السيادة)⁽¹⁾.

وقد وصفت السيادة أيضا على أنها "الخاصة السياسية الأم" أو "الصيغة الشرعية الرئيسية في المجتمع الدولي"، وقد تم تعريفها على أنها: (السلطة العليا من فوق المواطنين والرعايا والتي لا يقيدتها قانون)⁽²⁾.

كما ذهب فريق آخر في تعريفها (بأن تملك (الدول) السلطة العليا والهيمنة المطلقة والتحكم الكامل على/و في أرضها ورعاياها ومؤسساتها وخياراتها ومواقفها، وأن تكون مستقلة عن أي سلطان آخر سواء كان داخليا أو خارجيا، وأن تكون لها الكلمة العليا والوحيدة في جميع ما تقوم به من أعمال، وأن لا تغلو عليها أية سلطة أو أي هيكل أو كيان آخر)⁽³⁾.

كما عرفها نسيب محمد أزرقى على أنها: (سلطة سياسية عليا آمرة نابعة من ذات الدولة وقادرة على فرض نفسها وتنظيم توجيهااتها دون أن تكون خاضعة داخليا أو خارجيا لغيرها، فهي أعلى السلطات التي تملك أمر الحكم فيما ينشأ بين الأفراد والوحدات الداخلية من خلافات، وهي مع ذلك لا تخضع ماديا أو معنويا لسلطة أخرى) وعرفها أيضا إبراهيم محمد العاني بأنها: (سلطة الدولة العليا على رعاياها، واستقلالها عن أية سلطة أجنبية، وينتج عن هذا أن يكون للدولة كامل الحرية في تنظيم سلطاتها التشريعية والإدارية والقضائية، وأيضا لها كل الحرية في تبادل العلاقات مع غيرها في العمل على أساس من المساواة الكاملة بينها)⁽⁴⁾.

والظاهر من كل هذه التعريفات التي تطرقنا إليها أنها تتشارك قاسما واحدا يتجلى في تركيز جميعها على اعتبار السيادة سلطة عليا ضمن للدولة من أجل أن تتمتع باستقلاليتها وعدم خنوعها

(1) رحيمة لدغش، المرجع السابق، ص ص: 27-28.

(2) جوزيف فرانكل، العلاقات الدولية، ترجمة (غازي عبد الرحمن القصيبي)، الطبعة الثانية، مطبوعات تهامة، جدة، المملكة العربية السعودية، 1984، ص ص: 24-25.

(3) عبد الوهاب جمال، السيادة: مقوماتها وأركانها، 23 جويلية 2018 تم الاطلاع عليه بتاريخ 13 جانفي 2020 على الساعة 22:12، في الموقع: <https://www.lediplomate.tn/> السيادة-مقوماتها-أركانها/

(4) نقلا عن: حنان عماد زهران، تشريح مفهوم السيادة، 27 مارس 2019، تم الاطلاع عليه بتاريخ 13 جانفي 2020 على الساعة 22:30، في الموقع: <https://democraticac.de/?p=59802>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وخضوعها⁽¹⁾، كما بينت التعاريف أيضا بأن السيادة مرتبطة قصرا وحصرها بالدولة دون غيرها من الكيانات، ولا يمكن لها أن تتجزأ أو تتعرض للتقسيم، فالدولة وحدها منبع كل السلطات في إطار حدودها الإقليمية بقطع النظر عن نوع تلك السلطات أو مجال نشاطها أو حجمها، والسلطات داخل الدولة لا يمكن بشكل من الأشكال أن تتقاسم السيادة معها، فهي لا تتقاسم إلا الاختصاص فقط⁽²⁾. وتتقسم السيادة إلى داخلية وخارجية:

أ- السيادة الداخلية:

تتجلى السيادة الداخلية للدولة من خلال ذلك النفوذ والسلطة اللذان تبسطهما الدولة على حدودها الإقليمية، كما تتجلى أيضا من خلال السلطة التي تملكها الدولة على مواطنيها والتي تبسطها عليهم من خلال إخضاعهم لأنظمتها وتشريعاتها المختلفة⁽³⁾.

فهي إذا تستأثر بوجوب هذه السيادة بكل الممارسات السلطوية داخل البلاد، وتتحكم بالقضاء ولها كامل التصرف في الأجهزة الإدارية كما تتمتع بسلطة توقيع الجزاءات بما في ذلك سلب المواطن حريته وإكراهه ماديا، فالدولة تستأثر لنفسها ضمن السيادة الداخلية بالكثير من النشاطات التي لا تجوز لغيرها، وهذه الأعمال هي اختصاص حصري ومانع للدولة لا ينافيها فيها أحد وتمارسها على وجه العموم والإطلاق من خلال أجهزتها الداخلية من سلطة قضائية وتشريعية وتنفيذية⁽⁴⁾.

وتجدر الإشارة إلى أن مفهوم السيادة الداخلية وما يتضمنه من مضامين قد طرح العديد من الإشكالية والقضايا والتساؤلات ذات الطابع السياسي والقانوني، ومن بين أبرز هذه الإشكاليات المطروحة؛ منشأ السلطة العليا في الدولة وركائزها التي تقوم عليها، والارتباطات القائمة بينها وبين مواطنيها، وإشكالية جمع هذه السلطة في يد أشخاص أو جماعات محددة تستأثر بها دون غيرها ومدى قابلية هذه للتقسيم⁽⁵⁾.

ب- السيادة الخارجية:

تعتبر السيادة الخارجية للدولة مظهرا من مظاهر التمتع بالاستقلال السياسي فليس للدولة التي تتمتع بالسيادة أن يكون لها أي شكل من أشكال الخنوع أو الخضوع لإرادة الدول الأخرى بل هي متساوية المقام فيما بينها كلها، إذ أن نظام العلاقات التفاعلية بين الدول تقوم على مقتضيات

(1) عبد الوهاب جمال، المرجع السابق.

(2) حنان عماد زهران، المرجع السابق.

(3) سفيان العاقب، المرجع السابق، ص 25.

(4) خديجة غرداين، إشكالية السيادة والتدخل الإنساني (حالة الدول العربية)، مذكرة ماجستير في القانون العام المعمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2014-2015، ص 29.

(5) جوزيف فرانكل، المرجع السابق، ص 25.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

هذا الأساس، فالدولة في علاقاتها مع غيرها من دول العالم تنطبق في إدارة وتسيير شؤونها على أساس ما تم سنته واعتماده من أنظمة داخلية خاصة بها، وبكامل حريتها في إدارة جميع شؤونها الخارجية باعتبارها الممثل الشرعي الذي يحمل إرادة الأمة ويتصرف بإسمها⁽¹⁾.

وقد أكد القضاء الدولي على هذا المفهوم ضمن أحكام محكمة العدل الدولية في قضية " كورفو " سنة 1949 بأن: (ولاية الدولة في حدود إقليمها ولاية انفرادية ومطلقة، وأن احترام السيادة الإقليمية فيما بين الدول المستقلة يعد أساساً جوهرياً من أسس العلاقات الدولية)⁽²⁾.

فالسيادة الخارجية بهذا المعنى إذا، لا تشكل في حقيقة أمرها سوى الأهلية القانونية التي تضفي عليها القدرة على اكتساب الحقوق، وتحملها إزاء غيرها من أشخاص القانون الدولي العام بالالتزامات، وبهذا المعنى فإن للدولة الحق في أن تتصدى لأي شكل من أشكال الاعتداء عليها، كما لها بموجب هذه الأهلية كامل الحق في خلق ارتباطات والدخول في التحالفات وعقد الموائيق⁽³⁾.

وهناك مسألة مهمة يجدر الإشارة إليها في معرض بحثنا والتي ستتلور أهميتها بصفة خاصة في الباب الثاني من هذه الأطروحة وهي أن؛ فكرة السيادة الخارجية تتناقض وتتصادم مع بعض الاعتبارات القانونية الدولية، وأبرز هذه الاعتبارات فكرة القانون الدولي الذي يحمل في صلبه جوهر الضبط والتقييد، فرغم أن القانون الدولي يحمل في جوهره حماية المقتضيات التي يحميها القانون الداخلي، إلا أنه مع فكرة السيادة لا يستقيم له هذا الأمر، فيكون حينها عديم القوة أمام القانون الداخلي، والتناقض الذي تثيره السيادة الخارجية ينطلق عدم إمكانية إخضاع الدولة للقانون باعتبار السيادة، في حين أن هناك قوانين دولية موضوعية، وهذا الأمر يحول دون تكوين أنظمة قانونية مركزية فعالة، ومع ذلك هناك من وفق بين هذه التناقضات على أساس الرضا⁽⁴⁾.

2- مقتضيات السيادة:

أ- المساواة بين الدول:

يفرض مبدأ سيادة الدولة المساواة بين الدول في المحافل الدولية على ضوء علاقاتها في ما بينها، ويعتبر هذا المبدأ من أسمى مبادئ القانون الدولي التقليدي الذي يتبلور بشكل خاص من

(1) سفيان العاقب، المرجع السابق، ص 25.

(2) هاشم بن عوض بن أحمد آل إبراهيم، سيادة الدولة بين مفهومها التقليدي وظاهرة التدويل، رسالة ماجستير في القانون العام، كلية الحقوق،

جامعة الشرق الأوسط، يونيو 2013، ص 30.

(3) خديجة غرداين، المرجع السابق، ص 30.

(4) جوزيف فرانكل، المرجع السابق، ص ص: 25-26.

خلال الفقرة الأولى من المادة الثانية من ميثاق الأمم المتحدة التي تنص صراحة على أن هيئة الأمم المتحدة قائمة على مبدأ المساواة في السيادة بين جميع أعضائها، فواجبات الدول وحقوقها متساوية من وجه النظر القانونية ولا يمكن أن تتأثر بالاختلافات الموجودة بين الدول كالكثافة السكانية أو المساحة الجغرافية أو الموارد الاقتصادية⁽¹⁾، فالسيادة التي تتمتع بها الدول كلها أمام القانون الدولي سواء، وما من شيء يمكن أن يصنف السيادات تصنيفاً تدرجياً⁽²⁾.

غير أن هناك بعض الاستثناءات مثل تمتع الدول الخمس الكبرى بالعضوية الدائمة وحق النقض، وبتعديل ميثاق الأمم المتحدة وكذلك من خلال نظام التصويت في البنك الدولي للإنشاء والتعبير وصندوق النقد الدولي⁽³⁾.

فمقام الدول في هذه الأمثلة المذكورة يتعارض تماماً مع مقتضيات مبدأ المساواة بين الدول، فميثاق الأمم المتحدة قد منح امتياز العضوية دائمة في مجلس الأمن لخمس دول فقط، وأكثر من ذلك أثراً هو منح هذه الدولة امتيازات حال التصويت على قرارته⁽⁴⁾، ويعتبر بعض الفقهاء والباحثين أن هذه اللامساواة هي التي كانت سبباً في إخفاق كل الجهود الرامية إلى تطوير العلاقات الدولية⁽⁵⁾، ويرى البعض الآخر أن هذه اللامساواة ولاسيما في مضمون حق الفيتو يعد أداة تهيمن بها تلك الدول على غيرها⁽⁶⁾.

ب - التمتع بمزايا السيادة:

تخول السيادة للدولة الحق في ممارسة جملة من الحقوق المتعارف والمُعترف بها على الساحة الدولية كعقد الاتفاقيات الدولية وتبادل التمثيل الدبلوماسي والقنصلي، وحق التقاضي والتحكيم الدوليين، كما لها الحق في إثارة المسؤولية الدولية على أثر ضرر أصابها أو أصاب مواطنيها للمطالبة بالتعويض عنه أو إصلاحه، كما تمنح السيادة أيضاً للدولة عدة امتيازات على الساحة الداخلية إذ تملك السلطة في استغلال مواردها الطبيعية والمواد الأولية والتصرف فيها كما يمكن لها أن تطال بسلطانها كل من على إقليمها من سكان أكانوا مواطنين أم أجنبياً⁽⁷⁾.

(1) رحيمة لدغش، المرجع السابق، ص: 41-42.

(2) إبراهيم جودة علي العاصي، دور التشريعات الدولية الخاصة بحقوق الإنسان في الحد من سيادة الدولة، الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، مصر، 2019، ص 100.

(3) رحيمة لدغش، المرجع نفسه، ص: 41-42.

(4) إبراهيم جودة علي العاصي، المرجع نفسه، ص 89.

(5) طلعت جواد لحي الحديدي، مبادئ القانون الدولي العام في ظل المتغيرات الدولية: (العولمة)، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2012، ص 111.

(6) بطاينة، فؤاد، الأمم المتحدة: (منظمة تبقي ونظام يرحل)، الطبعة الأولى، المؤسسة العربية للدراسات والنشر ودار الفارس للنشر والتوزيع، الأردن، 2002، ص 46.

(7) رحيمة لدغش، المرجع نفسه، ص: 40-41.

ج- عدم التدخل في الشؤون الداخلية:

نصت المادة 2/7 من ميثاق الأمم المتحدة على أنه: (ليس في هذا الميثاق ما يسوغ للأمم المتحدة أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما) فمن هذا النص يثبت بمفهوم المغايرة أن مبدأ التزام عدم التدخل في الشؤون الداخلية للدول من بين المبادئ المستقر عليها دوليا للحفاظ على سيادة الدولة، فليس لأي دولة أن تملي على غيرها من الدول أو تجبرها على اختيار نهج سياسي معين، فالدولة تتمتع بالحرية المطلقة في انتهاج النهج السياسي والاقتصادي والثقافي والاجتماعي وتطوره بما يروق لها ويتناسب وفقا لإرادتها الحرة، ومع هذا ترد استثناءات متعلقة بشكل أساسي بالتدخل الإنساني ومقتضيات حقوق الإنسان⁽¹⁾، فتكون حينها السيادة مقيدة بأحكام ونصوص التشريعات التي تحظر جرائم الحرب، وجرائم الإبادة⁽²⁾.

ثانيا: أثر الفضاء الإلكتروني على سيادة الدول:

لقد وضع التطور التكنولوجي والتقني والفضاء الإلكتروني عموما العالم كله أمام جملة من المفاهيم الجديدة التي أثرت بشكل كبير على العلاقات القانونية والاجتماعية والمدنية وقد مست تقريبا كل مجالات الحياة الإنسانية، ويكمن سبب وراء هذا الإستجداد في هذه المفاهيم كلها كون الفضاء الإلكتروني مغاير للعالم الواقعي الذي كان سائدا بعالم له كيان آخر غير الكيان الملموس الذي تم الاعتياد عليه⁽³⁾؛

ومن بين أهم المفاهيم التي تعرضت للغير نجد مبدأ السيادة الذي تغيرت أبعادها لتشمل بعدا تقنيا جديدا يضاف إلى المعني الأصلي الذي تُعارف عليه، فالفضاء الإلكتروني قد أصبح العامل الأساسي الناقل للعولمة فهو وجه آخر لها، فرغم أن العولمة إبان ظهورها إلى الوجود على عهد الرئيس الأمريكي جورج بوش الأب كان لها من الآثار الاقتصادية والتكنولوجية والاجتماعية احمدها وأنفعها، إلا أن ذلك لم يكن الوجه الوحيد للعولمة، فقد كان لها الكثير من السلبيات التي تتمحور أساسا في محاولة فرض هيمنة الثقافة الغربية على باقي الثقافات الأخرى والعمل على تقويض السيادة وتحويل العالم إلى قرية صغيرة، ولعل أهم وجه حديث لهذه العولمة وأبرز وسائلها هو الإنترنت⁽⁴⁾.

(1) رحيمة لدغش، المرجع السابق، ص ص: 41-43.

(2) إبراهيم جودة علي العاصي، المرجع السابق، ص 101.

(3) فائز ذنون جاسم، تأثير الإنترنت على مبدأ السيادة، مجلة كلية الحقوق، المجلد 17، العدد 02، جامعة النهران، العراق، 2015، ص ص: 331-348.

(4) <https://www.iasj.net/iasj?func=issueTOC&isId=6646&uiLanguage=en>

(4) المرجع نفسه.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

ويجر هذا المتغير الكبير المصاحب للعولمة انتهاكا صارخا لسيادة الدولة لما أحدثه من إلغاء للتباعد الجغرافي بين كل دول العالم حتى أصبح قرية صغيرة، وقد أثر هذا على تفاعل الشعوب مع الكثير من القضايا التي لولا هذا الاختزال للطاق الجغرافي ما كانوا ليعرفوها، فالأحداث التي تقع في أي بقعة من بقع الأرض ذات انعكاس وأصداء واسع يشمل غيرها من المناطق دون أن يكون للحدود السياسية والسيادية أي اعتبار، كما أفضت من جهة أخرى إلى تغير التكوين الديمغرافي للمجتمع، وهذه التكوينة تتفاعل بشكل كبير مع العالم الخارجي، وهذا التفاعل بدوره يبلور أنماط حياة وتفكير جديدة⁽¹⁾.

وقد أشار الحبيب الجحاني في تعريفه للعولمة إلى التآكل الذي تشهده الدولة الحديثة من خلال اضمحلال وتصدع سيادة بقوله: " الكوكبة وهي مذهب القائلين بأن الرأسمالية هي ديانة الإنسانية، وهي رسملة العالم، وتتم السيطرة عليه في ظل هيمنة دول المركز وسيادة النظام العالمي الواحد، وبذلك تنهافت الدولة القومية وتضعف فكرة السيادة الوطنية وصياغة ثقافة عالمية واحدة تضمحل إلى جوارها الخصوصيات الثقافية "⁽²⁾.

إن الفضاء الإلكتروني مكن بفضل خواصه لمستخدميه النفاذ عبر الحدود الإقليمية والسيادية وفرض على الدولة تحديا كبيرا وصعوبة عميقة تتجلى في تقليص أو إعدام قدرة الدولة في التحفظ على حدودها فمن خلال هذا الفضاء يمكن للأفكار والمستندات والصور والمعلومات العبور بكل سير وسهولة إلى مواطنيها دون أن يكون لها النزر اليسير من القدر على منعها مما يحد من سيادتها إلى أدنى مستوياتها، فمن خلال هذا الفضاء تكونت كتل المعارضة والتنظيمات التي الأمر الذي يفضي إلى تصاعد ممارسات التدخل الأجنبي أمام عجز الدولة عن وقفها، فالفضاء الإلكتروني قد جعل الدول غير قادرة على تحقيق سيادتها على سياساتها وثقافتها واقتصادها ثم إن الفضاء الإلكتروني قد أحدث فجوة رقمية بين عالم متقدم ينمو باستمرار وبين عالم ثالث يعاني التهميش في كافة القطاعات بما فيها قطاع الاتصالات الذي أصبح شطر منه يدار خارج النطاق القانوني الدولي التقليدي الذي يصون سيادة الدولة وهيبتها⁽³⁾.

(1) هاشم بن عوض بن أحمد آل إبراهيم، سيادة الدولة بين مفهومها التقليدي وظاهرة التدويل، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، يونيو 2013، ص 62.

(2) نقلا عن: حجار ماجدة، العولمة والعنف: مقارنة سوسيولوجية لظاهرة العنف في ظل العولمة، أطروحة دكتوراه في التنمية وتسيير الموارد البشرية، كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة منتوري، قسنطينة، السنة الجامعية 2009-2010، ص 55.

(3) فانز دنون جاسم، المرجع سابق، ص ص 331-348.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

تتجلى من جانب آخر مظاهر تصدع السيادة على ضوء المتغيرات التكنولوجية في تغير القواعد الاقتصادية للدول عبر تقليص سلطتها لصالح السوق، فقد أدى الفضاء الإلكتروني إلى إقحام الدولة في عجز كبير عن مراقبة النواذ التي تتخذها الأموال في نفاذها إلى البلاد، ومكّن الشركات من التأقلم بشكل كبير مع التحولات التي تطرأ في الإجراءات الاقتصادية داخل الدولة وتتعامل معها على وجه السرعة بما يضمن لها أكبر قدر ممكن من الأرباح، فضلا عن أن الفضاء الإلكتروني قد أنتج حالة من الغموض المعاملات المالية والأموال المنتقلة في المعاملات بين الحدود⁽¹⁾.

وتجدر الإشارة في هذا المقام أن (وليام بريك) يرى بأن السيادة لا تتعرض للتهديد الإلكتروني بصفة مجملّة، فمن وجه نظره؛ السيادة تتخذ شكلين اثنين هما؛ السيادة الدستورية التي تمارسها الدولة على أراضيها، والسيادة العملانية التي هاهنا فعالية الدولة في الإشراف وبسط الرقابة على كل أراضيها، ويرى أن الفضاء الإلكتروني لا يهدد السيادة الدستورية لأنها سيادة محاطة بمجملّة من القوانين سواء على الصعيد الوطني أو على الصعيد الدولي، بل يرى أن السيادة التي تتعرض لأشكال من التهديد السيبراني هي السيادة العملانية، كما اعتبر عبد الحليم فضل الله أن السيادة السياسية تعتبر أيضا في قلب التهديد في ظل هذه العولمة⁽²⁾.

الفرع الثاني: الفضاء الإلكتروني والتحول الاستراتيجية في مفهوم القوة:

تعد القوة مطلبا من المطالب الأساسية التي تسعى الدول إلى تحقيقها والعمل على توظيفها بعد ذلك لفرض هيمنتها وسلطانها في خضم التعاملات والتفاعلات التي تقع بينها وبين بقية الدول، وتتخذ القوة أبعاد كثيرة قائمة على عناصر متعددة تمثل جوهر القوة وصلبها (أولا) ومن بين الأبعاد الاستراتيجية التي تسعى الدول تحقيقها لضمان المزيد القوة نجد البعد الإلكتروني الذي أصبح مجالا مهما وحيويا من مجالات القوة الدولية (ثانيا).

(1) صالح لبيد، إشكالية سيادة الدولة في ظل العولمة، رسالة ماجستير في العلوم السياسية، كلية العلوم السياسية والإعلام، جامعة الجزائر بن يوسف بن خدة، السنة الجامعية 2008-2009، ص ص: 102-103.

(2) نقلا عن: عبد الحليم فضل الله، علاقة المواطن بالسلطة في العصر الرقمي، ورقة قدمت إلى: مؤتمر مدرسة جيل الخريفية: التحوّل، الشفافية، الديمقراطية، المشاركة المدنية والسياسية في العصر الرقمي؛ تنظيم مركز علوم الإنسان ومنظمة الأونيسكو 4-8/2/2013:

https://www.google.com/url?sa=t&source=web&rct=j&url=http://www.dirasat.net/uploads/item_mak_m/6946792.pdf&ved=2ahUKEwjB5_O9vJboAhXv1uAKHfgfCCoQFjADegQIBBAB&usg=AOvVaw3n0QklRXqX_NKczRZ3MW

أولاً: القوة في العلاقات الدولية:

1- مفهوم القوة:

يعد مفهوم القوة من المفاهيم الأساسية في منظومة العلاقات الدولية الغربية أياً كان المعنى الذي يتم إضفائه عليها، والقوة في مجملها إنما هي متعلقة بشكل خاص بالمذهب الواقعي الذي يتجه إلى اعتبارها الدافع المحوري أو الوحيد في دائرة التفاعلات الدولية، فالقوى الكبرى باعتبار هذه الرؤية تضع القوة في قمة هرم أولوياتها، ساعية إلى اكتسابها من جهة، والحيلولة دون أن تتحول موازينها بمنح الآخر من أن ترجح إلى كفته⁽¹⁾.

وهذا ما يفضي تبعاً إلى تحول القوة وتداخله مع مفهوم الصراع، وتربطهما سببياً، فالسعي إلى تحقيق القوة والهيمنة عليها دون الغير يفضي تبعاً إلى الصراعات الدولية في بيئة تتناقض فيها المصالح، فالقوة في الاتجاه الذي ينظر إلى العلاقات الدولية كحلبة صراع يحاول فيها كل طرف بسط نفوذه والتأثير على الأطراف الأخرى تمثل مفهوماً أساسياً وجوهراً⁽²⁾.

ويعد مفهوم القوة من المفاهيم المركبة لكل باحث، ولا سيما للباحثين في المجال القانوني، ذلك أن مفهومها يتقلب بين العديد من المعاني ويتمازج مع الكثير من المصطلحات⁽³⁾، لذلك فإن التعريف الذي نراه مناسباً للقوة لأغراض هذه الدراسة هو: (مجمع الممكنات التي يملكها شخص أو مؤسسة أو دولة، وقدرتها على التأثير في سلوك الآخرين باتجاه فعل ما، أو التراجع عن فعل ما، من خلال الإكراه أو المساومة أو الاقتناع، للحصول على الأهداف المرجوة)⁽⁴⁾.

ومن خلال هذا التعريف يمكن أن نستنتج امرين مهمين، أولهما خصائص القوة وثانيهما هو التصنيف الفقهي لأنواع القوة؛

أ- أما عن الخصائص: فيمكن القوب بأن القوة تتمتع بجملة من الخصائص المتغيرة، مادية وغير مادية، وتمتلك قدراً كبيراً من الترابط فيما بينها باعتبارها مفهوم حركي وديناميكي، فالقوة مفهوم نسبي إذ أنه قائم على مبدأ القياس، أين يقاسم الفاعل الدولي بغيره من الفواعل

(1) مروة فكري، مدخل إلى العلاقات الدولية: (أزمة العولمة وآفاق العالمية)، الطبعة الأولى، مركز الحضارة للدراسات والبحوث، دار الكتاب المصري، دار الكتاب اللبناني، مصر، لبنان، 2021، ص 198.

(2) نادية محمود مصطفى، القوة الذكية في السياسة الخارجية: (دراسة في أدوات السياسة الخارجية الإيرانية تجاه لبنان 2005-2013)، الطبعة الأولى، دار البشير للثقافة والعلوم، مصر، 2014، ص 23.

(3) سيف الهرمزي، مقتربات القوة الذكية الأمريكية كآلية من آليات التغيير الدولي: الولايات المتحدة الأمريكية أنموذجاً، الطبعة الأولى، المركز العربي للأبحاث ودراسة السياسات، قطر، 2016، ص 35.

(4) المرجع نفسه، ص 37.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

الأخرى، كما أنها وسيلة لممارسة النفوذ وتحقيق لأهداف والمصالح أيا كان نوعها، ثم إن وزن القوة الذي تمتلكه الدولة يتغير تبعا لإمكانات الدولة وقدرتها في تحويل القوة المتاحة والمتوفرة إلى قوة فعلية يمكن التماسها على أرض الواقع⁽¹⁾.

ب- وأما عن التصنيف: فقد دأب الفقهاء والباحثون ولاسيما في مجال الدراسات في العلاقات الدولية على تصنيف القوة ضمن هذه البيئة الدولية التي يتجلى الصراع فيها كأهم مظهر للعلاقات والتفاعلات الدولية بين مختلف أطرافها، إلى صنفين إثنين:

• القوة الصلبة:

تعد القوة الصلبة قوة يتم اللجوء فيها إلى لغة الضغط والجبر والإكراه من أجل الوصول إلى تحقيق المرامي والغايات التي ترومها الدولة من خلال سياساتها الخارجية، وهذا كله ضمن النطاق التفاعلي الدولي⁽²⁾.

وتتجلى القوة الصلبة في نطاقها الواسع من خلال مظهرين أساسيين هما؛ القوة العسكرية التي يتم اللجوء إليها من خلال اعتماد خمسة أساليب هي؛ الدبلوماسية القسرية، التخريب، الردع، الدفاع، وأخيرا التدخل عسكريا بشكل مباشر، وثاني تجلى للقوة الصلبة هو؛ القوة الاقتصادية، وهي قوة صلبة تقوم على أساس الاعتبارات المتصلة بالعوامل الاقتصادية بكل عناصرها⁽³⁾.

• القوة الناعمة:

يشرح جوزيف ناي القوة الناعمة بقوله: (و القوة الناعمة ليست شبيهة بالتأثير فقط... كما أن القوة الناعمة أكثر من مجرد الإقناع أو القدرة على استمالة الناس بالحجة، ولو كان ذلك جزء منها. بل هي أيضا القدرة على الجذب، والجذب كثيرا ما يؤدي إلى الإذعان)⁽⁴⁾، فتصور جوزيف ناي للقوة الناعمة تقوم على ثلاث مرتكزات، أو تتجلى في ثلاث أشكال؛ التأثير والقدرة على الإقناع، الاستمالة بالبرهنة والاستدلال، وأخيرا القدرة على الجذب المولد للرضوخ.

⁽¹⁾ شيماء عويس، القوة في العلاقات الدولية: (دراسة تأصيلية)، 05 أكتوبر 2018، تم الاطلاع عليه بتاريخ 20 فيفري 2020 على الساعة 15:32، في المواقع: <https://eipss-eg.org/> القوة في العلاقات الدولية-دراسة تأصيلية/

⁽²⁾ نادية محمود مصطفى، المرجع السابق، ص 31.

⁽³⁾ حميد حمد السعدون، الاستخدام الأمريكي للقوة الصلبة والقوة الناعمة في السياسة الخارجية، مجلة الدراسات الدولية، العدد 64-65 (عدد مزدوج)، جامعة بغداد، العراق، 2016، ص ص: 1-16:

<https://www.iasj.net/iasj/article/117207>

⁽⁴⁾ جوزيف س. ناي، القوة الناعمة: (وسيلة النجاح في السياسة الدولية)، ترجمة (محمد توفيق البجيرمي)، الطبعة العربية الأولى، مكتبة العبيكان، المملكة العربية السعودية، 2007، ص 26.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وتعرّف أيضا على أنها: (...القدرة على الاحتواء الخفيّ والجذب اللين، بحيث يرغب الآخرون في فعل ما ترغب فيه القوة المهيمنة من دون الحاجة إلى اللجوء إلى استخدام القوة...) ⁽¹⁾، كما عرّفها مايكل آيزنشتات على أنها: (استخدام الأقوال والأفعال والصور الانفعالية في إطار حملة استراتيجية للتواصل، طويلة المدى لتشكيل الحالة النفسية لبلد معاد لأمريكا مثل إيران) ⁽²⁾.

ومبلغ القول في مفهوم القوة الناعمة أنها تلك القوة التي تنبذ وسائل الجبر والإكراه التقليدية في تحقيق الأهداف والسياسات الخارجية، واللجوء إلى التوصل مع الطرف الآخر وإغرائه سواء أكان ذلك بالبرهنة والاستدلال أو كان بالجذب والاستهواء.

2- عناصر القوة:

يمكن تقسم عناصر قوة الدولة إلى مجموعتين أساسيتين:

أ- العناصر التقليدية:

• العنصر الطبيعي:

يعتبر العنصر الطبيعي للدولة من أهم الأسس أو المحددات لقوة الدولة، والمقصود بالعنصر الطبيعي كل ما له علاقة بالموثرات الطبيعية للدولة، ولاسيما الجانب الجغرافي منه، من حيث اتساعه، كالتضاريس والمناخ وموقعها الجغرافي ⁽³⁾.

ويظهر العامل الطبيعي كأحد أسس ومقومات القوة في الدولة من خلال النظر إلى مجريات أحداث الحرب العالمية الثانية، حيث يظهر من خلالها نصر كبير حققه الاتحاد السوفياتي على ألمانيا النازية، ويعود هذا النصر إلى العناصر الطبيعية التي كان الاتحاد السوفياتي يتميز بها، وينطبق هذا الأمر أيضا على أفغانستان التي واجه فيها الجيش الأمريكي عقبات وصعوبات كبيرة جاء تضاريسها الطبيعية التكوينية لجغرافيا البلاد ⁽⁴⁾.

⁽¹⁾ رفيق عبد السلام، الولايات المتحدة الأمريكية بين القوة الصلبة والقوة الناعمة، الطبعة الرابعة، مركز صناعة الفكر للدراسات والأبحاث، لبنان، 2015، ص 10.

⁽²⁾ نقلا عن: صابر منصور، حروب الجيل الرابع، الطبعة الأولى، مؤسسة دار الفرسان للنشر والتوزيع، القاهرة، 2016، ص 80.

⁽³⁾ الموسوعة السياسية، عوامل قوة الدولة في المجال الدولي، تم الاطلاع عليه بتاريخ 22 فيفري 2021، على الساعة 08:02، مختصر الرابط: <https://cutt.us/Nm9O6>

⁽⁴⁾ حنان يوسف، الإعلام والسياسية: (مقاربة ارتباطية)، الطبعة الثانية، أطلس للنشر والإنتاج الإعلامي، القاهرة، 2006، ص 21.

• العنصر البشري:

يعتبر العامل السكاني من بين العناصر التي تقوم عليها قوة الدولة، غير أنه يجب النظر إلى العامل السكاني من زاويتي الكم والكيف، فلا بد لاعتبر العمال السكاني عنصرا من عناصر القوة أن يتماشى الم مع الكيف⁽¹⁾، والكيف هنا يمكنه فهمه بمعنى واسع ليشمل خصائصه وكيفية توزيعه جغرافيا⁽²⁾.

• نظام الحكم:

يمكن أن نعتبر أن الإدارة ونظام الحكم يمثل عنصرا من العناصر التكوينية لمعنى قوة الدولة وذلك من خلال مسارين اثنين؛ أولهما يتناول في أبعاد فاعلية نظام الحكم واستجابته بالسرعة والملائمة لأشكال التحديات التي تصادفهن والتهديدات التي تعترضه، وثانيهما؛ هو مدى حركيته وفاعليته على المستوى الداخلي من خلال تكريس الإرادة الشعبية⁽³⁾.

• العنصر الاقتصادي:

يعتبر العامل الاقتصادي آلية ذات أهمية قصوى ولاسيما في عصرنا الحاضر في تحديد قوة الدولة على ساحة العلاقات الدولية، وتتجلى من خلال توظيف العديد من الأساليب والآليات لذلك، فالإقتصاد يمثل عصب العلاقات الدولية، إذ أن تأثيره لم يعد يتوقف على رخاء الشعوب بل يتعدى ذلك إلى أمن الدولة نفسها⁽⁴⁾، وقد رأى بعض الباحثين أن انكماش وانحسار الجنب الاقتصادي مقارنة بالجنب العسكري يعتبر من بين العلل التي أفضت بالإتحاد السوفياتي إلى السقوط والتفكك⁽⁵⁾.

وقد أدركت الكثير من الدول الأبعاد التي يمثلها الإقتصاد في بناء قوتها، ولعل هذا هو السبب الذي أدى بالاتحاد الأوروبي إلى توحيد عملته، إذ يعتبر الدولار الأمريكي العملية الأكثر هيمنة، ولذلك فكر الاتحاد الأوروبي في التعاضد من أجل الوقوف أمام هذه الهيمنة من خلال

(1) حنان يوسف، المرجع السابق، ص 22.

(2) أنظر: فراس محمد أحمد الجحيشي، التوازنات الاستراتيجية الجديدة في ضوء بيئة أمنية متغيرة، الطبعة الأولى، الأكاديميون للنشر والتوزيع، الأردن، 2015، ص 145.

(3) مازن محمد علي، جيوبوليتيكا الأمن القومي العربي: (أمن الخليج العربي "مرتكزا")، مقال ضمن المنصف الجماعي: الأمن القومي الإماراتي والخليجي والجزر الإماراتية المحتلة، الطبعة الأولى، مركز المزملة للدراسات والبحوث، الإمارات العربية المتحدة، 2014، ص ص: 10-33.

(4) الموسوعة السياسية، عوامل قوة الدولة في المجال الدولي، المرجع السابق.

(5) نزيه علي منصور، حق النقض (الفيتو) ودوره في تحقيق السلم والأمن الدوليين، الطبعة الأولى، دار الكتب العلمية، لبنان، 2009، ص 98.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

إصدار عملة اليورو التي من المحتمل أن تمثل للدولار الأمريكي وهيمنتها على المالية الدولية تحدياً فعلياً⁽¹⁾.

بل إن من الباحثين من يرى أن عرقلة الازدهار الاقتصادي للصين يعد من ذو أهمية خاصة بالنسبة للولايات المتحدة الأمريكية ومصالحها، لأن ازدهارها وغناها سيكون له تداعيات إقليمية تتبلور في تحول الصين إلى دولة عدائية ومصرّة على الهيمنة في منطقتها، وهذا إن حدث فلن ينصب على الإطلاق في مصلحة الولايات المتحدة الأمريكية⁽²⁾.

وفي الأخيرة، جدير بالإشارة إلى أن القوة الاقتصادية لها ما يؤشر عليها، وقد أحصى هائل عبد المولى طشطوش 13 مؤشراً لبيان عنصر القوة الاقتصادية من أهمها؛ حجم الإنتاج الإجمالي، متوسط نصيب الفرد من الإنتاج القومي الإجمالي، حجم الصناعات في الدولة، معدل النمو الحولي، وحجم وإنتاج الطاقة وحجم احتياطي الدولة منها⁽³⁾.

• الإمكانيات العسكرية:

تعد الإمكانيات العسكرية من بين أهم العناصر التي تقرر قوة الدولة، وقياس القوة العسكرية للدولة يكون وفق العديد من المؤشرات وهي؛ حجم جيشها، والعوامل الطبيعية التي يتحرك فيها بآليته ومدى توفرها على بنية تحتية للحركة وما له من علاقة بنوعية بالتدريب والتكتيك، وكذلك قوة الدلة في الإنتاج الحربي، وحجم إنفاقها العسكري، ومستويات التدريب ونوعيته، وحجم الأسلحة ونوعيتها⁽⁴⁾.

كما أشار جوزيف ناي إلى ما أسماه بـ " الدبلوماسية القسرية" التي اعتبرها صور ثانية من صور القوة العسكرية، ومفاد هذا النوع من الدبلوماسية استعمال لغة التهديد دون اللجوء إلى لغة الحرب، من خلال العديد من الأشكال التي يمثل نشر القوات أحدها⁽⁵⁾، وليس بالضرورة أن يكون

⁽¹⁾ صمويل هنتنجتون، القوة العظمى الانفرادية: (البعد الجديد للقوة)، الطبعة الأولى، مركز فلسطين للدراسات والبحوث، قطاع غزة، 1999، ص 22.

⁽²⁾ جون ميرشايمر، مأساة سياسة القوى العظمى، ترجمة: (مصطفى محمد قاسم)، النشر العلمي والمطابع، جامعة الملك سعود، المملكة العربية السعودية، 2012، ص ص: 501-502.

⁽³⁾ هائل عبد المولى طشطوش، الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2012، ص ص: 94-97.

⁽⁴⁾ المرجع نفسه، ص ص: 77-82.

⁽⁵⁾ جوزيف إس. ناي، مستقبل القوة، ترجمة: (أحمد عبد الحميد نافع)، مراجعة: (السيد أمين شبلي)، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2015، ص 68.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

هناك تهديد مباشر، يكفي أن تكون حائزا لأسلحة الدمار الشامل يكون ذلك عنصرا رادعا للطرف المعادين ولاسيما إن كان من الدول الكبرى⁽¹⁾

ب- العناصر الحديثة:

• عنصر الإعلام:

يحتل الإعلام مكانة مرموقة ومتصدرة ضمن العناصر المكونة لقوة الدولة وتأثيرها على الرأي العام وصناعته⁽²⁾، وهي تفوق في قوتها القوة العسكرية وفي هذا الصدد يقول إبراهيم جابر السيد: (إن قوة الإعلان قد أصبحت أقوى من قوة الجيوش، ولم يعد من الممكن تجاهل هذه القوة وإهمال تأثيراتها وسطوتها، ذلك لان حادثة واحدة نقلها عبر الصحف المؤثرة وعلى الشاشات الصغيرة تحدث دويا هائلا يفوق في وقعه وإيذائه للعدو تأثير حرب كاملة بكل ما تعنيه الكلمة)⁽³⁾.

• العنصر الشبكي:

يعد تغير هيكل الدولة إلى الهيكلية الشبكية نتيجة الدخول في عصر العولمة والإنترنت سببا في تغيير مقومات النظام الدولي، وظهر ما يعرف بالقوة الرقمية أو القوة السيبرانية⁽⁴⁾، فالقوة في العصر الحديث هي؛ قوة الدولة على حماية منظوماتها المعلوماتية وشبكات الإنترنت والاتصال وتوفير فضاء إلكتروني آمن⁽⁵⁾.

ثانيا: القوة الإلكترونية في التفاعلات الدولية:

يعد الفضاء الإلكتروني مجالا واسعا لكل الفواعل الدولية أيا كان حجمها لتحويله إلى ساحة لممارسة أشكال وأنواع القوة الناعمة والصلبة، ويعود السر في ذلك إلى السمات التي يتسم بها هذا الفضاء الرحب من قلة التكلفة حال استغلاله، وإضفاء نوعا من الغفلية والمجهولية على المتعاملين فيه، وهذا الأمر لم يكون ممكنا ولا متاحا في ظل آليات القوة التقليدية، والقوة الإلكترونية واسعة اتساعا كبيرا مقارنة بمفهوم القوة في الأدبيات السياسية التقليدية، فالقوة التقليدية قد فرضت عليها

⁽¹⁾ voir: Camille **GRAND**, Pierre **GROSSER**, *Les Relations internationales depuis 1945*, Hachette Education (programme ReLIRE), 2000, P.38:

<https://www-cairn-info.snd11.arn.dz/les-relations-internationales-1945--9782011453150.htm>

⁽²⁾ مازن محمد علي، المرجع السابق.

⁽³⁾ إبراهيم جابر السيد، الاتجاهات الحديثة في الإعلام الصحفي، الطبعة الأولى، مؤسسة طيبة للنشر والتوزيع، القاهرة، 2015، ص 85.

⁽⁴⁾ فردوس محمد عبد الباقي، العلاقات بين الكوريتين ومصالح القوى الكبرى، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2019، ص ص: 74-73.

⁽⁵⁾ مازن محمد علي، المرجع نفسه.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

الكثير من الدول سيطرتها وهيمنتها غير أن هذا الفضاء يعتبر عصيا عن فرض السيطرة كونه لا يوجب أو يلزم بالتكافؤ في القدرات⁽¹⁾.

ومع ذلك، ورغم تعدد الفواعل وعدم تكافؤ القدرات كميزتين أساسيتين للقوة السيبرانية إلا أن جوزيف ناي يفرق بين مفهومين جوهريين فيما يتعلق بمفهوم القوة، أولهما اتساع القوة، وثانيهما توازن القوة، وأقر بأن الأول لا يعني الثاني، فاتساع القوة لا يعني بالضرورة توازنها، فالهجمات السيبرانية التي يقوم بها الفاعلون من غير الدول من غير الممكن أن تكون بنفس المستوى الذي تكون عليه لو ارتكبتها الدول، وذلك لاختلاق الإمكانيات والقدرات، وكذلك الأهداف التي يتم توجه الهجمات إليها⁽²⁾.

ولا تنطبق هذه الأطروحة فقط على الفاعلين من غير الدول، فتوازن القوى السيبرانية يشمل أيضا حتى الدول، ولفهم هذه النقطة، يجب العودة إلى الطبقات التكوينية للفضاء الإلكتروني، فهي المعيار الأساسي الذي يحدد توزيعات القوى السيبرانية وتوازنها في العالم، ومن خلال النظر فيها، نجد أن الولايات المتحدة الأمريكية تحتل صدارة القوى السيبرانية، وذلك لكون البنى التحتية للطبقة المادية مرتكزة فيها، فضلا عن سيطرتها على تجارة الوسائط المادية، أما الطبقة المنطقية فإن الكثير من الشركات المنتجة لأنظمة التشغيل والبرمجيات هي شركات أمريكية، وإرغام الحكمة لها بالتعاون معها يعد مركزا من مركز القوة السيبرانية، أما الطبقة المعلوماتية فهي بدورها مرتعا للصراعات على القوة والهيمنة، ويظهر ذلك من خلال سيطرة محتوى شركات مثل آبل أو أمازون أو قوقل على الفضاء الإلكتروني⁽³⁾.

لقد تمكن الفضاء الإلكتروني من الدخول بشكل كبير ضمن العناصر التكوينية الحديثة لمفهوم القوة بكل مضامينها سواء أكان ذلك في طبيعتها وأشكالها والتوظيف الذي تتجلى فيه، وحتى في طبيعة الفواعل التي توظفه، ولهذا فإن إمكانيات الدول وقوتها قد تأثرت بشكل كبير بهذا المفهوم في الجديد للقوة في علاقاتها بغيرها خارج حدودها، إذ تحول مفهوم قوة الدولة ليسع ويشمل الإمكانيات كلها مادية كانت أو غير مادية، حسية كانت أو غير حسية، التي تمكنها من تحقيق

(1) سميرة شرايطية، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي، *المجلة الجزائرية للأمن والتنمية*، المجلد 09، العدد 16، جامعة باتنة 1، باتنة، الجزائر، جانفي 2020، ص ص 396-410

<https://www.asjp.cerist.dz/en/article/105815>

(2) جوزيف إس. ناي، مستقبل القوة، المرجع السابق، ص 166.

(3) Voir: Taillat, Stéphane, Amaël Cattaruzza, et Didier Danet. *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, 2018, PP.22-23: <https://doi-org.snd1.arn.dz/10.3917/arco.danet.2018.01>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

المصالح وإحداث الفاعلية السياسية⁽¹⁾، وهذا خلافا لما كان عليه الأمر في ظل المفهوم التقليدي للقوة الذي لا يعترف إلا بالقوة المادية والترسنة العسكرية والعناصر المحسوسة.

يمكن اعتبار القوة السيبرانية في العصر الحديث بأنها قدرة الدولة القومية على فرض سيطرتها من خلال إحداث تأثيرات بالجوء إلى توظيف الفضاء الإلكتروني أو ممارسة أشكال السيطرة على ساحاته وهذا من أجل دعم المجالات الأخرى للسلطة في الدولة، ولا يتطلب تحقيق القوة السيبرانية إلى تعقيدات كبيرة كالتى كانت تنسم بها المجالات التقليدية إذ يكفي أن تقوم الدولة بتطوير البنية التحتية التكوينية لهذا الفضاء لتحقيق القدرة والقوة على فرض السيطرة والهيمنة⁽²⁾.

يعرف جوزيف ناي⁽³⁾ القوة الإلكترونية على أنها: (مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل)⁽⁴⁾.

كما يرى أيضا بأنها: (القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية " فهي على حد رأيه " مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية للمعلومات والمهارات البشرية المدربة للتعامل مع هذه المسائل)⁽⁵⁾.

لقد سمح الفضاء الإلكتروني بخلق أشكال وآليات جديدة لتوظيف وممارسة الهيمنة وفرضها على كل الأصعدة من خلال قدرة الدول الكبرى على السيطرة على المعلومات واستئثارها بها والتحكم في عملية تدفقها، والاستحواذ عن القوة الإلكترونية أيا كان نوعها، وقد استطاعت هذه الآليات في بسط النفوذ الخارجي على الكثير من الدول، الأمر الذي ساهم بشكل مباشر في إنشاء

⁽¹⁾ علاء الدين فرحات، الفضاء السيبراني: (تشكيل ساحة المعركة في القرن الحادي والعشرين)، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 03، كلية الحقوق والعلوم السياسية، جامعة حمة لخضر، الوادي، ديسمبر 2019، ص ص: 88-107

<https://www.asjp.cerist.dz/en/article/108478>

⁽²⁾ سميرة شرايطية، المرجع السابق.

⁽³⁾ جوزيف ناي (Josef NYE): أستاذ العلوم السياسية وعميد سابق لمدرسة جون كينيدي في جامعة هارفارد، أسس مركز الدراسات الليبرالية الجديدة والعلاقات الدولية، تولى العديد من المناصب، منها مساعد وزير الدفاع للشؤون الأمنية الدولية في حكمة كليتتون. نقلا عن الموسوعة الحرة، (ويكيبيديا)، جوزيف ناي.

⁽⁴⁾ نقلا عن: علاء الدين فرحات، المرجع نفسه.

⁽⁵⁾ إسماعيل زروقة، المرجع السابق.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

المنظومة الإعلامية الدولية لتسيطر بشكل كامل على عملية تنظيم تدفق المعلومات عبر الحدود، والتحكم فيها وتحديد سياسة الدول في المجالات الاقتصادية والثقافية⁽¹⁾.

لقد استطاع الفضاء الإلكتروني من تغيير قواعد اللعبة وإحداث تبدلات جذرية في أطرافها وفي مساراتها، لقد استطاعت الهيمنة الإلكترونية عبر هذه الآليات بكل جداره من أن تحتل محل الأشكال التقليدية للهيمنة وأصبح لها أبعاد ومرامي مختلفة كدورها الذي تلعبه في نقل القيم الثقافية الغربية إلى العالم بأسره، وتشكيل نوع من المواجهة ما بين هذه الثقافة الوافدة وبين الثقافة والقيم المحلية كما أن حجم تدفق المعلومات الدولي وإلى جانبي ما لها من تأثير على البنية الاقتصادية فإن لها تأثيرا معنويا فتاكاً، والذي يتحدد في قدرتها على استعباد العقول واحتلالها وخلق روافد داخلية لها عبر خلقي عقول لا ترتبط أو تعاطفت مع قوى خارجية⁽²⁾.

الفرع الثالث: ظهور الدبلوماسية الرقمية على الساحة السيبرانية:

تعتبر الدبلوماسية من المفاهيم التي تباينت فيها الآراء واختلفت بين موسع في تعريفها وبين مضيق ومع هذا تعتبر آلية ذات أهمية كبيرة في تمثيل الدولة خارجياً وهي الآلية التي تقوم الدولة من خلالها بتنفيذ استراتيجيتها الخارجية (أولاً) ومع التطور التقني وظهور الفضاء الإلكتروني أخذت في اكتساب بعداً رقمياً فتوسع مفهومها وتحولت أهدافها من نطاق ضيق إلى نطاق أوسع لتشمل الجماهير (ثانياً).

أولاً: الإطار المفهومي للدبلوماسية:

تعتبر الدبلوماسية من أهم الآليات التي تقوم الدولة من خلالها بتطبيق وإنجاز سياساتها الخارجية، وحماية بنيتها ونظامها من خلال صون سيادتها الوطنية وتعزيز أمنها واستقرارها، وتحسين قدراتها وقوتها، وترقية حجم الرخاء لمواطنيها، كما تهدف أيضاً إلى تحقيق التوسع بمفهومه الواسع، وتلبية متطلبات الدفاع عن نهجها ونظامها ورؤيتها السياسية قبل غيرها من الدول، فهي إذا آلية ذات أهمية حرجية في إحداث التأثير الذي تروم إليه الدولة على الساحة الدولية من خلال التعامل بشكل مباشر مع غيرها من الدول، والتي يمكن أن تحقق مصالحها معها بواسطة استخدام الوسائل والتكتيكات التي تتوفر عليها الدبلوماسية من مفاوضات واتصالات وغيرها، وأهمية هذه الدبلوماسية تكون أكثر قوة مع بروز فواعل دولية جديدة تشارك الدول عملية صياغة القرارات، وتكون أيضاً ذات أهمية خاص بالنسبة للدول التي لا تتمتع بقدر كبير من القوة،

(1) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المرجع السابق، ص 52 و 53..

(2) المرجع نفسه، ص 52.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

التي تسمح لها بحماية نفسها من أشكال التهديد التي تحقق بها، فتكون حينها الدبلوماسية سلاحا تواجه به هذه التهديدات والأخطار⁽¹⁾.

فالدبلوماسية هي: (علم وفن تمثيل مواقف الأشخاص القانونية الدولية في علاقاتها الخارجية عبر أجهزة يطلق عليها البعثات الدائمة أو المؤقتة) ويمكن تعريفها أيضا بأنها: (علم العلاقات بين أشخاص القانون الدولي العام أي الدولة والمنظمات الدولية للحفاظ على مصالحها المتبادلة وفن تمثيلها وإجراء المفاوضات، أي أنها وسيلة تطبيق القانون الدولي العام " ويعرف القانون الذي ينضم قواعدها وأسسها بأنه " فرع من فروع القانون الدولي العام الذي يضم القواعد القانونية التي تهتم بتنظيم العلاقات الدبلوماسية بين أشخاص القانون الدولي العام)⁽²⁾.

تعرف الدبلوماسية أيضا على أنها: (تسيير العلاقات الدولية بالأسلوب الودي والسلمي من خلال التفاوض وفقا للإجراءات والبراسيم المتعارف عليها، تحقيقا للمصلحة أو حفاظا عليها باستخدام الحكمة والنباهة)، وهي تتجلى في صورتين؛ أولهما التمثيل الدبلوماسي الذي يبرز الدبلوماسية في وجهها المهني والوظيفي وثانيهما هو التسيير الدبلوماسي للعلاقات الدولية وهذا توصيف يتخطى حدود النظرة التقليدية للدبلوماسية حيث اعتبرها آلية في تسيير وإدارة الشؤون الدولية⁽³⁾.

فالدبلوماسية في مفهومها الضيق ما هي إلى تكريس لسياسة الدولة الخارجية التي بمقتضاها يتفاوض ممثلو الدول مع نظرائهم من الدول الأخرى كوكلاء عن بلدانهم، فالدبلوماسية بمكوناتها البشري هي الآلية التي تتفاعل بها التواصل ضمن منظمة تواصل مباشرة ودائمة، فهي نظام اتصالي رسمي يسير على وتيرة مستقرة ودائمة بين الدول من خلال تبادل السفراء والإبقاء على السفارات في عواصم دول أخرى، والتراسل الرسمي من خلال مبعوثين يخول لهم تأهيلهم الانخراط في أعمال المؤتمرات والإسهام في المفاوضات المباشرة⁽⁴⁾.

⁽¹⁾ صالح عمر سرور، الدبلوماسية الفلسطينية تجاه القوى المؤثرة في عملية السلام منذ أوسلو، رسالة ماجستير في الدراسات الدولية، كلية الدراسات العليا، جامعة بيرزيت، فلسطين، العام الجامعي 2002-2003، ص 17-20.

⁽²⁾ أمال ديلمي، التنظيم القانون الدولي للعلاقات الدبلوماسية، مذكرة ماجستير في القانون العام، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2012، ص 11-12.

⁽³⁾ محمد الأخضر كرام، فعالية الدبلوماسية في توجيه مسار العلاقات الدولية، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01، السنة الجامعية 2012-2013، ص 23-24.

⁽⁴⁾ مارتن غريفيثس وتيري أوكالاهان، المفاهيم الأساسية في العلاقات الدولية، مركز الخليج للأبحاث، دبي، الإمارات العربية المتحدة، 2008، ص 203.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

يجب النظر إلى الدبلوماسية بنوع من الشمولية في الطرح من خلال النظر إليها نظرة جامعة تتناول كل القضايا المتعلقة والمرتبطة بها، مع عدم الاعتناء والخوض في جزئياتها البسيطة، فليس من الصواب النظر إلى الدبلوماسية على أنها وسيلة تعامل تلجا إليها الدول في علاقاتها مع بعضها فحسب، فلم تعد الدول هي الأشخاص الوحيدة في المجتمع الدولي، فقد ظهر فاعلون جدد على الساحة الدولية وأصبحت الدبلوماسية في شكل يضم المنظمات الدولية الحكومة وغير الحكومية، كما يجب التركيز أيضا على عدم حصر دور الدبلوماسية في التفاوض فحسب، فالدبلوماسية تلعب أدورا شتى وتؤدي شؤوننا عدة، أبرزها تمثيل الدول خارجيا، والمحافظة على مصالحها في إطار التفاعل الدولي متعدد الأطراف والفواعل، ورعاية السلمية فيها⁽¹⁾.

فنقول حينها أنها هي الآلية التي تمكن الدول من معرفة وتقييد علاقاتها الخارجية، فهي بكل بساطة حلقة وصل بين الدول يلجأ إليها الفرقاء منها من أجل حل نزاعاتهم دون الاحتكام إلى عنصر القوة، كما تستعين بها أيضا تلك الجبهات المتحالفة من أجل الارتقاء في مدارك التعاضد والتعاون⁽²⁾.

أو يمكن اعتبارها على أنها: (غرفة المحركات للعلاقات الدولية والطريقة الراسخة التي تحدد بها الدول أهدافها السياسية الخارجية، وتنسق جهودها للتأثير في قرارات وسلوكيات الحكومات والشعوب الأجنبية من خلال الحوار والمفاوضات وغيرها؛ من أجل الحفاظ على السلام، وتطوير النوايا الحسنة تجاه الدول والشعوب؛ لضمان تعاونها أو عدم حيادها)⁽³⁾.

ثانيا: الدبلوماسية الرقمية على ساحة الفضاء الإلكتروني:

1- تعريف الدبلوماسية الرقمية:

إنه لمن النادر أن تجد مراجعا تقوم بمعالجة قضية الدبلوماسية الرقمية وتناولها بالدراسة الوافية، كما أن موضوع الاجتماع على تعريف موحد دقيق غير وارد، فهناك اختلاف كبير بين التعاريف المقترحة بسبب انجراف كل تعريف واقتصره على التخصص الذي يتم توظيف الدبلوماسية الرقمية فيه، لكن المجمع عليه من قبل الدارسين لهذا الموضوع هو أن الدبلوماسية

(1) محمد الأخضر كرام، المرجع السابق، ص 23.

(2) مارتن غريفيش وتيري أوكالاها، المرجع السابق، ص 203.

(3) معاذ العامودي، بحث تحت عنوان: الدبلوماسية الرقمية وتأثيرها في السياسة الخارجية، دراسة مقارنة بين فلسطين والاحتلال الإسرائيلي، مجلة رؤية تركية، السنة 07، العدد 04، شتاء 2018، ص ص: 125-149.

<https://rouyaturkiyyah.com/> الدبلوماسية-الرقمية/الدبلوماسية-الرقمية-الرسمية-وتأثيرها في-السياسة-الخارجية-دراسة-مقارنة-بين-فلسطين-والاحتلال-الإسرائيلي

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

الرقمية ما هي إلا شكل من أشكال الدبلوماسية العامة التي تقوم باستغلال خدمات الفضاء الإلكتروني من أجل السعي إلى مخاطبة الشعوب الأجنبية دون أن يكون لذلك أثر على حجم الإنفاق⁽¹⁾.

إن السبب الذي يحول دون تقديم تعريف موحد للدبلوماسية الرقمية يتمثل في كون هذا المصطلح مصطلح يمتلك قدرا كبيرا من المرونة والتطور، وقد عرفها البعض على أنها: (الاستخدام المتزايد لمنصات الإعلام الاجتماعي من الدولة؛ لتحقيق سياستها الخارجية، وإدارة سمعتها وصورتها بشكل يستبق أي تشويش أو يتصدى له) كما عرفت أيضا بأنها: (استخدام أدوات الاتصال الرقمية بواسطة الدبلوماسيين للتواصل مع بعضهم ومع عامة الناس)، وعبر البعض الآخر عن الدبلوماسية الرقمية على أنها الاستفادة من الخدمات التي يتيحها الفضاء الإلكتروني وتوظيفه من أجل تعزيز المرامي والغايات العامة للدبلوماسية، كما اعتبرت الخارجية الفرنسية على أنها دبلوماسية تقليدية إلا أنها تتم من خلال توظيف الفضاء الإلكتروني في الأدوار التي تلعبها⁽²⁾.

ومبلغ ما ظهر لنا من تعريف الدبلوماسية الرقمية أن جوهرها وغاياتها تتماثل تماما مع جوهر وغايات الدبلوماسية التقليدية، والفرق الذي بينهما هو أن الدبلوماسية الرقمية تستعين بفضاء لا يمكن السيطرة عليه وواسع باتساع هذا الفضاء، فالدبلوماسية التقليدية محدودة الأثر مقارنة بالدبلوماسية الرقمية، وبشكل خاص في محور تواصل أي دولة بالشعوب الأخرى، حيث يمكن لأي رئيس أو أي جهة أخرى في الدولة أن تتواصل مع جميع شعوب الأرض في ظرف وجيز وبتكلفة هزيلة، وهذا ما لم يكن ممكنا في ظل الدبلوماسية البروتوكولية القديمة.

2- الدبلوماسية الرقمية بين المزايا والعيوب:

من خلال مراجعة الأدبية المتعلقة بالدبلوماسية الرقمية يمكن أن نتوصل إلى العديد من المزايا والأهداف التي ترمي إليها الدول من خلال اللجوء إلى الدبلوماسية الرقمية، وقد حصرها وائل عبد العال في 06 أهداف وهي:

" - تكتيل الجهود بين مختلف الجهات في الدولة من أجل التنسيق بين كافة الإدارات والموارد المترابطة في ما بينها كما تمكن الدبلوماسية الرقمية من الاستغلال الأمثل للثروة البشرية بما يحقق المصالح الوطنية في الخارج والزيادة من قوتها الناعمة؛

⁽¹⁾ وائل عبد العال، الدبلوماسية الرقمية ومكانتها في السياسة الخارجية الفلسطينية، سلسلة أبحاث وسياسات الإعلام، مركز تطوير الإعلام، جامعة بيرزيت، فلسطين، 2018، ص ص: 8-9

⁽²⁾ معاذ العامودي، السابق.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

- تعزيز أواصر التواصل مع الجماهير على ساحة الفضاء الإلكتروني وتعمل على تحقيق أكبر قدر من الاستفادة من آليات الاتصال الحديثة من أجل خلق جو من التقارب بين الدولة والجماهير من خلال الاستماع اليهم والتواصل معهم كما تعمل أيضا عبرها على التأثير فيهم؛
- استغلال هذا التدفق الهائل للمعلومات من أجل توظيفه في تحسين الأداء السياسي والعمل أيضا على تعزيز نهج التوقعات لما يستجد من تحركات اجتماعية وسياسية والاستجابة لها؛
- تعزيز التواصل بين القنصليات والجمهور من خلال إنشاء فضاء تواصل شخصي ومباشر بين القنصليات والجاليات في الخارج بما يضمن لهم السلامة في الأزمات؛
- تهدف بشكل خاص إلى دعم حريه الراي والتعبير وتعزيز مبادئ الديمقراطية والحرية كما تهدف أيضا إلى هدم الأنظمة الاستبدادية من خلال هذا الفضاء الإلكتروني الذي لم تعد تنفع معه الشمولية والاستبداد السلطوي واحتكار الرأي؛
- كما تعمل أيضا على خلق وبناء آليات رقميه من أجل العمل على الاستفادة من خبرات وموارد خارجيه من قنصليات وسفارات وتوظيفها من أجل أهداف النهضة الوطنية⁽¹⁾.
- كما تبرز أهداف اللجوء على الدبلوماسية الرقمية من خلال المزايا التي تتمتع بها، فالدبلوماسية الرقمية تتسم بالسرعة في الإنجاز، وقلة التكاليف، واختزال الوقت⁽²⁾.
- وتتسم أيضا بقدرتها التأثير على أشكال التنظيم الاجتماعي عبر تعزيز فكره الربط بين المجتمعات المختلفة وفتح مساحة للتجمعات الإلكترونية والعمل على عقل المجتمعات المحلية إلى مساحة أوسع وهي ساحة التفاعلات الدولية والسياسة العالمية وهذا من أجل خلق رأي عام دولي حول القضايا والمطروحة، وحشده وتعبأته، كما تتسم أيضا بالشفافية والتي بمقتضاها يتم تداول المعلومات ونشرها في وسط عالم متقارب إذ توفرت الآليات التي من خلالها يتم التكتل والنضال لدعم القضايا العالمية⁽³⁾، ولذلك تلجأ الدول إلى توظيفها واستعمالها.
- لكن، تحقيق الدولة لهذه الأهداف والمزايا يتوقف على حد رأي ديفيد ستيفن على عناية الدولة الكبرى في توعية وتدريب وتأهيل موظفي السلط الدبلوماسي، وذلك من خلال إحاطتهم بكل

(1) وائل عبد العال، المرجع السابق، ص 11.

- أنظر أيضا: محمد عدنان محمود، الدبلوماسية في العصر الرقمي والتطور النوعي في الدبلوماسية التقليدية، مركز البيان للدراسات والتخطيط، بغداد، 2020، ص 13.

(2) محمد عدنان محمود، المرجع نفسه، ص 14.

(3) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2009، ص ص: 64-65: متوفر على الموقع: https://www.elsiyasa-online.com/2019/07/blog-post_5.html?m=1

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

ما يتعلق بالتكنولوجيا الحديثة واستخداماتها وما قد ينجر عنها من مخاطر، ولا يتحقق ذلك إلا من خلال ممارسة فعلية ومكثفة⁽¹⁾.

ومع ذلك تبقى للدبلوماسية الرقمية عيوبها، وقد ظهرت هذه العيوب من خلال أسلوب الرئيس الأمريكي دونالد ترامب في التعامل مع ما يتيح الفضاء الإلكتروني من خدمات دبلوماسية، أسلوب يتضارب مع ما تعارفت عليه الاتفاقيات والأعراف الدبلوماسية، والذي قد ينجر عنه أحد احتمالين؛ إما أن يعطل هذا الأسلوب الفج الممارسات الدبلوماسية التقليدية ويعمل على إثارة الخلافات الدولية، أو يؤدي إلى ظهر أشكال جديدة من الاتفاقيات والأعراف الدبلوماسية التي يكون محورها الأساسي هذا التوظيف الجديد للفضاء الإلكتروني في المجال الدبلوماسي⁽²⁾.

وهذا الاحتمال الأخير هو بالفعل ما نشجع عليه، لأن الفضاء الإلكتروني لم تعد تتناسب مع طبيعته تلك القوانين التي صيغت منذ عقود، وليس من السهل لي أعناق تلك الأعراف الدبلوماسية لتتناسب مع الطفرة التي أحدثها الفضاء الإلكتروني في عالم الدبلوماسية، لذلك يتعين خلق ضوابط وأحكام جديدة تسير هذا الفضاء المتطور والمرن، وتحدد آليات اللجوء إليه والأحوال التي يوظف فيه، تقاديا لأثار الأزمات الدبلوماسية، خاصة وأن الدولة الآن لم تعد الفاعل الوحيد في منظومة الدبلوماسية، لذلك من الصعب جدا احتواء الأزمات التي تتمخض عن التوظيف السلبي للدبلوماسية الرقمية.

ففي السابق كان بالإمكان لأي أزمة دبلوماسية أن تحل بين طرفي أشخاص القانون الدولي المعنية، أما الآن فليس من السهل ذلك، وذلك لدخول الشعوب في هذا المضمار، وقد تبين لنا ذلك في الأحداث الأخيرة التي نتجت عن تغريدات الرئيس الفرنسي إيمانويل ماكرون حول تصريحاته السابقة حول الإسلام، والتي ألهم مواقع الإنترنت ووسائل التواصل الاجتماعي، وكان الرد عليها فوراً بمبادرات شعبية لمقاطعة المنتجات الفرنسية، وهذا الذي أطال في عمر الأزمة، وزاد من حدة تداعيتها سواء على مستوى الأمن أو على المستوى الاقتصادي لفرنسا.

3- الأبعاد الاستراتيجية للدبلوماسية الرقمية:

أ- البعد الجماهيري:

لقد أضحت الدبلوماسية الرقمية ذات أبعاد جماهيرية عندما أصبحت آلية يلجأ إليها الساسة

⁽¹⁾ نقلا عن: الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، الدبلوماسية الرقمية .. القوة الناعمة الجديدة، 22 نوفمبر 2018، تم الاطلاع عليه بتاريخ 06 فيفري 2021، على الساعة 17:23 سا، مختصر الرابط: <https://cutt.us/mgCZg>

⁽²⁾ ميلود حمزاوي، الدبلوماسية الرقمية وتوظيفها عند الرئيس الأمريكي دونالد ترامب، المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 01، جامعة الحاج لخضر باتنة 01، الجزائر، جانفي 2020، ص ص: 466-479:

<https://www.asjp.cerist.dz/en/article/105820>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

في تواصلهم مع شرائح ضخمة من الشعوب، سواء أكان ذلك على المستوى الداخلي أو على المستوى الدولي، وأصبح الفضاء الإلكتروني آلية فعالية في إحداث تأثيرات واسعة النطاق والتي لم يكن لها أن تحدث لولا أن الفضاء الإلكتروني لم يكن يعتاده ملايين البشر.

وقد ظهرت فعالية الدبلوماسية الرقمية من خلال قدرة الرئيس الأمريكي باراك أوباما والحزب الديمقراطي في استغلال هذه الميزة الرقمية لأحداث تأثير كبير على الجماهير إبان حملة الرئاسيات الأمريكية في 2008، فقد أنشأ هذا الحزب غرنا حوت أكثر من ستين ألف جهاز كمبيوتر بالإضافة إلى فرع عمل موزعة على كامل التراب الأمريكي في حملة لدعم المرشح من خلال ممارسة نوع من التأثير على الجماهير والترويج لبرنامجهم، فالمسؤولون في قطاع الدبلوماسية الرقمية يملكون قدرا كبيرا من المرونة والانتشار بحيث يمكنهم أن يكونوا قواعد بيانات كبيرة من خلال التقاط ما يدور على الإنترنت لمعرفة الإطار العام لنمط تفكير الطرف الآخر سواء أكان جمهورا أو الجهات جهات رسمية فاعلة في الداخل والخارج⁽¹⁾.

وتعد الحملة الإلكترونية التي أطلقها باراك أوباما هي العامل الأبرز الذي وقف وراء فوزه برئاسيات 2008، وهو الذي شجع إدارته بعد ذلك في إنشاء ودعم استراتيجيات الدبلوماسية الرقمية في إطار المشاريع التي تشرف عليها وزارة الخارجية، فالدبلوماسية الرقمية من وجهة نظر الولايات المتحدة الأمريكية هي استراتيجية بناء العلاقات والاتصال المباشر مع قطاع الشباب بدلا من الدبلوماسية القديمة القائمة على البعد الجغرافي والمكاني⁽²⁾.

ب- البعد السياسي للدبلوماسية الرقمية:

لقد فتح الفضاء الإلكتروني مجالا انتقلت إليه الشعوب وأصبحت تمارس فيها قدرا كبيرا ومستويا عليا من الرقابة متخطية بذلك المستوى الرسمي الحكومي، ولهذا وجت الحكومة نفسها ملزمة بالاتجاه إلى هذا الفضاء لمسايرة هذا المستوى العالي من خلال الدبلوماسية الرقمية التي أصبح الوسيط الأكثر أهمية في التواصل بين الشعوب والسلطات الحاكمة لتحقيق نوع من الاتزان السياسي، كما لا يخفي أيضا ما لهذه الدبلوماسية الرقمية من تأثير واضح وكبير على طبيعة العلاقات الدولية التي بدأت بواره في الظهور بإنشاء الولايات المتحدة الأمريكية لمكتب تخصصي في الدبلوماسية الرقمية سنة 2002⁽³⁾.

(1) معاذ العامودي، المرجع السابق.

(2) منير بودردابن، جهود الدبلوماسية العامة الأمريكية في تنفيذ السياسة الخارجية وتحسين الصورة ضمن معايير الترتيبات والمصالح الأمنية تجاه العالم العربي، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، السنة الجامعية 2017-2018، ص 300.

(3) معاذ العامودي، المرجع نفسه.

وكان ذلك بصفة خاصة مع الظروف السياسية الخارجية التي مرت بها الولايات المتحدة الأمريكية في تلك الفترة كتأزم الوضع في العراق وما ترتب عنه من خسائر كبرى، وعدم تمناها من تحقيق المرامي - أو المزاعم - من حربها في العراق وأفغانستان في نشر الديمقراطية والقضاء على التنظيمات الإرهابية التي ازدادت أداها ووتيرة عملها بعد الحادي عشر من سبتمبر 2001، هذا كله مع غياب سياسة أمريكية واضحة تجاه قوى دولية صاعدة وأخرى متعافية⁽¹⁾.

ج- البعد التواصلي للدبلوماسية الرقمية:

إن التغيرات التي ترتبت عن تحول الفضاء الإلكتروني إلى منصة كبرى تحوى كما هائلا من المعلومات أجبر الدول على إنشاء جيوش إلكترونية تعمل بصفة أساسية على ترشيح البيانات أو إعادة توجيهها كآلية بالغة الأهمية في السياسات الخارجية لها، وعلى هذا الأساس تزايدت التصريحات الرسمية للدول في هذه الساحة وتزايد معها تفسير مواقفها، وازداد بذلك كله تفاعل الاتجاهات الرسمية مما خلق نوعا من الثقة الجماهيرية بالمستوى الرسمي، وأصبح الدبلوماسية قوة تواصلية كبرى تنتهجها الكثير من الدول والكيانات وعلى رأسها الكيان الإسرائيلي الذي يوظف الدبلوماسية الرقمية بشكل ملفت للنظر وأبرز الوجود الإسرائيلية المعروفة في تحريك دفة التبريرات وتقديم التفسيرات للمجتمع الدولي نجد المتحدث الرسمي عن الجيش الإسرائيلي " أفخاي أدري " ⁽²⁾.

كما نجد أيضا الولايات المتحدة الأمريكية التي تعمل من خلال هذا الفضاء بما فيه من تقنيات عالية، وإمكانيات السيطرة وإحداث التغيرات عند بعد، على إدارة سلوكيات وتوجهات الأفراد من خلال التحكم فيهم وقيادتهم والتحكم في خياراتهم من أجل تحقيق غاياتها السياسية، وليس في هذا الطرح أي مغالاة ولا عزوف عن واقع، فالفضاء الإلكتروني أصبح له دور قيادي كبير وصف بأنه " تشي غيفار القرن الواحد والعشرين " ⁽³⁾.

واستخدمت بريطانيا أيضا أكبر عدد ممكن من المواقع وحسابات التواصل الاجتماعي بالعديد من اللغات لأغراض تنشيط الدبلوماسية الرقمية وتطويرها، كما تعتبر فرنسا من بين الدول الرائدة في هذا الميدان أيضا، فقد كان لها سبق في استغلال مجال الفضاء الإلكتروني لأغراض دبلوماسية كما نجد الدنمارك أيضا قد خطت خطوة كبيرة نحو الدبلوماسية الرقمية حين تفردت بتعيين أول سفير تكنولوجي في العالم ⁽⁴⁾.

(1) منير بودرداين، المرجع السابق، ص 301.

(2) معاذ العامودي، المرجع السابق.

(3) علي محمد الحاج حسين، الحرب الناعمة الأسس النظرية والتطبيقية، الطبعة الأولى، المركز الإسلامي للدراسات الاستراتيجية العتبة العباسية المقدسة، دون بلد النشر، 2018، ص 72.

(4) وائل عبد العال، المرجع السابق، ص ص: 14-16.

وخلاصة لما سبق، يمكن القول بأن الدبلوماسية الرقمية تحتل مرتبة عالية ومكانة مرموقة في سلم أولويات الدول، وذلك نظرا لأبعادها الثلاثة المذكورة آنفا، والتي تلخص في جوهرها أبعاد السيطرة والهيمنة على الرأي العام وتوجيهه وفق السياسات والإيديولوجيات التي تسعى إليها القوى الكبرى لتكريسها، فالدبلوماسية الرقمية في واقع أمرها، لا تعدوا أن تكون آلية ووسيلة أخرى من الوسائل الناعمة التي توظف من أجل فرض السياسات وإثبات القوة، وتوسيع النفوذ.

المطلب الثاني:

الفضاء الإلكتروني والتحول في مفهوم الأمن

يؤكد التاريخ والواقع أن الأمن من بين أكثر المقاصد الإنسانية أهمية، فمنذ فجر التاريخ والإنسان يحاول أن يحقق جوانبه ويضمن دوامه، ولهذا نجده مفهوما متشعبا في عناصره وكثير في مكوناته ومعقدا في مدلولاته وهذا نظرا لعلاقته الوطيدة بالكثير من الجوانب الأساسية المتعلقة بحياة الأفراد والمجتمعات، ومع ظهور الفضاء الإلكتروني أخذ مفهوم الأمن ستخذ مفهوما أكثر اتساعا وشمولا، وأخذ طبيعته تتغير كلما زاد الاعتماد على هذا الفضاء (الفرع الأول). كما أن هذا الاعتماد أيضا من شأنه أن يوسع من دائرة مكونات الأمن على الساحة السيبرانية ويفتح أبعاد أخرى له (الفرع الثاني) نظرا لما استجد على الفضاء الإلكتروني من أشكال وأنماط متعددة من التهديدات والتحديات التي تفرض على المجتمعات والدول أن تجابهها وترفعها (الفرع الثالث).

الفرع الأول: أثر الفضاء الإلكتروني في تغيير مفهوم الأمن:

إن مفهوم الأمن عموما يعتبر من بين أهم المتطلبات البشرية التي تضمن الاستمرارية والاستقرار للجنس البشري كونه البيئة التي في كنفها يمكن للإنسان سواء أكان فردا أو جماعة أن يتطور في كل المجالات ولاسما في قطاع التنمية الاقتصادية والاجتماعية (أولا) وقد مفهوم الأمن بعدة مراحل في تكوينه إلى أن ظهر الفضاء الإلكتروني كبعد أو مجال جديد من المجالات الحيوية فأصبح الأمن أكثر اتساعا وأكثر بعدا (ثانيا).

أولا: التطور المفهومي للأمن:

يعتبر الأمن من المتطلبات المحورية والضرورية للفرد والمجتمع، إذ أنه يعد القاعدة الجوهرية التي تنشأ عليها المدنيات والحضارات وتقوم، فلا يمكن تصور قيام المدنية والحضارة الإنسانية بغير مرتكز الأمن وقدر كبير من السلامة والطمأنينة التي لا تتحقق إلى بتوفر قدر كبير من الانطباع الفردي والجماعي بانعدام أي تهديد لها أو تعكير لصفو طمأنينيتها، وعلى هذا سعت المجتمعات

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

واعنتت بأوجه ومظاهر تفعيل القواعد التي تجرى عليها السلوكيات العامة كما بذلت جهدا كبيرا للوفاء بالمسؤوليات الملقاة على عاتقها تجاه رعاياها من أجل ضمان الأمن والاستقرار لمجتمعاتها وبذلك الحفاظ على المسيرة الآمنة للحياة البشرية بكاملها⁽¹⁾.

ويعتبر مفهوم الأمن من بين أكثر المفاهيم غموضا وتشابكا بشهادة المتخصصين في المجالات الأمنية والاستراتيجية حتى غدى من غير الممكن إيجاد اتفاق على تعريف موحد للأمن يمكن أن يركن إليه الباحثين والمهتمين بهذا الحقل، وقد كان هناك الكثير من الاجتهادات التأصيلية التي سعت إلى وضع تعريفه ومن أبرزهم دانيال كوفمن الذي صرح بأن مفهوم الأمن يكتنفه الكثير من الغموض وتحوم حوله العديد من الاختلافات التي تتباين وتختلف على حسب اختلاف ثقافات المجتمعات وأمكنتها⁽²⁾.

وترجع أسباب تعقيد مفهوم الأمن خاصة في السنوات الأخيرة إلى ثلاث عوامل أساسية حددها تيري بلزك والتي يتمثل أولها في التراجع الذي شهدته سمات ومدلولات السيادة، وثانيها يتمثل في هذه النقطة النوعية التي تشهدها التفاعلات الدولية، واتساعها توسعا كبيرا، وأما ثالثها فيتبلور في ارتفاع بؤر التوتر التي يشهدها العصر الحديث على الصعيد الدولي⁽³⁾.

فالتدهور الذي حصل مع إضفاء الطابع المؤسسي لمضمون سيادة الدولة، وكذلك الإيديولوجية المحركة لضمان حماية هذه السيادة، قد حول بشكل كبير وحوّر مفهوم الأمن، فضلا عن التفاعلات التي نتجت على الساحة الدولية وتنامي حدة الصراعات المشمولة بالطابع الهوياتي، أين تكون الهوية محورا أساسيا في تحديد مفهوم التهديد وشكله، ومن ثم تأثيره على مفهوم الأمن⁽⁴⁾.

كما يمكن إرجاع ضبابية مفهوم الأمن وغموضه إلى العولمة وما ترتب عنها من نتائج، فالعولمة على حد رأي علي عباس مراد قد كانت السبب في ظهور الأمن القومي وتعيين صورته، كما

(¹) خليفة إبراهيم عودة التميمي، الأمن والمجتمع: (دراسة في العلاقات بين المؤسسات الاجتماعية والمؤسسات الأمنية)، مجلة كويه، العدد 08، كلية القانون، جامعة كويه، أربيل، العراق، 2008، ص ص 352-382 =

https://scholar.google.com/citations?user=oak8ctMAAAAJ&hl=ar#d=gs_md_cita-d&u=%2F&view_op=3Dview_citation%26hl%3Dar%26user%3Doak8ctMAAAAJ%26citation_for_view%3Doak8ctMAAAAJ%3AKIAU1dfN6UC%26tzmom%3D-60

(²) محمد جمال مظلوم، الأمن غير التقليدي، الطبعة الثانية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2012، ص 15.

(³) عبير بهلولي، النظرية الواقعية البنوية في الدراسات الأمنية: (دراسة لحالة الغزو الأمريكي للعراق في 2003)، مذكرة ماجستير في العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية والإعلام، جامعة الجزائر 03، السنة الجامعية 2013-2014، ص 16.

(⁴) Thierry BALZACQ, *Qu'est-ce que la sécurité nationale ?*, *Revue internationale et stratégique*, Institut de relations internationales et stratégiques, N° 52, 2003, PP. 33-50: <https://www.cairn.info/revue-internationale-et-strategique-2003-4-page-33.htm>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

نتج عنها أيضا امتداد لمجاله وأبعاده وضوابطه، فضلا عن مساهمته للتحولات الدولية من جهة، ولمقتضيات العولمة من جهة أخرى⁽¹⁾، وهذا بلا شك قد أثر في الأدبيات والحوارات المتعلقة بمفهوم الأمن، وزادت من حجم الصخب الذي يثار حوله.

يعرف الأمن كونه: (حالة من السلم التي تسود وتتوفر وفقا لمجموعة من الإجراءات الملائمة والوسائل الاقتصادية والعسكرية والسياسية والاجتماعية والبيئية التي تهدف إلى حماية الدولة من الداخل وتدفع التهديد الخارجي عنها، سعيا للحفاظ على ثقافتها وهويتها بما يكفل لشعبها حياة مستقرة توفر شروط التطور والتقدم وذلك مع استمرار هذا الفعل في الحاضر والمستقبل)، كما يعرف أيضا في إطار النظام الدولي على أنه: (قدرة الدولة والمجتمعات على الحفاظ على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي تعتبر معادية)⁽²⁾.

ويعرفه الوزير السابق لوزارة الدفاع الأمريكي ليبمان على أنه: (المقدرة على المحافظة على الأمة وعلى كرامتها وأراضيها واقتصادها وحماية مواردها الطبيعية ودستورها من أي اعتداء خارجي) ويرى ولتر ليبمان⁽³⁾ أن: (الأمة آمنة طالما أنها ليست في خطر التضحية بالقيم الأساسية وأنها قادرة إذا تم تحديها على صيانة أمنها بالانتصار في تلك الحرب) كما عرفه دانيال كوفمن بأنه: (حماية الأمن والمحافظة عليه من أي عدوان خارجي)⁽⁴⁾.

ومن الواضح من التعريف الذي قدمه ليبمان يعول كثيرا على الجانب العسكري، ففي رأيه الأمن لا بد له من أمر يكفله، وهذا الأمر هو المجال العسكري وقوتها، فتحقيق امن الدولة وحمايته مرهون بما تملكه من القوة العسكرية ما تضمن به قدرتها على مواجهة مهددات أمنها وبذلك المحافظة على مصالحها، ومن خلال هذه التعاريف مجملا يمكن أن نلاحظ أن السياق الذي يجرى بها الأمن في الفكر الغربي هو مجرى الأمن والتهديدات الخارجيين، فتعريف كوفمن تضمن عبارة "عدوان خارجي" كما ضمن تعريف براون عبارة "اعتداء خارجي" وبالنسبة لتعريف ولتر فإنه استعمل عبارة "الانتصار في الحرب" ومن خلال هذا يمكن تكوين صورة نمطية لمفهوم الأمن في رأيهم، والذي يتمحور على أمور أساسية ومحاور جوهرية هي من هي من صلب الأمن

(1) علي عباس مراد، الأمن والأمن القومي: (مقاربة نظرية)، الطبعة الأولى، ابن النديم للنشر والتوزيع ودار الروافد الثقافية ناشرون، الجزائر-لبنان، 2017، ص ص: 29-30.

(2) المرجع نفسه، ص 19-20

(3) والتر ليبمان (WALTER LIPPMANN): 1974-1889: كاتب أمريكي ومراسل ومعلق سياسي شهير، وهو عضو في الاكاديمية الأمريكية للفنون والعلوم، والجمعية الأمريكية للفلسفة، والأكاديمية الأمريكية للفنون والآداب، حصل على جائزة بوليتزر عن فئة الصحافة الدولية.

(4) نقلا عن: محمد جمال مظلوم، المرجع السابق، ص 15.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

على حد رأيهم، والتي تتمثل في مسألة القوة وقضايا الدفاع وضمان الحرية بالتصدي للتهديدات الخارجية وحماية السيادة وتكوين بنية اقتصادية قوية ومزدهرة، ومن هذا الفكر انطلق السباق نحو التسلح وإنفاق ميزانيات كبرى على اقتناء الأسلحة وصيانتها⁽¹⁾.

ومن الملاحظ أيضا أن لمفهوم لأمن ارتباطا تاريخيا وثيقا بمبدأ الحفاظ على سلامة الدولة من خلال ضمان الحماية الكاملة لمواطنيها، ومن خلال ضمان الحماية الكاملة للحدود الإقليمية مما قد يشكل تهديدا له، ومع التطور الذي طال المجتمع وما تمخض عن تصاعد ظاهرة العولمة والطفرة الكبرى الحاصلة في الكثير من المجالات، تغيرت معها طبيعة التهديدات التي تحق بالدول بما لا تطبق مواجهه بصفة منفردة الأمر الذي انعكس أثره على الأطروحة الأمنية ونطاق دراستها فتحول الأمن من مفهومه التقليدي إلى مفهوم جديد يقوم على أطروحة أمن الأفراد بدل الدول والتي تنطلق من مبدأ كون الإنسان هو المحور الأساسي الذي تدور حوله فكرة نشوء الدولة، وبهذا نشأ الأمن الإنساني ببعده الصحي، البيئي، الغذائي، الشخصي، السياسي، والاجتماعي⁽²⁾، وأصبح هو المسألة المحورية للأمن الذي تسعى الدولة إلى تحقيقه خاصة مع ارتفاع نسبة الهجرة من الدول الفقيرة إلى الدول الغنية وما يترتب عن ذلك صدمات وتوتر في العلاقات بين المكون المجتمعي في الدولة⁽³⁾.

فالتغيرات الدولية المختلفة والتداخل الحاصل بين الشعوب والأمم وكذلك ظهور أشكال جديدة من التهديدات التي تنتهك حرمة الدول وسلامتها داخليا وخارجيا أفضي بشكل كبير إلى ظهور مفهوم الأمن الإنساني والذي غير من طبيعة الأمن ووسع من إطاره.

و تعرف لجنة الأمن الإنساني هذا الأمن الحديث بأنه: (حماية الجوهر الحيوي لكل الحياة الإنسانية، بالطرق التي تحسن من الحريات من الإنسانية، والوسائل الأمنية التي تحمي الحريات الأساسية يعني حماية الإنسانية من التهديدات والأوضاع الحرجة، والواسعة الانتشار، خلال إيجاد نظم سياسية واجتماعية وثقافية واقتصادية وعسكرية، تمنح الأفراد لبنات البقاء على قيد الحياة وكسب العيش والكرامة)⁽⁴⁾.

(1) محمد جمال مظلوم، المرجع السابق، ص ص: 15-16.

(2) مختار يحيوي، تطور آليات مكافحة الإرهاب وانعكاساتها على فكرة الأمن الدولي والأمن الإنساني، مجلة أبحاث قانونية وسياسية، العدد 06، كلية الحقوق والعلوم السياسية، جامعة الصديق بن يحي، جيجل، الجزائر، جوان 2018، ص ص: 279-289: <http://www.univ-jijel.dz/revue/index.php/rjp/article/view/483>

(3) جريدة حمزاوي، التصور الأمني الأوروبي: (نحو بنية أمنية شاملة)، مذكرة ماجستير في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2010-2011، ص 35

(4) العيد ذويوب، مفهوم الأمن في الفكر الديني: (دراسة لأبعاد الأمن الإنساني في الإسلام)، مجلة الدراسات القانونية والسياسية، العدد 05، المجلد 01، كلية الحقوق والعلوم السياسية، جامعة عمار التليجي، الأغواط، جانفي 2017، ص ص: 244-268: <https://www.asjp.cerist.dz/en/article/38037>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

غير أن الأمن الإنساني ليس هو المفهوم الوحيد الذي طرأ على الدراسات الأمنية وسياساتها، فقد نتج عن التطور الكبير الذي شهده العالم في مجال التكنولوجيا المعلوماتية والاتصالية على ظهور مفهوم جديد للأمن يشمل في جوهره كل المفاهيم السابقة مع لمسة حصرية أين يكون للفضاء الإلكتروني وقعه وأثره، وبذلك يظهر الأمن السيبراني كمصطلح جديد في مجال الدراسات الأمنية.

ثانيا: الأمن في الفضاء السيبراني:

إن بيئة الفضاء الإلكتروني أخذت تشغل حيزا كبيرا مع نشاط حركة التطور التكنولوجي في مجال المعلومات والاتصال وأصبحت متعلقة بعد ذلك بأعمال المال والاقتصاد والمجتمع الدولي، وظهرت الكثير من القطاعات الاستراتيجية الهامة في المجال الاقتصادي تعتمد بشكل كبير على هذا البيئة الحيوية، حتى أصبح من الضروري إدراج الأمن ضمن العناصر التكوينية للأمن الوطني لما في ذلك من أهمية في حماية الاقتصاديات المعاصر خاصة مع ارتباط الفضاء الإلكتروني بالظاهرة الإرهابية والبنية التحتية، وقد أخذت أهمية هذا التضمين في الانتشار على نطاق واسع على المستوى الدولي، وقد ظهر ذلك من خلال تبني سياسات أمنية متعددة على صعيد القطاع العام والخاص من خلال خلق جملة من التشريعات والعمل على تبادل الخبرات والرؤى وإنشاء مواقع من أجل ضمان الأمن على الساحة السيبرانية بتأمين المعلومات من التهديدات التي تقوض الأسس الأمنية على الصعيدين الوطني والدولي وتشكل إرباكا شديدا بالنمو الاقتصادي⁽¹⁾.

وبهذا الصدد أصدر اتحاد العلماء الأمريكيين بيانا جاء فيه: (...إن العالم لم يعد يدار بالأسلحة بعد الآن أو الطاقة أو المال، إنه يدار بالأرقام والأصفار الصغيرة... إن هناك حربا تحدث الآن... إنها ليست لمن يملك رصاصا أكثر إنها حول من يسيطر على المعلومات، ماذا نسمع أو نرى؟ كيف نقوم بعملنا؟ كيف نفكر؟ إنها حرب المعلومات.) فمدلول الأمن قد زاد في حيز اتساعه بعد زيادة مفهوم الأمن المعلوماتي إلى مدلولاته المتعددة⁽²⁾.

يعرف الأمن السيبراني من وجه آخر بأنه: (أمن المعلومات على الأجهزة وشبكات الحاسب الآلي والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح بها وتغير أو اختلاف قد يحدث، حيث يتم استخدام

(¹) حكيم غريب، الإرهاب السيبراني والأمن الدولي: (التهديدات العالمية الجديدة وأساليب المواجهة)، المجلة الجزائرية للدراسات السياسية، المجلد 05، العدد 02، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، ديسمبر 2018، ص ص: 104-119:

<https://www.asjp.cerist.dz/en/article/66221>

(²) جمال منصر، تحولات في مفهوم الأمن: (من أمن الوسائل إلى أمن الأهداف)، مجلة دفاتر السياسة والقانون، العدد الأول، جامعة قصدي

مرياح، ورقلة، جانفي 2009، ص ص: 125-139:

<https://www.asjp.cerist.dz/en/article/28305>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع استخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، حيث أن الفضاء السيبراني لا يقتصر على شبكة الإنترنت فقط وإنما شبكات عالمية وخاصة أخرى: (ACARS/SWIFT/GSM/PSTN/GPS)⁽¹⁾.

وتم تعريف الأمن السيبراني بناء على أهدافه ومهامه أيضا باعتباره: (النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصال 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، وبحيث لا تتحول الأضرار إلى خسائر دائمة)، كما يمكن تعريفه أيضا من الزاوية الإجرائية بأنه: (مجموعة من الأدوات والسياسات والمفاهيم الأمنية، والضمانات الأمنية، والمبادئ التوجيهية، من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات، والتدريب، وأفضل الممارسات، وضمان التقنيات التي يمكن أن استخدمها لحماية البيئة الإلكترونية وتنظيم أصول المستخدم)⁽²⁾.

وذهب دارسون آخرون في تعريفه بأنه: (مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، والاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية البيانات الشخصية ولحماية المواطنين)⁽³⁾.

ولقد قدمت وزارة الدفاع في الولايات المتحدة الأمريكية تعريفا للأمن السيبراني باعتباره (جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الإلكترونية والمادية) وعرفه أيضا الإعلان الأوروبي بأنه: (قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات) كما عرّف أيضا بأنه: (عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قرصنة الكمبيوتر وخواصها ويتضمن تنفيذ

(¹) جميلة سلايمي، يوسف بوشي، التحول الرقمي بين الضرورة والمخاطر، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 02، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر، الوادي، سبتمبر 2019، ص ص: 944-967.

<https://www.asjp.cerist.dz/en/article/101691>

(²) سمير بارة، الأمن السيبراني (CYBER SECURITY) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 01 الحاج لخضر، العدد 04، جويلية 2017، ص ص: 255-280.

<https://www.asjp.cerist.dz/en/article/66092>

(³) فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحول الرقمي: (الصن نموذجا)، المجلة الجزائرية للأمن الإنساني، السنة الخامسة، المجلد 05، العدد 01، جامعة باتنة 01 الحاج لخضر، جانفي 2020، ص ص: 789-216.

<https://www.asjp.cerist.dz/en/article/108105>

الفصل الأول الفضاء الإلكتروني والتحول الرقمي في المفاهيم الاستراتيجية

التدابير المضادة) وقد أكد على هذه التعاريف ريتشارد كمرر حين عرف الأمن السيبراني كونه مجموعة آليات ووسائل التي يمكن بها التصدي بالكشف والإحباط للعمليات التي يقوم بها القرصنة، وتم تعريفه أيضا باعتباره أيضا آلية ووسيلة للوقوف أصاد خطر الهجمات التي من شأنها أن تستهدف البرمجيات أو أجهزة الكمبيوتر أو الشبكات وتتضمن هذه الآليات تلك الأساليب والوسائل التي يتم الاستعانة بها في مواجهة ومجابهة القرصنة والكشف عن الفيروسات وتدميرها وتوفير التشفير والسرية للاتصالات⁽¹⁾.

وعرفه الاتحاد الدولي للاتصالات بأنه: (مجموع الأدوات والسياسات، وضوابط الأمن ومبادئ التوجيه، ونهج إدارة المخاطر والإجراءات والتدريب، وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستخدمين، وتشمل أصول المؤسسات والمستخدمين أجهزة الحوسبة الموصولة بالشبكة، والموظفين، والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية)⁽²⁾.

والظاهر لنا من خلال هذه التعاريف أن هناك خلط كبير في أوساط الباحثين بين أمن المعلومات وأمن الفضاء الإلكتروني أو السيبراني، فأمن المعلومات هو جانب من جوانب أمن الفضاء الإلكتروني، وعنصر من عناصره، وذلك باعتبار أن المعلومات في حد ذاتها جزء تكويني للفضاء الإلكتروني، فلا يمكن بذلك تعريف عنصر من عناصر أمن الفضاء الإلكتروني وبسطه على كامل الفضاء الإلكتروني، إذ ليس من المستساغ عقلا ولا منطقا تعريف الجزء وحمل الكل على معنى الجزء.

وثمة فرق جوهري بين أمن المعلومات والأمن السيبراني حدده بتول عتوم في مقال له نشر على موقع (عربي) والذي يتمحور في أن أمن المعلومات أشمل من الأمن السيبراني، لأن المعلومات تتطلب الحماية في جميع أشكالها، حتى ولو لم تتخذ شكلا إلكترونيا، في حين أن الأمن السيبراني لا يهتم إلا بحماية المعلومات على الفضاء السيبراني، ويلخص بتول عتوم العلاقة بين أمن المعلومات والأمن السيبراني بقوله: (باختصار يمكن اعتبار الأمن السيبراني جزءاً أو تخصصاً من أمن المعلومات)⁽³⁾.

(1) عنتر بن مرزوق ومحمد الكر، البعد الإلكتروني للسياسة الأمنية الجزائرية، مجلة العلوم الإنسانية والاجتماعية، جامعة باتنة 01 الحاج لخضر، الجزائر، العدد 38، جوان 2018، ص ص: 29-50:

<https://www.asjp.cerist.dz/en/article/55161>

(2) فاطمة بيرم، المرجع السابق.

(3) بتول عتوم، ما الفرق بين أمن المعلومات والأمن السيبراني؟، 18 نوفمبر 2019، تم الاطلاع عليه بتاريخ 11 فيفري 2021، على الساعة

17:37 سا، مختصر رابط الموقع: <https://cutt.us/chVCo>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

ومع أننا نشاركه في نظرتة إلى الفارق بين أمن المعلومات والأمن السيبراني إلا أننا لا نوافقه في اعتبار هذا الأخير تخصص أو جزء من أمن المعلومات، لأن الأمن السيبراني أكثر شمولاً من أمن المعلومات، فالصواب أن يكون أمن المعلومات السيبرانية جزء من أمن المعلومات وليس الأمن السيبراني بقضه وقضيضه.

وحتى إذا افترضنا أن تعريف بعض الباحثين قد انطلق من اعتبار المعلومات جوهر الفضاء الإلكتروني وغاية السياسات الأمنية التي تحميه لكونها أيضاً غاية المهاجمين والإرهابيين، وأن حماية الطبقات الأخرى غايته الأساسية هو حماية المعلومات، يبقى مع ذلك منطلق غير مقبول، لأن السياسات الأمنية التي تشمل حماية العناصر الأخرى للفضاء الإلكتروني لا تستهدف بالضرورة حماية المعلومات، فقد يكون هدفها حماية البنى التحتية التي تدار عبر الفضاء الإلكتروني، فلا عبرة هنا بحماية المعلومات دائماً، فقد يكون العبرة منها حماية البيانات التي تسيّر من خلالها هذه البنى، والبيانات والمعلومات ليسا مصطلحين مترادفين⁽¹⁾.

وعلى ضوء ما تقدم من تعريفات ونقد، يمكن القول بأن الأمن السيبراني أو الأمن الإلكتروني هو: (القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات وهذا يتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الصرر أو الوصول غير المصرح به، وبعبارة أخرى فإنه لا يعني أكثر من حماية البيانات)⁽²⁾.

الفرع الثاني: الأمن السيبراني: المكونات والأبعاد:

لقد رأينا مما سبق ضرورة العمل على تأمين الفضاء السيبراني ليكون بيئة ملائمة للنمو الاقتصادي على وجه الخصوص وفي كل مجالات حياة الإنسان على وجه العموم، وعلى هذا يجب على الدول وضع خطط واستراتيجيات تتناسب مع طبيعة هذا الفضاء ويجب أن تكون استراتيجيات شاملة لكل العناصر والمكونات التي يتأس منها الأمن السيبراني (أولاً)، كما يجب أن يكون أكثر اتساعاً بحيث يضمن الحماية لكل الأبعاد التي يشملها الأمن السيبراني (ثانياً).

⁽¹⁾ الفرق بين البيانات والمعلومات هو فرق شاسع، فالبيانات هي المادة الخام للمعلومات والتي لا يمكن أن يفهمها الإنسان، في حين أن المعلومات من مدركات الإنسان، حيث تتميز بالتنظيم والترتيب والمفهومية، أنظر في ذلك: خضر مصباح إسماعيل طيطي، إدارة المعرفة: (التحديات والتقنيات والحلول)، الطبعة الأولى، دار الحامد للنشر والتوزيع الأردن، 2010، ص 24.

⁽²⁾ عنتر بن مرزوق ومحمد الكر، المرجع السابق.

أولاً: مرتكزات أمن الفضاء الإلكتروني:

1- العنصر البشري:

يمكن النظر إلى العنصر البشري كمرتکز أو مكون من مكونات أمن الفضاء الإلكتروني من ناحيتين:

أ- الأفراد:

يكتسي الطابع البشري أهمية كبيرة في العملية الأمنية المتعلقة بالفضاء الإلكتروني إيجاباً أو سلباً، فقد يمثل العامل البشري العنصر الجوهری الذي يقف وراء ضمان الحماية الفعالة للفضاء الإلكتروني، كما قد يكون عنصراً مهدداً لأمن البيئة الإلكترونية كلها وذلك حين يعتمد إلى استغلال الثغرات ونقاط الضعف لتحقيق مآرب الشخصية أو مصالح جهات معادية، فمن نسبة 50 بالمئة التي تمثل الأفعال غير المقصودة من حوادث أمن المعلومات نجد أن 15 إلى 20 بالمئة منها راجع إلى انعدام الأمانة، وإذا نظرنا إلى هذه الأفعال سواء منها ما كان مقصوداً أو غير مقصود ندرك ما للعامل البشري من دور مهم في الحد من الخسائر التي تتعرض لها البيئة الرقمية⁽¹⁾.

وعلى هذا الأساس يمكن القول بأن وعي الأفراد واستيعابهم لنطاق الصلاحيات الممنوحة لهم وحدودها، وكذلك سلامة عمليات الإشراف والمتابعة الرقابية على أعمالهم بما يتوافق مع مقتضيات حقوقهم القانونية، تعتبر من بين المواضيع الرئيسة والأساسية التي تتضمنها السياسة الأمنية بصفة عامة، فضلاً عن أساسيتها وحيويتها الخاصة في مجال أمن المعلومات⁽²⁾ بصفة خاصة وأمن الفضاء الإلكتروني بصفة عامة.

ويدخل أيضاً ضمن العناصر الجوهرية والمرتكزات الأساسية للأمن الإلكتروني، أمن المستخدمين أنفسهم، سواء أعلق الأمر بأمنهم الجماعي، أي أمن المجتمع عموماً، أو أمنهم فرادى، ويشكل ذلك أمنهم المادي وأمنهم المعنوي.

ب- الإدارة:

إن أول ما ينظر إليه في الإدارة كمرتکز من مرتكزات أمن الفضاء الإلكتروني وعنصر جوهري من عناصره، هو اختيار قادتها، والذين يتعين أن تكونوا فوق مستوى الشبهات، وأن يتسموا بالحكمة والدراية، فضلاً عن الخصائص الأخرى التي يتعين توفرها في القائد الفذ.

⁽¹⁾ محمد عبد الرحمن أبو حمام، دور نظم المعلومات الإدارية في تحقيق الأمن المعلوماتي في جهاز الشرطة الفلسطينية، رسالة ماجستير في برنامج القيادة والإدارة، أكاديمية الإدارة والسياسة للدراسات العليا، جامعة الأقصى، 2014، ص: 44-47.

⁽²⁾ فايز جمعه النجار، نظم المعلومات الإدارية: (منظور إداري)، الطبعة الثالثة، دار الحامد للنشر والتوزيع، الأردن 2010، ص 265.

وذلك لأن المنشآت عموماً يجب أن تكون تحت قيادة قادرة على ضمان الحدود الدنيا من الجهود البشرية المطلوبة التي تكفل لها تحقيق الأهداف التي وضعت من أجلها وترعى لها استمراريتها، ولا يتحقق ذلك إلا عندما يكون العاملون تحت قيادة تمتلك الحكمة اللازمة لحفظهم والحصول على تعاونهم⁽¹⁾.

ودور الإدارة يكمن في دعم الوضعية الأمنية للبيئة الإلكترونية من خلال جملة من الإجراءات والأعمال والمهام التي تحقق بها الأمن المعلوماتي في شقه المادي وهذا من خلال تأمين البنى التحتية وأجهزة الحواسيب والمعدات الأخرى للبرمجيات وأجهزة اتصال وأجهزة تكييف وطاقة وغيرها وكذلك العمل على تحقيق الأمن المعلوماتي في شقه البشري الذي يشمل كل العاملين في الإدارة وهذا بضمان أمنهم وسلامتهم وكذلك تحقيق الأمن من تصرفاتهم التي قد تهدد الأمن المعلوماتي⁽²⁾.

2- أمن البنية التحتية لتكنولوجيا الفضاء الإلكتروني:

تعد الطبقة المادية للفضاء الإلكتروني والبنى التحتية اللازمة لتشغيله وتوظيفه بالإضافة إلى الوسائط الضرورية لذلك، من بين العناصر الأساسية التي قوم عليها الفضاء الإلكتروني، فضلاً عن نظم التشغيل والبرامج الضرورية التي تمثل الطبقة البرمجية للفضاء الإلكتروني وهي بمثابة الروح في الجسد، لذلك يتعين أن تشمل السياسات الأمنية المتعلقة بالفضاء الإلكتروني على قواعد وإجراءات واضحة لحماية هذا العنصر الجوهري المكون للفضاء الإلكتروني.

ويجب أيضاً ضمان الحماية الكاملة لسلامة أنظمة التشغيل والبرمجيات وحياسة الأساليب والآليات الدفاعية ضد محاولات التخريب بمختلف أنماطها وأشكالها، فلا بد من العمل امتلاك منظمة لها القدرة الأمنية ذات درجة عالية من الموثوقية، كما يجب الأخذ بعين الاعتبار في السياسة الأمنية المتعلقة بنظم التشغيل آليات حماية البرامج الداخلية لها، وأساليب حفظ كلمات المرور، وتثبيت جدول الصلاحيات واختيار طرق إدارة نظم التشغيل، وفي سياق متصل لا بد من وجود مركزية حال وضع برامج التأمين بحيث تراعي الخواص الأمنية للحواسيب والبرمجيات فلا تتخطاها أو تتجاوزها، وكذلك تحديد طبيعة وشخصية وصلاحيات المستخدم أو المستفيد⁽³⁾.

(1) عبد الله جعفر كوفي، العمل الأمني الناجح: (دراسة نظرية-تحليلية)، الطبعة الأولى، دار الخليج للصحافة والنشر الأردن، 2019، ص 170.

(2) محمد عبد الرحمن أبو حمام، المرجع السابق، ص ص: 44-47.

(3) المرجع نفسه، ص ص: 44-47.

3- أمن المعلومات:

يعرف أمن المعلومات على أنه: (الحفاظ على سرية وتوفر وسلامة المعلومات كأصل في مراحل المعالجة والحفظ والنقل، ويتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعليم والتدريب)⁽¹⁾.

ومن خلال هذا التعرف يمكن أن نقول أن العناصر الجوهرية لتأمين المعلومات تتمثل في الحفاظ على العمل على توفيرها في كل وقت وبدون انقطاع، وسلامتها من أي شكل من أشكال التهديد التي قد تتعرض لها أيا كان نوعه وطريقته، والحفاظ على سريتها وهويتها⁽²⁾، والقدرة على إسناد أي تصرف متعلق بالمعلومات إلى من قام به⁽³⁾.

فتأمين المعلومات يعد من بين العناصر الأساسية والجوهرية وجزء لا يتجزء من أمن الفضاء الإلكتروني، وعليه فإن أي سياسة أو استراتيجية تستهدف حماية الفضاء الإلكتروني يجب أن تتضمن على قواعد وأسس لحماية المعلومات.

ثانيا: أبعاد الأمن السيبراني:

يتخذ الأمن السيبراني العديد من الأبعاد المختلفة في طبيعتها تبعا للأبعاد التي يتخذها توظيف الفضاء الإلكتروني نفسه، وهذه الأبعاد تتجلى في:

1/ البعد العسكري:

إن الأصل المفجر للنظام الشبكي يعود في أصوله إلى الأبعاد ذات الطبيعة العسكرية، فمن خلال هذا النظام تضمن المؤسسة العسكرية قدراتها العسكرية المختلفة، غير أن لهذا الفضاء قد فتحت أيضا في الوقت نفسه مواضع خلل وثرغات، خاصة إذا لم تتمتع الشبكات على قدر وفير من الحماية بما يضمن لها التصدي للاختراقات التي قد تؤدي إلى إصابة قواعد البيانات العسكرية بالدمار، أو قطع الاتصال بين قيادة المؤسسة العسكرية والوحدات التابعة لها، وكذلك إمكانية

(1) أسماء فيلاي، مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثيره بطبيعة التهديدات وطبيعة الحماية المطبقة، أطروحة دكتوراه في الإدارة الاستراتيجية والذكاء الاقتصادي، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2018-2019، ص 58.

(2) سهيلة بضياف وأمنة حمراي، أمن المعلومات في الجزائر: (الإجراءات والتحديات)، المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 01، جامعة باتنة 1 الحاج لخضر، الجزائر، جانفي 2020، ص ص: 177-190.

<https://www.asjp.cerist.dz/en/article/105799>

(3) مصطفى يوسف كافي، الإدارة الإلكترونية، المرجع السابق، ص 432.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

تعرض منصات بعض الأسلحة للخروج عن السيطرة عبر التحكم فيها عن بعد من قبل الطرف المهاجم⁽¹⁾.

ولذلك يقتضي أن يتخذ الأمن السيبراني بعدا عسكريا لتأمين المجالات التي تتعلق بالجانب العسكري، كما هو الحال مثلا بحلف النيتو الذي يعمل على تأمين المواقع العسكرية من أشكال التهديدات السيبرانية، وحماية الكوادر العسكرية المهمة من عمليات التجسس، وكذلك حماية البيانات والمعلومات ذات الطبيعة العسكرية⁽²⁾.

2- البعد الاجتماعي:

يعتبر الفضاء الإلكتروني من أكبر التجمعات البشرية على الإطلاق، حيث بلغ عدد الذين يقومون باستخدام الإنترنت وتوظيفه ما يزيد عن 4 مليارات شخص حول العالم، بما في ذلك مستخدمي مواقع ومنصات التواصل الاجتماعي الذين يفوق عددهم 2.6 مليار شخص، ورغم ما لهذا التجمع المهول من ثمار حميدة وآثار إيجابية في تبادل الأفكار وتشارك الخبرات إلا أنه في المقابل يشكل أكبر تهديد على القيم الأخلاقية للمجتمعات نظرا لصعوبة بسط الرقابة على ما فيه من محتوى، كما يشكل أيضا تهديد بالغا للهويات التي يمكن أن تتعرض للاختراق الأمر الذي يترتب عنه تهديد مباشر للأمن الاجتماعي للدولة، وهذا ما يلح بشكل شديد على العمل من أجل توعية المواطنين بأشكال المخاطر التي تهددهم على الفضاء السيبراني من أجل تحقيق الأمن في بعده الاجتماعي⁽³⁾.

ونظرا لكون القيم من أهم الأدوات التي تضمن ضبطا اجتماعيا وإطارا سلوكيا عاما ينتج آلية استقرار وتوازن اجتماعي فإن أي شكل من أشكال التحول المرفوض فيها أو إحداث أي اضطرابات في مقوماتها يفضي بالضرورة إلى اضطراب البنية الاجتماعية وحلول الفوضى الأخلاقية والسلوكية في جو من اللامعيارية الأخلاقية وفقدان التنظيم والتوازن وزعزعة الانتماء الوطني ودخول المجتمع في نفق من التدهور والفساد، وتبرز بعض مظاهر الخطورة التي تهدد المعايير الاجتماعية والأخلاقية على الساحة السيبرانية في تهديد الهوية وهتك القيم الاجتماعية وتغريب الفرد عن مجتمعه وتفكيك التواصل بينه وبين محيطه الأسري والاجتماعي والاعتداء على خصوصيات، كما أصبح الفضاء الإلكتروني مستنقعا للمواد الإباحية التي تجر الفرد إلى الانحراف الأخلاقي والوقوع

(1) إسماعيل زروقة، مرجع سابق.

(2) إيهاب خليفة، وحدة الأمن السيبراني: الميدان الخامس: الفضاء السيبراني في العقيدة العسكرية لحلف الناتو، المركز المصري للفكر والدراسات الاستراتيجية، 09 فيفري 2020، تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 16:45، على الموقع:

<https://www.ecsstudies.com/8085/>

(3) إسماعيل زروقة، المرجع نفسه.

الفصل الأول الفضاء الإلكتروني والتحول التكنولوجي في المفاهيم الاستراتيجية

في الاختلاط المنبؤ والخيانة الزوجية، فضلا عما في هذا الفضاء من العنف الرمزي والانتشار الواسع للجريمة الإلكترونية⁽¹⁾.

3- البعد القانوني:

إن التطور الذي يشهده العصر الحديث في التكنولوجيا والوتيرة المتسارعة التي تخطو بها تفرص بإلحاح شديد على خلق منظمة قانونية تسايرها وتنظمها وهذا من خلال إيجاد صيغ تشريعية وأطر قانونية للتصرفات القانونية وغير القانونية على الساحة السيبرانية، فالكثير من دول العالم لا تزال تتعامل مع الجرائم السيبرانية بنوع من الإغفال والتغيب للأطر القانونية التي تكافحها فضلا عن ضرورة إيجاد صياغة دولية لتفعيل التعاون الدولي في محاربتها⁽²⁾.

وقد اعتبرت دولة بوتسوانا: (عدم مواءمة التشريعات المتعلقة بالجريمة السيبرانية وحماية البيانات بين مختلف الدول والولايات القضائية يجعل التحقيق في الأنشطة الإجرامية على الفضاء السيبراني أمرا بالغ الصعوبة) كما اعتبرت أيضا: (عدم وجود إطار دولي لتبادل معلومات الأمن السيبراني بين مختلف الأجهزة في البلدان المختلفة يمثل تحديا فيما يخص حماية الشبكات والتحقيق في الأنشطة الإجرامية التي تشمل ولايات قضائية متعددة)⁽³⁾.

ولا بد للأمن القانوني أن ينبت في بيئة قانونية سليمة تبدأ من جودة القواعد القانونية وتنتهي بإنزالها على النوازل والطوارئ وما صيغت من أجله على الوجه الأكمل لتكون بذلك الإطار الذي به يتم ضمان الأمن والأمان وليست مصدر قلق وارتباك، ولا بد أيضا للقواعد القانونية أن تتمتع بقدر معين من المرونة لتستطيع مواكبة التحولات التي يعرفها المجتمع المعاصر⁽⁴⁾.

4- البعد الاقتصادي:

أصبحت العلاقة بين الاقتصاد وبين الفضاء الإلكتروني في العصر الحديث ظاهرة وجلية، ولا تكاد تخفى على أحد، إذ أن الطبقات التكوينية للفضاء الإلكتروني وما تتميز به من خواص

⁽¹⁾ وليدة حدادي، الفضاء السيبراني وأزمة القيم الأخلاقية في المجتمعات العربية: (الشبكات الاجتماعية نموذجا)، مجلة الحقيقة للعلوم الإنسانية والاجتماعية، المجلد 17، العدد 04، جامعة أحمد دراية، أدرار، الجزائر، ديسمبر 2018، ص ص: 403-433.

<https://www.asjp.cerist.dz/en/article/69535>

⁽²⁾ إسماعيل زروقة، المرجع السابق.

⁽³⁾ الفقرة 43 من تقرير الأمين العام لهيئة الأمم المتحدة رقم 130/47 الصادر عن الجمعية العامة بتاريخ 30 جويلية 2019 والمتضمن مكافحة استخدام تكنولوجيا المعلومات والاتصال الأغراض الإجرامية.

⁽⁴⁾ المجيد لخازري وفطيمة بن جدو، الأمن القانوني والأمن القضائي: (علاقة تكامل)، مجلة الشهاب، المجلد 04، العدد 02، معهد العلوم الإسلامية، جامعة الشهيد حمه لخضر، الوادي، جوان 2018، ص ص: 387-406.

<https://www.asjp.cerist.dz/en/article/52499>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

نادرة تساهم وبشكل أساسي وكبير في بناء المنظومات الاقتصادية في كل دول العالم، فضلا عن دورها المؤثر في الشركات أيا كان حجمها.

يلعب الفضاء الإلكتروني دورا كبيرا وأثر بالغ في أشكال وحجم المنافسة، كما يقع أثره أيضا على هيكل السوق، فضلا عن دوره المحوري في رفع مستوى معدلات التطور والازدهار الاقتصادي، كما يملك تأثيرا على إجراء وتنفيذ المعاملات التجارية وعلى أساليبها أيضا⁽¹⁾.

ويلعب الفضاء الإلكتروني أيضا دورا مهما وحاسما في صياغة وبناء القرارات الاقتصادية والاستثمارية، وذلك لما يوفره من آليات قوية ونافذة للتحكم في المعلومات والتوظيف الناجح لها⁽²⁾.

لقد تحول الفضاء السيبراني فعلا إلى سوق كبرى للمعاملات التجارية والمالية والاقتصادية، وتعتبر الحواسيب من بين الآليات الأساسية والقاعدية في إدارة دفة الاقتصاد وتسيير قطاع الصناعات وتطويرها⁽³⁾، وفي المقابل ظهر تهديدات خطيرة وجدية تعصف بهذا النوع من الاقتصاد جراء التزايد المستمر لمعدلات الإجرام السيبراني، مما يلزم الدول بتأمين هذه البيئة⁽⁴⁾، ومن هنا يظهر البعد الاقتصادي للأمن السيبراني.

5- البعد السياسي:

تبرز الأوضاع الراهنة سواء على المستوى الوطنية أو على المستوى الدولي أن الفضاء الإلكتروني قد اتخذ فعلا أبعادا سياسية كبرى، وذلك عندما أصبح آلية يتم التمرير تحت عبائه نشاطات ذات طابع سياسي، فالفضاء الإلكتروني في العصر الحاضر قد أصبح وسيلة في أيدي الدول لإحداث تأثيرات سياسية واسعة النطاق، لذلك فإن الأمن السيبراني يجب أن يتماشى مع هذا التوظيف الجديد للفضاء الإلكتروني، ومن هنا ظهر البعد السياسي للأمن السيبراني.

إذا أن هذا البعد الجديد له تمليه في حقيقة الأمر ضرورة الحفظ على شكل الدولة، وذلك من خلال حماية نظامها السياسي وكيانها ومصالحها⁽⁵⁾، والتي تتعرض يوما بعد يوم لنشاطات سياسية

(1) خالد أحمد على محمود، اقتصاد المعرفة وإدارة الأزمات المالية في إطار المؤسسات الاقتصادية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2019، ص 260.

(2) أسامة عبد السلام السيد، الاقتصاد الرقمي، الطبعة الأولى، دار غيداء للنشر والتوزيع، الأردن، 2019، ص 15.

(3) إسماعيل زروقة، مرجع سابق.

(4) الموسوعة السياسية، الأمن السيبراني، (د.ت.ن)، تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 16:25، في موقع الموسوعة،

مختصر رابط الموقع: <https://cutt.us/ZOROL>

(5) إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد 01، العدد 01، المدرسة العليا العسكرية للإعلام والاتصال، الجزائر، ديسمبر 2019، ص ص: 100-123:

<https://www.asjp.cerist.dz/en/article/125955>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

معادية لها على الساحة السيبرانية، وقد دل على هذا التدخل الروسي في الانتخابات الرئاسية الأمريكية السابقة وما تمخض عن التسيريات والاختراقات للمعلومات الحساسة من أزمة دبلوماسية⁽¹⁾، كما يمكن للأمن السيبراني أيضا أن يكون أداة يتم توظيفها للهيمنة السياسية⁽²⁾.

الفرع الثالث: مهددات الأمن السيبراني:

ظهر الفضاء الإلكتروني وظهرت معه شمولية استخدامه في جميع مجالات القطاع العام والخاص على حد سواء، وأصبح العماد حتى في قطاعات البني التحتية الحرجة رغم ما يعيب هذا الفضاء من شوائب وثغرات أمنية يمكن أن تشكل تهديدا أمنيا ومن هنا ظهرت الجرائم الإلكترونية كصورة لسوء استعمال هذا الفضاء (أولا) كما ظهر معها أيضا استغلال هذا الفضاء ك مجال من المجالات الحربية فأصبحت الدول تؤسس لنوع جديد من الحروب (ثانيا).

أولا: الجرائم الإلكترونية:

1- تعريف الجريمة الإلكترونية:

تعتبر الجريمة الإلكترونية من بين الجرائم التقنية المستترة التي تظهر وتتسأ في بيئة خفية معتمدة وتقوم بشكل أساسي على استهداف المعلومات التي يتم تنقلها عبر الفضاء الإلكتروني، ولقد تنامت معدلات هذه الجريمة وأخذت في اتخاذ أنماط وأشكال متعددة ومتفرعة، الأمر الذي ترتب عنه حالة من القلق ودق ناقوس الخطر نظرا لما تهمله من تهديدات للأمن الإلكتروني ومخاطر كبرى تظهر بصورة فعلية في الاعتداءات التي تمس الحياة الخاصة للأفراد وتهدد الأمن والسيادة الوطنية وتعمل على خلق جو مشحون يتلاقى فيه فقدان الثقة بالتقنيات الحديثة مع ضياع إبداع العقل البشري⁽³⁾.

فالجريمة الإلكترونية إذا هي مجموعة من التصرفات أو الأفعال أو الأنشطة أو السلوكيات التي توصف كونها أعمالا مخالفة للقانون والتي ترتكب على أو من خلال مختلف الطبقات التكوينية للفضاء الإلكتروني، وهي من جرائم التي تتطلب مستوا معين من الحذاقة والإلمام والمعرفة الخاصة بتقنيات الحاسب الآلي ونظم معلوماته من أجل القيام بارتكابها أو التحقيق فيها أو مقاضاة الجناة فيها⁽⁴⁾.

(1) إسماعيل زروقة، المرجع السابق.

(2) رغبة البهي، علاقات متشابكة: كيف تدعم التجارة الرقمية سياسات الأمن السيبراني؟، 02 أكتوبر 2019، تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 03:23، مختصر الرابط: <https://cutt.us/NSZQb>

(3) فضيلة عاقل، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال المؤتمرات، المؤتمر الدولي الرابع عشر، مركز جيل البحث العلمي، طرابلس، 24-25 مارس 2017، ص ص: 115-136: <http://jilrc.com/> مؤتمر اتنا/

(4) ياسمين بونعارة، الجريمة الإلكترونية، مجلة المعيار، المجلد 20 العدد 39، كلية أصول الدين، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، 19 جوان 2015، ص ص: 273-314: <https://www.asjp.cerist.dz/en/article/17999>

ويمكن تعريف الجريمة الإلكترونية على أنها: (عبارة عن نشاط إجرامي تستخدم فيه تقنيات الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي) كما تعرف أيضا بأنها: (مجموعة الأفعال والأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية) ورأى البعض الآخر من فقهاء القانون المصري على أنها جريمة تتكون من الاستخدام غير المشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال أو الأشياء المعنوية⁽¹⁾.

وتم تعريفها أيضا على أنها: (الاعتداء القانوني الذي يرتكب بواسطة المعلومات الحاسوبية بغرض تحقيق الربح " كما عرفت أيضا وبشكل أوسع على أنها: " كل فعل إجرامي متعمد أيا كانت صلته بالمعلومات، ينشأ عنه خسارة تلحق المجني عليه، أو كسب يحققه الفعل)⁽²⁾.

وتم تعريف الجريمة الإلكترونية أيضا في الفقه البلجيكي على أنها: (كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، ويعد استخدام مصطلح الجريمة المعلوماتية للدلالة على الجرائم الناشئة عن استخدام الإنترنت)⁽³⁾.

2- تداعيات الجريمة الإلكترونية:

تعتبر الخطورة الإجرامية التي بدأت تلوح في أفق الاستخدام الواسع لشبكة الإنترنت وتعاظمها وازديادها الدافع الذي يقف وراء إطلاق الكثير من المنظمات والهيئات مختلفة المستوى من إطلاق سلسلة من التحذيرات من خطورة هذه الظاهرة التي غدت خطرا يهدد كل مستخدم شبكة الإنترنت⁽⁴⁾.

وتتباين التداعيات وتختلف على حسب نوع الجريمة التي تم ارتكابها على الفضاء الإلكتروني أو عبره، لكن الأمر المؤكد أن الجريمة الإلكترونية لها تأثيرات خطيرة تمس مجالات كثيرة من حياة الأفراد والدول، وخطورها يزداد يوما بعد يوم مع زيادة تطور التقنيات الإلكترونية المستعملة في الإجرام الإلكتروني من جهة، وأيضا زيادة حجم الاعتماد على هذا الفضاء في مجالات الحياة الإنسانية.

⁽¹⁾ فضيلة عاقل، المرجع السابق.

⁽²⁾ عبد الله بن عبد العزيز بن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي: (دراسة تطبيقية) رسالة ماجستير في العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص 64.

⁽³⁾ مليكة عطوي، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت: (دراسة وصفية تحليلية)، أطروحة دكتوراه في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة دالي براهم، الجزائر، السنة الجامعية 2009-2010 ص 202.

⁽⁴⁾ حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية: (تصور مقترح)، المجلة العربية للدراسات الأمنية والتدريب، المجلد 27 العدد 53، جامعة نايف العربية للعلوم الأمنية، الرياض، رجب 1432، ص ص: 05-54.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وإذا أخذنا الجرائم الإلكترونية المتعلقة بالعرض نجد الباحثين والفقهاء قد أحصوا العديد من الولايات التي تتجر عنها والتي تتنوع بين الآثار الاجتماعية والأسرية والنفسية والأخلاقية والسلوكية والقانونية والعقائدية⁽¹⁾.

فضلا عن تداعيات الجرائم الإلكترونية على الأمن العام من خلال إشعال النعرات الطائفية والعرقية والمذهبية، أو استهداف البنى التحتية وعرقه وظائفها، وتداعياتها أيضا على الصحة العمومية سواء أكان ذلك بتعطيل أجهزة المستشفيات أو من خلال نشر أخبار كاذبة تهدد الصحة العمومية، والذي تجلى لنا بوضوح شديد خلال جائحة كورونا أين نشرت أخبار كاذبة تهدد بشكل صريح الأمن الصحي للأفراد سواء بالتهويل أو التفريط.

يمكن أيضا أن يكون للجرائم الإلكترونية تداعيات على المستوى البيئي سواء بإتلاف المعلومات الحيوية المتعلقة بحفظها أو من خلال التحكم في أجهزة المصانع المنتجة للمواد السامة وإطلاقها في البيئة، ويمكن أيضا أن يترتب عن الجرائم الإلكترونية أضرار شديدة حال التحكم في أجهزة تأمين المعامل والمخابر المتعلقة بالدراسات والتجارب المخبرية الأمر الذي يفضي إلى إطلاق أشكال من الفيروسات الفتاكة.

وللجرائم الإلكترونية آثار مهولة ومدمرة للاقتصاد، فزيادة عن السيطرة على المعلومات الحيوية والخصوصيات الاقتصادية للدول، يمكن أن تؤدي الجرائم المالية الإلكترونية إلى خسائر مالية كبرى، إذ وفق شركة غرانت ثورنتون للاستشارات والمحاسبة يمكن أن يصل حجم الخسائر المالية المترتبة على الجرائم الإلكترونية إلى 06 تريليون دولار في هذا العام⁽²⁾.

وأكد استطلاع 2015 لشركة (كاسبيرسكي) بمشاركة (بي تو بي إنترناشونال) أن التعافي من اختراق أمني واحد يتطلب مبلغ 551.000 دولار بالنسبة لكبار المؤسسات و38.000 دولار لصغار المؤسسات⁽³⁾، فضلا عن حجم الإنفاق لتأمين هذا الفضاء الإلكتروني والذي قد يبلغ في

(1) راجع: هيثم عبد الرحمن البقلي، الجرائم الإلكترونية الواقعة على العرض: (بين الشريعة والقانون المقارن)، الطبعة الأولى دار العلوم للنشر والتوزيع، القاهرة، 2010، ص ص: 71-72.

(2) نقلا عن: حسام علم الدين، 6 تريليونات دولار خسائر الجرائم الإلكترونية سنوياً.. بحلول 2021، 09 فبراير 2020 تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 00:39، مختصر الرابط: <https://cutt.us/doNwr>

(3) موقع صانعو الحدث، ما هو أثر الجريمة الإلكترونية على اقتصادات الدول؟، 19 أكتوبر 2016، تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 00:43، مختصر الرابط: <https://cutt.us/e4Akx>

الفصل الأول الفضاء الإلكتروني والتحول الرقمي في المفاهيم الاستراتيجية

الشرق الأوسط لوحده في عام 2020 ما يقارب 1.7 مليار دولار⁽¹⁾، ناهيك عن الخسائر التي تترتب عن انتهاك حقوق الملكية الفكرية وقتل صور الإبداع الفكري⁽²⁾.

أما عن الدول العربية الأكثر تعرضا للهجمات الإلكترونية فنجد المملكة العربية السعودية التي تحتل المرتبة الأولى عربيا كما تحتل الإمارات العربية المتحدة المرتبة الثانية عربيا، بينما تحتل الجمهورية الجزائرية المرتبة الثالثة عربيا والرابعة والعشرين عالميا حيث بدأ معدل الهجمات السيبرانية يرتفع مؤشره في الآونة الأخيرة ، وقد سجلت المصالح الأمنية الجزائرية ما يعادل 2500 جريمة إلكترونية خلال سنة 2017⁽³⁾.

3- صور الجريمة الإلكترونية:

من خلال استقراء النصوص القانونية المختلفة والمتعلقة بالجرائم الإلكترونية يمكن أن نستوحي منها العديد من صور الإجرام التي تمارس على الفضاء الإلكتروني أو بواسطته، والتي يمكن تقسيمها على أساسين مختلفين؛ على أساس موضوعها، أو على أساس ضحاياها.

أ- صور الجريمة الإلكترونية على أساس موضوعها:

يمكن تقسيم هذه الصورة إلى صورتين فرعيتين أيضا، أولهما تتعلق بالفضاء الإلكتروني كمحل للجريمة، وثانيهما تتعلق بالفضاء الإلكتروني كوسيلة للجريمة:

أ-1: الفضاء الإلكتروني كمحل للجريمة:

يمكن أن نميز بين 03 حالات أين يكون فيها الفضاء الإلكتروني كمحل للجريمة، أولهما أن تقع صور الإجرام على الطبقة المادية للفضاء الإلكتروني، كالأجهزة والمعدات والكابلات وشبكات الوصل، وأجهزة الطباعة، والشرائط الخامة، وثانيهما هي التي تلك التي تقع على الطبقة المنطقية للفضاء الإلكتروني، كالبرامج، والبيانات والمعطيات⁽⁴⁾، وثالث هذه الحالات هي أن تكون

⁽¹⁾ نقلا عن: حسام علم الدين، المرجع السابق.

⁽²⁾ نقلا عن: مزاراة الاتصالات وتقنية المعلومات، تقرير: الجرائم الإلكترونية تكبد الاقتصاد العالمي خسائر بقيمة 445 مليار دولار سنوياً، (د.ت.ن)، تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 00:48، على الموقع الوزارة:

<https://www.mcit.gov.sa/ar/media-center/news/94698>

⁽³⁾ وليد رمزي، الجزائر - 44 بالمائة من الجزائريين محاولات قرصنة إلكترونية، حدث منشور على موقع: TSA عربي بتاريخ 28 مارس 2018، على الساعة 11:48 تم الاطلاع عليه في 18 فيفري 2020 على الساعة 10:16:

<https://www.tsa-algerie.com/ar/الجزائر-44-بالمائة-من-الجزائريين-واجهو/>

⁽⁴⁾ سليمة ذياب، بلال بوترة، الجريمة الإلكترونية: (الأسس والمفاهيم)، مجلة تطوير العلوم الاجتماعية، المجلد 13 العدد 01، جامعة زيان

عاشور، الجلفة، الجزائر، نوفمبر 2020، ص ص: 07-20:

<https://www.asjp.cerist.dz/en/article/134169>

المعلومات نفسها هي محل للجريمة، -أي على الطبقة المعلوماتية- وهي الجرائم التي تمس الوثائق الشبكية وأبرز هذه الجرائم تلك المتعلقة بانتهاكات حقوق الملكية الفكرية سواء أكان لبرامج الحاسب الآلي أو لأي إنتاج فني أو أدبي أو علمي آخر⁽¹⁾.

أ- 2: الفضاء الإلكتروني كوسيلة للجريمة:

لا تتناول هذه الصورة تلك الجرائم التي يكون فيها الفضاء الإلكتروني محلا للجريمة، فالفضاء الإلكتروني في هذه الحالة لا يكون هدفا للهجمات الإجرامية، ولكن يتم توظيفه لأغراض جرائم أخرى⁽²⁾، ونرى أن هذه الصورة لا يمكن حصر حالات السلوك الإجرامي المتعلق بها، إذ أنها في حقيقتها جرائم تقليدية يتم توظيف الفضاء الإلكتروني كوسيلة لارتكابها.

2- الجرائم الإلكترونية على أساس ضحاياها:

يتأسس هذا القسم على الضحايا أو الجهات التي يتم استهدافها بالسلوك الإجرامي على الفضاء الإلكتروني، ويستوى في ذلك أكان الفضاء الإلكتروني محلا للجريمة أو وسيلة له، ويمكن تقسيمها إلى ثلاث طوائف، نرتبها على أساس خطورتها الإجرامية، وهي:

أ- جرائم ضد الدولة:

تتمحور الجرائم الأساسية التي تمس كيان الدولة من خلال الفضاء الإلكتروني في الإرهاب الإلكتروني الذي تمارسه التنظيمات الإرهابية من خلال آلية مختلفة كالترويج والدعاية وتجنيد وشن حروب نفسية، كما نجد أيضا جرائم أخرى كالجريمة المنظمة أين يقوم جماعات الجريمة المنظمة باستغلال الفضاء الإلكتروني لتحقيق أرباحا غير مشروعة وأيضا نجد جريمة التجسس الإلكتروني وجرائم المساس بالأمن الفكري⁽³⁾.

ب- جرائم ضد الأموال:

هناك من الفقهاء من يعرف الجريمة المعلوماتية على أنها اعتداء غير قانوني يقوم على أساس الآليات المعلوماتية من أجل تحقيق أرباح، فهذا الاتجاه في تعريف الجريمة الإلكترونية

(1) إبراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية: (دراسة تحليلية تطبيقية)، مجلة كلية الشريعة والقانون بطنطا، المجلد 30 العدد 02، كلية الشريعة والقانون، جامعة الأزهر بطنطا، أبريل 2015، ص ص 360-403: https://mksq.journals.ekb.eg/article_7802.html

(2) سليمة نياض، بلال بوترعة، المرجع نفسه.

(3) يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 06 مارس 2013، ص ص: 54-58.

يركز الجرائم ضد الأموال، ويقطع النظر عن مدى صحة هذا التعريف ودقته، وسواء أتعقنا أم لم نتفق على أن الربح هو دائما الهدف من الإجرام المعلوماتي، إلا أنه في الأخير يثبت أن الجرائم المعلوماتية يمكن تستهدف الأموال بشكل خاص⁽¹⁾.

تتعدد صور الجرائم المرتكبة ضد الأموال، فمنها مثلا؛ جريمة الاعتداء على أرقام بطاقات الائتمان وتحويل الأموال إلكترونيا بطريق غير مشروع ومنها أيضا جريمة القمار من خلال الأندية افتراضية وغسل الأموال على شبكات الإنترنت وجريمة السرقة والسطو على البنوك والمصاريف وغيرها من المؤسسات المالية واختلال الأموال أو نقلها أو إتلافها، كما نجد أيضا على الساحة السيبرانية جريمة ترويج المخدرات والاتجار بها بل ويتخطى الأمر لدرجة تعليم طرق تصنيع وزراعة المخدرات بشتى أنواعها وأصنافها وبما أتيح من آليات ووسائل⁽²⁾.

ج- الجرائم ضد الأشخاص:

إن من بين أهم الاستخدامات غير المشروعة والإجرامية ضد الأشخاص نجد جريمة التهديد والمضايقة والملاحقة، كما نجد أيضا جريمة انتحال شخصية آخر من أجل الاستفادة مما قد يختص به من مال أو جاه أو صلاحيات، وجريمة التغير والاستدراج التي يكون غالبا المجني عليهم فيها أحداثا، كما نجد أيضا جرائم خادشة للحياء كصناعة الأفلام والصور الإباحية ونشرها والتحريض على الممارسات الجنسية واستغلال الأطفال في ذلك، وهناك على ساحة الفضاء السيبراني أيضا قذفا وسبا وهتكا للسمعة وكلها جرائم معاقب عليها في النصوص الجنائية⁽³⁾.

ويتم التوظيف الفضاء الإلكتروني لهذه الأغراض الإجرامية عبر الكثير من المنافذ التي يتيحها هذا الفضاء، ومن بينهما؛ شبكات الاتصالات أو خدمة البريد الإلكتروني، أو من خلال صفحات الإنترنت، أو غرف المحادثة، وتطبيقات التواصل الاجتماعي وما إلى ذلك من الخدمات التي يوفرها هذا الفضاء⁽⁴⁾.

وتجدر الإشارة هنا، أن هاذين التقسيمين ليسا هما التقسيمين الوحيدين للجرائم المعلوماتية، فهنا تقسيم (Ulrich Sieber) الذي يقسمها إلى ثلاث أصناف، جرائم الحاسب الآلي المتعلقة بالاقتصاد، وتلك المتعلقة بانتهاك الحياة الخاصة، وأخيرا تلك التي تنتهك المصالح القومية وسلامة

(1) أيمن عبد الله فكري، المرجع السابق، ص ص: 94-95.

(2) يوسف صغير، المرجع السابق، ص ص: 44-49.

(3) المرجع نفسه، ص ص: 49-54.

(4) محمد رحموني، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة للعلوم الإنسانية والاجتماعية، المجلد 16، العدد 03،

جامعة أحمد دراية، أدرار، الجزائر، سبتمبر 2017، ص ص: 432-451:

<https://www.asjp.cerist.dz/en/article/52539>

الأفراد، وهناك أيضا تقسم (Martin Vasik)، والذي بدوره يقسمها إلى ثلاث أقسام أيضا، الدخول والاستعمال غير المصرح بهما إلى النظم المعلوماتية، الاحتيال والسرقة المعلوماتية، الجرائم التي يلعب فيها الحاسب الآلي دورا مساعدا في ارتكابها⁽¹⁾.

ثانيا: الحرب السيبرانية:

1- تعريف الحرب الإلكترونية:

لقد مرت الحروب في تاريخ البشرية كلها بعدة أجيال مختلفة، كان أولها يتجلى في الحروب التي تقع بين جبهتين معلومتين، وتنتهي بغلبة جبهة على جبهة أخرى، ثم أعقبتها حروب الجيل الثاني أين أصبحت كل موارد الدولة بالإضافة إلى القطاع العسكري تسخر مجملا في القطاع الحربي، ثم بعد ذلك أتت حروب الجيل الثالث والتي تجلت صورتها الأساسية في الحروب بالوكالة، ثم ظهر جيل رابع من الحروب والذي كان يعتمد على الترويع وشمولية التدمير من خلال الاغتيالات والتفجيرات والاختطاف وأثارة الحروب الأهلية، ثم وفي الأخير ظهر جيل خامس من الحروب والذي يعتبر نهجا أقل عنفا كالمظاهرات والاعتصامات والاحتجاجات والعصيان المدني، وتدخل الحروب السيبرانية ضمن قائمة الأساليب والآليات التي يتم الاعتماد عليها في شن الهجمات بل هي أهمها وأكثرها خطرا لما فيها من مجهولية المصدر وإبهام الهدف⁽²⁾.

ومفهوم الحرب الإلكترونية يعد مفهوما غامضا بعض الشيء، فمن خلال دراستنا لمختلف المراجع والأبحاث التي تناولت مضمون الحرب الإلكترونية، نلاحظ أن هناك اختلافات كبيرة في توظيف هذا المصطلح، وسنبين هذا الاختلاف من خلال عرض موجز لبعض التعاريف المقدمة للحرب الإلكترونية.

يعرف بعض الباحثين الحرب الإلكترونية على أنها: (عبارة عن هجمات تتم بواسطة استخدام الكومبيوتر أو الشبكات أو الأنظمة ذات الصلة، وتهدف إلى تعطيل أو تدمير أنظمة الإنترنت، أو الممتلكات أو الوظائف الحاسوبية الخاصة بالخصم، كما ويستخدم هذا المصطلح للإشارة إلى وسائل وأساليب القتال التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح، أو تجرى في سياقه ضمن المعنى المقصود في القانون الدولي الإنساني)⁽³⁾.

⁽¹⁾ أنظر في هذا التقسيم: أيمن عبد الله فكري، المرجع السابق، ص ص: 137-141.

⁽²⁾ نانيس عبد الرزاق فهمي، الحرب السيبرانية: حرب القرن القادم، 15 نوفمبر 2018، تم الاطلاع عليه بتاريخ 17 جانفي 2020 على الساعة 15:47 ساء، في موقع: <https://www.raiayoum.com/index.php/> الحرب-السيبرانية-حرب-القرن-القادم/

⁽³⁾ مر محمود أعمار، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة دراسات، علوم الشريعة والقانون، المجلد 46، العدد 03، الجامعة الأردنية، 2019، ص ص: 134-155.

<https://journals.ju.edu.jo/DirasatLaw/article/view/101907>

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

وعرفها البعض الآخر على أنها: (أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها)⁽¹⁾.

وذهب آخرون في تعريفها على أنها: (مجموعة من الإجراءات التي تنفذ بهدف الاستطلاع الإلكتروني للنظم والوسائل الإلكترونية المعادية، وإخلال عمل هذه النظم والوسائل الإلكترونية، ومقاومة الاستطلاع الإلكتروني المعادي، وتحقيق استقرار عمل النظم الإلكترونية الصديقة تحت ظروف استخدام العدو أعمال الاستطلاع والإعاقة الإلكترونية)⁽²⁾.

يمكن أن نأخذ جملة من الملاحظات من وعلى هذه التعريفات، فالتعريف الأول يركز على الفضاء الإلكتروني كوسيلة وكهدف للحرب الإلكترونية، كما وأنه يجلي بوضوح شديد الطابع العسكري للفضاء الإلكتروني من جهة، وطابعه كساحة وفضاء من فضاءات النزاع المسلح من جهة ثانية.

أما التعريف الثاني فيبرز السمة العسكرية والسياسية والاقتصادية للفضاء الإلكتروني⁽³⁾، غير أنه اقتصر على آلية واحدة من آليات الحرب الإلكترونية وهي الاختراق، في حين أن أسلحة الحرب الإلكترونية متعددة، وهذا يوحي بأن الحرب الإلكترونية مقتصرة حسب هذا التعريف على حرب الإنترنت فحسب وهذا غير صحيح من وجهة نظر فيصل محمد عبد الغفار الذي يرى أن حرب فضاء الإنترنت ما هي إلا مجال من مجالات الحرب الإلكترونية⁽⁴⁾.

و يشترك التعريفين الأول والثاني في كونهما يقتصران فقط في تعريف الحرب الإلكترونية على الطابع الهجومي، وأهملا مع الطابع الدفاعي في الحرب الإلكترونية.

أما التعريف الثالث فهو التعريف الأكثر جودة، إذ أنه ركز على الطابعين الهجومي والدفاعي للحرب الإلكترونية من جهة، ومن جهة ثانية فقد بيّن أهم الأهداف والصورة أو النشاطات التي تتجلى من خلالها الحرب الإلكترونية ووسع من دائرتها أيضا.

(1) كريم رقولي، أحلام و غليسي، الحرب الإلكترونية بين الولايات المتحدة وروسيا، مجلة أكاديميا للعلوم السياسية، المجلد 06، العدد 02، جامعة حسيبة بن بوعلي، شلف، الجزائر، جويلية 2020، ص: 143-134.

<https://www.asjp.cerist.dz/en/article/120448>

(2) فيصل محمد عبد الغفار، الحرب الإلكترونية، الطبعة الأولى، الجنادرية للنشر والتوزيع، الأردن، 2016، ص 27.

(3) حكيم غريب، شرقي صبرينة، تداعيات الحرب الإلكترونية على العلاقات الدولية: (دراسة في الهجوم على إيران "فيروس ستكنست")، مجلة دفاتر السياسية والقانون، المجلد 12، العدد 03، جامعة قصدي مرباح، ورقلة، الجزائر، جوان 2020، ص: 107-92.

<https://www.asjp.cerist.dz/en/article/115664>

(4) فيصل محمد عبد الغفار، المرجع نفسه، ص: 14-13.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

غير أن التعريفات الثلاثة قد ركزت على الفضاء الإلكتروني كهدف من أهداف الحرب الإلكترونية وكوسيلة أيضا، وأهملت الأهداف الأخرى، وهي الأكثر إضرار من مجرد الهجوم على أنظمة المعلومات، وهو استهداف البنى التحتية الحرجة، كما وأهملت أيضا الهجمات المادية على عناصر الفضاء الإلكتروني، مع إهمالها أيضا الطابع الهجين للحرب الإلكترونية، والتي لا يستهدف فيها الفضاء الإلكتروني بحد ذاته، كما وأهملت أيضا المعنى الحقيقي والجوهري للحرب.

وعموما يمكن أن نقترح تعريفا للحرب الإلكترونية من خلال تفادي هذه الانتقادات من جهة، ومن خلال وضع الحرب الإلكترونية في الإطار المفهومي العام للحرب من جهة أخرى مستثنين في ذلك إلى التعرف الآتي للحرب: (الحرب هي نزاع مسلح تبادلي بين دولتين أو أكثر من الكيانات غير المنسجمة، حيث الهدف منها هو إعادة تنظيم الجغرافية السياسية للحصول على نتائج مرجوة ومصممة بشكل ذاتي)⁽¹⁾.

وبذلك يمكن أن نعرف الحرب الإلكترونية على أنها:

"الحرب الإلكترونية هي نزاع تبادلي على الفضاء الإلكتروني بين مختلف الفواعل الدولية، من خلال توجيه أسلحة الفضاء الإلكتروني المتعددة أو أي سلاح آخر من الأسلحة التقليدية إلى أحد العناصر التكوينية للفضاء الإلكتروني أو كلها، بهدف شل حركتها أو تدميرها، إضرار بما تحمله من محتوى أو بما تقوم به من أدوار أساسية، وذلك من أجل التأثير على موازين القوى".

وبذلك يمكن القول أن الحرب الإلكترونية - بهذا المعنى - هي حرب غير تناظرية، فأسلحتها لا تحتاج إلى تكلفة باهظة، كما أنها حرب يتمتع فيها المهاجم بأفضلية على المدافع، وهي حرب لا ينفع معها الردع، نظرا لمجهولية مصدرها، كما أن أهدافها لا تنحصر فقط في المواقع العسكرية بل وتتخطاها إلى العديد من المجالات والمواقع، كما وتتميز أيضا بكونها حربا رقمية تستعمل فيها التقنية والوسائل الإلكترونية⁽²⁾.

2- الحرب الإلكترونية: نظرة واقعية:

تتخذ الحرب الإلكترونية أنماطا ثلاث، فهي إما أن تكون منخفضة الشدة وذلك حينما يوظف الفضاء الإلكتروني في شن الحروب النفسية أو الاختراقات أو التجسس، وسرقة المعلومات وما إلى ذلك، كما يتخذ أيضا نمطا متوسط الشدة أين تكون الحرب فيها مماثلة للحرب التقليدية، والتي قد

(1) ويكيبيديا، حرب، الموسوعة الحرة، مختصر الرابط: <https://cutt.us/KgeVX>

(2) حكيم غريب، شرقي صبرينة، المرجع السابق.

الفصل الأول الفضاء الإلكتروني والتحول الكبري في المفاهيم الاستراتيجية

تؤول إلى حرب عسكري، وقد تتخذ في المستقبل نمطا ثلاثا وهو النمط مرتفع الشدة، أين يكون الفضاء الإلكتروني هو المسيطر والغالب في العمليات الحربية، ورغم أننا لم نعش مثل هذه الحروب إلا إن إمكانية حدوثها في المستقبل يبغي أمرا واردا ومحتملا⁽¹⁾.

والحرب الإلكترونية كما أسلفنا لا تنحصر فقط في استهداف المواقع العسكرية، بل تتخطى ذلك إلى العديد من المواقع والقطاعات الأخرى، والواقع قد أثبت أن الحرب الإلكترونية يمكن أن تستهدف بشكل خاص؛ قطاع الاتصالات والمعلومات، الذي هو العاقد الذي تستند إليه الدولية، وكذلك قطاع الأعمال والاقتصاد، وقطاعات التوزيع المختلفة، بالإضافة إلى القطاع العسكرية الذي أصبح يعتمد على الفضاء الإلكتروني بشكل كبير مما جعله أهدافا توجه إليها أشكالا خطيرة من الهجمات الإلكترونية⁽²⁾⁽³⁾، وقد أصبح هذا القطاع في العصر الحديث من أهم القطاعات التي وقعت تحت نيران الصراعات الإلكترونية⁽⁴⁾.

تثير الحرب الإلكترونية أو السيبرانية العديد من الإشكاليات القانونية المعقدة، ولاسيما في تطبيق القانون الدولي الإنساني، وتقرير التناسب، وقد عالج الدكتور عادل عبد الصادق تطبيق القوانين الدولية في الصراعات والحروب السيبرانية بتفصيل واسع، وخلص في النهاية إلى أن إخضاع الفضاء الإلكتروني للقانون الدولي يتطلب حركة تغيير واسعة تشمل أبعاد تنظيمية، قانونية سياسية، أمنية، وثقافية⁽⁵⁾.

(1) كريم رقولي، أحلام وغيبي، المرجع السابق.

(2) وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، أطروحة ماجستير في التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح، نابلس، فلسطين، 2013، ص: 90-95.

(3) الأكثر خطورة منها هو تعرض المنشآت النووية لمثل هذه الهجمات، وقد حذر تقرير صادر عن معهد تشاتام هاوس من تنامي خطر تعرض أنظمة الأسلحة النووية لهجمات إلكترونية، الأمر الذي قد يؤدي إلى فقدان التحكم في أنظمتها مما قد ينجم عنه عمليات إطلاق غير مقصودة، والأمر المهم الذي لفت النظر إليه هذا التقرير هو أن الأنشطة الإلكترونية العدوانية وفي حال السلم قد يترتب عنها كارثة تحل بالدول المستهدفة كونها قد لا تكون على علم أنها تحت تهديد هجوم إلكتروني مما يؤثر على اتخاذ القرارات العسكرية بما في ذلك القرارات التي تؤثر على سياسته أسلحه الردع النووي:

<https://m.youm7.com/story/2018/1/11/3596079-تقرير-الهجمات-الإلكترونية-على-المنشآت-النووية-تؤدي-لتخريب-التحكم-بها/3596079>

(4) إن المنظومة العسكرية الإيرانية تتعرض لهجمات إلكترونية متكررة من قبل الولايات المتحدة الأمريكية، ورغم أن الولايات المتحدة لم تصرح بأنها نفذت هجمات إلكترونية واسعة النطاق على منظومة الصواريخ الإيرانية كردة فعل على إسقاط الطائرة المميرة الأمريكية ألا أن مصادر في صحيفة واشنطن بوست تؤكد أن وحدات الأمن الإلكتروني الأمريكية قد هاجمت حواسيب في منظومة الصواريخ الإيرانية ليلة 20 يونيو/حزيران 2019 والتي أثبت نفس المصدر بأن الهدف منها هو القيام بشل منظومة الدفاع الصاروخية لإيران بتعطيل منصات الصواريخ أو إحداث أضرار فيها لا يمكن إصلاحها: (أيوب رقيب، تخريب أم تحكم؟ هجوم إلكتروني أمريكي على إيران، 2019/06/23، تم الاطلاع عليه بتاريخ 06 جانفي 2020 على الساعة 4:25 على موقع الجزيرة):

<https://www.aljazeera.net/news/scienceandtechnology/2019/6/23/هجوم-إلكتروني-إيران-ان-نجت-من-الرد-العسكري-ولكنها-تحت->

[هجوم-إلكتروني](#)

(5) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المرجع السابق، ص 153.

أما عن مسألة التناسب، فالاتجاه العام فيه لا يزال يكتنفه الإبهام والغموض والضبابية، والأجوبة على مضامينه تتطلب توضيحا وإجلاءً، ولا سيما في تكريس مبدأ التناسب في الرد على الاعتداءات السيبرانية، أما الولايات المتحدة الأمريكية، [فالظاهر أنها قد حسمت في حق الرد أمراً]، وذلك حين أقرت بأن أن هجوم عليها بالصواريخ أو من خلل هجمات سيبرانية يجعل من الرد باستعمال قوة السلاح المناسب وجيهاً⁽¹⁾.

(1) أزهر عبد الأمير الفتلاوي، العمليات العدائية طبقاً لقواعد القانون الدولي الإنساني، الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، مصر، 2018، ص 132.

الفصل الثاني:

الإرهاب الإلكتروني: خطر يهدد الأمن الدولي

يشكل الفضاء الإلكتروني الأرضية المناسبة لما لها من خصائص ومميزات لإنتشار النشاطات والأعمال الإرهابية والتخريبية، فالطبيعة التكوينية لهذا الفضاء وما يتيح من نوافذ خدمائية، قد منح للإرهابيين آلية جديدة وفضاء رحبا للعمل بشكل أوسع في توظيفه في الأعمال الإجرامية والإرهابية التي تتنافي مع مقتضيات الأمن والسلامة على الصعدين الوطني والدولي.

لقد فتح الفضاء الإلكتروني منفذا واسعا لظهور نمط فريد من الإرهاب والذي يتمثل في الإرهاب الإلكتروني الذي لم تحدد معالمه ولم تتضح طبيعته القانونية إلى حد الساعة نظرا للتزاوج في طبيعته بين مفهومين لا يزالا يعانيان من الإبهام والغموض وهما الفضاء الإلكتروني الذي تقدم بيانه وبين الإرهاب كظاهرة تقليدية لا تزال تعاني من الخلافات في تحديد تعريفها وبيان طبيعتها، غير أنه ومع ما في مفهومه من إشكاليات وما في طبيعته من جدليات إلا أن هناك عمل جدي يقوم به الباحثون والفقهاء من أجل بلوغ الجذور الرئيسية التي ينبع منها هذا الوباء الأمني الذي يجتاح العالم، فالعمل على تحديد أسبابه دون تحيد لأي مجال معرفي معين سيكون من شأنه رسم الخطوط الرئيسية له وتشكيل صورة منهجية توضح فيها كل الحثيات والظروف التي تنمو فيها هذه الظاهرة وتتطور، وهذا من أجل وضع اليد على أصل الداء ومعالجته بالطرق السليمة التي تضمن القضاء عليه دون أن يكون لتلك الطرق أي آثار جانبية تعود بالأثر العكسي على الأمن والسلم العالميين (المبحث الأول).

إن الداعي إلى دراسة الإرهاب الإلكتروني في الوقت الراهن لم يعد مسألة نظرية لإشباع الفضول العلمي والفلسفي، ولا خيالا علميا جامحا، بل هو واقع مفروض وتهديد فعلي تواجهه البشرية كأبرز تحدي أمني في العصر الحديث، فتداعياته أصبحت واقعا ملوسا يمكن ملاحظته بكل وضوح من خلال العديد من الهجمات الإلكترونية التي تقوم بها جهات فاعلة باستخدام أسلحة ذات طبيعة إستثنائية من أجل استهداف الأمن والاستقرار على البيئة الإلكترونية بهدف نشر الخوف والرعب والهلع لأغراض سياسية، وإن آثاره لوخيمة على كل المستويات وما زادها حدة وشدة هو غياب الإطار التشريعي الذي بموجبه تتعقد المسؤوليات وتتحدد (المبحث الثاني).

المبحث الأول:

ماهية الإرهاب الإلكتروني

يعمل الإرهاب بشكل أساسي وممنهج على تقويض دعائم الأمن وإحداث شرخ في صرح الدول، خاصة مع اتساعه ليشمل كل أرجاء العالم، ولهذا فقد أصبح في يحتل المقام الأول في انشغالات السياسيين ورجال القانون والهيئات الأمنية، ورغم أن مصطلح الإرهاب قد أصبح من أكثر المصطلحات السياسية والقانونية تداولاً، إلا أن مفهومه لا يزال يعوزه الوضوح ويكتفه الغموض، وهذا الأمر قد صار على الإرهاب الإلكتروني كظاهرة مستجدة لها من الخصوصية ما يعزز فرص الاختلاف في مفهومها، الأمر الذي وسع من دائرة الإشكال في التميز بينها وبين غيرها من المفاهيم (المطلب الأول).

ومع هذا فإن الباحثين والمتخصصين قد بذلوا من الجهد أطيبه من أجل الوصول إلى تحديد إطار للبيئة التي تكون منبثاً للظاهرة الإرهابية بما فيها ظاهرة الإرهاب الإلكتروني وهذا من أجل فهمها فهما سليماً يمكن من تحديد معالمها ومفهومها ومن ثم العمل على وضع استراتيجيات فعالة ومؤثرة لاجتثاثها من أصولها وجذورها (المطلب الثاني).

المطلب الأول:

مفهوم الإرهاب الإلكتروني

تعتبر جريمة الإرهاب الإلكتروني شكلاً مستحدثاً من أشكال الإرهاب، ونمطاً جديداً من أنماطه، وفرعاً من فروعها، التي تهدد المجمع الدولي وبنيتة التحية، لذلك فإن إشكالية تعريف هذه الظاهرة المستجدة تبدأ عند بداية إشكالية تعريف الإرهاب عموماً (الفرع الأول) إذ عمد الكثير من الدارسين إلى دراسة الإشكالية دراسة وافية لبلوغ تعريف شامل وجامع يصف الظاهرة وصفا تحليلياً دقيقاً مبيناً عناصره ومميزاً له عن غيره من المفاهيم المتشابهة (الفرع الثاني)، ساعين إلى أبرز السمات والخصائص التي تتميز بها هذه الظاهرة عن غيرها لمحاولة وضعها في إطار مفهومي محدد تتجلى فيه مواطن الخطورة وتتضح فيه آليات المكافحة (الفرع الثالث).

الفرع الأول: إشكالية تعريف الإرهاب الإلكتروني:

إن ظاهرة الإرهاب الإلكتروني تعتبر من أكثر فروع الإرهاب أهمية وخطورة، وقد تزامن ظهورها وانتشارها مع ظهور الطفرة المعلوماتية والتنامي السريع للتكنولوجيا الرقمية، وبما أنها تعتبر نمطاً من أنماط الإرهاب، فلا ريب أن إشكالية تعريف الإرهاب تأثر عليها بصفة مباشرة (أولاً)

وسنصل في النهاية وضع الإرهاب الإلكتروني في الإطار المفهومي العام الذي من خلاله نتمكن إلى فهم دقيق وواضح لإشكالية الإرهاب الإلكتروني (ثانياً).

أولاً: إشكالية تعريف الإرهاب:

لقد أثارت الدراسات المختلفة للظاهرة الإرهابية جدلاً واسع النطاق في موضوع بيان وتحديد تعريف لهذه الظاهرة، واختلفت فيه وجهات النظر اختلافاً بيناً، وتباينت فيه الآراء تبايناً كبيراً، وهذا عائد في الأصل إلى الاختلاف المنهجي في دراسة الظاهرة الإرهابية من جهة، وإلى اختلاف العقائد وتضارب الإيديولوجيات من جهة أخرى.

1- تعريف الإرهاب لغة:

إن أول استخدام لكلمة إرهاب كان لاحقاً للفترة التي دونت فيها أمهات كتب اللغة العربية، فلم يكن معروفاً حينها استخدام هذا اللفظ، كما لم يكن هناك أي مصدر لغوي قديم ذكر فيها استخدام مصطلح "الإرهابي"، ولذلك فإن عمدة القواميس العربية القديمة لم تتطرق في أي موضع من مواضعها على تعريف لغوي لهذا المصطلح⁽¹⁾، غير أن مجمع اللغة العربية قد اعتمده وضبط له معنا لغوياً، وأصدر بذلك قراراً يعرفه فيه استناداً إلى مصدره اللغوي، فالإرهاب لفظ مشتق من الفعل الماضي "أرهب" وهو بمعنى أخاف وأفزع⁽²⁾، فكان التعريف اللغوي الذي تقدم به مجمع اللغة العربية لمصطلح الإرهاب هو: "الإخافة والتفزع"⁽³⁾.

أما في اللغة الفرنسية فإن مصطلح الإرهاب قد ظهر خلال الثورة الفرنسية، إذ تم استخدام المصطلح في التعبير عن البطش الذي كانت تمارسه الحكومة اليعقوبية ضد الثائرين من أجل الردع والإخافة والإفزاز بهدف الإخضاع للنظام والسياسية الإقطاعية وفرض سلطتها على الشعب⁽⁴⁾، ويعرفه القاموس الفرنسي لاروس بأنه: (مجموعة من الأعمال أو التصرفات المرتكبة من منظمة أو فرد من أجل خلق جو من انعدام الأمن وهذا لغرض ممارسة الابتزاز على الحكومة لغاية إرضاء كراهية ضد مجتمع، ضد دولة، ضد نظام معين)⁽⁵⁾.

(1) مصلح الصالح، ظاهرة الإرهاب المعاصر: (طبيعتها وعواملها واتجاهاتها)، مركز الملك فيصل للبحوث والدراسات الإسلامية، الرياض، المملكة العربية السعودية، 2002، ص 16.

(2) إرهاب: قاموس المعاني: <https://www.almaany.com/ar/dict/ar-ar/> أرهب

(3) القرار السابع بشأن تعريف مصطلح الإرهاب المنشور بتاريخ 12 مايو 2015 عن مجمع اللغة العربية: <https://www.m-a-arabia.com/site/15829.html>

(4) أحمد عطية الله، القاموس السياسي، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1968، ص 45.

(5) **terrorisme**: dictionnaire Larousse sur web : <https://www.larousse.fr/dictionnaires/francais/terrorisme/77478>
" Ensemble d'actes de violence (attentats, prises d'otages, etc.) commis par une organisation ou un individu pour créer un climat d'insécurité, pour exercer un chantage sur un gouvernement, pour satisfaire une haine à l'égard d'une communauté, d'un pays, d'un système "

2- التعريف الفقهي للإرهاب:

لقد بذل الدارسون جهدا كبيرا في محاولة تقديم تعريف شامل وواسع للظاهرة الإرهابية، ونظرا لاختلاف الزاوية التي ينظر منها إليها، فإن كل التعاريف المعروضة والمقترحة لها، تقتصر إلى الموضوعية والدقة والضبط، وتتسم بالارتجالية والذاتية والقصور، وهذا نظرا لتأثرها بالإيديولوجيات والمعتقدات الفكرية والسياسية والدينية المختلفة، كما أنها واقعة تحت تأثير السياسة العامة للجماعة أو الحزب التي ينتمي إليه الدارس، دون إغفال دور صنّاع القرار في مختلف دول العالم في إعطاء صورة غير دقيقة للقلب الذي تتشكل فيه الظاهرة الإرهابية، وحذت هذا الحذو وسائل الإعلام والصحفيين الذين قدموا نفس تلك الصورة النمطية السائدة في أروقة الساسة، مما صرف هذه الظاهرة عن حطها في دراسة أكاديمية محايدة وموضوعية⁽¹⁾.

إن الاتجاهات الفقهية المعتمدة في محاولة التوصل إلى تعريف يضبط المعنى الصائب للظاهرة الإرهابية قد رصدها الدارسون والفقهاء والباحثون، وهي متعددة ومتباينة⁽²⁾، لكن أكثرها أهمية وعمقا هي تلك التي تتناول الأسس التي بنيت عليها تلك التعاريف، وهما اتجاهان اثنان:-

1- الاتجاه المادي:

لقد ذهب أنصار هذا الاتجاه إلى تعداد الأفعال الإجرامية التي تعطي صورة تعريفية لجريمة الإرهاب، فهم يرون أن مسألة تعريف الإرهاب غير قابلة للطرح إذا لم يتم تحديد الأفعال المكونة له، مع بيانها بيانا مفصلا، وتقديم تعريف موضوعي لكل فعل منها، مع الاستبعاد التام لأغراض والغايات التي تقف وراء ارتكابها، فهذا الاتجاه إذا يقف موقفا مادي بحتا في نظريته للظاهرة الإرهابية⁽³⁾.

فالإرهابي لا يعد إرهابيا إلا بعد إثبات فعل أو سلوك من السلوكيات المحددة سلفا بوصفها أفعالا إرهابية لذاتها وبطبعاتها، وهذا بقطع النظر عن طبيعة ومقاصد مرتكبيها⁽⁴⁾، وعليه عمد الكثير من أنصار هذا الاتجاه على صياغة التعريف الآتي للإرهاب : (القتل والاغتيال والتخريب

(1) عبد الرحمن بن معلا اللويح، الإرهاب والغلو: (دراسة في المصطلحات والمفاهيم)، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، جامعة الملك محمد بن سعود الإسلامية، المملكة العربية السعودية، 1425 هجرية، ص ص 93-133:

<https://units.imamu.edu.sa/colleges/sharia/rnd/Pages/7thqf.aspx>

(2) عباس شافعة، الظاهرة الإرهابية بين القانون الدولي والمنظور الديني، أطروحة دكتوراه في القانون الدولي والعلاقات الدولية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2010-2011، ص 24.

(3) المرجع نفسه، ص 26.

(4) فرج محمد لامة، إعادة اختراع الإرهاب بعد 11 سبتمبر، مؤسسة البراق للنشر والتوزيع، الأردن، 2015، الصفحة 20.

والتدمير وإتلاف الوثائق العامة، ونشر الشائعات واحتجاز الممتلكات، وكل هذا عندما تتشارك في تحقيق نتيجة واحدة تتضمن نشر الرعب⁽¹⁾.

فالإرهابي هو كل من يرتكب هذه الأفعال دون النظر إلى القصد والغاية من ارتكابها⁽²⁾، وهذا ما أوضحه الأستاذ بريان جنكينز (Braine Michael Jenkins)⁽³⁾ حين قال: (بأن أي مجموعة تقوم بأحد تلك الأفعال فإنها تحمل وصف الإرهابية الذي يلتصق بها، سواء أكانت تقصد من أفعالها إنشاء حالة الإرهاب أم لا...)⁽⁴⁾.

ونظرا لصعوبة أو استحالة إجراء عملية ضبط من أجل تحديد الأفعال الموصوفة بالإرهاب على سبيل الحصر، لجأ أتباع هذا الاتجاه إلى أسلوب آخر، وهو محاولة تحديد الخصائص الجوهرية التي بها يتميز الإرهاب عن بقية الأفعال الإجرامية المماثلة له⁽⁵⁾.

رغم كثرة العيوب التي تشوب هذا الطرح وتعدد مستويات النقد لمضمونه إلا أنه قد وجد منفذا إلى أوساط الهيئات القانونية والتشريعية، فاللجنة القانونية لمجموعة الدول الأمريكية في تقريرها المعد على خلفية إعداد مشروع اتفاقية لمكافحة الإرهاب والاختطاف قد اشتمل على شكل من أشكال التعريف المادي للإرهاب⁽⁶⁾.

كما أن الوفد الأمريكي في الدورة الثامنة والعشرين للجمعية العامة في الأمم المتحدة كان اقتراحه لتعريف الإرهاب اقتراحا ماديا صرفا، فالإرهاب في رأيهم هو: (فعل منسوب إلى كل

⁽¹⁾ الهواري عبد الرحمن رشدي، التعريف بالإرهاب وأشكاله، أعمال ندوة الإرهاب والعولمة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2002، ص 23.

⁽²⁾ <https://www.google.com/url?sa=t&source=web&rct=j&url=https://repository.nauss.edu.sa/bitstream/handle/123456789/54096/%25D8%25A7%25D9%2584%25D8%25A5%25D8%25B1%25D9%2587%25D8%25A7%25D8%25A8%2520%25D9%2588%25D8%25A7%25D9%2584%25D8%25B9%25D9%2588%25D9%2584%25D9%2585%25D8%25A9%3Fsequence%3D1%26isAllowed%3Dy&ved=2ahUKEwihxfv3gbfoAhXBnOAKHTXOAG0QFjADegQIBBAB&usg=AOvVaw0WaiGULVPqwzguHe6pKsW>

⁽³⁾ هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، الطبعة الأولى، دار الكتب العلمية، بيروت، لبنان، 2005، ص 23.

⁽⁴⁾ بريان ميكائيل جنكينز (Braine Michael Jenkins) 1942 شيكاغو: هو مستشار أمريكي وخبير في دراسة الإرهاب وأمن المواصلات، وعضو سابق في القوات الخاصة الأمريكية حيث التحق بها عن حين بلوغه سن 19 سنة، ثم اشتغل كمندني في مجموعة مهام التخطيط بعدة المدى، ثم نائبا لرئيس شركة الأمن (KROLL)، عمل أيضا كمدير مركز سلامة النقل في معهد النقل مينيتا، وأيضا عضو في لجنة البيت الأبيض لسلامة وأمن الطيران، ومستشار اللجنة الوطنية لإرهاب، ألف العديد من الكتب أهمها: (Unconquerable Nation Terrorist Go Nuvlear)، نقلا عن الموسوعة الحرة، ويكيبيديا: https://fr.wikipedia.org/wiki/Brian_Michael_Jenkins

⁽⁵⁾ الهواري عبد الرحمن رشدي، التعريف بالإرهاب وأشكاله، المرجع نفسه.

⁽⁶⁾ حيدر أدهم عبد الهادي، دراسات في قانون حقوق الإنسان، دار حامد للنشر والتوزيع، الطبعة الأولى، 2009، ص 24.

⁽⁷⁾ الهواري عبد الرحمن رشدي، المرجع السابق، ص 23.

شخص يقتل شخصا آخر في ظروف مخالفة للقانون أو سبب له ضررا جسديا بالغاً أو خطفه أو يحاول القيام بفعل كهذا أو يشارك شخصا قام أو حاول القيام بفعل كهذا⁽¹⁾.

نقد الاتجاه المادي:

لقد وجهت عدة انتقادات لهذا المذهب والمسلك في تعريف الإرهاب، ولعل من أهم الانتقادات التي أبداهها معارضوه ترتكز أساساً على نقد الأهداف التي أراد أنصار هذا الاتجاه تحقيقها من وراءه، وهي تفادي التشتت القانوني والانتقادات الفقهية.

إن الاتجاه المادي لم يرعي مرونة الظاهرة الإرهابية، والبعد التطوري لأساليبها وأنماطها وأغراضها الإجرامية، مما يجعل حصرها أمراً صعباً، والتنبؤ بها أمر مستحيل، كما أن إغفال الأهداف من مجموع تعريفات الاتجاه المادي قد أخرج شكلاً خطيراً من أشكال الإرهاب من دائرة التجريم القانوني، وهو الإرهاب لتحقيق أغراض سياسية⁽²⁾، والذي يعد من أهم وأبرز الأهداف التي تقف وراء ارتكاب الأعمال الإرهابية، إذ أن المرمى الذي يراد أصابته في المقام الأول من كل الأعمال الإرهابية هو مرماً سياسياً بامتياز، الأمر الذي يمنحها أهمية خاصة فضلاً عن تفاقم وجسامتها أخطارها⁽³⁾.

كما أن مثل هكذا مذهب في تعريف الظاهرة الإرهابية يعزز القوى الاستعمارية، كما يعزز أيضاً الكيانات الغاصبة، ويغل يد المكافحين عن المطالبة بحقوقهم المشروع في تقرير مصيرهم⁽⁴⁾.

2- الاتجاه الموضوعي:

يقوم هذا الاتجاه على خلاصة ومخرجات الدراسات الموضوعية التي يجريها ذوي الاختصاص للعمل على بلوغ الأهداف والغايات التي تريد البشرية بلوغها والتي ترمي في جوهرها إلى القضاء على هذه الظاهرة، دون النظر إلى طبيعة تلك الأعمال سواء في شكلها أو في أساليبها⁽⁵⁾، إذاً هو اتجاه يضع نصب عينيه في دراسة الظاهرة الإرهابية، الغايات والأهداف التي يريد أصحاب هذه النشاطات الإرهابية الوصول إليها ونيلها وراء تلك النشاطات، فهو يقوم على

(1) نقلاً عن: هيثم عبد السلام محمد، المرجع السابق، الصفحة 24.

(2) الهواري عبد الرحمن رشدي، المرجع السابق، ص 24.

(3) الهواري عبد الرحمن رشدي، المرجع نفسه، ص 33.

(4) هيثم عبد السلام محمد، المرجع نفسه، ص 24-25.

(5) المرجع نفسه، ص 25.

دراسة الأهداف والغايات التي تكمن وراء الأعمال والتصرفات الإرهابية، دون النظر إلى طبيعة تلك الأعمال، وهذا من خلال تحليل الخصائص المشتركة في الأعمال الإرهابية⁽¹⁾.

وقد اختلف مؤيدو هذا الاتجاه في تحديد طبيعة تلك الأهداف، حيث ذهبوا فيها مذاهب شتى، منهم من يرى أنها أهداف سياسية ومنهم من يرى أنها دينية، ومنهم من يرى أنها فكرية⁽²⁾.

ومن الواضح جداً أن للدراسة التي أجراها شميد وجونجمان والتي فحصت 109 تعريفاً ووجدت 22 "عنصر تعريف" مستخدمة بشكل متكرر فائدة كبيرة كدليل في الفكر الأكاديمي⁽³⁾، حيث قام أليكس بيتر شميد (Ales P. SCHMID)⁽⁴⁾ من خلال دراسة مما يزيد عن مئة تعريف ليصل إلى عزل العناصر الرئيسة أو القواسم المشتركة التي تتشارك فيها التعاريف والتي تتمثل في:

-الرعب كنتيجة للأعمال الإرهابية

-ضحايا مقصودين لذاتهم أو كوسيلة أو لإرهاب الآخرين

-مستهدفين أوليين توجه إليهم الأعمال الإرهابية

-استخدام مختلف أنواع العنف من أجل تحقيق أهداف سياسية⁽⁵⁾.

لكن هل هناك ضرورة تحتم الوصول إلى تعريف للإرهاب وخاصة على الصعيد الدولي؟

هناك جانب من الفقه يرى أن فهم وإدراك جوهر الظاهرة الإرهابية يكون متاحاً وميسوراً حينما يكون على أساس وصفي لا تعريفي، إذ أنه ليس من اليسير الوصول إلى صياغة تعريفات يمكن أن تكون على مستوى من الإقناع، فانعدام هذا الأخير هو نتيجة للنوايا المبطنة في اتهام كل طرف من الأطراف للآخر، وهناك جانب آخر من الفقه يرى ضرورة تقديم تعريف له⁽⁶⁾.

(¹) فرج محمد لاهم، المرجع السابق، ص 21.

(²) عباس شافعة، المرجع السابق، ص ص: 27-28.

(³) Gregor BRUCE, *Definition of Terrorism – Social and Political Effects*, *Journal of Military and Veterans' Health*, Issues 21, volume 02, published by the Australasian Military Medicine Association, Australie, may 2013, PP. 26-30: <https://jmvh.org/wp-content/uploads/2013/05/JMVH-May-2013.pdf>

(⁴) أليكس بيتر شميد (Ales P. SCHMID) 1943 شور: هو باحث هولندي سويسري في دراسات الإرهاب، ومسؤول سابق عن فرع منع الإرهاب في الأمم المتحدة، شغل العديد من المناصب الرفيعة الأخرى، وألف العديد من المصنفات والأوراق البحثية، أهمها: (Links between (Terrorism and Migration: An Exploration)، (Foreign Terrorist) Fighters with IS: A European Perspective)، (Challenging the Narrative of the "Islamic State")، أنظر:

- <https://icct.nl/people/dr-alex-p-schmid-visiting-research-fellow/>
- https://en.wikipedia.org/wiki/Alex_P._Schmid

(⁵) فرج محمد لاهم، المرجع السابق، ص 21.

(⁶) عباس شافعة، المرجع السابق، ص 25.

وتعود هذه الضرورة إلى الآثار التي ترتبت حتى الآن جراء غياب تعريف للإرهاب، ومن أبرزها التحول من المواجهة الجنائية لهذه الظاهرة إلى إعلان الحرب عليها، وكذلك سعي بعض الدول الغربية إلى ربط الظاهرة الإرهابية بالدين الإسلامي، كما ينتج أيضا عن غياب تعريف للإرهاب هشاشة وضعف أشكال التعاون المختلفة بين الدول في مواجهته والتصدي له⁽¹⁾.

فالإجماع على تعريف للإرهاب سيكون له أثر كبير على العديد من المستويات، فهو سيساعد بشكل كبير في مجال الأبحاث والدراسات، وإحراز المزيد من نهج المواجهة، كما أن التعريف القانوني الدقيق للإرهاب يشكل أهمية كبيرة للقيام بتحقيق قضائي ناجح وتقديم الإرهابيين للمقاضاة داخل إطار النظام القضائي القائم⁽²⁾، فعدم فهم جوهر الظاهرة الإرهابية سيكون له دور سلبي على مجال البحث العلمي المعني بهذه الظاهرة وتشتيتها، فضلا عن عدم تبلور المفهوم القانوني لها والذي تقوم عليه جميع إجراءات المتابعة والمحاكمة.

ثانيا: تعريف الإرهاب الإلكتروني:

لا يوجد تعريف مجمع عليه لمصطلح الإرهاب، وإلحاق مصطلح "ساير" بالإرهاب قد زاد من تشويش تعريف هذا الظاهرة رغم أن لهذا الإلحاق أثر طيب في بلورة أهمية الظاهرة الإرهابية، وتحويل النقاش إلى التعامل الفعال للمواجهة بما يتناسب مع تقنياتها الجديدة، وما يزيد من صعوبة إيجاد تعريف متفق عليه هو ازدواجية تصنيفه الفرعي، فهو ينطوي تحت التصنيف الفرعي لظاهرتين إجراميتين أحدهما هي الإرهاب، تلك الظاهرة قديمة والمعقدة، وثانيهما هي الجريمة الإلكترونية التي تتسم بالحدثية النسبية⁽³⁾.

لقد دأب الباحثون على تقسيم الإرهاب الإلكتروني إلى نوعين اثنين؛ الإرهاب الإلكتروني بمساعدة أجهزة الكمبيوتر أين يكون النشاط الإرهابي ذو هجمات مباشرة فعالة وخطيرة، وهو إرهاب تقليدي خالص، لكنه يستعين بتقنيات الكمبيوتر من أجل تسهيل تنفيذ الأعمال الإرهابية، وهذا النوع لا يعده بعض الباحثون إرهابا إلكترونيا، لأنه لا يشكل أي تهديد بأمن البيئة المعلوماتية، وهناك إرهابا إلكترونيا يطلق عليه الدارسون اسم الإرهاب السيبراني، ويتم فيه استخدام أجهزة الكمبيوتر لكن ليس من أجل ارتكاب أعمال إرهابية بصفة مباشرة، فهو إرهاب يستهدف أنظمة

(1) نورة سحري، صعوبات تعريف الإرهاب في القانون الدولي والتي تعيق مكافحته بفعالية، مجلة القانون، المجتمع والسلطة، المجلد 08، العدد 01، جامعة محمد بن أحمد، وهران 02، الجزائر، مارس 2019، ص ص: 175-193: <https://www.asjp.cerist.dz/en/article/82605>

(2) Gregor BRUCE, *Op.cit.*

(3) Jeffrey Thomas BILLER, *Cyber-Terrorism : (Finding a Common Starting Point)*, Journal Of Law, Technology & THE Internet, Vol.04, Iss.02. Case Western Reserve University, Cleveland, Ohio, 2013, pp.275-351: <https://scholarlycommons.law.case.edu/jolti/vol4/iss2/3/>

المعلومات والبنية التحتية التي ارتبطت نشأتها بعالم الحاسوب والفضاء السيبراني، وهو الذي يعدّه الباحثون إرهاباً إلكترونياً⁽¹⁾.

وقد ظهر مصطلح الإرهاب الإلكتروني في الثمانيات وكان باري كولين⁽²⁾ هو أول من استخدمه في دراساته التي صرح فيها بصعوبة وضع تعريف دقيق له⁽³⁾، وقد عرفه بأنه: (سوء الاستخدام القسري لنظام المعلومات الرقمي والشبكات أو مكوناتها لتحقيق هدف يدعم أو يشمل حملة إرهابية أو فعل إرهابي)⁽⁴⁾، كما عرفه أيضاً على أنه: (هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو إيديولوجية وأن الهجمة لا بد أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب)⁽⁵⁾.

ويعرفه نجيب بن عمر عوينات⁽⁶⁾ بأنه: (هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسب أو الشبكات أو المعلومات المخزنة إلكترونياً توجه من أجل الانتقام أو ابتزاز أو إجبار أو تأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة، ولكي يعتبر المرء إرهابياً على الإنترنت وليس فقط مخترقاً فإن الهجمات التي يشنها يجب أن تؤدي إلى عنف ضد الأشخاص أو الممتلكات أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب)⁽⁷⁾، وتم تعريفه أيضاً بأنه: (استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية)⁽⁸⁾.

(¹) Jonathan A. MATUSITZ, cyberterrorism : (A postmodern view of networks of terror and how computer law security exper and enforcement officials fight them), submitted to the graduate faculty in partial fulfillment of the requirements for the degree of Doctor of Philosophy university of Oklahoma, 2006, P.22.

(²) كريستوفر باري كولين (Christopher Barry COLLINS): عالم الكونيات الذي كتب العديد من الأوراق مع ستيفن هوكينج، وهو أستاذ فخري في الرياضيات التطبيقية في جامعة واترلو، حصل على الدكتوراه سنة 1972 من جامعة كامبريدج، ومن بين أعماله مع هوكينج: ورقة أعمال في استخدام مبدأ الأنثروبيا لتوفير حل مشكلة التسطّيح: نقلا عن: https://en.wikipedia.org/wiki/C._B._Collins

(³) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص 111.

(⁴) نجيب بن عمر عوينات، الإرهاب الإلكتروني: (المفهوم والجهود الدولية والإقليمية لمكافحته)، مجلة الأستاذ الباحث، المجلد 02 العدد 02، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، جوان 2017، ص ص 9-26: <https://www.asjp.cerist.dz/en/article/76780>

(⁵) سليمان الطعاني، الوجيز في التربية الإعلامية، الطبعة الأولى، دار الخليج للنشر والتوزيع، عمان، الأردن، 2020، ص 105.

(⁶) نجيب بن عمر بن عبد القادر عوينات (1979 تونس): أستاذ جامعي بكلية إدارة الأعمال بجامعة المجمعة بالملكة العربية السعودية، واشتغل أيضاً أستاذاً محاضراً بكلية الحقوق والعلوم السياسية بتونس، كما اشتغل أيضاً محاضراً مكلف بالدروس بالجامعة العربية للعلوم بتونس، كما تقلد مجموعة من المهام الإدارية أهمها: منسق بين فريق تدريس مادة العلاقات الدولية بكلية الحقوق والعلوم السياسية بتونس، وعضواً بالجمعية الدولية للقانون الدولي النووي، وعضو ومقرر باللجنة العلمية لقسم القانون بكلية العلوم القانونية والإنسانية بجامعة المجمعة، حصل على الدكتوراه من كلية الحقوق والعلوم السياسية بتونس في القانون العام التي كان عنوان أطروحتها: القانون الدولي النووي والطاقة الذرية، نقلا عن: <https://faculty.mu.edu.sa/naouinette/mycv>

(⁷) نجيب بن عمر عوينات، المرجع السابق.

(⁸) طوبي بحري ودلال بحري، آليات مواجهة الإرهاب الإلكتروني في ظل العولمة، مجلة البحوث والدراسات، المجلد 13، العدد 01، جامعة حمة لخضر، الوادي، الجزائر، سبتمبر 2017، ص ص: 187-208: <https://www.asjp.cerist.dz/en/article/25355>

وهناك من ذهب في تعريفه بأنه: (جريمة العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية سواء كان صادرا من الدولة أو الجماعات أو الأفراد على الإنسان بشكل عام وعلى سبيل المثال الأعمال غير المشروعة التي يكون فيها الكمبيوتر أو الهاتف إما وسيلة أو هدفا أو كليهما والتي من شأنها أن تؤدي إلى الأنشطة التخريبية أو التهديد بها في عالم الإنترنت مع نية تحقيق المزيد من الأهداف الدينية أو السياسية أو نحوها أو لتخويف أي شخص وبث الرعب في نفسه)⁽¹⁾.

وعرفه ذياب موسى البداينة⁽²⁾ بأنه: (أي فعل إرهابي باستخدام نظم المعلومات أو التقنية الرقمية ومعاداتها وبرامجها وناقلاتها وحواياتها وشبكاتها كأداة أو كهدف بدافع سياسية أو اجتماعية أو عقائدية)⁽³⁾.

ويعرف دوروثي ديننج (Dorothy Denning)⁽⁴⁾ الإرهاب السيبراني: (بأنه هجمات غير قانونية أو تهديدات بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها، عند القيام به لتخويف أو إكراه حكومة أو شعبها على تعزيز أهدافهم السياسية أو الاجتماعية)، فالإرهاب الإلكتروني وفق ديننج يجب أن يتكون من عناصر أساسية وهي؛ أن يكون هناك هجمات غير قانونية، أن تكون الهجمات والتهديدات واقعة على الفضاء الإلكتروني، وأن يكون الغرض من هذا النوع من الهجمات هو تخويف الحكومة أو المجتمع أو التأثير عليها لتحقيق

⁽¹⁾ سعيد عبيدي، الإرهاب الإلكتروني، مجلة العلوم الإنسانية، المجلد 01، العدد 02، المركز الجامعي علي كافي، تندوف، الجزائر، سبتمبر 2017، ص ص: 32-43: <https://www.asjp.cerist.dz/en/article/82865>

⁽²⁾ ذياب موسى البداينة (الأردن): مؤسس ورئيس مركز ابن خلدون للدراسات والأبحاث، ويحمل درجة دكتوراه في علم الاجتماع التطبيقي، تخرج في جامعة غرب ميشيجان في الولايات المتحدة الأمريكية سنة 1990، عمل في مجال التدريس والبحث العلمي والشاركة المجتمعية، وأسس مختبرا حاسوبيا تعليميا في قسم علم الاجتماع بجامعة مؤته، وشارك في تطوير الخطط الدراسية بجامعة نايف العربية للعلوم الأمنية والجامعات الأردنية، والمؤسسات الأمنية، نشر العديد من الكتب أهمها: (Understanding terrorism, APA Publication maual)، نقلا عن موقع مركز ابن خلدون للدراسات والأبحاث، مختصر الرابط: <https://cutt.us/C3oib>

⁽³⁾ ذياب موسى البداينة، الإرهاب المعلوماتي: (التعريف-المفهوم-المجالات-النتائج)، الحلقة العلمية: الإنترنت والإرهاب، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، القاهرة، 2008، ص ص: 3-31.

⁽⁴⁾ دوروثي إليزابيث ديننج (Dorothy Elizabeth Denning) 1945: باحثة أمريكية في مجال أمن المعلومات وهي معرفة بنظام التحكم في الوصول إلى الشبكة، وأنظمة كشف التسلل وغيرها من الابتكارات في مجال الأمن السيبراني، حصلت على الماجستير سنة 1969 في جامعة ميشيجان، وحصلت على الدكتوراه حول تدفق المعلومات والأمن في أنظمة الكمبيوتر سنة 1975، بدأت حياتها كأستاذ مساعد في جامعة بورديو، ثم مهندسة برمجيات رئيسية في مركز بالو ألتو لأبحاث الأنظمة في شركة المعدات الرقمية، ثم عادت إلى الجانب الأكاديمي كرئيسة قسم علوم الكمبيوتر في جامعة جورج تاون، ثم أستاذة في قسم تحليل الدفاع في كلية الدراسات البحرية بكاليفورنيا، نشرت أربع كتب وأكثر من 200 مقال، وهي الآن أستاذة فخريّة في كلية الدراسات البحرية العليا بعد تقاعدها: ومن أهم مؤلفاتها: (Cryptography and data security, information warfare and security)، نقلا عن: https://en.wikipedia.org/wiki/Dorothy_E._Denning

أهدافها السياسية أو الاجتماعية، وأن تؤدي الهجمات إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تسبب ضرراً كافياً لإثارة الخوف⁽¹⁾.

أما جيمس لويس (James Lewis) فيعرف الإرهاب الإلكتروني على أنه: (استخدام أدوات شبكة الكمبيوتر لغلق البنى التحتية الوطنية الحرجة مثل الطاقة، النقل، المعاملات الحكومي، أو لإكراه أو تخويف الحكومة أو السكان المدنيين)⁽²⁾.

وقدم أيضاً مكتب هيئة الأمم المتحدة تعريفاً للإرهاب السيبراني يعرفه بأنه: (استغلال الشبكات الحاسوبية عن عمد باعتبارها وسيلة لشن هجوم، وتهدف هذه الهجمات عادة إلى تعطيل النظم التي تستهدفها، وتتضمن تلك الأهداف نظم الحاسب، والخوادم وبنيتها التحتية الأساسية، وذلك عبر استخدام الاختراق الحاسوبي، أو التقنيات المتقدمة للتهديد المستمر، أو فيروسات الحاسوب أو البرمجيات الضارة أو الإغراق أو غيرها من وسائل الدخول غير المصرح به أو ذي الأهداف الضارة وقد تحتل الهجمات السيبرانية سمات عمل إرهابي بما في ذلك الرغبة في زرع الخوف دعماً لأهداف سياسية أو اجتماعية)⁽³⁾.

يمكن تعريفه أيضاً بأنه: (الاستخدام غير القانوني أو التهديد باستخدام القوة أو العنف من قبل شخص أو مجموعة منظمة ضد الأشخاص أو الممتلكات مع نية تخويف أو إجبار المجتمعات أو الحكومات، غالباً لأسباب أيديولوجية أو سياسية)⁽⁴⁾.

قام المركز الوطني الأمريكي لحماية البنية التحتية بتعريف الإرهاب السيبراني على أنه عمل إجرامي يتم اللجوء إليه من أجل محاولة خلق نوع من الرهبة والخوف والذعر من خلال توظيف أجهزة الحاسب الآلي وذلك كله من أجل إجبار الحكومة على تغيير سياساتها⁽⁵⁾.

⁽¹⁾ Zahri Yunos, Rabiah Ahmad and Noor Azwa Azreen Abd Aziz, *The Concept of Cyber Terrorism, SEARCCCT'S sélection of articles*, volume 01, Southeast Asia Regional Centre for Counter-Terrorism, ministry of foreign affairs, Malaysia, 2013, PP. 68-79.

⁽²⁾ Zahri Yunos, Rabiah Ahmad and Noor Azwa Azreen Abd Aziz, *Ibid.*

⁽³⁾ الأمم المتحدة، استخدام الإنترنت لأغراض إرهابية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، نيويورك 2013، ص 12:

http://www.unodc.org/documents/terrorism/Publications/The_Use_of_Internet_for_Terrorist_Purposes/Use_of_the_Internet_for_Terrorist_Purposes_Arabic.pdf

⁽⁴⁾ Mitko BOGDANOSKI, Drage PETRESKI, *Cyber terrorism—global security threat*, *Contemporary Macedonian Defense-International Scientific Defense, Security and Peace Journal*, vol. 13, no 24, 2013, PP. 59-73: <https://core.ac.uk/download/pdf/35330211.pdf>

⁽⁵⁾ Bernadette SCHELL, Clemens MARTIN, *Webster's New World Hacker Dictionary*, 1st edition, Wiley Publishing, Inc, USA, 2006, P..87.

وقد قدم أيضا مارك بوليت، الوكيل الخاص لمكتب التحقيقات الفيدرالي تعريفا عمليا حين صال بأن الإرهاب الإلكتروني هو: (الهجوم المتعمد ذي الدوافع السياسية ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلى عنف ضد أهداف غير قتالية من قبل مجموعات وطنية فرعية أو وكلاء سريون)⁽¹⁾.

وعلى ضوء ما سبق من تعريفات للإرهاب الإلكتروني يمكن أن نلاحظ أن أغلبها يرى أن جريمة الإرهاب الإلكتروني لا تختلف في جوهرها عن الإرهاب التقليدي من ناحية القصد الإجرامي للجاني، إنما الفارق بينهما هو في الآلية التي يتم توظيفها لذلك⁽²⁾، فقد ركزت أغلب التعاريف على أوجه الشبه بين الإرهاب التقليدي والإرهاب الإلكتروني، كما أن أغلب التعاريف قد انصرفت عما قد يكون له أثر سلبي على التطور التكنولوجي وطبيعة المنافسة بين المؤسسات المنتجة للنظم والتقنيات، كما نلاحظ أيضا تركيز بعض التعاريف على نظم الحواسيب أو وسائل الاتصال كآلية للهجوم كما ركزت عليها أيضا كهدف للعمليات الإرهابية، وتتفق معظم التعاريف على الهدف السياسي الذي يقف وراء تلك الهجمات⁽³⁾.

ونلاحظ في التعريف الذي قدمه مارك بوليت أنه قد عزل العديد من السلوكيات والنشاطات التي لا ترتبط بظاهرة الإرهاب الإلكتروني، فمصطلح الإرهاب الإلكتروني يجب أن يتمتع بالخصوصية والمعنى والجوهر الذي يمكن أن يتميز به عن غيره من التصرفات والنشاطات الأخرى الواقعة على الفضاء الإلكتروني، وذلك من خلال تحديد البعد السياسي⁽⁴⁾، فتطرق التعريف إلى البعد السياسي من شأنه أن يعزل بين الإرهاب الإلكتروني كظاهرة مستقلة ويفردها عن صور أخرى من الجرائم الواقعة على الفضاء الإلكتروني.

وتظهر لنا أهمية تعريف مارك بوليت من خلال المشاكل التي لاقاها ريتشارد كلارك رئيس الأمن السيبراني السابق في البيت الأبيض في توظيف مصطلح الإرهاب الإلكتروني، إذ يرى أنه

(¹) Serge KRASAVIN, What is Cyber-terrorism, Computer Crime Research Center, accessed in 05/02/2021, at 10:55, in:

<https://www.crime-research.org/library/Cyber-terrorism.htm#:~:text=In%20the%20same%20year%20Mark,national%20groups%20or%20clandestine%20agents.%22>

(²) إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني: (دراسة مقارنة)، مذكرة ماجستير في القانون العام، كلية الحقوق، جامعة النهرين، العراق، 2012، ص 24.

(³) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، ص 111 وما بعدها.

(⁴) Sam BERNER, Cyber-terrorism: reality or paranoia, South African Journal of Information Management, Volume 5, No.01, African Online Scientific Information Systems (Pty) Ltd t/a AOSIS, South Africa, 2003: <https://sajim.co.za/index.php/sajim/search/search?simpleQuery=Cyber-terrorism%3A+reality+or+paranoia&searchField=query#>

من غير الممكن في هذه المرحلة وصف جميع المجرمين الذين ينشطون على ساحة الفضاء الإلكتروني بأنهم إرهابيون، لأن بنية الفضاء الإلكتروني فيها من الثغرات الأمنية ما يجعلها توظف من قبل الكثير من الفئات، كما يرى أيضا بأن استغلال الفضاء الإلكتروني لأغراض الإرهاب التقليدي لا يمكن اعتباره من قبيل الإرهاب الإلكتروني، فالإرهاب عند ريتشارد كلارك هو ما ينجم عنه وفيات⁽¹⁾.

والظاهر لنا أن ريتشارد كلارك ينظر إلى الإرهاب الإلكتروني من منظور الهجوم على البنى التحتية الحرجة، وما ينجر عنها من وفيات حال السيطرة عنها، ومع ذلك نرى أنه جانب الصواب فيما ذهب إليه، فحتى الإرهاب التقليدي لا يشترط فيه وجود وفيات، يكفي قدر معين من الإضرار وقصد جنائي خاص لنكون أمام ظاهرة إرهابية.

كما أن الظاهر من أغلبية التعاريف أنها تركز بشكل أساسي في تعريفها للإرهاب الإلكتروني على الهجمات أو التهديدات التي يكون من شأنها أن تستهدف الفضاء الإلكتروني بجميع عناصره، أو البنية التحتية الحرجة، وتستبعد في غالبيتها توظيف الفضاء الإلكتروني كآلية لأغراض الإرهاب التقليدي من دائرة الإرهاب الإلكتروني، فالإرهاب الإلكتروني على رأي غالبية الباحثين هو ذاك الذي يستهدف الفضاء الإلكتروني بطبقته المادية والمعنوية، غير أننا نرى أن ندرج في دراستنا هذه التوظيف الإرهابي للفضاء الإلكتروني ضمن دائرة الإرهاب الإلكتروني الهجين، ولذلك نرى أن الإرهاب الإلكتروني بشكل عام هو:

" الاستغلال غير المشروع للثغرات الأمنية في نظم تشغيل أجهزة الكمبيوتر وآلات الاتصال والشبكات المتصلة المغلقة أو المفتوحة، أو بتنفيذ هجوم مادي، من أجل القيام بأعمال موصوفة بالخطورة والضرر على نفس تلك الأجهزة أو الآلات أو الشبكات وملحقاتها، والبنى التحتية الحرجة المتعلقة بها، أو عن طريق توظيفها لدعم الأعمال الموصوفة بالإرهاب، بهدف ممارسة الضغط عن طريق إثارة الذعر والرعب بدافع سياسي أو إيديولوجي أو بدافع الانتقام من شخص طبيعي كان أو معنوي "

الفرع الثاني: تمييز الإرهاب الإلكتروني عن غيره من المفاهيم:

إن التوصيات الدولية في إطار مكافحة الإرهاب تشدد على ضرورة احترام مبادئ حقوق الإنسان واحترام حق الشعوب الواقعة تحت سيطرة الاستعمار في الدفاع عن نفسها وتقرير مصيرها (أولا)، وتدعو إلى محاكمة المتورطين في الأعمال الإرهابية وفقا لمبادئ العدالة التي يجب أن

(1) Bernadette SCHELL, Clemens MARTIN, Op.cit. P..87.

تتناسب فيه العقوبة مع طبيعة الجرم (ثانياً)، بالإضافة أن تحول الفضاء الإلكتروني كساحة حرب معلوماتية أوجب الفصل بين الإرهاب الإلكتروني وبقية المفاهيم (ثالثاً).

أولاً: تمييز الإرهاب الإلكتروني عن المقاومة الإلكترونية:

إن مقاومة العدو الغاصب يعتبر حق طبيعي مشروع، معترف به في كل القوانين والأعراف الدولية، ومشروعيته تقوم على أكثر الأسس القانونية الدولية قداسة واعتباراً، إذ يستند فيها على الحق في الدفاع الشرعي، والحق في تقرير المصير، كما يستند أيضاً على الاعتبارات الضامنة لاحترام حقوق الإنسان⁽¹⁾.

فالقانون الدولي قد منح بما لا يدع مجالا للشك الشرعية الكاملة للدفاع عن النفس بما يتناسب مع طبيعة العدوان، إذ نص ميثاق الأمم المتحدة على ما يلي: (ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فردى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة)⁽²⁾، كما تنص أيضاً المادة الثانية من قرار الجمعية العامة رقم 1514 عن أحقية الشعوب في تقرير مصيرها وتحديد مركزها السياسي، كما نصت المادة الأولى منه على إدانة واضحة للاستعباد الأجنبي واعتبرته إنكاراً لحقوق الإنسان⁽³⁾.

ويتسع مفهوم المقاومة إلى أن يشمل العديد من العناصر الأخرى التي لا علاقة لها بالاحتلال، فقد شمل المقاومة أيضاً الحركات الاحتجاجية التي تسعى إلى تغيير واقع غير مرغوب فيه، أو تسعى في مواجهة صور الاستبداد السلطوي والظلم والإجحاف والتمييز الواقع عليها⁽⁴⁾، فليس الاحتلال شرطاً لقيام المقاومة بل يمكن أن تقوم في الوطن الواحد دفعا للظلم أو نصرة للحق.

لقد أدى التطور التكنولوجي الكبير وظهور الساحة المعلوماتية إلى بروز المقاومة الإلكترونية التي يصفها المحققون بأنها "حرب بلا نار، وقصف بلا أنقاض، وغزو بلا جيوش، إنها مقاومة لا تحاصرها حدود السيادة، وتتنوع فيها الأساليب الهجومية، مقاومة يشارك فيها كل أطراف المجتمع، فلا عبرة للجنس ولا للعمر فيه"⁽⁵⁾، وقد قال عنها ماجد أبو مراد⁽⁶⁾: (إنني أرى أن الحرب

(1) صباح نوري علوان العجيلي، استراتيجية حروب التحرير، الطبعة الأولى، مركز الكتاب الأكاديمي، الأردن، 2015، الصفحة 109.

(2) أنظر المادة 51 من ميثاق الأمم المتحدة لعام 1945.

(3) قرار الجمعية العامة رقم 1514، الدورة 15، المتضمن إعلان منح الاستقلال للبلدان والشعوب المستعمرة الصادر بتاريخ 20 ديسمبر 1960.

(4) يوسف الحسن، ثقافة المقاومة، 14 فبراير 2017، تم الاطلاع عليه بتاريخ 12 نوفمبر 2019 على الساعة 17:12، في الموقع:

<https://www.alittihad.ae/article/9523/2017/ثقافة-المقاومة>

(5) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص 132.

(6) كاتب وإعلامي فلسطيني.

الإلكترونية هي سبيل وطريق من طرق الجهاد الحديث⁽¹⁾، وأشار إليها أيضا نعيم مرار⁽²⁾ بقوله: (ومن المفروض أن تزيدنا تكنولوجيا المعلومات عبر الفايبروك وغيره قوة على مقاومة الاحتلال)⁽³⁾، وتتخذ هذه المقاومة نمطين اثنين في آليات كفاحها وهما:

1- نمط المقاومة السلمية:

إنه النمط الذي يهدف إلى التأثير على الرأي العام عبر جعل الساحة الإلكترونية كمسرح إعلامي للمقاومة، وهذا عن طريق استخدام الخدمات التي تتيحها شبكات الإنترنت في إطار حرية الرأي والتعبير، ومن أهم نشاطات المقاومة على الساحة السيبرانية نجد جمع التوقعات على عريضة إلكترونية، واستطلاع الرأي الإلكتروني الذي يبلور مواقف المشاركين حول الموضوع المتنازع فيه، وكذلك استعمال موقع التواصل الاجتماعي والمنديات وغرف الدردشة كمنصة لتأييد القضية وكسب المؤيدين، وإلى غير ذلك من آليات المقاومة السلمية⁽⁴⁾.

كما يمكن أيضا اعتبار العصيان المدني الإلكتروني بمفهومه اللين كشكل من أشكال المقاومة الإلكترونية السلمية، فهو يماثل تماما ما يحدث في الشارع غير أنه بعيد كل البعد عن إحداث خسائر مادية، فآلياته هي نفسها التي توفرها الخدمات العامة للشبكة العنكبوتية، والتي يتم توظيفها على نحو إعلامي بغية التأثير على الرأي العام⁽⁵⁾.

والعصيان المدني الإلكتروني يمكن تعريفه على أنه: (...شكل من أشكال الضغط على المؤسسات الحكومية أو الرسمية المنخرطة في أعمال غير أخلاقية أو غير قانونية أو تضر بالإنسانية أو بأخرى حيث يمكن من خلال بيئة الكترونية تدويل وحشد وتنظيم وتأييد الرأي العام العالمي...) ⁽⁶⁾.

فالعصيان المدني الإلكتروني فضلا عن كونه يهدف إلى التأثير على الرأي العام، يعمل أيضا على تقديم الدعم الكبير والمهم للاحتجاجات البدنية في الشوارع، إذ كان وراء نجاح الكثير

(1) نقلا عن: راني محمد خريس، الخطاب الصحفي الفلسطيني تجاه المقاومة الفلسطينية، الطبعة الأولى، مركز الزيتونة للدراسات والاستشارات، بيروت، لبنان، 2016، لبنان الصفحة 18.

(2) منسق هيئة المتابعة للمقاومة الشعبية

(3) نقلا عن: راني محمد خريس، المرجع نفسه، ص 25.

(4) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، 138 وما بعدها.

(5) صلاح محمد عبد الحميد ويمنة عاطف، الإعلام والفضاء الإلكتروني، الطبعة الأولى، أطلس للنشر والإنتاج الإعلامي، الجيزة، 2015، ص 50.

(6) علي جاسم محمد التميمي، الإرهاب الإلكتروني وأثره على المجتمع، المجلة السياسية والدولية، مجلد 2016، العدد 33-34، كلية العلوم

السياسية، الجامعة المستنصرية، العراق، 2016، ص ص: 89-106:

<https://www.iasj.net/iasj/article/117300>

من الاحتجاجات في العالم، خاصة تلك التي شهدتها الوطن وعلى رأسها انتفاضة 25 يناير 2011 بجمهورية مصر العربية، وانتفاضات أخرى في الوطن العربي⁽¹⁾.

بل إن من الباحثين أمثال علي حرب يعتبر ثورات الوطن العربي ، ثورات رقمية شبانية ناعمة، تختلف تماما عن الثورات السابقة التي كانت الإيديولوجيات العلمانية والاتجاهات الدينية والنخب هي من تسيرها، فهذه الثورات هي من رحم القوة الإلكترونية الناعمة التي أتاحها هذا العصر⁽²⁾، وعبر عن هذه الساحة الثورية التي ثار فيها هؤلاء الفاعلين الجدد بـ " الميادين الافتراضية"⁽³⁾.

2- نمط المقاومة العنيفة:

قد تستبدل المقاومة الإلكترونية نهج السلمية والحوار بالنهج الاحتجاجي العنيف، مستخدمة آليات هجومية تدميرية عن طريق اللجوء إلى استعمال القرصنة والاختراق، بغية شل المواقع أو إيقافها بصورة نهائية، وعادة ما تكون تلك الهجمات عن طريق إرسال رسائل إلكترونية في نفس الوقت وبأعداد كبيرة، مما يسبب ضغطا على المواقع فتشل حركتها، وفي بعض الأحيان تكون تلك الرسائل مصحوبة بفيروسات وديدان الإلكترونية، تحدث أثارا تخريبية في الأنظمة، وتفتح ثغرات أمنية يمكن السلوك من خلالها الاستلاء وسرقة المعلومات المخزنة في المواقع والأجهزة، كما يعمل بعض شباب المقاومة على نشر رسائل احتجاجية بطريقة مكثفة ومزعجة، يعرضون فيها ما يحدث على أرض الواقع من انتهاكات لحقوق الإنسان تعجز على معرفتها وسائل الإعلام التقليدية⁽⁴⁾.

أما الإرهاب الإلكتروني فهو من بين تجليات الحرب الإلكترونية وصورة من صورها، فهو ينطلق من الأسس والتصورات الإيديولوجية التي تتبناها الجماعة وتؤمن بها، وهدفه واضح ومحدد ويتمثل في تجسيد التصورات الإيديولوجية للجماعة الإرهابية وإدراجها في صيغتها المادية،

⁽¹⁾ دعت القوى السياسية في تونس إلى العصيان المدني ضد الرئيس الأسبق زين العابدين بن علي من خلال منصات مواقع التواصل الاجتماعي الأمر الذي ترتب عنه استقالة الرئيس وسفره خارج البلاد، وكذلك فعل شباب الحراك في الجزائر الراضين لترشح الرئيس السابق عبد العزيز بوتفليقة لعهدة خامسة، وكانت وسائل التواصل الاجتماعي كلها منبرا إعلاميا للشباب الجزائري المعارض الذي دعي إلى عصيان مدني فعلي، والذي تمت الاستجابة له على نطاق واسع في أغلب الولايات مما أجبر الرئيس على تقديم استقالته إلى المجلس الدستوري الذي أعلن حالة الشغور ليتولى بعدها رئيس مجلس الأمة عبد القادر بن صالح تسير شؤون البلاد وفقا لما تنص عليه المواد الدستورية، واستمرت المقاومة الإلكترونية لهذا الوضع خاصة عند تجاوز رئيس مجلس الأمة للمدة المنصوص عليها في الدستور والمقدرة بـ 90 يوما، ورفعت عبر منصات التواصل الاجتماعي أصوات داعية لمقاطعة الانتخابات التي يشرف عليها رموز النظام المنحل.

⁽²⁾ أنظر: علي حرب، ثورات القوة الناعمة في العالم العربي: (من المنظومة إلى الشبكة)، الطبعة الثانية، الدار العربية للعلوم ناشرون، لبنان، 2012، ص 72.

⁽³⁾ المرجع نفسه، ص 69.

⁽⁴⁾ عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص ص: 145-146.

والجماعات الإرهابية تدرك بيقين تام أهمية الفضاء الإلكتروني في توسيع نطاق نشاطها وتحسين نوعية هجماتها، ولذلك فهي تسعى باستمرار إلى تحسين أدائها الفني فيه، وتكثيف تواجدها في ثغوره، فهي إذا جعلت من الفضاء الإلكتروني مسرح حرب تستغله لتكثيف هجماتها عن طريق تسخير آلياته كممبر إعلامي قادر على تكوين وجهات نظر عالمية تؤثر بشكل كبير عن الرأي العام الدولي من جهة وتضاهي به وسائل الإعلام التقليدية من جهة أخرى، وتشكل به قاعدة شعبية مؤيدة، يمكن تجنيدها في ما بعد، كما تقوم بعمليات هجومية تستهدف بها المواقع المعادية لصياغاتها الفكرية وقراءاته السياسية ومعتقداتها المذهبية، كما تستغلها أيضا في تنمية خبرتها ووضع استراتيجياتها والتواصل بين أفرادها⁽¹⁾.

فالفارق بين الإرهاب والمقاومة ينكشف بوضوح من خلال النظر إلى القصد الذي تسعى إلى تحقيقه، فالمقاومة تهدف في جوهرها إلى إزاحة اعتداء صدر عن محتل أو عن سلطة مستبدة، وغالبا ما يكون في إطار داخلي ولا يكتسب صفة العالمية، بينما الإرهاب ذو طابع دولي، ومقاصدها مستوحاة من إيديولوجيات متطرفة، وهجماتها ليست ذات أهداف نهائية بل هي وسيلة للتأثير السياسي وقلب موازين القوى⁽²⁾.

وفي الأخير تجدر الإشارة إلى أنه رغم المواثيق الدولية حوال مسألة شرعية كفاح الشعوب المستعمرة ومشروعية العمل من أجل تحقيق التحرر والاستقلال من قبضة الاحتلال وتقرير مبدأ تقرير المصير إلا أن هناك خلافا شديدا واقعا بين دول العالم الثالث التي تشكل الدول العربية جزء منها وبين العالم الغربي حول مسألة الكفاح المسلح من أجل تحقيق الاستقلال والحرية وتقرير المصير إذ يرى جانب كبير من فقهاء الغرب ودولهم ولاسيما الولايات المتحدة الأمريكية وكندا وإيطاليا وهولندا أن الكفاح لا بد أن ينتهج النهج السلمي فيما ترى دول العالم الثالث أن كفاحها ضد الاحتلال يعتبر مشروعا بكافة التدابير التي تراها ملائمة لدفع الظلم والقهر بما في ذلك الكفاح المسلح، وعلى هذا الأساس فإن الدول الغربية نظر الذين ينتهجون النهج المسلح في الكفاح والمقاومة بأنهم إرهابيون فضلا عن العزوف عن تظمين معاهداتها ومؤتمراتها المتعلقة بمكافحة الإرهاب ما يضيفي الشرعية عن الكفاح لتحقيق التحرر وتقرير المصير، في حين نجد الدول العربية على سبيل المثال تأكد على ضوء سبل مكافحة الإرهاب عن حق الشعوب في تقرير مصيرها والكفاح ضد المستعمر الغازي وصور العدوان بما أتيح من آليات ووسائل وهذا ما عبرت

(1) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص: 145-146.

(2) حسين العزاوي، موقف القانون الدولي من الإرهاب والمقاومة المسلحة، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2013، ص 122.

عنه الاتفاقية العربية لمكافحة الإرهاب الصادرة عن مجلسي وزراء الداخلية والعدل العرب في أبريل 1998⁽¹⁾، وهذا الخلاف ينطبق أيضا على مكافحة الإلكترونيات⁽²⁾.

ثانيا: التمييز بين الإرهاب الإلكتروني وحرب المعلومات:

يمكن تعريف حرب المعلومات على أنها: (استخدام نظم المعلومات لاستغلال وتخريب وتدمير وتعطيل معلومات الخصم، وعملياته مبنية على المعلومات ونظم معلوماتها وشبكة الحاسب الآلي الخاصة بها، وكذلك الحماية من خطر الهجوم من قبل الخصم لإحراز السبق والتقدم على نظمه العسكرية والاقتصادية)⁽³⁾، ومن خلال هذا التعريف يمكن أن نفرق بين نوعين من الحرب المعلوماتية:

1- حرب معلوماتية هجومية:

هو القيام بتنفيذ هجمات معلوماتية معينة على معلومات ونظم معلومات طرف آخر بهدف تحقيق مكاسب استراتيجية سواء أكانت عسكرية أو استخباراتية أو اقتصادية، أو بهدف تعطيل المعلومات وتدميرها أو تشويهاها وتزييفها، وتصدر عادة من الدول والجهات التنافسية كالشركات الكبرى، وقد يقوم بها أفراد بغية الحصول على معلومات ذات قيمة تصلح كمحل للبيع، وقد يقدم عليها الهاكرز بدافع المتعة⁽⁴⁾.

2- حرب معلوماتية دفاعية:

هي حرب من شأنها أن تعمل على الحد والتقليل من المخاطر ومن وطأة الأعمال التخريبية الهجومية عن طريق انتهاز نهج الوقاية بالأساليب التقنية والفنية لضمان أمن المعلومات، وبالاعتماد على الرصد والتنبه حال وجود هجمات معلوماتية، كما يدخل ضمن نطاق عملها

(1) محمد محي الدين عوض، واقع الإرهاب واتجاهاته، أعمال ندوة مكافحة الإرهاب، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 1999، ص ص: 29-30.

(2) فهي ليست في منأ عن هذا الخلاف المحتدم، فرغم أن الغرب قد يقبل على مضض فكرة وجود مقاومة على الفضاء الإلكتروني، إلا أنه في المقابل قد يضع لها صورة نمطية سيعمل على تيسير تداولها، وسيعمل على ترسيخها لتكوين قناعة عالمية تجعل من المقاومة الإلكترونية التي قد تخذل مصالحهم شكلا من أشكال الإرهاب الذي تفرض الأعراف والقوانين الدولية مكافحته، فالخلاف على شرعية المقاومة الإلكترونية لن يكون أقل حدة عن الخلاف الذي يسود المقاومة المسلحة، ولن ينصب هذا الخلاف أبدا في صالح تحقيق العدالة ومقتضيات حماية الإنسان وحقوقه من الانتهاك بقدر ما ينصب في صالح قوى القهر والاستعمار كما أنه لن يحقق إلا مزيدا من الحروب والاضطرابات الدولية بدعوى مكافحة الإرهاب وتحقيق السلم والأمن الدوليين.

(3) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص 133.

(4) قاطفي حكيم، حرب المعلومات: (المفهوم والتطبيق)، مذكرة ماجستير في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر، السنة الجامعية 2005-2006، ص ص: 69-71.

ضمان إعادة نظم المعلومات إلى حالتها التي كانت عليها قبل الهجوم ومحاولة جمع الأدلة الرقمية التي تكشف عن مرتكبها لمتابعته أمام الجهات القضائية المختصة⁽¹⁾.

يرى بعض الباحثين أن ما من فارق حاصل بين الإرهاب الإلكتروني وحرب المعلومات⁽²⁾، فثمة علاقة وطيدة بين الإرهاب الإلكتروني وحرب المعلومات، ولكن ومع ذلك فإن هنا فارق بينهما، وهذا الفرق لا يمكن أن نميزه إلا وفق نظرية الغائية، فالإرهاب الإلكتروني يحوم حول مفهوم حرب المعلومات، إذ أن الإرهابي في حربه الإلكترونية يستعين بها لتحقيق أهدافه، والحرب المعلوماتية قد تتحول إلى إرهابي إلكتروني تأخذ تكييفها القانوني، وهذا إما لكونها أداة في تستعملها الجماعات الإرهابية، وإما لكون وسائلها وأهدافها هي نفس تلك الأهداف والوسائل التي تتبناها الجماعات المتطرفة⁽³⁾، وهذه التداخل من شأنه أن يحدث نوعا من الاعتبارية في التمييز بينهما مما ينعكس سلبا على التكييف القانوني لهما.

ثالثا: التمييز بين الإرهاب الإلكتروني والجريمة الإلكترونية:

لقد اقترح الأستاذ عبد الله دغش العجمي تعريفا شاملا لظاهرة الجريمة الإلكترونية، فعرفها على أنها: " كل فعل أو امتناع يتم إعداده أو التخطيط له ويتم بموجبه استخدام أي نوع من الحاسب الآلي، سواء حاسب شخصي أو شبكات الحاسب الآلي أو الإنترنت أو وسائل التواصل الاجتماعي لتسهيل ارتكاب جريمة أو عمل مخالف للقانون أو تلك التي تقع على الشبكات نفسها عن طريق اختراقها بقصد تخزين أو تعطيل أو تحريف أو محو البيانات أو البرامج التي تحويها"⁽⁴⁾.

من خلال هذا التعريف للجريمة الإلكترونية يظهر جليا سبب إشكال بعض الناس في التمييز بين الاستخدام الإجرامي للفضاء السيبراني وبين الإرهاب الذي يوظف الفضاء السيبراني كأداة إرهابية، والسبب هو اشتراكهما في الوسيلة ونطاق التوظيف الإجرامي، لكن للتمييز بينهما لا بد إلى النظر إلى الغاية التي تحرك كل منهما، فالإرهاب الإلكتروني له أهداف سياسية يسعى إلى تحقيقها باللجوء إلى الساحة الإلكترونية، بينما الجريمة الإلكترونية لا ترتقي إلى هذا المستوى في قصدها

(1) قاطفي حكيم، المرجع السابق، ص ص: 72-73.

(2) زروال معزوزة، بلغازي نور الدين، الإرهاب الإلكتروني للأمن المعلوماتي، المصنف الجماعي: (الجريمة المعلوماتية وأثرها على التنمية الاقتصادية)، الجزء الأول، الطبعة الأولى، المركز الديمقراطي العربي، ألمانيا، جويلية 2020، ص ص: 304-324.

(3) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق ص ص: 137-138.

(4) عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية: (دراسة مقارنة)، مذكرة ماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص 14.

الإجرامي، فمفهوم الإرهاب الإلكتروني وإن كان يتضمن جرائم إلكترونية كالتجسس والاختراق والقرصنة والتشهير والتحريض عبر المواقع الإلكترونية وانتحال الشخصية وانتهاك الخصوصية وتهديد التجارة الإلكترونية والتعدي على التعاملات المالية والمصرفية ولكن هذا يتضمن مقتصر فقط على التوظيف ولا يتعداه إلى الغاية⁽¹⁾، فكل الأعمال الإرهابية الإلكترونية هي من ضمن الجرائم الإلكترونية ولكن العكس غير صحيح⁽²⁾.

الفرع الثالث: خصائص الإرهاب الإلكتروني:

تعتبر جريمة الإرهاب الإلكتروني من أحدث التهديدات الأمنية التي تهدد المجتمع الدولي، فطبيعتها الفريدة من نوعها تضيف عليها نوعا من التميز والتعقيد (أولا)، كما أن الطفرة الإلكترونية الكبير في العصر الحديث والاعتماد المتزايد عليها في إنشاء وإدارة البنى التحتية الحرجة قد منح للهجمات الإرهابية أهدافا استراتيجية مهمة وآليات إبداعية متجددة، الأمر الذي عزز التوجه إليها كبديل عن الإرهاب التقليدي لما بينهما من فوارق تكتيكية جمة (ثانيا)، فأصبحت البيئة المعلوماتية والبنى المرتبطة بها تواجه أصنافا مميزة من التهديدات غير المتوقعة ذات الأثر التدميري الكبير (ثالثا).

أولا: الخصائص المتعلقة بطبيعة الجريمة:

1- جريمة الإرهاب الإلكتروني جريمة خفية:

يعتبر الخفاء من أهم السمات البارزة التي تميز الإرهاب الإلكتروني عن الإرهاب التقليدي، ففي الحين الذين يمكن الكشف فيه عن جرائم الإرهاب التقليدي، وتحديد الجهات المتورطة فيه وبيان أهدافها منه، فإن الإرهاب الإلكتروني يفتقر إلى الآليات التي ترفع بها اللبس عن طبيعة الجريمة، فالهجمات الإلكترونية ذات الأثر التخريبي يمكن أن يتورط فيه أشخاص لا علاقة لهم بالأهداف والغايات الإرهابية، وعلى رأسهم نجد الباحثون عن الشهرة الذين تستهويهم عمليات الاختراق والقرصنة، وبعض الدول ذات الاتجاه القومي التي تنفذ هجمات إلكترونية بأساليب وآليات متعددة في إطار صراعها من أجندة أخرى، هذا، كما يمكن أن تكون تلك الهجمات داخلة ضمن أساليب المقاومة الإلكترونية المشروعة وشكلا من أشكال الاحتجاج⁽³⁾، ويمكن حصر محاور الخفاء الذي تتميز به جريمة الإرهاب الإلكتروني في العناصر التالية:

(1) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص 131 ما يليها.

(2) حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، الجزء الثاني، أطروحة دكتوراه في العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، السنة الجامعية 2013-2014، ص 793.

(3) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص 122.

أ- خفاء هوية الجناة:

إن التعرف على الجناة بذواتهم يعتبر ذو أهمية كبيرة وأبعاد عميقة تنصب كلها في تحقيق مقتضيات العدالة الجنائية، فالتعرف على الجناة بالوسائل القانونية المشروعة يعتبر إجراء أوليا وعنصرا جوهريا لتحقيق العدالة، وضمان حق العقاب الذي ينزله المجتمع بهم عبر ممثلهم أمام القضاء، ومن غير ذلك فإن العدالة تكون عاجزة ومعطلة، والجناة أحرارا طلقاء⁽¹⁾.

ويعتبر المسؤولون في الأعمال الإرهابية من بين أكثر الجناة فرارا من العدالة، وهذا لصعوبة وتعقيد عملية التعرف عليهم، فرغم أن هناك الكثير من الأعمال الإرهابية التي تعلن جهات معينة مسؤوليتها عن تنفيذها إلا أن هذا لا يشكل آلية للتعرف عليهم بذواتهم مما يبقي العدالة معلقة، وحق الأفراد في التعويض عن الخسائر والضحايا وتطبيب خاطر ضائعا⁽²⁾.

ويضيع أيضا معه حق المجتمع في العقاب الممنوح للسلطة بموجب العقد الاجتماعي، وإذا كان التعرف على هوية الجناة في الأعمال الإرهابية التقليدية أمرا يتسم بكل هذه الصعوبة والبطء والتعقيد فإن الجناة في الأعمال الإرهابية الإلكترونية يعتبر أكثر تعقيدا، نظر لكون المجهولية السمة البارزة في ملايين المتعاملين والمستخدمين للشبكات الإلكترونية⁽³⁾.

فالفضاء الإلكتروني يوفر بما له من خصائص متعددة نوعا من الحماية للإرهابيين، وذلك من خلال إخفاء هويتهم الحقيقية، فالدخول إلى الفضاء الإلكتروني لا يتطلب بروتوكولات معقدة، أو استظهار لبطاقات الهوية، وفتح الحسابات في المواقع والخدمات التي يوفرها هذا الفضاء لا تعتمد إلا على البيانات والمعلومات التي يقدمها فاتح الحساب، ونادرا ما يتطلب الأمر مسح لبطاقات إثبات الهوية، فضلا عن وجود آليات تقنية وبرمجية تمكن الإرهابيين أيضا من إخفاء مواقعهم الجغرافية حال دخولهم إلى ساحات الفضاء الإلكتروني.

ب- خفاء الكشف والاستدلال:

إن انعدام الدليل المادي الضروري لاكتشاف وإقامة الدليل على جريمة الإرهاب الإلكتروني، يعتبر من بين أهم مظاهر خفاء هذه الجريمة وتستترها، فعدم وجود دليل مادي ملموس يعتبر عائقا في تطبيق منهجية التحقيق التقليدية التي تعتمد أساسا على معطيات مادية بحتة، مما يجعل مسألة إقامة الدليل على مرتكبيها مسألة غاية في الصعوبة، ونظرا لكونها جريمة مرتبطة بآليات تقنية

(¹) علاء بن محمد صالح الهمص، وسائل التعرف على الجاني، الطبعة الأولى، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2012، ص 5-6.

(²) حسين هاشمي، الإرهاب بين الفقه الإسلامي والقانون الدولي، الطبعة الأولى، مركز الحضارة لتنمية الفكر الإسلامي، بيروت، 2014، ص 333.

(³) عبد القادر بن عبد الله الفتوخ، الجريمة في الأنترنت: طرق الحماية منها، مكتبة العبيكان، الرياض، 2012، ص 24.

حساسة، فإن الدليل فيها غالبا ما يتعرض للتلاعب، سواء بمحوه أو بتزييفه، كما أن غياب الكشف المبكر عنها يعرضها للتلف والضياع، ضم إلى ذلك أن معظم الأعمال الإرهابية الإلكترونية لا يتم التبليغ عنها خشية التورط بها ⁽¹⁾، - ومما يزيد الأمر تعقيدا - كون الدليل الرقمي في الإثبات الجنائي غير متفق على حجبه نظرا لاختلاف الإثبات الجنائي في الأنظمة المقارنة ⁽²⁾.

ومع ذلك تبقى هذه الخاصة نسبية نوعا ما، إذ أنه من الممكن جدا الوصول إلى اكتشاف هذه الجريمة والتوصل إلى جناتها، ومن ذلك التوصل إلى الهاكر الإسرائيلي الذي انتهك معلومات حساسية في أجهزة الحاسب التابعة للولايات المتحدة الأمريكية وإسرائيل، وهذا ما حققته أيضا السلطات الألمانية حين ضبط مرتكب جرم إلكتروني بالتعاون مع السلطات السويسرية، كما تتسم صعوبة الاستدلال عليها بالنسبية أيضا، وذلك أن هناك بعض الأنظمة كثيرا ما تترك آثارا للجريمة فضلا عن وجود تقنيات وبرامج يمكن بواسطتها استرجاع الأدلة الجنائية من الفضاء الإلكتروني ⁽³⁾.

2- جريمة الإرهاب الإلكتروني جريمة عابرة للحدود:

لقد أتاحَت عالمية الشبكة الإلكترونية لأن تكتسب جرائم الإرهاب الإلكتروني الطابع العالمي، إذ تم تكيفها قانونيا بالجرائم العابرة للحدود، كونها تتخطى الحدود السيادية للدولة كما أنها تتجاوز نطاق الجغرافي الإقليمي، إذ يمكن أن تحدث في أي مكان في العالم وخلال أي زمان دون أي يكون هناك أي تقارب بين الفعل الإجرامي وبين النتيجة التي تتمخض عنه ⁽⁴⁾، ورغم أن الإرهاب التقليدي مصنف من بين الجرائم المنظمة العابرة للحدود إلا أن الطبيعة التقنية لإرهاب الإلكتروني تحدث بينما فرقا.

3- جريمة الإرهاب الإلكتروني جريمة ناعمة:

تعتبر جريمة الإرهاب التقليدي من الجرائم الصلبة التي تتطلب بذل الكثير من الجهد الجسدي من أجل تنفيذها، جهد يبدأ بالتخطيط لها واقتناء المعدات لأجلها، وقد يصل إلى حد التضحية بالنفس لإنجاحها كما هو الحال في الهجمات الانتحارية، أما الإرهاب الإلكتروني فلا يحتاج منفذه إلا إلى معدات آلية بسيطة، ودراسة مستفيضة بتقنيات المعلومات وعلم البرمجيات ليحدث بعد ذلك آثار تدميرية هائلة ⁽⁵⁾.

⁽¹⁾ لورنس سعيد الحوامة، الجريمة الإلكترونية، أركانها وآلية مكافحتها، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد 04، العدد 01، الجامعة الإسلامية العالمية، عمان، الأردن، كانون الثاني 2017، ص ص: 187-220.

<https://www.wise.edu.jo/ar/node/2451>

⁽²⁾ خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الشروع في الجرائم المعلوماتية، الطبعة الأولى، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2012، ص: 149.

⁽³⁾ ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي: (دراسة مقارنة)، الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، مصر، 2017، ص ص: 31-23.

⁽⁴⁾ لورنس سعيد الحوامة، المرجع نفسه.

⁽⁵⁾ المرجع نفسه.

وهنا أيضا تبرز خصوصية الجناة في الأعمال الإرهابية الإلكترونية، فهم جناة متخصصون وعلى درجة عالية من الاحتراف تملكنهم من تجوز كل العقبات الأمنية الإلكترونية⁽¹⁾.

4- جريمة الإرهاب الإلكتروني ذات هدف سياسي:

إن تعريف الإرهاب بما فيه الإرهاب الإلكتروني يقوم على عنصر الهدف، فالهدف الذي اتفق عليه جانب كبير من الفقه والقانون هو الهدف السياسي، وهذا ما تمت الإشارة إليه في ما تقدم من كلامنا، يُعتبر الهدف السياسي الذي يقف وراء تنفيذ هجمات الإرهاب الإلكتروني، الحد الفاصل بين الإرهاب الإلكتروني وبين إساءة استخدام الكمبيوتر، فالهدف من وراء الهجمات الإلكترونية يحدث فارقا كبيرا في التكيف القانوني لطبيعة الجرم المرتكب⁽²⁾.

وهذه الخاصية إنما هي خاصية عامة لكل أشكال الإرهاب، وتحمل في كنهها معنى الابتزاز، ومفادها في الغالب القيام بتوجيه الهجمات الإرهابية إلى الجهات التي ليس من صلاحياتها إصدار القرارات التي يردها المهاجمون، ولكن إلى الجهات التي تدخل ضمن نطاق بيئتها، من حمل الجهات التي تمتلك صلاحية إصدار القرار على الرضوخ والانصياع⁽³⁾، فالإرهابيون كثيرا ما يوجهون هجمات ضد المستشفيات، أو ضد الشركات، رغم أنها مؤسسات ليس لها أن تصدر قرارا سياسيا، إلا أن استهدافها يشكل ورقة ضغط على الجهات الفعلية للانصياع لرغبات الإرهابيين.

ثانيا: الخصائص المتعلقة بطبيعة الهجمات:

1- المروغة والمناورة التكتيكية:

يعتمد الإرهابيون التقليديون على منهجية محددة في قيامهم بالأعمال التخريبية، فهم يعتمدون بصفة أساسية على أسلوب المروغة والتدليس وحرب العصابات، حتى أن الانتحاريين منهم يراوغون حتى عن الموت، فلا حتى أسلوب الردع ينفع في حماية الأمن القومي منهم⁽⁴⁾.

وهذا الأسلوب في النشاط الإرهابي تمت محاكاته بدقة على الساحة الإلكترونية، فأصبحت هجماتهم فيها كر وفر، والغالب فيها لمن استبق وفر قبل أن يدركه الآخر، وينتج عن هذه

(1) عبد العال الديري ومحمد صادق إسماعيل، الجريمة الإلكترونية: (دراسة قانونية قضائية مقارنة: مع أحد التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت) الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص ص: 58-59.

(2) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص ص: 123-124.

(3) عمرو العروسي، الشرطة والحرب الأهلية: (دراسة تطبيقية في القانون الدولي الإنساني)، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص ص: 48-49.

(4) دفيد كين، حرب بلا نهاية: (وظائف خفية للحرب على الإرهاب) ترجمة (معين الإمام)، الطبعة العربية الأولى، العبيكان للنشر، الرياض، المملكة العربية السعودية، 2008، ص 141.

الضربات سعي كل طرف في تقوية ترسانته الإلكترونية، وتجديد طرق الحماية والأمان⁽¹⁾.

2- سرعة التنفيذ:

إن ما يميز هجمات الإرهاب الإلكتروني عن الإرهاب التقليدي هي السرعة في تنفيذها، وتضييق التباعد الزمني بين الهجمات الكبرى من جهة⁽²⁾، وبين التخطيط والتنفيذ من جهة أخرى، وهذا غير متاح للإرهابيين التقليديين، فهجماتهم متباعدة، والفارق الزمن في كل مرحلة من مراحلها يعد كبيرا نظرا للطبيعة المادية التي تنسم بها، وارتباطها بمجال أو فضاء فزيائي.

3- هجمات الإرهاب الإلكتروني آلية حرب:

بقطع النظر عن الخلاف السائد بين الفقهاء والأجهزة التشريعية الدولية عن مسمى " إرهاب الدولة " إلا أن آثاره ظاهرة من خلال الممارسات التي تنتهجها بعض الدول ضد مواطنيها أو ضد دولة أخرى، إذا تقوم بعض الدول باللجوء إلى التقنية الإلكترونية من أجل ممارسة الرعب والعدوان ضد مواطنيها عن طريق القيام بهجمات إلكترونية تهدف إلى غلق الصفحات أو المدونات المعارضة لها، أو هتك خصوصياتهم الإلكترونية، للكشف عن هويتهم من أجل القيام باعتقالهم أو إخفائهم قسريا، كما تقوم أيضا بتسديد ضربات إلكترونية إلى مرافق ومؤسسات دولة معادية لها⁽³⁾.

ثالثا: الخصائص المتعلقة بتقييم طبيعة التهديد:

1- تقييم القدرات الإرهابية:

يختلف تقييم قدرات المهاجمين الإلكترونيين وفق لأهدافهم السياسية، فالإرهاب الذين تمارسه الدول التي تتمتع بالتقنيات العالية والقدرات الفنية المذهلة غير ذاك الذي تمارسه الجماعات الإرهابية، أو ذاك الذي تمارسه الذئاب المنفردة، إذ أنها لا تملك نفس تلك القدرات التي تملها الدول ولا المعرفة الفنية اللازمة لتسديد الهجمات على صعيد واسع، كما أنها غير متاحة لجمع التنظيمات الإرهابية⁽⁴⁾.

لكن الأمر قد لا يدول طويلا، فقد بدأ التنظيمات الإرهابية مؤخرا في توظيف الفضاء الإلكتروني كمعسكر بديل للتدريب من خلال إصدار عددا من الأدلة التطبيقية عبر ما الوسائط

(1) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق ص 124.

(2) إيهاب خليفة، مجتمع ما بعد المعلومات: (تأثير الثورة الرابعة على الأمن القومي)، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2019، ص 110.

(3) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص: 120-121.

(4) المرجع نفسه، ص: 121-122.

المتاحة على الويب كما تنتشر العديد من المقاطع الصوتية والبصرية وما إلى ذلك، وتقدم نماذج عملية وتطبيقية لطرق الانخراط في هذه التنظيمات، وأساليب صنع المتفجرات أو الأسلحة النارية الأخرى، فالفضاء الإلكتروني عموماً أصبح يشكل معسكر تدريب افتراضي بالفعل⁽¹⁾.

و رغم أن هذه المسألة خلافية بين الباحثين، وأن هناك جانب كبير منهم يرفض هذا الطرح، إلا أنه قد طرح فيه جانب من الصواب، فتتظيم القاعدة مثلاً، قد أصدر موسوعة كاملة - حصلنا على نسخة منها - في تكوين فني تقني لكوادر الاختراق الإرهابي مع منحهم مواقعاً لها ثغرات للتدريب عليها.

2- تقييم آثار التهديد:

إن أهداف الأعمال الإرهابية في الإرهاب التقليدي تكون محددة سلفاً ونتائجها معروفة مسبقاً، وهي نتائج وآثار يصعب تداركها أما هجمات الإرهاب الإلكتروني فهي هجمات ضد أهداف مجهولة وآثارها غير معروفة، إذ يمكن تداركها بالسرعة الهجمات نفسها⁽²⁾.

المطلب الثاني:

أسباب الإرهاب الإلكتروني

إن الأسباب الفعلية التي تقف وراء ظاهرة الإرهاب الإلكتروني متعددة ومتفرعة، ولا يمكن إطلاقاً معالجة هذه الظاهرة الإرهابية الحديثة بطبيعته التي تنسم بالخطورة القصوى على الأمن الدولي والقومي، وكما أنه لا يمكن إطلاقاً مكافحتها بالشكل السليم والفعال دون معرفة الأسباب الحقيقية التي تقف وراءها وتغذيها، وهي في غالبيتها أسباب متعلقة بالحياة النفسية والاجتماعية (الفرع الأول) التي تساندها أسباب سياسية متعددة ومعقدة (الفرع الثاني) والتي تسمح بظهور أفكار وإيديولوجيات عنيفة ومتطرفة (الفرع الثالث) أوجدت لها الآليات التقنية والفنية منفذاً إلى الساحة العملية والمجال التطبيقي (الفرع الرابع).

الفرع الأول: الأسباب النفسية والاجتماعية:

تعتبر ظاهرة الإرهاب من بين أكثر الظواهر المؤثرة للمجتمع الدولي لما عانتها البشرية منه في العقود الماضية من انعدام للأمن والاستقرار، ولذلك منح لها المختصون في علم النفس وأسس علم الإجرام أولوية خاصة في دراساتهم بهدف الوصول إلى معرفة الأسباب التي تقف وراءها ومن ثم وضع

(1) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الإنترنت في أغراض إرهابية، الأمم المتحدة، نيويورك، حزيران 2013، ص 08.

(2) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص: 121-122.

استراتيجية فعالة في محاربتها وتجفيف منابعها (أولا) وسائرهم في ذلك الدارسون في الحقل السوسيولوجي لمحاولة إيجاد الخيط الضابط الرابط بين الأوضاع الاجتماعية والسلوكيات الإرهابية (ثانيا).

أولا: الأسباب النفسية:

عند الحديث عن الأسباب النفسية للإرهاب فإن البادرة الأولى التي تتبادر إلى الذهن هي كون الظاهرة الإرهابية ظاهرة مرضية واختلال نفسي معقد التفاصيل بتعدد النفس البشرية، وأن هذا الاختلال النفسي يتشكل في قالب سلوكي غير سوي ينتج أثرا مريكا للبنية الاجتماعية، ولهذا نجد أن بعض الدارسين يرفضون هذا المنحى في دراسة الظاهرة الإرهابية، واعتبروه من باب إصدار الحكم المسبق على السبب الإجمالي للظاهرة دون التطرق إلى أنواعه المتعددة، وهذا الانتقاد يعتبر انقادا وجيها وصائبا، إذ إن إصدار الحكم على هذه الظاهرة بصفة مسبقة وتشخيصها على أنها حالة من حالات عدم السوية النفسية، يعبر حتما على اعتبارها بشكل واضح بأنها اختلال في الوظائف العقلية⁽¹⁾، وهذا قد ينتج أثرا عكسيا في مكافحة هذه الظاهرة.

ينسب علماء المدرسة التحليلية ظاهرة الإرهاب إلى أمراض نفسية واضطرابات عقلية وانفعالية، منها ما يكون نتيجة للتأثير المباشر الذي تحدثه البيئة الاجتماعية بكل مكوناتها من مشاعر الوسواس القهري والإحباط، ومنها ما يكون طبعا فطريا في نفسية الإرهابي، والتي تخلق فيه نوعا من الميل الطبيعي إلى العنف والعدوان، وقد صنف العلماء الأسباب النفسية التي تقف وراء السلوكيات الإرهابية إلى الأسباب الآتي ذكره⁽²⁾:

1- الفطرة العدائية:

يعتقد عالم النفس التحليلي **سيجموند فرويد**⁽³⁾ أن الأعمال التدميرية بما في ذلك الأعمال الموصوفة بالإرهابية، وغيرها من مظاهر العنف والتخريب راجعة إلى غريزة إنسانية أطلق عليها عبارة "غريزة الموت"⁽⁴⁾، وهذه الغريزة الفطرية التي جُبل عليها الإنسان تورث فيه ميلا جامحا إلى

(1) عبد المجيد مبلغي، الإرهاب تعريفه وآليات مكافحته، الطبعة الأولى، مركز الحضارة لتنمية الفكر الإسلامي، بيروت، 2015، ص: 37-38.

(2) محمود عرابي، الإرهاب: (مفهومه-أنواعه-أسبابه-آثاره-أساليب مواجهته)، الطبعة الأولى، الدار الثقافية للنشر، القاهرة، مصر، 2007، ص: 45-46.

(3) **سيجموند شلومو فرويد (Sigmund Schlomo freud)** 1856-1939 النمسا: هو طبيب من أصل يهودي، اختص بدراسة الطب العصبي وهو مفكر حر، يعتبر مؤسسا لعلم التحليل النفسي ومدرستها، اشتهر فرويد بنظريات العقل واللاوعي، وآليات الدفاع عن القمع وخلق الممارسة السريرية في التحليل النفسي لعلاج الأمراض النفسية من خلال الحوار مع المريض والمحلل النفسي، كما اشتهر بتقنية إعادة تحديد الرغبة الجنسية والطاقة التحفيزية الأولية للجنس البشري، كتب العديد من المؤلفات التي تعتبر عمادا في علم النفس التحليلي ومن بين أهم كتبه نجد: تفسير الأحلام، الجنس عند فرويد، خمس محاضرات في التحليل النفسي، السلوك، الذاكرة، الطوطم والتابو، نقلا عن: الموسوعة الحرة، ويكيبيديا: سيجموند فرويد

(4) سيجموند فرويد، أنا والهو، ترجمة (محمد عثمان نجاتي)، الطبعة الرابعة، دار الشروق، بيروت والقاهرة، 1982، ص 20.

الكرهية، وتخلق فيه نوعا من العداء للجميع، وتدفعه دوماً إلى ارتكاب مختلف أشكال العنف. والإنسان يقف أمام هذه الغريزة الفطرية موقفين اثنين؛ فإما أن يقاومها، الشيء الذي يخلق فيه نوعاً من أنواع الكبت النفسي، ويصعب عليه أن يعيش في إطار ثقافي حضاري، وإما أن يشبعها فتحدث أثراً تدميرياً معادياً للنمو الثقافي والتطور الحضاري⁽¹⁾.

2- اضطرابات الأنا الأعلى:

يشكل ضعف الأنا الأعلى أو تضخمه سبباً كبيراً في بروز التصرفات الإرهابية، فضعفه يخلق في الفرد عقدة النقص التي تجعل فريسة للهوى ومشاعر العدوان التي تطيب له بمقتضى الغريزة من جهة، والتقصص من جهة أخرى، فيقع إما في مغبات التصرفات الغريزية، وإما أن يتصرف وفق إحياءات عقلية تركيبها مصادر خارجية ممن يعتقد فيهم المثل الأعلى⁽²⁾. وأما تضخمه فيكون سببه الرئيس توتر حاصل بين الأنا الأعلى من جهة وبين الأنا الأدنى، فيشكل شعوراً بالذنب⁽³⁾، يعبر عنه بمحاولة لإرضاء الأنا الأعلى عبر التصرفات العدائية التي يراها مكفرة لتقصيره نحوه⁽⁴⁾.

3- جنون العظمة:

يرتبط الإرهاب ارتباكاً وثيقاً بمرض جنون العظمة الذي يدفع الفرد إلى ممارسة العنف بكل أشكاله، متوهماً عظمته وسمو مرتبته الثقافية أو العرقية، وقد كان أدولف هتلر النموذج الأمثل لجنون العظمة المنبثق من اعتقاده الراسخ بعظمة وسمو الجنس الآري الذي ينحدر منه، فارتكب بذلك أكثر الأعمال الإرهابية جنونا في تاريخ البشرية⁽⁵⁾.

كما نجد في التاريخ اليهودي المبكر أشكالاً قميئة من أشكال الإرهاب، والتي تبلورت في أعمال عنف ومجازر والإبادة الجماعية للشعوب الأخرى يصف بشاعتها العهد القديم في الكثير من أسفاره⁽⁶⁾.

(1) سيجموند فرويد، الحب والحرب والحضارة والموت، ترجمة (عبد المنعم الحفني)، الطبعة الأولى، دار الرشاد للطبع والنشر والتوزيع، القاهرة، 1992، ص ص: 75-81.

(2) محمود عرابي، المرجع السابق، ص ص: 46-47.

(3) سيجموند فرويد، الحب والحرب والحضارة والموت، المرجع نفسه، ص 83.

(4) محمود عرابي، المرجع نفسه، ص 47.

(5) المرجع نفسه، ص 47.

(6) تصور التوراة أشكالاً خطيرة من المجاوز التي ارتكبتها العبرانيون ضد الشعوب المتاخمة لهم، وتعتبر الأسفار التاريخية في العهد القديم من أهم المصادر التاريخية التي وثقت تلك المجاوز، كما يعتبر سفر يشوع من أهم أسفار العهد القديم بشاعة لاسيما الإصحاح العاشر منه في الأعداد من 28-40، كما نجد أيضاً وصفاً شنيعاً لجرائم العبرانيين في سفر التثنية الإصحاح 07 العدد 1-7: (متى أتى بك الرب إلهك إلى الأرض التي أنت داخل إليها لتملكها، وطرد شعوباً كثيرة أمامك: الحثيين والجرجاشيين والأموريين والكنعانيين والفرزيين والحوين واليبوسيين، سبع شعوب أكثر وأعظم منك، ودفعهم الرب إلهك أمامك وضربتهم فإنك حرمتهم) ومعنى التحريم هنا هو الإبادة كما نقل إلينا ذلك سفر يشوع في الإصحاح 8 الأعداد من 25-29: (فكان جميع الذين سقطوا في ذلك اليوم اثني عشر ألفاً. جميع أهل عاي، ويشوع لم يرد يده التي مدها بالمزراق حتى حرم جميع سكان عاي... وأحرق يشوع عاي وجعلها تلاً أبدياً خراباً إلى اليوم).

ولعل السبب الرئيس في ذلك هو اعتقادات اليهود التي تصورهم بأنهم شعب الله المختار، وأنهم الأطهر والأنقى من بين الخليقة كلها، وأنهم دون سواهم بشر وغيرهم ما هم إلا حيوانات خلقت في قالب آدمي ليتمكنوا من خدمتهم⁽¹⁾ وهذا الاعتقاد الراسخ في الأوساط اليهودية قد ورطهم في أحقاد ضد البشرية وصور لهم بأنهم مخولي الحق في ممارسة الإرادات والمجازرة ضد من يعتقدون أنهم مملوكين لهم⁽²⁾.

4- هذاء الاضطهاد:

هو مرض نفسي خطير بموجبه يعتقد المريض أنه محور المؤامرات، وأن هناك دائما من يتربص به الدائرة ليلحق به الأذى، وهو مرض تحتضنه الشخصية الاكتئابية والحساسة، وقد يكون في بعض الأحيان نتيجة لمرض انفصام الشخصية⁽³⁾، وهو دافع مهم للكثير من القادة لارتكاب أعتى الأعمال الإرهابية بشاعة وخطورة⁽⁴⁾.

5- مرض الشيزوفرينيا:

يعتبر من أكثر الاضطرابات الذهانية خطورة وانتشارا، وهو مرض يتجلى في عرضين مهمين: الهلوسة والأوهام، والتي تجعل المريض بها، منفصلا عن واقعه من خلال العيش في مدركات حسية لا وجود لها في الواقع، وتجعله دائم الشعور بالتهديد عبر نظريته الوهمية لتصرفات الغير⁽⁵⁾، ويشكل هذا المرض تهديدا فعليا لظهور السلوكيات العدائية والإرهابية⁽⁶⁾.

وهذا الأسباب النفسية حتى وإن كان الفقهاء والعلماء قد أدركوها وحددها كأسباب للإرهاب التقليدي، إلا أنها تحتفظ بقوتها كأسباب نفسية لظاهرة الإرهاب الإلكتروني، وذلك لان الإرهاب الإلكتروني في أصله هو نوع من أنواع الظاهرة الإرهابية بعمومها، فقد يلجأ المريض النفسي إلى استهداف الفضاء الإلكتروني للتنفس عن عقده النفسية المختلفة، وإذا أخذنا تضخم الأنا الأعلى نموذجا، فإننا سندرك علاقته بالإرهاب الإلكتروني من أول وهلة.

(1) وصف سفر التثنية هذاء العظمة في الإصحاح 10 العدد 15 وقال: (و لكن الرب إنما التصق بأبائكم ليحبهم من بعدهم نسلهم الذي هو أنتم فوق جميع الشعوب كما في هذا اليوم).

(2) إسماعيل أحمد ياغي، الإرهاب والعنف في الفكر الصهيوني، الطبعة الأولى، مكتبة العبيكان، الرياض، 2003، ص 63.

(3) عبد الناصر موسى، مرض الوسواس القهري: (الأسباب-الأعراض-الوقاية والعلاج)، الطبعة الأولى، دار خالد اللحاني للنشر والتوزيع، الأردن، 2017، ص ص: 90-92.

(4) محمود عرابي، المرجع السابق، ص ص: 47-48.

(5) كريج ستيل، الشيزوفرينيا: (انفصام الشخصية: العلاج السلوكي المعرفي للمرض والتدخلات القائمة على الأدلة والتوجيهات المستقبلية)، ترجمة

(مراد على عيسى)، الطبعة العربية الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2014، ص ص: 11-13.

(6) محمود عرابي، المرجع السابق، ص 48.

فعندما يشاهد الفرد المضطرب كل السلوكيات المخالفة لاتجاهاته الفكرية أو العقائدية تمارس على الفضاء الإلكتروني ويدافع عنها بكل شراسة، فإن ذلك يخلق في نفسه شعورا بالذنب عن عدم اتخاذه من الفضاء الإلكتروني آلية لعرض اتجاهاته والدفاع عنها، وبدلا من تدارك ذلك، وممارسه حقه في الدفاع عن فكرة، يقوم بانتهاج نهج آخر، وهو الهجوم على المخالفين له في المعتقد أو الفكر، فيقرصن حساباتهم، ويخترق أجهزتهم، ويعرضهم لفقدان خصوصياتهم، فضلا عن مهاجمة الفضاء الإلكتروني الذي سمح لهم بعض أفكارهم التي يراها منحطة أو غير سليمة.

ثانيا: الأسباب الاجتماعية:

إن دراسة الأسباب السيسولوجيا للظاهرة الإرهابية لا تكاد تنفك عن الدراسات السيكولوجية النفسية، لما لهما من تداخل في تكوين شخصية الفرد الإرهابي، ولعل من أبرز الأسباب الاجتماعية التي تقف وراء ظهور الإرهاب وتناميه في العصر الحديث ما يلي:

1- البطالة:

تعد البطالة من بين الظواهر الاجتماعية الخطيرة التي تقف وراء تنامي ظاهرة الإرهاب وتوغلها في أوساط الشباب، فالبطالة بالمفهوم الاجتماعي مقترنة بالفراغ وهو الذين يشكل منعطفا خطيرا في حياة الفرد الاجتماعية والنفسية، والتي تفتح عليه أبواب الوقوع في بؤر الإجرام، وقد أشارت الدراسات التي أجريت من خلال استطلاعات الرأي من 8 بلدان عربية أن البطالة بين المتعلمين تؤدي إلى زيادة احتمال اعتناق أفكار متشددة، وأن هناك علاقة وطيدة بين الفكر المنطرف وبين البطالة، كما أوضح استطلاع لـ 3500 شابا عربيا من 16 دولة أنهم يعتبرون أن البطالة هي السبب الذي يشجع الناس على الالتحاق إلى صفوف داعش⁽¹⁾.

وتظهر البطالة كسبب اجتماعي لتفاقم ظاهرة الإرهاب الإلكتروني من خلال الأوقات التي يقضيها الشباب على الفضاء الإلكتروني، والذي يعرضهم في كثير من الأحيان لتلقي أفكار متطرفة، والانجراف نحو تبنيها، فضلا عن أن البطالة تخلق حنقا ضد الأنظمة والمجتمع بأسره، والفضاء الإلكتروني هو الوسيلة المثلى للتعبير عن هذا الحنق، سواء باتخاذ شكل هجومي أو دعائي لفكر منحرف.

2- تفكك البنية الاجتماعية:

إن البنية الأساسية في المجتمع هي الأسرة، فهي اللبنة القاعدية في هرم البناء المجتمعي، فإذا ما أصابها نوع من أنواع الضعف والتشتت، وانتشر بين ثانيا أفرادها الجهل والتخلف، انهارت

(¹) خالد الغالي، البطالة والإرهاب... ماذا تقول الدراسات؟، 04 ديسمبر 2016، تم الاطلاع عليه بتاريخ 19 ديسمبر 2019 على الساعة 22:23 في الموقع: <https://www.irfaasawtak.com/rights-and-liberties/2016/12/04/البطالة-والإرهاب-تقول-الدراسات؟>

وانهار معها المجتمع كله، فالأسرة هي الوحدة الأولية في خط الدفاع المدني ضد الإرهاب، فالفرد الذين يكون مشبع الرغبات المادية والعاطفية في ظل أسرة متكاملة يكون بعيدا عن بؤرة الإرهاب وفكر التطرف، وتجدر الإشارة هنا إلى دور الحوار بين أفراد الأسرة، وكسر بعض الحواجز العرفية التي تحول بين الاتصال السليم والفعل بين الآباء والأبناء، وكذلك انغلاق بعض الأسر والتجمعات على أنفسها، وانعدام منافذ الحوار والتعامل الحضاري بين أفراد المجتمع، كل هذا يؤثر سلبا على البنية الاجتماعية⁽¹⁾، وتوجه بدفته إلى التنفيس عن نفسها في الشبكات الافتراضية والفضاء الإلكتروني والغوص في الفكر الإرهابي والراديكالي.

3- غياب العدالة الاجتماعية:

إن غياب العدالة الاجتماعية وانتشار المحسوبية والتوزيع غير السليم للثروات، والتعامل مع المجتمع على أساس الانتماء الديني أو العرقي أو الإثني أو اللغوي، ينتج طبقة كادحة ينعدم فيها حس الوطنية، وينتشر بين أفرادها الشعور بالتهديد والاضطهاد، مما يشكل فيهم أحقادا وضغائن تجاه الطبقات الثرية والغنية أو الطبقة الحاكمة، ورغم أن الفقر كافة اجتماعية لا تنتج لمفردها إرهابا، إلا أن الشعور الناتج عن الظلم والقهر والإقصاء يكون عاملا أساسيا في تكون الفكر الإرهابي وتوغله بين أفراد المجتمع المظلوم⁽²⁾، لأن من شأن تلك المشاعر أن تكون لدى المجتمع نوعا من الغضب المحتدم ضد الدولة أو حتى ضد الطبقات الثرية، ومن ثم ينفجر هذا الغضب على شكل أعمال وتصرفات إرهابية، منها ما يكون تحت غطاء دفع الظلم وتحقيق العدل وإعادة الأمل في المجتمع، ومنها ما يكون تحت غطاء انتقامي بحث⁽³⁾.

وقد أشار التقرير الذي نشرته منظمة الأمن والتعاون في أوروبا، إلى أن الأحكام المسبقة التي تصيغها قوات الأمن في قواعد بياناتها، والتي تقوم على أسس عرقية أو دينية أو إثنية، تلعب دورا في تكوين المجتمع المضطهد، كما أن تصرفاتها أثناء أداء عملها من تميز حال التفتيش أو القبض في إطار محاربة الإرهاب قد يكون له أثر العامل المنشأ للإرهاب أو الداعم له⁽⁴⁾.

(1) محمود عرابي، المرجع السابق، ص 50-51.

(2) ميثاق بيات الضيفي، أكسجين الحرية، الطبعة الأولى، " E-kutub Ltd " للنشر، لندن، بريطانيا، 2019، ص 17-18.

(3) محمود عرابي، المرجع السابق، ص 51.

(4) منظمة الأمن والتعاون في أوروبا، الوقاية من الإرهاب ومكافحة التطرف العنيف والراديكالية المؤدبين إليه: (مقاربة الشرطة المجتمعية)، فيينا،

فبراير 2014، ص 44.

https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.osce.org/ar/secretariat/119499%3Fdownload%3Dtrue&ved=2ahUKEwjE4OGBgrroAhXldd8KHdYD_QQFJAAegQIBxAC&usg=AOvVaw0fdFp1aRQl5vt56gxTnZ6h

الفرع الثاني: الأسباب السياسية والاقتصادية:

يرجع الإرهاب الإلكتروني في جذوره وأصوله ومنبته إلى حالات السخط أو عدم الرضا عن الأحوال والظروف السياسية التي تنتج غالباً عن الأنظمة الاستبدادية والشمولية أو الأنظمة الثيوقراطية القومية، فضلاً عن الحركات الاستعمارية والتدخلات الأجنبية في الشؤون الداخلية للشعوب والذي يثير فيهم حنكا وغيضا يعبر عنه باللجوء إلى العنف الإلكتروني (أولاً)، فضلاً عن الأوضاع الاقتصادية التي تورث مشاعر الإحباط والحرمان في نفس الأفراد (ثانياً).

أولاً: الأسباب السياسية:

تعتبر الأسباب السياسية من بين أهم الأسباب التي ينجر عنها العنف والإرهاب والتطرف، ويمكن اختزالها في النقاط التالية:

1- الأنظمة السياسية المستبدة:

لا ريب أن الأنظمة السياسية الديكتاتورية المستبدة، والأنظمة العسكرية المتسلطة، تعتبر من أكبر الأنظمة المنتجة للإرهاب والحاضنة له، فالتعامل مع الشعوب بطريقة فجّة، وبأساليب قمعية وقهرية، وانتهاج نهج الرهبة والإرهاب يترتب عنه إرهاباً مضاداً، فالدول التي لا تتمتع بالتعددية السياسية والحزبية في التمثيل السياسي، والتي لا تسمح بالتداول السلمي للسلطة عبر الوسائل القانونية الديمقراطية، والتي تعتمد سياسة الإقصاء في التعامل مع المعارضين، وسياسة الاضطهاد في التعامل مع اختلاف التوجهات الأيدلوجية والرؤى السياسية وحرية التعبير والرأي، هي دول في حقيقة أمرها تمهد للإرهاب بكل أشكاله، وتمنحه المسوغ المنطقي لأعماله، وتألّف عليه قلوب الناس المحبطة والمضطهدة⁽¹⁾.

وبهذا الصدد يقول الكتاب والفكر والمناضل السوري نضال نعيّسة أن: (الاستبداد حاضن للإرهاب، ومنتج، ومصدر له، والمجتمعات التي تعيش على الخوف، لا بد سيقتلها العنف. ولكي يحمي الاستبداد نفسه، ويدافع الخوف الكبير، ربما أكبر من ذاك الذي يحاول أن يلحقه بضحاياه، يلجأ عادة، لأبشع، وأشد أنواع العنف، وأكثرها دموية، وفتكاً، لإحداث تلك الحالة المأمولة من الهجوع الدائم، والاستكانة، وعدم الحراك في صفوف "أعدائه المفترضين" في الداخل. إلا أن نفس تلك القوة الباطشة الغاشمة، والهائلة، التي ترفض أي نوع من المصالحة

(1) ميلود ولد الصديق، مكافحة الإرهاب بين مشكلة المفهوم واختلاف المعايير عند التطبيق: (أوراق بحثية مقدمة في إطار ندوة علمية، الجزء الأول، الطبعة الأولى، مركز الكتاب الأكاديمي، عمان، الأردن، 2018، ص ص: 111-112).

والحوار، والاعتراف بأي من مكونات المجتمع المختلفة، تتحول فجأة، إلى نوع من الوداعة، والمهادنة، والاستكانة مع الخارج⁽¹⁾.

ويستأنف كلامه قائلاً: (إن انعدام حرية التعبير والكلام تدفع الإنسان إلى البحث عن بدائل أخرى لإثبات الذات، والتعبير عن النفس. وفي مجتمعات تفتقر لادنى ثقافة وممارسة ديمقراطية، يصبح الإقصاء المتبادل هو الخيار الأخطر، وهو في نفس الوقت، السبيل الأرقى للتعبير عما يجول في مكونات النفوس التي أدمنت المذلة، والخضوع، والخنوع، والتبعية العمياء، والهوان⁽²⁾).

ونرى أن نضال نعيصة قد وضع يده على موضع الداء فعلاً، فالتأمل في الأوضاع الراهنة، وجغرافيا الإرهاب يدرك لأول وهلة أن مواضع انتشاره تتجلى في الدول التي لا تحضي فيها الشعوب بأنظمة حكم ديمقراطية تعترف بالتعدد والتنوع والاختلاف، وبالتداول السلمي للسلطة، والتي لا تفتح المجال لحرية الرأي والتعبير وتنتهج سياسية الأرض المحروقة من خلال قمع كل فكر أو قلم من شأنه أن تستفيد منه منظمة وصرح الديمقراطية، بحيث لا تترك مجالاً للشعوب إلا في التعبير عن ذاتها وآرائها باستخدام لغة السلاح والعنف.

وقد أشارت الجمعية العامة للأمم المتحدة في إطار جدول أعمالها الرمي إلى القضاء على الإرهاب الدولي أيضاً إلى كون الإقصاء السياسي والظلم والاضطهاد من بين الأسباب الجذرية التي تقف وراء الظاهرة الإرهابية وانتشارها⁽³⁾.

2- الأنظمة السياسية الثيوقراطية والقومية:

إن الأنظمة السياسية القائمة على إيديولوجيات قومية عرقية أو ثقافية أو على إيديولوجية دينية أو مذهبية هي من أهم الدول التي ينشأ فيها الإرهاب ويتوغل، ذلك لأن سياسات الحكم فيها قائمة على محاباة عنصر من عناصر الشعب دون الآخر، مما يخلق شروخاً داخلياً بين القوميات الثقافية والعرقية وبين أتباع الأديان والمذاهب في المجتمع الواحد، وهذا الشرخ سيشكل النواة الأولى لبروز مشاعر الاضطهاد والإقصاء وانعدام روح الوطنية، والمناخ الملائم لتشكل الفكر القومي أو

(1) نضال نعيصة، الاستبداد، (د.ت.ن)، تم الاطلاع عليه بتاريخ 27 مارس 2020 على الساعة 09:39 سا، في الموقع:

<http://www.arabtimes.com/A2006/may/9.html>

(2) المرجع نفسه.

(3) أنظر البند 06 من محضر موجز للجلسة الثالث للجنة السادسة للجمعية العامة المتضمنة التدابير الرامية إلى مكافحة الإرهاب الدولي، الدورة

69، المؤرخ بتاريخ 27 أكتوبر 2014: <https://daccess-ods.un.org/TMP/2758755.08785248.html>

الديني المتطرف، والذي سيخلق في الأخير بيئة قابلة للانفجار في أي لحظة عبر ممارسة الأعمال الإرهابية ضد أي قومية من القوميات أو دين من الأديان، أو ضد نظام الحكم نفسه⁽¹⁾.

وهذا إنما يتضح لنا من خلال استقضاء الظروف والأحوال عبر التاريخ البشري وإلى اليوم، فكثيرا ما يكون الإرهاب سببه الحيف والعدول عن تطبيق مبدأ المساواة بين أفراد المجتمع، والتفريق بينهم على أسس قومية أو دينية، وهذا بلا شك سيكون سببا لشعور المنتمين إلى قومية من القوميات أو دين من الأديان بأنهم إما أنهم ليسوا مواطنين، وإما أنهم مواطنون من درجة ثانية، مما يخلق حنقا وغضبا على النظام القائم أو على الأفراد المنتمين إلى القومية أو الدين الحاكم، لذلك فإنه من الضروري بمكان، أن تكون الدولة ونظامها الدستوري في صورة تبلور كافة قوميات الدولة، أو إثنياتها الثقافية، أو أديان شعوبها، فإن تعذر ذلك لكثرتها وتعددتها فإنه من الضروري أن يكون نظامها الدستوري بعيد كل البعد عن إضفاء الطابع القومي أو العرقي على الدولة، فضلا عن اعتماد العلمانية كنظام حكم في البلدان التي توجد فيها أكثر من ديانة واحدة.

3- الأنظمة الاستعمارية:

يعرف الاستعمار على أنه (نزوع الدول الكبيرة لفرض سلطانها وإرادتها على البلدان الأخرى، والاحتفاظ بهذه السيطرة بمختلف الوسائل السياسية، والاقتصادية والعسكرية، ومحاولة تغيير هوية البلدان المستعمرة ربطها بالدولة الاستعمارية ربطا عضويا ولغويا وثقافيا واقتصاديا واستغلال ثرواتها، وأيضا إقامة المشروعات المتعددة فيها)⁽²⁾، ومن هذا التعريف نستطيع أن ننطلق إلى بيان الترابط الوثيق بين الأنظمة ذات النزعة الاستعمارية وبين بروز الإرهاب كظاهرة عالمية.

إن الأنظمة الاستعمارية قد أحدثت في العالم تفاوتات كبيرة بين دول غنية تستحوذ على أموال وثرواته العالم، وبين دول فقيرة غارقة في وحل التشنات والفقر والاستغلال والعبودية، وإهدار أبسط الحقوق الأساسية في الحياة، وإن هذا لمن شأنه أن يحدث في الشعوب المستعمرة مشاعر الإحباط وفقدان الأمل، والذي سيجريها في الأخير إلى انتهاج النهج العنيف والمتطرف من أجل محاولة تغيير الواقع المزرى الذي تعايشه⁽³⁾.

(1) ميلود ولد الصديق، المرجع السابق، ص 111.

(2) رامي عطا صديق وفاطمة شعبان أبو الحسن، الإعلام والتنمية في مواجهة الإرهاب: (دليل مصطلحات)، الطبعة الأولى، أطلس للنشر والإنتاج الإعلامي، 2017، ص 56.

(3) بلقاسم سلاطينة وآخرون، علم الاجتماع الإعلامي، الطبعة الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2012، ص 106.

إن الأثر الذي ينتجه الاستعمار في ظهور الإرهاب وتناميه، قد تنتجه أيضا سياسات الحرب عليه، فقد أفضت سياسة الولايات المتحدة الأمريكية في حربها ضد الإرهاب في العراق وأفغانستان، إلى جعل العالم بيئة أكثر قابلية لتنامي الظاهرة الإرهابية وازدياد هجماتها عليها، وعلى حلفائها الذين ساندوها في سياستها بغية الحصول على امتيازات نفطية مستقبلية محتملة في العراق⁽¹⁾.
فقد رأى بعض النقاد أن سياسة المحافظين الجدد في حربها إلى الإرهاب، كانت لها انعكاسات خطيرة على الداخل والخارج الأمريكي، فقد هوى الاقتصاد الأمريكي إلى القاع، وازدياد حجم البغض والعداء تجاهها، وازدادت المخاوف الأمنية للأمريكيين، واتسعت رقعة الإرهاب في العالم، وأما خارجيا فقد ظهر العنف الطائفي في العراق وازداد تنظيم القاعدة في تحقيق مكاسب جديدة، وسادت التوترات والمخاوف في دول الجوار⁽²⁾.

إن الانتهاكات الأمريكية لحقوق الإنسان في حربها على الإرهاب، قد زاد في تفاقم الوضع سوءاً، فما حدث على سبيل المثال بأسرى الحرب الذين تعرضوا لأشكال غير آدمية من التعذيب في سجن غوانتانامو وأبو غريب، قد أوجع الرأي العام الدولي، وأحدث ردات فعل شعبية كبيرة إزاء الخرق المتعمد للمواثيق الدولية الراعية لحقوق الإنسان وأسرى الحرب⁽³⁾، فكل هذا من شأنه أن يزيد من تفاقم الظاهرة الإرهابية والتعاطف الشعبي معها.

ليس هذا فحسب، فقد أدت السياسات الخارجية الأمريكية والأوروبية أيضا في انحيازها إلى الأنظمة المستبدة في الوطن العربي، من حدة الانتهاكات الإرهابية السلطوية عبر الدعم المادي لها، وهذا من خلال تزويدها بالأسلحة التي تعلم مسبقا بأنها ستستعمل بشكل غير قانوني لقمع مواطنيها، وإرغامهم على الخضوع والخنوع لسيادتها، وفرض سياساتها عليهم عن طريق بث الرعب والترويع، كما تقدم لها دعما معنويا من خلال السكوت عن الجرائم الفظيعة التي ترتكبها في حق شعوبها من جانب، ومن خلال وسائل الإعلام التي تصور للعالم أن الشعوب العربية غير قابلة لخوض التجارب الديمقراطية من جهة أخرى⁽⁴⁾.

(1) أنتوني أرنوف، العراق: (منطق الانسحاب)، ترجمة: (محمود برهوم ورعدة محمد حسن عزيزية)، الطبعة الأولى، المؤسسة العربية للدراسات والنشر، بيروت، 2006، ص ص: 15-16.

(2) أحمد فايز صالح، دور المحافظين الجدد في السياسة الخارجية الأمريكية، الطبعة الأولى، باحث للدراسات الفلسطينية والاستراتيجية، بيروت، لبنان، 2011، ص ص: 138-139.

(3) محمد خليل موسى، الآخر والحرب على الإرهاب: (نحو نموذج تفسيري للنظام القانوني الدولي المعاصر)، الطبعة الأولى، دار الفكر، دمشق، 2009، ص 109.

(4) عبد الفتاح ماضي، العوامل الخارجية والثورات العربية: (أربع إشكاليات للبحث)، سياسات عربية، العدد 36، المركز العربي للأبحاث ودراسة السياسية، يناير 2019، تم الاطلاع عليه بتاريخ 19 نوفمبر 2019 على الساعة 01:00 سا، في موقع:

<https://siyasatarabiya.dohainstitute.org/ar/issue036/Pages/art01.aspx>

ولا شك بعد ذلك أن يكون الإرهاب الإلكتروني بما يتمتع به من خواص، آلية أو أسلوب يتم اللجوء إليه لإحداث تغيرات سياسية في مواجهة السلطة القمعية والحركات الاستعمارية، ومن هنا يبرز أيضا الخط بين مفهوم الإرهاب الإلكتروني كنشاط غير مشروع وبين غيره من المفاهيم التي تلتبس معه.

ثانيا: الأسباب الاقتصادية:

إنه لمن الثابت في الأوساط العلمية المتعلقة بدراسة الظاهرة الإرهابية ولاسيما مدارس علم الإجرام والسياسة الجزائية أن الظروف الاقتصادية وتحولات التي تحدث في مؤشرات لها وقع كبير على معدلات الإجرام بما في ذلك الظاهرة الإرهابية التي تملك قدرا كبيرا من الترابط بينها وبين الظواهر الاقتصادية، وهناك العديد من النظريات التي تحاول تفسير هذا الترابط.

ومن بين أهم النظريات الاقتصادية التي تم اعتمادها من أجل تسليط الضوء على العلاقة بين المؤشرات الاقتصادية والظاهرة الإرهابية نجد نظرية الحرمان الاقتصادي النسبي، وهي نظرية تعالج الأثر الناتج عن التنامي الاقتصادي الكبير في الدول والمقرن بانعدام العدالة، فالتنامي الاقتصادي الكبير الذي لا يشمل الطبقات الكادحة والمحرومة داخل المجتمع يكون سببا في ظهور الإرهاب عندما يبلغ الأمر حدا من انعدام التوازن، بحيث تظهر فوارق كبرى بين المؤمل والمرجي من هذا التنامي الاقتصادي وبين الخلل في عملية توزيعها لتطال الفئات المحرومة⁽¹⁾.

فالظاهرة الإرهابية من خلال هذا المنظور. ما هي إلا تحول شخصي يطرأ على الفرد في ظل استجابته إلى المظالم المتعلقة بالتطرف الاقتصادي والاجتماعي⁽²⁾.

وهناك أيضا نظرية أخرى وهي نظرية الافتقار التي أطلقها أوسون (Olson)⁽³⁾ سنة 1963، وهي نظرية تقوم بالربط بين الظواهر الاقتصادية والظاهرة الإرهابية من زاوية الأثر المترتب عن التنامي المتسارع للاقتصاد، حيث تربط بين التنامي المتسارع والمفاجئ للمؤشرات الاقتصادية وما يصحبه من تغيرات كبرى في شكل المصالح وأبعادها بحث تشكل طبقة خاصة في

(¹) سمر حسن الباجوري، الأسباب الاقتصادية لتنامي ظاهرة الإرهاب في إفريقيا جنوب الصحراء، المستودع العلمي (MPRA)، 31 ماي 2016، تم الاطلاع عليه بتاريخ 16 فيفري 2020 على الساعة 5:57 سا، في الموقع: <https://mpra.ub.uni-muenchen.de>

(²) هبة غري، نظرية الحرمان النسبي وأسباب التطرف والعنف، مجلة الدراسات الاستراتيجية للكوارث وإدارة الفرص، المجلد 01، العدد 04، المركز الديمقراطي العربي، برلين، يناير 2020، ص ص: 27-43: <https://democraticac.de/?p=64642>

(³) مانكار أولسون (MANCUR Olson) 1998-1932 بالولايات المتحدة الأمريكية: متخصص أمريكي في علم الاقتصاد د، تخرج من جامعة ولاية داكوتا الشمالية وعلى الدكتوراه في الاقتصاد عن جامعة هارفارد، عمل كمحاضر في علم الاقتصاد بجامعة برينستون ثم في جامعة ماريلاند سنة 1990، أسس مركز الإصلاح المؤسسي والقطاع غير الرسمي في جامعة ماريلاند، ومن أبرز مؤلفاته نجد: (The logic of collective action, Power and prosperity, The rise and decline of nations)

- https://fr.wikipedia.org/wiki/Mancur_Olson

المجتمع يغلب عليها طابع الجشع الأمر الذي ينعكس سلبا على بقية أفراد المجتمع ويجعلهم ضحايا مقهورة، وبين الظاهرة الإرهابية حين تنصرف هذه الطبقة التي وقعت عليها مغبات جشع الآخرين في مغبات الإرهاب حين يصبحون فريسة سائغة للجماعات المتطرفة⁽¹⁾.

كما أن الأزمات الاقتصادية أيضا تعد من أهم الأسباب التي تقف وراء الركون إلى العنف والإرهاب، ذلك لما ينتج عنها من آثار سيئة على المجتمع، وعلى مستواهم المعيشي، إذ تعد من بين الأسباب التي تقف وراء تفشي البطالة وانعدام فرص الشغل، وانتشار الفقر نظرا للتضخم المالي وانخفاض القدرة الشرائية للأفراد، كما ينتج عنها أيضا تفاوت طبقي بين فئات المجتمع، تفاوت يتجلى ظهور طبقتين متفاوتتين ماديا بشكل كبير؛ طبقة برجوازية ذات نزعة استعلائية تملك كل مقومات الحياة الرفيعة، وطبقة عاملة بأجور متدنية، تعاني الفقر والتهميش والنظرة الإزدرائية، وهذا الوضع الكارثي داخل المجتمع قد يؤدي بما لا يدع مجالا للشك إلى خلق مشاعر الإحباط وفقدان حس الحياة والقسوة على الذات، والتي بدورها ستؤدي إلى تطورات خطيرة تتجلى معظمها في الانحرافات السلوكية والنفسية المهيئة للعنف والإرهاب⁽²⁾.

وبعيد بعض الباحثين انتشار الظاهرة الإرهابية إلى العولمة في شقها الاقتصادي، ذلك أن دول العالم الثالث غير مؤهلة لاستقبال هذا الانفراج الاقتصادي الكبير، مما أدى إلى تدهور الحال الاقتصادية للمجتمع والذي استغلته الجماعات الإرهابية المتطرفة المعادية للمدنية والعولمة في بث ونشر ثقافة العنف في أوساط الفئات المعوزة والفقيرة، فبيئة الحرمان هي البيئة الأمثل لتوغل الفكر المتطرف العنيف الذي يترتب عنه التخريب والإرهاب⁽³⁾.

كما أن النظم الاقتصادية في ظل النظام العالمي الجديد وسياساتها المتبعة القائمة على الاحتكار والجشع، قد أحدث فجوة كبيرة في المستوى المعيشي للأفراد، فالكثير من دول الشمال تقوم بفرض التبعية الاقتصادية على دول الجنوب من خلال استغلال ثرواتها وممتلكاتها، والتدمير الممنهج والمقصود لاقتصادها، وإغراقها في دوامة من الديون الخارجية، وفرض عقوبات اقتصادية جائرة تنعكس بشكل كبير على القدرة المعيشية للأفراد⁽⁴⁾ مما يزيد من تفاقم الظاهرة الإرهابية من خلال انتهاز الجماعات المتطرفة لهذا الوضع في تزييف وعي الشباب وتسميم عقولهم وتهيج

(1) سمر حسن الباجوري، المرجع السابق.

(2) ميلود ولد الصديق، المرجع السابق، ص 113.

(3) محمد مسعود قيراط، الإرهاب: (دراسة في البرامج الوطنية واستراتيجيات مكافحته: مقارنة إعلامية)، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص ص: 91-92.

(4) سفيان عيساوي، مكافحة الإرهاب الدولي في منطقة الساحل الإفريقي، أطروحة دكتوراه في القانون الدولي الجنائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، السنة الجامعة 2017-2018، ص ص: 126-127.

مشاعرهم ومن خلال انتهاز الجماعات المتطرفة لهذا الوضع في تزيف وعي الشباب وتسميم عقولهم وتهيج مشاعرهم وتحريضهم من أجل حملهم على القيام بالأعمال الإرهابية ضد من سبب لهم البأس والشقاء، والزج بهم في مستنقع العنف والكراهية لخدمة أغراضهم ومناهيجهم⁽¹⁾.

إن المعيار والمؤشر الذي يربط الإرهاب بالمشاكل الاقتصادية وعلى رأسها الفقر، ليس معياراً فردياً، فالواقع والتجربة قد أثبتا أن الأغنياء أيضاً ينخرطون في الأعمال الإرهابية⁽²⁾، لكن المعيار أو الزاوية التي ينظر إليها إلى الفقر كسبب من أسباب الإرهاب تكمن في تأثيراتها السلبية على الحس النفسي للأفراد، فمؤشر الربط إذاً، متعلق بالمشاعر التي تنتج عن الفقر والحرمان من فقدان للأدمية والدخول في معتزك الإحباط والضياع وفقدان الأمل في الوصول إلى تحقيق حياة كريمة⁽³⁾.

وقد أحصى إيريك جنسن أربع تأثيرات خطيرة للفقر على الإنسان وعلى العوائل ويمكننا اعتبارها مؤشراً خطيراً وبادراً تتباً بالانحراف السلوكي والنفسي الذي يوجه الفرد إلى اتخاذ سلوكيات عدائية نحو المجتمع ككل، والتي يتجلى الإرهاب كأبرزها، وهذه التأثيرات هي؛ العراقيل والمشاكل الانفعالية والاجتماعية، توترات حادة ومزمنة، الإفقار والعجز المعرفي، وأخيراً مشاكل متعلقة بالصحة والأمن⁽⁴⁾.

ليس هذا فحسب، فالفقر قد تنتج عنه آفات خطيرة أبرزها الهجرة غير الشرعية أو البقاء في موطن طلب اللجوء السياسي بعد رفض الطلب، والواقع أن طلبات اللجوء عادة ما يكون سببها الفقر والظروف الاقتصادية المزرية، وهذا بطبيعة الحال يعود سلباً على الأمن كونه يهدد السيادة ويخل بالتوازن العرقي في البلاد⁽⁵⁾، وقد اثبت لنا الواقع أن الكثير من الهجمات الإرهابية كان وراء تنفيذها مهاجرين غير شرعيين ومن أمثلة ذلك منفذ العملية الإرهابية في نيس، الذي كان مهاجراً غير شرعي يحمل الجنسية التونسية⁽⁶⁾، وهناك من ربط بين ارتفاع أعداد الهجمات الإرهابية في أوروبا سنة 2015 بزيادة وارتفاع حجم الهجرة غير الشرعية⁽⁷⁾.

(1) علي لونيبي، آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الفردية، رسالة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص 68 وما بعدها.

(2) بيرز أسامة بن لادن كأهم عينة لانخراط الأثرياء والأغنياء في التنظيمات الإرهابية، فثروة عائلته كما ذكر الأستاذ إياد محي الدين أمين في كتابه الاغتيالات السياسية في الحصر الحديث قد قدرت بسبعة مليارات دولار.

(3) محمود عرابي، المرجع السابق، ص 51.

(4) إيريك جنسن، الفقر والتعليم: (ماذا يفعل الفقر بمخ أطفالنا؟ وماذا تفعل المدرسة لتصلح ما أفسده الفقر؟)، ترجمة (صفاء الأعسر)، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2015، ص 17.

(5) راي بوش، الفقر والليبرالية الجديدة: (الاستمرارية وإعادة الإنتاج في جنوب العالم)، ترجمة: (إلهام عيداروس ووليد سليم)، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2015، ص 114.

(6) مراسل آر تي، منفذ العملية الإرهابية في نيس مهاجر غير شرعي يحمل الجنسية التونسية، 29 أكتوبر 2020، تم الاطلاع عليه بتاريخ 18 فيفري 2021، على الساعة 22:55، مختصر الرابط: <https://cutt.us/AQyFv>

(7) رولان مربع، تداعيات الهجرة غير الشرعية على أوروبا وأبعادها، منشورات، العدد 98، تشرين الأول 2016، موقع الدفاع الوطني اللبناني، تم الاطلاع عليه بتاريخ 18 فيفري 2021، على الساعة 22:58، مختصر الرابط: <https://cutt.us/PF6y6>

وقد أشارت الجمعية العامة للأمم المتحدة إلى هذه النقطة المهمة في الربط بين الإرهاب وبين المشاكل الاقتصادية في التدابير الرامية إلى معالجة الظروف المؤدية إلى الإرهاب حين نصت على التوصية التالية: (السعي إلى تحقيق تعزيز خطط التنمية والإدماج الاجتماعي على الصعيد بوصفها أهدافاً قائمة بحد ذاتها، انطلاقاً من إدراك أن إحراز نجاح في هذا المجال، ولاسيما في ما يتعلق ببطالة الشباب، أمر يمكن أن يحد من التهميش وما يستتبعه من شعور بالغبن يغذي التطرق وتجنيد الإرهابيين)⁽¹⁾.

وبما أن الإرهاب الإلكتروني في جوهره ما هو إلا نوع وصورة من صور الإرهاب، وآلية يتم توظيفها لأحداث تغيرات محددة، فإنه بذلك يشكل آلية من آليات الاحتجاج على الأوضاع الاقتصادية، وصورة من صور التعبير غير المشروع عن الحرمان وغياب العدالة الاجتماعية والفقر.

الفرع الثالث: الأسباب الإيديولوجية والمذهبية:

تشكل الإيديولوجيات المنحرفة القاعدة الأساسية التي يقوم عليها الإرهاب والمحنة الأولى التي ينطلق منها عابراً إلى ساحة الغلو والتطرف العنيف (أولاً)، كما تشكل المعتقدات الدينية الفاسدة المبنية على أفكار خاطئة وقراءات متشددة مترتبة إلى توليد مشاعر الكراهية والبغض والتي تشمل نقطة التحول الجذري من المنهج الفكري المتنوع إلى المنهج الحركي العنيف (ثانياً).

أولاً: التطرف الإيديولوجية:

يُرجع الكثير من الباحثين جزءاً كبيراً من الإرهاب المعاصر إلى الإيديولوجيات التي كانت سائدة في القرنين المنصرمين، ويعتبرونه المنبع الأساسي لظهوره وانتشاره خاصة عندما اقترن مع النمو التكنولوجي الكبير، الذي كان الوسيلة الفعالة في أيدي الإرهابيين للعمل على ارتكاب نشاطات تخريبية مذهلة على قلة عددهم ومحدودية إمكانياتهم، فالإيديولوجية والعلم هما إذاً النواة الأولى التي انبثق منها الإرهاب المعاصر، وهما اللذان يشكلان القاسم المشترك بين كل أنماطه وأشكاله، ولذلك من غير الممكن أن ينقطع هذا الارتباط حتى وإن تغيرت صورته وتعدد مظاهره⁽²⁾.

تتنوع الإيديولوجيات التي تقف وراء ظهور الظاهرة الإرهابية وانتشارها، وتعدد المشارب الفكرية التي تقوم على أساسها، نذكر منها على سبيل المثال:

(¹) أنظر البند 6 من قرار الجمعية العامة للأمم المتحدة رقم 288/60 المتعلقة باستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، المؤرخ بتاريخ 08 سبتمبر 2006: <https://daccess-ods.un.org/TMP/6154880.52368164.html>

(²) Arnaud BLIN, Le Terrorisme, Edition Le Cavalier Bleu (Idées reçues), Paris, 2005, PP. 45-46

1- الإيديولوجيات الثورية:

لقد ربط الكثير من الفقهاء بين الإيديولوجية الثورية وبين الإرهاب ربطاً وثيقاً رغم اختلافهم في درجة العنف الذي بمقتضاه تؤول الثورة إلى إرهاب، والمذهب السائد في ذلك يرى أن كل ثورة تحمل في طياتها تهديداً بحرب أهلية تعتبر من قبيل الجرائم الإرهابية⁽¹⁾.

ولعل من أهم الأمثلة المتعلقة بالإرهاب الإيديولوجي تلك الجرائم التي نتجت عن الإرهاب الثوري الشيوعي في روسيا القيصرية إبان ثورة البلاشفة والتي تدعى بالإرهاب الأحمر⁽²⁾، وإرهاب الخمير الأحمر في كمبوديا والذي كان أسوأ أنواع القهر الإنساني ضد الشعب⁽³⁾.

كما تتصف الكثير من التنظيمات الانفصالية العنيفة في بعض الدول كتنظيمات إرهابية خطيرة، وعلى رأسها حركة (الباسك) الانفصالية والتي يطلق عليها اسم (إيتا)⁽⁴⁾، والتي تتادي بالانفصال عن إسبانيا مدعية تعرض الشعب الذي تمثله للقمع والعنف ومحاولة طمس الهوية، ويعتبر هذا التنظيم من أعنف التنظيمات الإرهابية في أوروبا⁽⁵⁾.

وتثير الإيديولوجية الثورية للإعمال الإرهابية إشكالية كبيرة في الشرعية، تمخض عنها تباين للمواقف وتناقض في الآراء، ولعل الثورة السورية تعتبر من أهم هذه الثورات التي تلتبس فيها المفاهيم وتتعدد حيالها المواقف، فهي من وجهة نظر بعض الدول ثورة مشروعة تستمد شرعيتها من الدفاع الشرعي عن النفس الذي تقره كل القوانين الدولية، بينما تراها دول أخرى إرهاباً يفترض محاربته واجتثاثه⁽⁶⁾.

وهذا الوضع ينطبق أيضاً على جبهة البوليساريو في الصحراء الغربية، وحزب العمال الكردستاني في تركيا، فهناك مزج بين المفاهيم، وازدواجية في المعايير، وعدم القدرة على التزام الحيادية وقواعد العدل والإنصاف في التعامل مع الكثير من القضايا الدولية ولاسيما تلك التي تدور

(¹) عودة يوسف سلمان الموسوي، جريمة استهداف إثارة الحرب الأهلية عبر الإعلام: (دراسة مقارنة)، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2018، ص ص: 61-63.

(²) ألكسندر سولجيتسين، أرخبيل غولاغ، ترجمة (نجم سلمان الحجار)، دار علاء الدين ودار ومؤسسة رسلان، دمشق، سوريا، 2017، ص 210.

(³) دفيد كين، المرجع السابق، ص 172.

(⁴) منظمة إيتا: منظمة منشقة عن جماعة أكين، تأسست في 31 يوليو 1959 بإقليم الباسك في إسبانيا، اعتمد الكفاح المسلح في الدفاع الهوية الباسكية، ومعادة الإسبان، أعلنت المنظمة التوقيف النهائي لنشاطها المسلح في 20 أكتوبر 2011، وفي 17 مارس 2017 أعلنت إلقاء سلاحها بشكل نهائي من جانب

واحد ودون قيد أو شرط (موقع ويكيبيديا). <https://ar.wikipedia.org/wiki/%D8%A5%D9%8A%D8%AA%D8%A7>

(⁵) فرغلي على تسن هريدي، هذا هو الإرهاب: (دراسة في محاكم التفتيش قديماً وحديثاً)، الطبعة الأولى، دار روابط للنشر وتقنية المعلومات، القاهرة، مصر، 2018، ص 205.

(⁶) أنظر: عماد الدين الجبوري، الفكر الإسلامي بين النظرية والواقع، الطبعة الثانية، " E-Kutub Ltd " للنشر، لندن، إنجلترا، يوليو 2015، ص ص: 182-185.

حول حمى الإرهاب، وقد نقل لنا نعوم تشومسكي كلمات رائعة لوصف هذه الازدواجية فقال: (...إرهابهم ضدنا وضد من يوالينا هو الشر المطلق، بينما إرهابنا ضدهم غير موجود -و في حالة ما إذا وجد، فهو ملائم تماما...) (1).

2- الإيديولوجية العنصرية:

إن العنصرية من بين أهم الإيديولوجيات التي يعبر عنها عادة بالاتجاه إلى التطرف العنيف، وهذا كما حدث بالأقليات التي منحت لها السلطات الألمانية بعض الامتيازات التي لم ترق لبقية فئات المجتمع الألماني (2)، وأيضاً كما قام النظام النازي بقيادة هتلر في ألمانيا أيضاً بارتكاب أفظع صور الإرهاب بشاعة ضد الأقليات اليهودية والعجرية في أوروبا بدوافع عنصرية، تلك العنصرية التي لاحت بوادرها الأولى من خلال السياسية التشريعية المناهضة لليهود التي ظهرت من خلال مجموعة من القوانين سيمت بقوانين نورمبرغ، التي ألغت صفة المواطنة عن اليهود، إذ تنص المادة الثانية من قانون الرايخ على: (راعي الدولة والدم الألماني هو الوحيد الذي يكتسب صفة مواطنة الرايخ، والذي ظهر من سلوكه أنه لديه الإرادة والقدرة لخدمة الشعب والرايخ الألماني بكل ولاء) (3).

كما قامت بحضر التزاوج مع اليهود من خلال قانون حماية الدم والشرف الألماني إذ نصت المادة الأولى: (تعتبر الزيجات بين اليهود ومواطني الدم الألماني محظورة، وكل العقود المبرمة لغم هذا الحضر تعتبر باطلة، حتى ولو تم إبرامها في الخارج للتحايل على هذا القانون) (4).

لقد أفضت السياسية العنصرية النازية إلى ارتكاب إبادة جماعية في حق اليهود والعجور من خلال محرقة الهولوكوست الشهيرة، ولقد انطلق هتلر في عنصريته تلك من معاداته للسامية واعتقاده بسمو الجنس الآري (5)، ويظهر ذلك جلياً من خلال كتابه الشهير "كفاحي"، والذي ينص فيه صراحة على خسارة ووضاعة الأجناس الأخرى مقابلة مع الجنس الآري فيقول: (... من عبره أن امتزاج دم الآري بدم شعوب وضيعة قد أدى دائماً إلى خراب الشعب ذي الرسالة

(1) نعوم تشومسكي، الدولة الفاشية: (إساءة استعمال القوة والتعدي على الديمقراطية)، ترجمة: (سامي الكعكي)، دار الكتاب العربي، لبنان، 2007، ص 11.

(2) نسيم بلهول، التطرف الديني: (رؤى دينية أمنية وسياسية)، الطبعة الأولى، أمواج للطباعة والنشر والتوزيع، عمان، الأردن، 2014، ص 197.

(3) قانون جنسية الرايخ المؤرخ بتاريخ 15 سبتمبر 1935.

(4) قانون حماية الدم والشرف الألماني المؤرخ بتاريخ 15 سبتمبر 1935.

(5) ماجد مورييس إبراهيم، الإرهابي: (شهوة الدم ولغز الانتحار)، الطبعة الأولى، دار النهضة العربية، بيروت، لبنان، 2018، ص 102.

التمدينية...) (1)، ويقول عن اليهود: (و لكن قذارتهم المادية ليست شيئا مذكورا بالنسبة إلى قذارة نفوسهم، فقد اكتشفت مع الأيام أن ما من فعل مغاير للأخلاق وما من جريمة بحق المجتمع إلا ولليهود فيها يد...) (2).

وفكرة معادة السامية هذه، هي نفسها الإيديولوجية التي كونت في ما بعد إرهابا جديدا قاداته المنظمة الصهيونية في فلسطين، لقد مثلت تلك الإيديولوجية، المادة الأولى التي تمكنت بها من تمرير مشروعها القومي في فلسطين، واركتبت تحت غطاءها أبشع الجرائم الإرهابية في الشعب الفلسطيني، وهذا عن طريق إقناع الأوساط اليهودية بالهجرة إليها فرار من اللاسامية المنتشر في أوروبا، وعملت منذ نهاية الحرب العالمية الثانية على تصوير تلك المعادة على أنها ظاهرة سياسية واجتماعية عالمية، فاختلط الأمر بينها وبين معادة الصهيونية باعتبارها منظمة إرهابية، حتى وصل الالتباس إلى الساحة التشريعية الدولية الأمر الذي ترتب عنه إلغاء الجمعية العامة للأمم المتحدة لقرارها رقم 3379 الذي يعتبر الصهيونية شكل من أشكال العنصرية (3).

وتبعا لهذه العنصرية المتوارثة بين النازية والصهيونية نشأت دولة إسرائيل، التي لا تزال تمشي على نفس خط المسير العنصري الذي رسمته الصهيونية، خط بلغ مداه بتشريعات وقوانين تركز العنصرية، مانحة له السند الشرعي للممارسات السابقة واللاحقة التي يرتكبها اليمين الإسرائيلي (4).

وفي العصر الحديث انتقلت العنصرية وخطاب الكراهية إلى ساحة الفضاء الإلكتروني، وظهر معها مصطلح " العنصرية السيبرانية " " cyber-racim " والذي يمكن تعريفه على أنه مصطلح يستخدم للنقاط ظاهرة العنصرية على الإنترنت، ويشمل المصطلح الخطاب العنصري الذي يتم توزيعه من خلال الوسائط التي يتيحها الكمبيوتر، وأول من صاغ هذا المصطلح هو

(1) أدولف هتلر، كفاحي، ترجمة: (لويس الحاج)، الطبعة الثانية، منشورات بيسان، (د.م.ن)، 1995، ص 162.

(2) المرجع نفسه، ص 19.

(3) عزمي بشارة، أصبح أن معادة الصهيونية هي أحد الأشكال الحديثة لمعاداة السامية، المركز العربي للأبحاث ودراسة السياسات، 28 فبراير 2019، تم الاطلاع عليه بتاريخ 18 أكتوبر 2019 على الساعة 18:05 سا، في موقع:

<https://www.dohainstitute.org/ar/PoliticalStudies/Pages/Is-Anti-Zionism-a-Form-of-Anti-Semitism-Anti-Zionism-as-a-Jewish-Phenomenon.aspx>

(4) عزمي بشارة، قانون القومية: (كم مرة سوف يعلنون قيام إسرائيل)، المركز العربي للأبحاث ودراسة السياسات، 24 يوليو 2018، تم الاطلاع عليه بتاريخ 18 أكتوبر 2019 على الساعة 18:20 سا، في الموقع:

<https://www.dohainstitute.org/ar/PoliticalStudies/Pages/Israel-Nation-State-Law-Repeatedly-Declaring-State.aspx>

ليس باك " Les Back " ⁽¹⁾ سنة 2002، وتتجلى العنصرية الإلكترونية في عدة أشكال إذ يمكن أن تتخذ شكل النكات أو التعليقات التي تسبب الإساءة أو الأذى، أو الشتائم أو الإساءة اللفظية، أو المضايقة أو التخويف، أو التعليق العام الذي يوجج العداء تجاه مجموعات معينة ⁽²⁾.

لقد كان لكل هذه التغيرات والتبدلات الحاسمة والحرجة في كل من التكنولوجيا والسياسة الدور الرئيس في نمو خطاب الكراهية يتيح الويب إمكانية الإنشاء الفوري تقريباً لشبكات الترابط، في حين أن عزل الجناة وإخفائهم المحتمل يحميهم من المساءلة ⁽³⁾.

ولا شك حينها في أن هذه العنصرية وخطاب الكراهية الذي أخذ في التوسع والنشاط على نطاق عابر للحدود من خلال الفضاء السيبراني الذي يجمع في ساحته كل الأجناس والأعراق والإثنيات أنه يشكل سببا مهما ومحوريا في ممارسة أشكال التطرف الإلكتروني وإرهاب الآخر من خلال تنفيذ هجمات سيبرانية سواء أكان استباقية تستهدف ضحايا التمييز العنصري أو دفاعية ينفذها المعتدى عليهم بخطابات الكراهية والتمييز، وفي كل الأحوال، إذا كان الباحثون والدارسون وكبار المفكرين قد أجمعوا كلهم على أن هناك علاقة وطيدة بين الإرهاب والتمييز العنصري وخطاب الكراهية، فنحن نرى أنه ما من مانع يحول دون إطلاق تسمية الإرهاب العنصري السيبراني على أشكال الإرهاب السيبراني الذي تغذيه دوافع ودوافع عنصرية.

وقد أعربت الجمعية العامة للأمم المتحدة عن قلقها إزاء ازدياد لجوء تلك الجماعات والأفراد الذين يعتقدون إيديولوجيات الكراهية على شبكة الإنترنت من أجل نشر الأفكار القائمة على التفوق العنصري أو الكراهية العنصرية، وتنظيم الاجتماعات والاحتجاجات وجمع الأموال، وغيرهما من النشاطات، كما أكدت بشدة في بندها 43 على التوصية التي قدمها المقرر الخاص إلى الجمعية العامة في دورتها الرابعة والستين التي تؤكد فيها أهمية تدريس التاريخ في التعريف بالأحداث المأسوية والمعاناة البشرية التي نشأت عن اعتماد إيديولوجيات من قبيل النازية والفاشية ⁽⁴⁾.

⁽¹⁾ ليس باك (les Back): أستاذ علم الاجتماع بجامعة جولدسميث بجامعة لندن ومؤلف

⁽²⁾ الموسوعة الحرة، ويكيبيديا: cyber racism:

https://en.wikipedia.org/wiki/Cyber_racism#cite_note-6

⁽³⁾ Andrew JAKUBOWICZ, Kevin DUNN, Gail MASON, Yin PARADIES, Ana-Maria BLIUC, Nasya BAHFEN, Andre ONOLER, Rosalie ATIE, Karen CONNELLY, Cyber Racism and Community Resilience: (Strategies for Combating Online Race Hate), Switzerland, 2007, P.(V)

⁽⁴⁾ أنظر؛ قرار الجمعية العامة للأمم المتحدة رقم 157/73 المتعلق بمحاربة تمجيد النازية والنازية الجديدة والممارسات الأخرى التي تساهم في

إثارة الأشكال المعاصرة من العنصرية والتمييز العنصري وكراهية الأجانب وما يتصل بذلك من تعصب، المؤرخ بتاريخ 17 ديسمبر 2018:

<https://daccess-ods.un.org/TMP/7539337.87345886.html>

ثانيا: التطرف العقائدي:

إن العقائد الدينية في أصلها تعتبر رمزا للسلام والوئام والتعايش، مرتكزة على نبذ العنف والتطرف والقسوة، غير أن بعض أتباعها أخرجوها من أصلها، واتخذوها شعارا للارتكاب الأعمال الإرهابية، فالاختلافات الدينية والمذهبية تشكل سببا جوهريا في الأنشطة الإرهابية بحيث تقوم الأغلبية باضطهاد الأقليات الدينية والتي بدورها تشكل جماعات إرهابية دفاعية من أجل حماية نفسها والذب عن عقيدتها (1).

تروى لنا كتب التاريخ أيضا قصة الفيلسوفة المصرية هاييتايا التي كانت تحمل مبادئ الفكر الأفلاطوني والتي راحت ضحية التعصب وإرهاب الجهل، حيث أضمرت الكنيسة لها الشر بسبب أنها بقيت على الديانة اليونانية القديمة، وأنها صورة من الفلسفة المرتبطة في تلك المرحلة بالوثنية، وأنها كانت السبب في الخلافات التي تقع بين المسيحيين وأعدائهم كونها مقربة من حاكم المدينة، فتم جرّها إلى الكنيسة وتجريدها من ملابسها ورجمها بالقرميد حتى توفيت وعمدوا بعدها إلى تقطيع جسدها (2).

يشكل الإرهاب الذي يمارسه الجيش والأمن الميانماري ضد الأقلية الهورنغارية (3) المسلمة في إقليم أراكان مظهر معاصرا من مظاهر الإرهاب الغاشم الذي تقف وراءه البواعث الدينية، ففي الثالث من شهر يونيو 2012 قام الجيش الميانماري بقتل 11 مسلما في طريق عودتهم من العمرة، الأمر الذي تجاوب معه مسلمي إقليم أراكان بسلسلة من الاحتجاجات العنيفة التي راح ضحيتها عشرون ألف مسلم حسب الإحصائيات الرسمية، ثم انطلقت بعدها سلسلة من الأعمال الإرهابية الوحشية ضد مسلمي الهورينغا حيث بلغت قسوتها حدا لا يقبل الوصف (4).

وعلى أثر ذلك أعربت الجمعية العامة للأمم المتحدة في دورتها الثالثة والسبعون، عن قلقها الشديد عما يحدث من انتهاكات جسيمة وممنهجة لحقوق الإنسان، وتجاوزات واسعة النطاق من

(1) ميلود ولد الصديق، المرجع السابق، ص 194.

(2) على عبود المحمداوي، الفلسفة والإرهاب أو في سلم السؤال وعنف الجواب: (سرد في الجريمة المنظمة ضد العقل)، الطبعة الأولى، دار ومكتبة عدنان، بغداد، 2016، ص ص: 78-81.

(3) روهينجا أو هورينغا: هو اسم لقومية عرقية تنتمي إلى عائلة الشعوب الهندية، وتنتشر في مقاطعة أركان غربي ميانمار (بورما سابقا)، يبلغ عددهم 800 ألف روهينجي، وينحدرون من دولة بنغلاديش، وهم شعب مسلم على مذهب أهل السنة (ويكيبيديا).

- <https://ar.wikipedia.org/wiki/%D8%B1%D9%88%D9%87%D9%8A%D9%86%D8%BA%D9%8A%D8%A7>

(4) أحمد موسى بدوي، الإبادة في بورما: (حين يتحول المسلمون إلى قرابين للعنصرية)، المركز العربي للبحوث والدراسات، 13 يوليو 2015، تم الاطلاع عليه بتاريخ 20 أكتوبر 2019 على الساعة 19:43 سا، في الموقع: <http://www.acrseg.org/39187>

عمليات للإعدام خارج إطار القانون واغتصاب وغيرها من أشكال العنف الجنسي والجسدي والاحتجاز التعسفي والاختفاء القسري، ونزوح سبعمائة وثلاث وعشرون ألف مسلم إلى بنغلادش مما ينبأ عن كارثة إنسانية حقيقية، وقد شددت الجمعية العامة في قرارها بالإلحاح على الحكومة الميانمارية بوقف كل تحريض على الكراهية ضد المسلمين الروهينغيا، والقضاء على ظاهرة انعدام الجنسية، وإتاحة كامل الإمكانيات لوصول المساعدات الإنسانية، ومحاسبة المسؤولين عن تلك الجرائم مع الإقرار بحق العودة الآمنة والطوعية والكرامة والمستديمة للاجئين، ودعوة الحكومة الميانمارية للوفاء بالتزاماتها وتعهداتها الدولية في مجال حقوق الإنسان المكفولة للجميع في ميانمار، بما في ذلك المسلمين الهوينغيا والمنتمين إلى الأقليات الأخرى⁽¹⁾.

وانتشرت بنفس الحدة أيضا جماعات إسلامية متطرفة - والتي تمثل الدولة الإسلامية في العراق والشام أبرزها- والتي اتخذت من الدين مطية لعنفها، مستخدمة نصوصا دينية إسلامية إنقائية لخدمة مصالحها المعاصرة، محاولة إنزال أحكام وفتاوى فقهية على النوازل والمتغيرات المعاصرة بصرف النظر عن الشروط التاريخية التي كانت وراء إنتاجها، لقد حولوا الدين ومقاصده إلى إيديولوجية موجهة للممارسة، إذ لا يكفي التعاطي مع الإسلام بوصفه ديناً، بل يتعاملون معه على أساس أنه إيديولوجية موجهة للعمل السياسي⁽²⁾.

فالإسلام في نظر تلك الجماعات ليس ذاك الدين الذي ينظم علاقة العبد بربه، وعلاقة الأفراد بعضهم البعض في جوانبها الخلقية، بل هو نظام سياسي يفرض نفسه على المجتمع المسلم، والخطر في الأمر، أنهم يصورونه على أنه نهج سياسي جامد، غير قابل للتطوير والتماشي مع متطلبات العصر، ولا يمكن أن يتبدل زمكانيا، وهذا هو عين الخطر، وهو مضمون وجوه التصادم المولد للإرهاب، لأنه ورغم وجود الكثير من جماعات الإسلام السياسي إلا أنها في غالبيتها لا تميل إلى استخدام العنف والإرهاب، ذلك لأنها تعتقد أن الجانب السياسي في الإسلام هو جانب مرن، يتغير حسب الزمان والمكان، وحسب مقتضيات العصر، وهذا ما ترفضه الجماعات الأصولية المتشددة.

(¹) أنظر؛ قرار الجمعية العامة للأمم المتحدة رقم 264/73 المتعلق بحالة حقوق الإنسان في ميانمار، المؤرخ بتاريخ 22 ديسمبر 2018:

<https://daccess-ods.un.org/TMP/4260596.63295746.html>

(²) عزامي بشارة، تنظيم الدولة المكنى "داعش": (أطار عام ومساهمة نقدية في فهم الظاهرة)، المركز العربي للأبحاث ودراسة السياسات، تم الاطلاع عليه بتاريخ 22 ديسمبر 2019 على الساعة 19:23 سا، في الموقع:

<https://siyasatarabiya.dohainstitute.org/ar/issue035/Pages/art01.aspx>

وتقوم هذه الجماعات في عمومها على فكرة كفر المجتمع وتحريم التفاعل مع مؤسساته، وجواز الخروج على ولاية الأمور لكفرهم أو فسقهم أو باعتبارهم طواغيت، كما تقوم أيضا على فكرة إلزامية التعامل مع هذا الواقع الاجتماعي وتغييره بالغضب والقوة، فضلا عن التعامل بنوع من السطحية مع بعض المفاهيم الإسلامية الذي يمثل الأمر بالمعروف والنهي عن المنكر أبرزها، ويقوم أيضا على تبني فكرة العداة لكل مكون اجتماعي غير مسلم يتهم في نظرهم بالولاء للذين يعادونهم، كما أن سرية أعمال ونشاطات بعض الجماعات يعد حاضنا للفكر التثويري والإنقلابي وتعطي انطبعا بالتعرض للاضطهاد⁽¹⁾.

وهذه الأفكار بشكل عام لا تصور إلا جانبا من جوانب الفكر الإرهابي في العالم الإسلامي، وهو الإرهاب على المستوى الداخلي أو الإقليمي، وبمعنى أدق، الإرهاب الذي يكون ناطقة الجغرافي محدودا بالعالم الإسلامي فحسب، أما الفكر الإرهابي في العالم الإسلامي الذي يمس المجتمع الدولي ككل فالأفكار التي تتبني عليها كثيرة.

وقد نقل برنارد لويس نظرية في تفسرا يسير في هذا المنحنى، فهو يرى أن الإرهاب في المجتمع المسلم آت من ازدواجية المشاعر نحو الحضارة الغربية، بين الإعجاب بها وبين الحقد عليها، والذي يرجع إلى تراجع المسلمين وتخرفهم وعجزهم عن دخول الحداثة، فالأصولية المعاصرة التي تعادي الغرب بشكل عام آتية في جذورها من الغضب والخيبة وعدم القدرة على التعاطي مع القيم التي تفرضها الحداثة والديمقراطية، والحركة الثورية المعاصرة قد أنتت من مشاعر الإذلال التي سيطرت على المسلمين الذين اعتادوا فكرة أنهم حراس العقيدة وحاملو لواء دعوة الكفار إلى الدين، ثم تجد نفسها إما تحت سيطرة هؤلاء الكفار أو تحت تأثيرهم، بالإضافة إلى الإذلال تجد هناك الإحباط الذي ساد من عدم توافق النماذج المستوردة لتحسن أوضاع الشعوب الإسلامية، وبعد الإذلال والإحباط أنتت العزة بالنفس التي تشكلت خلال أزمة النفط⁽²⁾.

ولا يعتبر التطرف والتنطع والقراءات المتشددة للأديان فقط من تكون سببا لممارسة الإرهاب، بل قد يكون بين أتباع الدين الواحد، فعلى هذا النمط انتشر الإرهاب الطائفي بين السنة والشيعة، حيث تمارس السلطات الإيرانية نوعا من الإرهاب القهري على أتباع المذهب السني من خلال ممارسة كل أنواع القهر على رموزهم ومنعهم من التنقل بحرية داخل الأراضي الإيرانية، كما منعت أيضا بناء

(¹) أبو العلا ماضي، جماعات العنف المصرية وتأويلاتها للإسلام: (الجذور التاريخية-الأسس الفكرية-المراجعات)، الطبعة الأولى، مكتبة الشروق الدولية، القاهرة، 2006، ص ص: 41-44.

(²) نقلا عن: معتز الخطيب، المرجع السابق، ص ص: 150-151.

مساجدهم أو تجديدها، وقد هدمت آخر مسجد لأتباع المذهب السني في طهران متذرعة بأسباب إدارية⁽¹⁾، كما يحدث أيضا ذلك للشيعة في المملكة العربية السعودية عبر التحريض على الكراهية باستخدام الألفاظ المهينة محتقرين عقائدهم وممارساتهم، من خلال نعتهم بأوصاف مبتذلة⁽²⁾.

لقد كانت محاكم التفتيش الدينية التي نشأت في أوروبا، من بين أقسى مظاهر الإرهاب القائم التطرف الطائفي بين أتباع الدين الواحد، حيث نسبت الكنيسة الرومانية إلى كل مخالفاتها تهمة الهرطقة والارتداد عن المسيحية الصحيحة، الأمر الذي دعاها إلى الاعتقاد بضرورة اتخاذ أساليب العنف وأشكاله بما في ذلك التعذيب الجسدي والقتل لردعهم، فقد تعرض أتباع المذاهب المسيحية المخالفة لمذهب الروم الكاثوليك إلى كل أصناف التعذيب والحرق والتقتيل بتهمة الهرطقة أو الردة⁽³⁾، الأمر الذي قابلته تلك الطوائف بعنف مماثل دافعا عن نفسها، وأشهر تلك الممارسات الإرهابية كانت بينها وبين الكنيسة البروتستانتية، والتي تعود أصولها إلى الحركة الإصلاحية التي قامت في أوروبا والتي تدعو إلى التجديد داخل الكنيسة الرومانية والتي قادها مارتن لوثر⁽⁴⁾.

ولما علم لدينا من خلال ما تقدم ذكره، بأن التطرف المذهبي يشكل الشرارة الأولى والدافع الجوهري للكثير من الهجمات والتهديدات الإرهابية فإن ذلك سيساق حتما على الهجمات الإلكترونية التي تستهدف أهدافها بناء على الانتماءات الدينية والمذهبية، فالتطرف المذهبي والديني يعد سببا من أسباب التهديد الإلكتروني، وهناك الكثير من الشواهد على ذلك، ففي يناير 2015 شنت جهات إسلامية متطرفة هجمات على مواقع إلكترونية مسيحية على خلفية أزمة تشارلي هيبود⁽⁵⁾.

وفي هجمة فيروس الفدية الخبيثة على الهند في 2017 وجد 10 من أجهزة الحاسب الآلي في معبد تيروباتي متأثرة بهذا الفيروس، كما تعرضت أيضا كنيسة لامونت المسيحية في كوبرسفيل بكندا إلى تشويه لموقع الويب التابع لها عندما تم اختراقها من قبل مجموعة تدعي أنها الخلافة الإلكترونية المتحدة⁽⁶⁾.

(1) محمد السيد الصياد، أهل السنة في إيران: (دراسة في التأسيسات الإيديولوجية والسياسية المذهبية تجاه أهل السنة)، المعهد الدولي للدراسات الإيرانية، الرياض، 1440 هجري، ص ص: 12-13: <https://rasanah-iiis.org/> مركز الدراسات والبحوث/أهل السنة-في إيران/

(2) أنظر؛ آدم مايدة، ليسوا إخواننا: (خطاب الكراهية الصادر عن المسؤولين السعوديين)، مقال منشور على الموقع العربي لهيومن رابنس واتش، 26 سبتمبر 2017، تم الاطلاع عليه بتاريخ 19 ديسمبر 2019 على الساعة 23:25، في الموقع: <https://www.hrw.org/ar/report/2017/09/26/309427>

(3) بسام اسخطة، قصة محاكم التفتيش في العالم، الطبعة الأولى، دار هيا للنشر والتوزيع، دمشق، 2000، ص 20.

(4) ويكيبيديا، بروتستانتية، الموسوعة الحرة: <https://ar.m.wikipedia.org/wiki/> بروتستانتية

(5) see: Rédaction 7seizh.info, Nantes / Cyber-guerre islamique : les hackers s'attaquent aux sites chrétiens, publier le 10 janvier 2015, vu le 02/11/2020 à 00:55 sur le site: <http://7seizh.info/2015/01/10/cyber-guerre-islamique-les-hackers-sattaquent-aux-sites-chretiens/>

(6) Are religious organizations at risk of being hacked? Seven steps you can take to battle cyber crime, October 1, 2018, Accessed in 24/11/2020 At 22:21 in: <https://blog.24by7security.com/are-religious-organizations-at-risk-of-being-hacked-seven-steps-you-can-take-to-battle-cyber-crime>

وفي تحليل أجره بلقاسم شابي لجدول توزيع مؤشرات الغلو على فئات التحليل لموقع البوارق يظهر من خلاله التوظيف الإرهابي والتطرفي للمواقع الإلكترونية، فقد أشار الباحث إلى وجود نسبة تتجاوز الثلثين من وقائع الموقع المذكور يظهر فيها العنف العملي، ونصفه يتضمن بين ثنياء أفكار العنف والتكفير، وربع الفتاوى فيه تحمل طابع العنف العلمي، وحتى الأناشيد فيه تتذبذب بين الغلو والتعصب وبين سمات العنف العلمي بنسبة كبيرة (1).

وهذه العينة التي تم تحليلها إنما هي غيض من فيض وحة رمل في صحراء، فالكثير من المواقع الإلكترونية بما في ذلك مواقع التواصل الاجتماعي فيها ويلات وطامات جسام، إذ تتضمن غلوا صارخا وتتطعا شديدا كأقل مظهر فيها، وتصل في الكثير من الأحيان إلى دعوات للقتل والتجنيد للإرهابيين فضلا عن استعمالها في الدعاية والترويج للأعمال الإرهابية.

الفرع الرابع: الأسباب التقنية والفنية:

إن ما يميز أسباب الإرهاب الإلكتروني عن الإرهاب التقليدي هي الساحة التي يوظف فيها أهدافه، فهي ساحة عالمية هشة وضعيفة يغلب عليها طابع الخفاء في هوية المتعاملين فيها، وغياب الأثر المادي في الكشف والتحري عما يقع فيها (أولا) كما أن الساحة التي يتم النشاط فيها بالأعمال الإرهابية تعتبر ساحة تعوزها الرقابة ويشوبها القصور الفني في متابعة تحدياتها ومستجداتها (ثانيا).

أولا: الأسباب التقنية:

1- هشاشة أنظمة المعلومات وضعفها:

إن التكنولوجيا المعلوماتية وتقنيات المعلومات صممت أنظمتها بشكل يتناسب مع الدخول المفتوح إليها بيسر وسهولة، بحيث تمكن الأفراد من الاستغلال الأمثل والأنجع للمزايا والخدمات التي تقدمها، فلا قيود ولا حواجز أمنية تضبطها، والنظم المعلوماتية هي نظم يشوبها وجود ضعف وثغرات أمنية في بنيتها، تمكن الإرهابيين اختراقها والتسلل من خلالها للوصول إلى قواعد البيانات الحيوية والبنية التحتية وارتكاب أعمال إرهابية وتخريبية (2).

(1) بلقاسم شابي، النزوع إلى المغالاة في الممارسات الدينية عبر المواقع الإلكترونية الإسلامية: موقع البراق ومنبر التوحيد والجهاد أنموذجا، مجلة التواصل، المجلد 21، العدد 04، جامعة باجي مختار، عنابة، الجزائر، ديسمبر 2015 ص: 205-219.

<https://www.asjp.cerist.dz/en/article/41673>

(2) عنتر بن مرزوق، جريمة الإرهاب الإلكتروني: (الأسباب وآليات العلاج)، مجلة الحقوق والعلوم الإنسانية، المجلد 11 العدد 02، جامعة زياد عشور، الجلفة، الجزائر، جوان 2018، ص: 509-520.

<https://www.asjp.cerist.dz/en/article/53266>

وهذه الثغرات الأمنية في أنظمة المعلومات تعتبر مصدر قلق كبير لجميع قطاعات البنى التحتية التي تعتمد اعتمادا كبيرا على شبكات الإنترنت التي سطرت لتكون متاحة للجمهور بشكل واسع النطاق، فقواعد البيانات ووحدات تخزين المعلومات، لا سيما تلك التي تتسم بالحساسية والحر، قد أصبحت عرضة لتهديد وخطر الهجمات الإرهابية والقرصنة⁽¹⁾.

إن من أهم مظاهر الهشاشة والضعف في أنظمة المعلومات تلك التي تتجلى بصفة خاصة في أنظمة التشغيل والبرامج الملحقة به، ففي كل يوم يتم تحديد مظاهر جديدة من مظاهر الضعف في الأنظمة، ولا يكاد يخلو نظام من ثغرات تهدده، وأغلب هذه الثغرات تعود إلى الشركات المصنعة نفسها أو إلى القرصنة⁽²⁾.

إن التطور التكنولوجي المهل الذي عرفه العالم في الحصر الحديث، أحدث تغيرات جذرية في المفاهيم الاستراتيجية المتعلقة بالحدود الجغرافية والإقليمية، وعلاقتها بالأمن القومي، فأصبح العالم كله قرية صغيرة، متخطيا بذلك كل القيود الجغرافية والسياسية، والأنظمة القانونية، فالعالمية التي يتسم بها الفضاء الإلكتروني قد وضع الدول أمام نموذج جديد من العلاقات التفاعلية في ما بينها، كما أنه وضع المنظمة القانونية والقضائية أمام هيكلية جديدة من الأسس غير التقليدية المبنية على الافتراضية التي يتلاشى معها الحيز الجغرافي، ورغم ما لهذه الخاصية التي يتمتع بها الفضاء الشبكي من خصائص إيجابية ومكاسب على الصعيد الإنساني والسياسي والاقتصادي، إلا أنه قد كَوّن معها مفاهيم جديدة متعلقة بالأمن والسلامة، وأنتج ساحة جديدة من ساحات الصراع الدولي، فتغير بموجبها مفهوم الحرب وكل المفاهيم القانونية المتعلقة بها، كما أفضت بالتبعية إلى نشوء أشكال جديدة من التهديدات والتحديات الأمنية التي يشكل الإرهاب الإلكتروني واحدة منها⁽³⁾.

وفي هذا الصدد يقول الدكتور بيرنارد رولاند⁽⁴⁾: (العواقب السلبية للعولمة الاقتصادية كثيرة خاصة منها الفقر وانعدام الأمان: الفقر الذي هو المصير وراء مشاكل التغذية والهجرة السكانية، إنعام الأمان المرتبط بانتشار الأسلحة الإرهاب الإلكتروني، التطرف والإرهاب)⁽⁵⁾.

(1) فريج بن سعيد العويضي، حروب تقنية المعلومات: (كيف يشنها القرصنة والإرهابيون على البنية التحتية العالمية؟ وكيفية مواجهتها؟)، الطبعة الأولى، دار العلوم العربية للنشر والإعلام، مصر، 2016، ص 42.

(2) Didier GODART, *sécurité informatique : (resèques, stratégiques et solutions)*, 2^{ème} Édition, éditions des Cci de wallonie SA, Belgique, 2005, P.33.

(3) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المرجع السابق، ص: 78-80.

(4) بيرنارد رولاند (Bernard Roland) 1938 فرنسا: مهندس ومتخصص في قانون العمل.

(5) Roland BERNARD, *La France, Son Passé Et Notre Avenir, mon petit Édition, Paris, France, 2010, P.209.*

إذا نحن بصدد الحديث عن تحديات جديدة تواجهها الدول على الصعيدين الداخلي والخارجي، من أجل الحفاظ على أمنها القومي ضد هجمات الإرهاب الإلكتروني، تحديات فرضتها عليها الظروف المصاحبة لعولمة الفضاء الإلكتروني وارتباط مؤسساتها به، فمستوى التهديدات التي تمس بالبنية التحتية لمؤسسات الدولة، والخطر الاستراتيجي الذي يزرع أمنها القومي، لم يعد مرتبطا بالحدود والنطاق الجغرافي، ولا ينقضي بتأمينها، إنما هو عالمي بعالمية حيز الفضاء الإلكتروني⁽¹⁾.

2- المجهولية والغفلية:

تعتبر المجهولية وإخفاء الهوية على الساحة السيبرانية آلية جديدة لضمان الحقوق الجوهرية للأفراد، ومظهرا حديثا من مظاهر الممارسة الآمنة لحرية الرأي والتعبير، في بيئة ديمقراطية تنقلص فيها المخاطر التي تهددهم، من اضطهاد وتكيل جراء تفاوت القوى، غير أن بعض الباحثين يرون أن إطلاق العنان للمجهولية على الفضاء السيبراني يشكل هواجس مقلقة وقد دعا للحد منها، كما يصفها البعض الآخر أيضا بأنها ممارسة خطيرة⁽²⁾.

إن أوجه الخطورة في المجهولية والغفلية عند استخدام الشبكة الإلكترونية تكمن في عجز أجهزة الأمن عن تتبع المجرمين المتورطين في الجرائم السيبرانية، فهي تشكل لهم الغطاء الحمائي الأمثل ضد الرقابة الأمنية، فالجرم الذي يأمن العقاب يسترسل حتما في الإجرام ويتفنن في ابتكار أساليبه، وعلى الرغم من وجود آليات فعالة نسبيا في الكشف عن هوية المتورطين في الإجرام الإلكتروني، إلا أن الضعف والثغرات الأمنية التي تشوب الفضاء الإلكتروني قد تحول دون بلوغ هذا الهدف⁽³⁾، فالإرهابي خلال هجماته الإلكترونية قد يلجأ إلى مناورات تكتيكية معتمدا على برمجيات عالية التقنية تمكنه بكل يسر وسهولة من تجاوز الرقابة والرصد الإلكتروني وبذلك الإفلات من المسائلة والعقاب.

يخلط بعض الدارسين بين المجهولية وبين الشخصية الوهمية التي تعتبر تزييفا للهوية. فرغم وحدة الهدف الذي يسعى إليه كل منهما، والذي يتمحور في إخفاء الهوية الحقيقية للمجرم، إلا أن ثمة خلاف بينهما من حيث طبيعة الجرائم التي تتعامل بها، فالمجهولية تكون في الجرائم التي لا

(1) عادل عبد الصادق، المرجع نفسه، ص 158

(2) لوري أندروز، أعرف من أنت ورأيت ماذا فعلت: (مواقع التواصل الاجتماعي وفقدان الخصوصية)، مكتبة العبيكان للنشر، الرياض، 2015، ص ص: 96-97.

(3) عبد القادر بن عبد الله الفتوخ، المرجع السابق، ص ص: 24-25.

تتطلب إبرازاً للهوية، بينما تكون الشخصية الوهمية في الجرائم التي تستلزم وجود هوية معينة وتتطلب تعريفاً بها⁽¹⁾، وطبيعة الإرهاب الإلكتروني تقتضي في كثير من الأحيان التعامل بهما معاً، إذ يمكن للإرهابي ألا يبرز أي هوية، كما يمكنه أن يتعامل بهوية وهمية خلال تنفيذه للهجمات الإرهابية الإلكترونية⁽²⁾.

3- صعوبة اكتشاف وإثبات الجريمة:

إن الكشف عن جريمة الإرهاب الإلكتروني وإثباتها يعتبر أمر بالغ الصعوبة، وهذا نظراً للعراقيل التقنية الكثيرة التي تقف أمام عملية الكشف والتحري، إذ يتم عادة الكشف عنها عن طريق الصدفة، شأنها شأن بقية أشكال الجريمة الإلكترونية، فالإرهاب الإلكتروني جريمة لا أثر مادي لها، فهي إذا جريمة خفية في سلوكياتها، إذ يمكن للإرهابي أن يخفي بسهولة أي هجوم يقوم به عن طريق التلاعب الرقمي بالبيانات، كما أنها جريمة خفية في أثرها، فهي لا تترك وراءها أي أثر مادي خارجي ملموس، وهذا ما يجعل عملية التحري عنها صعبة جداً، فطبيعة هذه الجريمة واتسامها بخاصية الخفاء تولد انجذاب الإرهابيين إليها أملاً في الأمن من العقاب والمسائلة⁽³⁾.

ثانياً: الأسباب الفنية:

1- غياب رصد اتجاهات المشاكل والحلول:

تعاني المؤسسات المنتجة للأنظمة والبرامج والتطبيقات من انعدام الأطر التخصصية في رصد المشاكل واقتراح الحلول، فهي في كثير من الأحيان تتربص بالبلاغات والشكاوى التي يتقدم بها المستخدمون في معرفة مواطن الخلل، ثم تعتمد بعد ذلك لإصلاحه، فهي في الحقيقة لا يتقدم نسخة جديدة للنظام أو التطبيق، بل تقوم بترقيع النسخة القديمة لحل المشكل المثار⁽⁴⁾.

يعتبر غير كافياً مطلقاً إصدار أنظمة أو تطبيقات موصوفة سلفاً بالأمانة لتكون حقاً كذلك، بل يجب على تلك المؤسسات المنتجة أن تخصص جزءاً من موظفيها من أجل متابعة التطورات المتعلقة بأمن الأنظمة وتركيب التحديثات التي من شأنها أن تسد الثغرات، كما يجب أن تكون تلك التحديثات غير متباعدة زمنياً، فالمؤسسات التي لا تزال تعتمد على النظام السنوي في التحديث

(1) عبد القادر بن عبد الله الفتوخ، المرجع السابق، ص 25.

(2) مصطفى يوسف كافي، الإدارة الإلكترونية: (إدارة بلا أوراق - إدارة بلا مكان - إدارة بلا زمان - إدارة بلا تنظيمات جامدة) المرجع السابق، ص 440.

(3) ثيان ناصر آل ثيان، إثبات الجريمة الإلكترونية: (دراسة تأصيلية تطبيقية)، رسالة ماجستير في السياسة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص ص: 24-27.

(4) Didier GODART, Op.cit. PP.132-133

تواجهها عدة مخاطر، فتباعد التحديثات يترك المجال الأمني مفتوحاً لشغرات ينفلت منها المخترقون والقراصنة إلى الأنظمة المعلوماتية⁽¹⁾.

ومن هنا وضعت المؤسسات المنتجة نظام التحديثات التلقائية، الذي تبرز أهميته عند معرفة الأخطاء الشائعة التي تشوب النظم والتطبيقات والبرامج، والتي ثبت خطرها يقيناً، إذ هي السبب الرئيس لوقوع الكثير من الهجمات على الأنظمة الإلكترونية، ولذلك تسعى الكثير من الشركات المنتجة إلى وضع تحديثات تلقائية لتعزيز جدار الحماية للأنظمة المعلوماتية، غير أن هذا النظام المتبع في تطبيق التحديثات مثيرة للقلق أيضاً، إذ أن بعض الأبحاث والمقالات قد أثبتت أن بها أثر كبير على أمن وسلامة المعلومات⁽²⁾.

2- غياب الاختبارات:

إن الدوافع التجارية والتنافسية بين الشركات المنتجة للبرامج والتطبيقات والنظم الإلكترونية، وكذلك ارتفاع تكلفة الفحوصات الأمنية، قد أثرت كثيراً على سلامتها حين اقتضب واختزل مدراء تلك المشاريع مرحلة الاختبارات الأمنية، حتى أن بعضهم ذهب مذهباً أكثر تراخياً من ذلك، إذ يعتقدون أن المستهلك هو ميدان التجربة، وأن المستهلكون هم من سيجرون الاختبارات لصالحهم، إن الاختبارات الضرورية للأمن الإلكتروني لا يجب أن تتمحور فقط على فحص مدى توفر الوظائف والخصائص المطلوبة، بل يجب أن تكون الاختبارات مبنية على مبدأ فحص المخاطر أيضاً، وهذا عن طريق إجراء تجارب سلبية بمحاولة القرصنة والتغلب على نظم الأمان، وذلك لتقرير مدى فعاليتها وكذلك على تقدير آجال التحديثات⁽³⁾.

إن محاكاة أساليب الهجوم الإلكتروني بإجراء مناورات أمنية إلكترونية من شأنه أن يعزز من تطوير أساليب درء الخطر، فمثل هذه التجارب المباشرة والاستثنائية ستفضي حتماً إلى معرفة مواطن الخلل والتيقن من مدى فعالية الأنظمة وصلابة آليات دفاعها ضد أي هجوم محتمل⁽⁴⁾.

⁽¹⁾ Didier GODART, Op.cit. P.133

⁽²⁾ خالد بين سليمان الغثير ومحمد بن عبد الله القحطاني، أمن المعلومات بلغة مبسرة، الطبعة الأولى، مركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، 2009، ص ص: 99-100.

⁽³⁾ Didier GODART, Ibid.. P.134

⁽⁴⁾ مصطفى يوسف كافي، الحكومة الإلكترونية: (في ظل الثورة العلمية والتكنولوجية المعاصرة)، دار ومؤسسة رسلان للطباعة والنشر والتوزيع، دمشق، سوريا، 2009، ص 161.

المبحث الثاني:

الإرهاب الإلكتروني: الهجمات والتداعيات

يعد الفضاء الإلكتروني الساحة التي يلجأ إليها الفاعلين من الدولي أو من غيرها بارتكاب أنشطة إرهابية نظرا لما يتسم به هذا الفضاء من سمات تخفي معالم الجريمة وتعطل العدالة وتحمي الجناة من المسائلة الجنائية، وقد عملت تلك الجهات على جعل البيئة الإلكترونية وسطا يحمل صورا متعددة من التهديدات الأمنية من خلال توظيف جملة من الأسلحة الإلكترونية المبتكرة ذات البعد التقني المعقد فيها، كما عملت أيضا على تهجين الخدمات التي يتيحها هذا الفضاء لتشكيل أسلحة فتاكة تهدد بها الأمن السيبراني عن طريق القيام بهجمات إلكترونية متعددة الأساليب ومتنوعة الأشكال والصور (المطلب الأول) حتى أصبح الفضاء الإلكتروني يشكل نوعا خطيرا من التهديدات التي تنصب خطورتها بشكل مخيف على الأمن القومي للدول وعلى بنيتها التحتية الحرجة خاصة في أوساط الدول التي يمثل فيها الوسط الإلكتروني مجالا حيويا واستراتيجيا، كما تبرز أيضا أشكال وصورة خطيرة من التهديدات التي تستهدف أمن وسلامة الأفراد والمجتمعات، وقد أتاح هذا الفضاء للإرهاب الإلكتروني أن يصبح ظاهرة عالمية تهدد طبيعة العلاقات الدولية (المطلب الثاني).

المطلب الأول:

هجمات الإرهاب الإلكتروني

تتمحور أولوية الفضاء الإلكتروني في تعزيز الرفاهية وتوفير الرخاء الإنساني، وتمكين الأفراد والمؤسسات من إدارة وتسيير شؤونها باليسر والسهولة مع ضمان الدقة والجودة، فكان أن تحول هذا الفضاء إلى مصدر قلق وتهديد للأمن والاستقرار بفعل استغلالها للأغراض إرهابية ومقاصد إجرامية من قبل الدول والأفراد والجماعات (الفرع الأول) فقد فتح مجالا واسعا لتوظيف خدماته دعم النشاط الإرهابي وتعزيز قوته والتمكين لبطشه وسطوته، كما تحول إلى ساحة تفعل فيه أسلحة مبتكرة تهدف إلى إحداث آثار مدمرة وإشعال فتيل صراعات وأزمات مروعة (الفرع الثاني) باللجوء إلى هجمات بأساليب متعددة وصورة متفرعة بهدف بسط النفوذ والسيطرة من جانب والترويع والتخويف من جانب آخر (الفرع الثالث).

الفرع الأول: مصادر الهجمات الإرهابية الإلكترونية:

إن التحولات الجوهرية التي أحدثتها التطور التكنولوجي الكبير قد أجبر الكثير من الدول على الخوض في مظهر جديد من مظاهر الصراع، وأصبحت توظف الإرهاب الإلكتروني كآلية لبسط النفوذ داخليا وخارجيا (أولا)، مما أفضى تبعا إلى تشكل تنظيمات وجماعات متطرفة تعمل بنفس النمط وعلى نفس السياق بالإضافة إلى دخول الأفراد هذا المعترك من خلال النشاط الإرهابي الانفرادي على الساحة السيبرانية (ثانيا).

أولا: إرهاب الدولة:

لم يرد أي إجماع تام بين الفقهاء والباحثين على الجزم بخوض الدولة غمار الإرهاب، وتورطها فيه بشكل أو بآخر، إذ شككوا في وجود إرهاب تمارسيه الدولة أو تقوده أو ترعاه، فهم يرون أن أي شكل من أشكال العنف الذي تمارسه الدول يدخل ضمن إطار العدوان المنصوص عليه في القوانين الدولية، لكن مجمل الآراء قد انصبت في الإقرار بوجوده واعتباره صورة من صور الإرهاب المجرم دوليا⁽¹⁾.

وهو الرأي الصحيح على أرجح الاحتمالات، فالتاريخ والواقع يقران على أن إرهاب الدولة هو الصورة الجوهرية والأساسية في الإرهاب المنظم، فالولايات المتحدة الأمريكية قد ارتكبت إرهابا فضيعا في حق الشعب الياباني من خلال إلقاء القنبلة الذرية على مدينة من مدنها، وقد أتهمت الولايات المتحدة الأمريكية أنها تنتصر وتأسس تاريخا جديدا لإرهاب الدولة⁽²⁾.

كما أشار نعوم تشومسكي الذي يعد حجة في دراسة الإرهاب في البيئة السياسية الأمريكية إلى إرهاب الدولة الذي دعمته أمريكا أثناء فترة الستينيات في أمريكا اللاتينية، وحرب ريغان على الإرهاب في فترة الثمانينيات في نفس المنطقة أيضا، فضلا عن التفجيرات في بيروت سنة 1985 والتي تشير الدلائل إلى تورط الولايات المتحدة الأمريكية وبريطانيا فيها، ودعم الهجوم الإسرائيلي لتونس العاصمة الذي أشادت به الولايات المتحدة وساندته، وكل هذه العمليات هي في حقيقتها إرهاب مساند ومؤيد من قبل الدولة⁽³⁾.

(1) زياد محمد السباعي ومجيد خضر السباعي، جريمة قتل الحسين وآل بين النبوة عليهم السلام: (رؤية معاصرة في القانون الجنائي الداخلي والخارجي)، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2018، ص 92.

(2) حسام أبو حامد، إرهاب الدولة ودولة الإرهاب، 6 نوفمبر 2019، تم الاطلاع عليه بتاريخ 28 نوفمبر 2019، على الساعة 23:41، في موقع: <https://blogs.aljazeera.net/blogs/2019/11/6/إرهاب-الدولة-ودولة-الإرهاب>

(3) نعوم تشومسكي، الهيمنة أم البقاء: (السعي الأمريكي إلى السيطرة على العالم)، ترجمة: (سامي الكعكي)، دار الكتاب العربي، لبنان، 2004، ص ص: 229-230.

وتورطت أيضا الحكومة السودانية والجيش السوداني في تأجيج نزاعات عرقية وقبلية في ما يعرف بأزمة دارفور سنة 2003، بالإضافة إلى ما جرى في روندا من جرائم فظيعة، ومجازر الهولوكوست التي قامت بها الحكومة النازية⁽¹⁾، ويمكن أيضا أن نشهد في هذا العصر صورا مخيفة ومرعبة من صور إرهاب الدولة كالتى نشاهدها يوميا من خلال القنوات الإخبارية أين تقوم الدولة السورية بإبادة جماعية للعزل من شعبها⁽²⁾.

إن ما يعزز الفكرة التي تجعل من الدولة أساسا للإرهاب هي ما تفضل به الأستاذ أحمد عطية الله⁽³⁾ الذي يرجع مصطلح الإرهاب نفسه إلى القمع الذي تعرض إليه المعارضين من الدولة إبان الثورة الفرنسية إذ يقول: (والإرهاب وسيلة تستخدمها حكومة الاستبداد لإرغام الشعب الخضوع والاستسلام لها، والمثال التقليدي هو قيام حكومة الإرهاب إبان الثورة الفرنسية عام 1892 لأغراض سياسية، والإرهاب وسيلة تتخذها دول تفرض سيادتها على شعب من الشعوب لإشاعة روح الانهزامية والرضوخ لمطالبها التعسفية)⁽⁴⁾.

فما حدث إبان الثورة الفرنسية من ممارسة الإرهاب ضد المعارضين، ودعم ذلك بجملة من القرارات والمراسم التي تشرعنه، وإنشاء المحاكم الاستثنائية التي احتكرت السلطة الحاكمة توظيف الإرهاب حال وجود ضرورة⁽⁵⁾ لهو خير دليل على أن هناك فعلا مسمى " إرهاب الدولة" وأن هناك فعلا ممارسة إرهابية للدولة.

وهذه الدولة الفرنسية التي عان شعبها من الإرهاب، قاد مارسه بعد ذلك بشكل رسمي وغير رسمي في الدول التي احتلتها، والتي تعتبر الجزائر أبرزها وأكثرها معاناة من الإرهاب الفرنسي، وقد أشار جاك فرجيس إلى عینتين بسيطتين من ذلك، أولهما تمثل الشكل غير الرسمي والمتجلية في

(1) جورج رينتز، العولمة: (نص أساس)، ترجمة: (السيد إمام)، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2015، ص: 345-346.

(2) ما من شك يساورني في اعتبار بشار الأسد نموذجا صرخا للإرهاب الدولة، فالحكومة السورية منذ ما يقارب تسع سنوات وهي تمارس أشنع أنواع الهمجية في شعبها، بداية من الاعتقالات التعسفية والإختفاءات القسرية، نهاية ببراميل الكيماوي والأسلحة المحرمة دوليا، ولا يمكن بحال من الأحوال تصوير حجم الدمار الذي حل بالشعب السوري جراء تعاقب عمليات القصف الجوي الذي يمارسه التحالف السوري الروسي الإيراني، بمشاركة ميليشيات حزب الله اللبناني، لقد أفنى بشار الأسد شعبه، فهو بين قتل وجريح ونازح ولاجئ ومكره على العيش تحت نظامه عنوة وقسرا، لقد دعمت جرائم نظام الأسد رأي إرهاب الدولة بما لا يقبل النقض، ولا يصمد أمامه أي مستوى من مستويات النقد.

(3) أحمد عطية الله 1983-1906 مدينة أسوان مصر: هو مؤرخ إسلامي أخذ تعليمه عن مدرسة المعلمين العليا ثم أوفد بعدها إلى إنجلترا للتخصص في علم النفس والفلسفة، تقلد العديد من المناصب منها مديرا للجامعة الشعبية ومديرا لإدارة النشر والثقافة بوزارة الإرشاد القومي ثم مراقبا عاما للصحافة وهو منشأ متحف التعليم، كان له العديد من المؤلفات أشهرها: القاموس السياسي، القاموس الإسلامي، أنظر الموسوعة الحرة:

- https://ar.wikipedia.org/wiki/%D8%A3%D8%AD%D9%85%D8%AF_%D8%B9%D8%B7%D9%8A%D8%A9_%D8%A7%D9%84%D9%84%D9%87

(4) أحمد عطية الله، المرجع السابق، ص 45.

(5) عبد القادر زهير النفوزي، المفهوم القانوني لجرائم الإرهاب الداخلي والدولي، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2008، ص 53.

بول أوسارس الذي قتل دون محاكمة بين سنتي 1955 و1957 آلاف الجزائريين، بالإضافة إلى 24 ألف سجين، وثانيهما هو الشكل الرسمي الذي يتجلى في أناتول ديبلر الذي ذبح بالمقصلة تنفيذاً لأحكام قضائية 396 شخصاً محكوماً عليهم بالإعدام⁽¹⁾.

كما أن الإرهاب أضحى الآلية التي يتم توظيفها واستغلالها في محاربة الدول لبعضها البعض من خلال دعم المنشقين وأصحاب المطامح السياسية والمغرضين، تقادياً للمواجهة المباشرة للخطر والمكلفة، وقد اعترفت المواثيق الدولية والإقليمية بهذا الشكل من الإرهاب حينما دعت على وضع إجراءات لمنع، وما عقد من اتفاقيات قاضية بموقف ما بين الدول من هكذا نشاط، ودعم المنظمات الإرهابية فيما بينها⁽²⁾. وخطورة هذا النوع من الإرهاب تتجلى بصفة خاصة في صورتين أساسيتين؛ أولهما أنه إرهاب تترتب عنه مآسي إنسانية وجرائم بشعة بحق الأفراد، وثانيهما أنه إرهاب يمكن شرعنته، بمعنى أنه إرهاب يمكن أن يكون تحت مظلة تشريعية قانونية، وهذا من خلال إصدار مختلف التشريعات والتنظيمات التي ترهب الأفراد بعقوبات شديدة من جهة، أو من خلال إطلاق العنان لصلاحيات الأجهزة الأمنية وإنشاء محاكم ثورية انتقامية⁽³⁾.

يذهب بعض الباحثين إلى الاعتقاد بأن أول إشارة لإرهاب الدولة بصفة قانونية كانت عام 1954 في إطار مشروع القانون الخاص بالجرائم المخلة بسلم الإنسانية في مادته الثانية الفقرة السادسة⁽⁴⁾، لكن الصواب أن أول إشارة إليه كانت سابقة لهذا التاريخ، فأول إشارة إليه كانت عام 1937، في اتفاقية عصبة الأمم للوقاية من الإرهاب والمعاقبة عليه في المادة الأولى منه⁽⁵⁾. وينقسم إرهاب الدولة من حيث نطاق ممارسته إلى نوعين اثنين، إرهاب الدولة الداخلي وإرهاب الدولة الخارجي:

1- إرهاب الدولة الداخلي:

إرهاب الدولة الداخلي هو: (الاستخدام المنظم لدرجة كثيفة من العنف بواسطة الأجهزة المركبة للدولة بهدف قمع أو الحد من المعارضة السياسية بين أفراد الشعب)، فهو إذا كل

(¹) جاك فرجيس، جرائم الدولة: (الكوميديا القضائية)، ترجمة: (حسين حيدر)، الطبعة الأولى، دار عويدات للنشر والطباعة، لبنان، 2004، ص 93.

(²) المرجع نفسه، ص 54.

(³) إبراهيم الحيدري، سوسولوجيا العنف والإرهاب، الطبعة الأولى، دار الساقى، لبنان، 2015، ص 46.

(⁴) نسيب نجيب، التعاون الدولي في مكافحة الإرهاب، مذكرة ماجستير في قانون التعاون الدولي، كلية الحقوق، جامعة مولود معمري، تيزي وزو، نوقشت بتاريخ 2009/07/19، ص 52.

(⁵) Article 01 de la convention pour la prévention et la répression du terrorisme, société des nations 1937: (les hautes parties contractantes, réaffirmant le principe du droit international d'après lequel il est du devoir de tout État de s'abstenir lui-même de tout fait destiné à favoriser les activités terroristes dirigées contre un autre État et d'empêcher les actes par lesquels elles se manifestent, s'engagent, dans les termes ci-après exprimés, à prévenir à réprimer les activités de ce genre et à se prêter mutuellement leur concours).

أعمال غير مشروعة تصورها الدولة على أنها مشروعة وتقوم بها من خلال مؤسساتها الرسمية كتصفية المعارضين أو من ينازعها الحكم والسلطان أو عن طريق كبت الحريات العامة وقمعها أو معاملة الشعب بما لا يتناسب مع القيم الإنسانية من أجل إبعادهم عن المشاركة السياسية لتظل السلطة الحاكمة مترتبة على عرش الحكم ومتفردة به⁽¹⁾.

2- إرهاب الدولة الخارجي:

يمكن تعريف إرهاب الدولي الخارجي على أنه: (استخدام حكومة دولة لدرجة كثيفة من العنف ضد المدنيين من موطني دولة أخرى من أجل إضعاف أو تدمير روحهم المعنوية أو إرادتهم في دعم أو تأييد الحكومة التابعين لها) وتمارس ذلك عن طريق مباشر واستخدام القوة العسكرية أو عن طريق غير مباشر ويكون ذلك عبر منظمات أو جماعات تعمل لحسابها⁽²⁾.

وفي هذا الإطار كله يندرج الإرهاب الإلكتروني الذي تمارسه الدولة بنفسها أو تحت رعايتها وإشرافها من خلال توجيه ضربات إلكترونية أو أعمال تخريبية أو دعائية تستهدف بها خلق جو من الخوف والرغبة بين مواطنيها وهذا من خلال فرض قيود على الدخول إلى الفضاء الإلكتروني أو حجب المواقع والمدونات وغيرها من أساليب القمع الإلكتروني وهذا من أجل إخضاعهم لرغباتها، أو تلك التي توجهها ضد دولة أخرى لاستنزافها عبر استهداف بنيتها التحتية من مرافق ومؤسسات عبر هجمات إلكترونية ممنهجة لدرجة اعتبارها حربا باردة⁽³⁾.

وبهذا الصدد يقول الدكتور عادل عبد الصادق⁽⁴⁾: (بالرغم ن الأدبيات الغربية كلها ركزت في دراسة الإرهاب الإلكتروني على أنه يتعلق فقط بالجماعات الإسلامية أو الرديكالية إلا أنني أرى أن الجانب العربي لا بد أن يكون له إسهام في هذا المجال، أنا أرى أن الإرهاب الإلكتروني

(¹) نور الحلو حسن عزيز، الإرهاب في القانون الدولي: (دراسة قانونية مقارنة)، أطروحة ماجستير في القانون العام، الأكاديمية العربية المفتوحة في الدنمارك، هلسنكي، فنلندا، 2007، ص ص: 105-106.

(²) المرجع نفسه، ص ص: 106-114.

(³) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المرجع السابق، ص ص: 120-121.

(⁴) عادل عبد الصادق: هو مؤسس ومدير مشروع المركز العربي لأبحاث الفضاء الإلكتروني، وعضو فريق حوكمة الإنترنت وعضو اللجنة الاستشارية للمنتدى العربي لحوكمة الإنترنت، وعضو جمعة الإنترنت الدولية، وعضو الهيئة الاستشارية لمجلة ناقد للدراسات الاستراتيجية الصادرة عن جامعة محمد خيضر بولاية بسكرة الجزائرية، كما أن له مقال شهري لدى كل من مجلة لغة العصر، ومجلة الدبلوماسية الصادرة عن النادي الدبلوماسي المصري، ويعتبر رائدا في مجال الدراسات المتعلقة بالفضاء السيبراني وله العديد من المؤلفات أهمها: الفضاء الإلكتروني والعلاقات الدولية، الفضاء الإلكتروني والتدخل الخارجي في الشؤون الداخلية، الفضاء الإلكتروني والثورة في شؤون أجهزة الاستخبارات الدولية، الحملات الإلكترونية وغيرها، أنظر:

- <https://aliqtisadi.com/%D8%B4%D8%AE%D8%B5%D9%8A%D8%A7%D8%AA/%D8%B9%D8%A7%D8%AF%D9%84-%D8%B9%D8%A8%D8%AF-%D8%A7%D9%84%D8%B5%D8%A7%D8%AF%D9%82/>

أصبح لا يتعلق فقط بالجماعات الإرهابية الإسلامية أو المتشددة، ولكن أصبح يتعلق بجماعات أخرى متعددة بالإضافة أيضا إلى أن الدول أصبحت تستخدم هذا النمط الجديد من الاستخدام العنيف للفضاء الإلكتروني⁽¹⁾.

إن الإرهاب الإلكتروني هو في حقيقة أمره إرهاب الدولة أكثر منه إرهاب الجماعات والأفراد. فليس هناك مثلا تسجيل لأي هجوم إلكتروني حاد موجه إلى البنى التحتية الأكثر حرجا في الولايات المتحدة الأمريكية، وغاية مبلغ الهجمات الإرهابية للجماعات اختراق لا يعبأ به، أو جعل الفضاء الإلكتروني منصة إعلامية لهم، بينما تعتبر الهجمات الإلكترونية من فعلها من الدول الأكثر شيوعا والأحد أثرا، حيث حددت الدراسات المختلفة أشكالا كثيرة من تصعيد الهجمات الإلكترونية المتبادلة بين الدول، في قمتها نجد روسيا والشيشان، تدخل الناتو في حرب كوسوفو، الهجمات الصينية على الولايات المتحدة، هجمات روسيا ضد إستونيا⁽²⁾، كما نجد أيضا صورا من القمع السلطوي الإلكتروني داخل الدول، من خلال عمليات حجب الإنترنت كما حدث أثناء الاحتجاجات الإيرانية⁽³⁾.

ثانيا: إرهاب الأفراد والجماعات:

قد يقدم الأفراد بمفردهم أو في إطار تنظيم جماعي بارتكاب أعمال إرهابية ضد الدولة أو مؤسستها ومرافقها، أو ضد الشعب بغية المساس بأمن البلاد واستقرارها، منطلقين من فكرة الفوضى الخلاقة، فيسددون هجمات متفاوتة الخطورة بغية زعزعة استقرار البلد وأمنه وجره إلى مستوى عالي من الرعب والذعر تمهيدا لإسقاط نظام الحكم فيها⁽⁴⁾، ومن هنا يمكن تعريف إرهاب الأفراد والجماعات على أنه: (الممارسات العنيفة غير القانونية الصادرة عن شخص أو عدد من الأشخاص ينتمون إلى منظمة إرهابية تسعى إلى تحقيق أهداف وغايات محددة، أو تسعى لحل مشكلاتها الخاصة وتحقيق مرادها على حساب مصالح الآخرين وحقوقهم الشخصية)⁽⁵⁾.

(1) عادل عبد الصادق، الإرهاب الإلكتروني والصراع الدولي، ندوة المركز الدولي للدراسات المستقبلية والاستراتيجية، أبريل 2012، تم الاطلاع

على الندوة مصورة بتاريخ 12 نوفمبر 2019 على الساعة 15:35 سا، على الرابط التالي: <https://youtu.be/gB8H4PZWvQk>

(2) إيهاب خليفة، القوة الإلكترونية: (كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت)، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2017، ص ص: 20-21.

(3) قناة العربية، بعد عودة الإنترنت... إيران تحجب كل شبكات التواصل الأجنبية، 21 نوفمبر 2019، تم الاطلاع عليه بتاريخ 16 ديسمبر 2019 على الساعة 01:33 سا، في الموقع:

<https://www.alarabiya.net/ar/iran/2019/11/21/بعد-عودة-الانترنت-ايران-تحجب-كل-شبكات-التواصل-الأجنبية>

(4) يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الاستراتيجية، السليمانية، 2007، ص 47.

(5) ياسر لطفي العلي، الإرهاب: (مفهومه وأحكامه في الشريعة الإسلامية: دراسة فقهية مقارنة)، رسالة ماجستير في الفقه الإسلامي وأصوله، كلية الشريعة، جامعة دمشق، دمشق، 2007، ص 136.

إن السمات التي تميز إرهاب الأفراد عن إرهاب الجماعات كون هذه الأخيرة تتميز بالاستمرارية وتعدد الأهداف والأساليب⁽¹⁾، فهو إرهاب يملك قدرا معينا من التنظيم والقدرة على التخطيط، ضمن جدولة زمنية محددة لتنفيذ أعماله الإرهابية، كما أنه يملك نظاما هرمي يتصدر الزعماء والقادة قمته، أما الإرهاب الفردي فهو إرهاب محدود الانتشار، محصور الأهداف، مفتقر التنظيم، خالي من الاستمرارية⁽²⁾، ويمكن أن نمثل للإرهاب الجماعات بتنظيمي القاعدة وداعش، وبالنسبة للإرهاب الأفراد فإن أدق واقعة له كانت هجم المتطرف بيرنتون هاريسون تارنت على مسجدين بنيوزلندا، وإسقاطه لعدد كبير من الضحايا.

يعتبر البعض من الفقهاء أن إرهاب الأفراد والجماعات ما هو إلا ردة فعل طبيعية عن الإرهاب القهري أو السلطوي الذي تمارسه الدولة، فهو إرهاب يمارس من منطلق اليأس والخيبة، ولذلك أطلق عليه اسم "إرهاب الضعفاء"، فيما يرى البعض الآخر أنه إرهاب تمردى، وليس من المنطق تسميته "إرهاب الضعفاء"، فالعمليات الإرهابية تحتاج قدر كبير من التمويل والتقنيات الحديثة الباهظة من أجل تنفيذه⁽³⁾، غير أن لا ينطبق على هجمات الإرهاب الإلكتروني التي لا تتطلب إلا القدر اللازم من المعرفة بالتقنيات المعلوماتية.

إن هذا التأسيس الفقهي للجرائم والعمليات الإرهابية التي يمارسها الأفراد والجماعات يحتفظ بنفس قيمته العلمية فيما يتعلق بالهجمات الإرهابية الإلكترونية، فربط الفرع بالأصل من بين أهم الآليات التي تضمن سهولة التعامل معها، وإيجاد الحلول ناجعة للعقبات التي تفرزها، والأخطار التي تتمخض عنها. فالجماعات الإرهابية جعلت من الفضاء السيبراني آلية تمارس فيه أو به أنشطة إرهابية خطيرة تبدأ بإرهاب سيبراني هجين، تعمل بمقتضاه للداعية والتوظيف ونشر التطرف العنيف، والتواصل في ما بينها وجمع المعلومات، وتصل إلى إرهاب سيبراني فعلي بشن حرب نفسية، أو تجنيد الأفراد، والدعوة إلى ارتكاب عمليات فردية⁽⁴⁾.

الفرع الثاني: أسلحة الهجمات الإرهابية الإلكترونية:

لقد أصبح الفضاء الإلكتروني ساحة يتعامل فيها ملايين البشر من خلال الخدمات التي يقدمها، وتنشأ على أسسها البنى التحتية للدول، لكن التنظيمات الإرهابية والجماعات التخريبية

(¹) ياسر لطفي العلي، مرجع سابق، ص 137.

(²) نسيب نجيب، المرجع السابق، ص ص: 48-49.

(³) يوسف كوران، المرجع السابق، ص 47.

(⁴) Mayssa ZERZRI, The Threat of Cyber Terrorism and Recommendations for Countermeasures, Center for Applied Policy Research, C-A-Perspectives on Tunisia, 2017, P.02.

لجأت لاستغلال تلك الخدمات وتهجينها لتصبح سلاحا قابلا للتوظيف (أولا)، كما سنح التقدم التقني للمجال الإلكتروني إمكانية اختلاق وابتكار أسلحة قابلة للاستخدام على الساحة السيبرانية وبإمكانها إحداث أضرار جسيمة وتداعيات خطيرة (ثانيا).

أولا: الأسلحة الإلكترونية الهجينة:

إن الأسلحة الإلكترونية الهجينة لا تعتبر بطبيعتها سلاحا، بل هي خدمات موجهة إلى خدمة الإنسانية، وتحقيق المصلحة العامة، فاستغللتها الجماعات الإرهابية وهجنتها، وغيّرت من طبيعتها الخدمانية إلى طبيعة تجعلها أسلحة فتاكة تقوض بها الأمن والسلم العالميين، ويمكن حصر هذه الأسلحة فيما يلي:

1- البريد الإلكتروني:

يعتبر البريد الإلكتروني الوسيلة الأثر شيوعا وانتشارا للاتصال، بحيث أصبح من الصعب الاستغناء عنها في معظم المجالات، فقد تحولت بفعل توفرها على الهواتف المحمولة الوسيلة المثلى لتبادل المعلومات كلها، بما ذلك الأكثر حساسية منها، ورغم هذه الفائدة الكبيرة والمهمة التي يقدمها البريد الإلكتروني للمتعاملين به، إلا أنه يعتبر وسيلة يصعب العمل على تأمينها، فكلما زاد الاعتماد عليها تفاقم الخطر المحدق بها⁽¹⁾.

وتكمن المخاطر الإرهابية التي تنتج عن البريد الإلكتروني في كونه الآلية التي تسهل للإرهابيين التواصل والتنسيق وتبادل المعلومات فيما بينهم، فقد ثبت أن الكثير من العمليات الإرهابية التي تمت في الآونة الأخيرة كان البريد الإلكتروني السبب فيها⁽²⁾، كما يمكن أن يكون الآلية التي تعرّض الجهاز المستقبل والشبكة التي يعمل عليها لمخاطر الهجمات الفيروسية التي تنقلها الرسائل غير المرغوب فيها⁽³⁾.

2- مواقع الشبكة الإلكترونية:

لقد أتاحت الشبكة العالمية للإنترنت للإرهابيين إمكانية إنشاء وتصميم مواقع إلكترونية تساعد على تنفيذ هجماتهم الإرهابية من خلال جعلها منصة إعلامية، تسمح لهم بنشر أفكارهم وبيان مبادئهم وتسلط الضوء على نشاطاتهم، كما أخذوا في ذلك أبعادا أكثر خطورة، بجعلها بدائل عن مخيمات التدريب التقليدية فأصبحوا يعلمون فيها طرق تصنيع المتفجرات وسبل اختراق المواقع

(1) حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص ص: 97-98.

(2) حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، المرجع السابق، ص 803.

(3) خالد بن سليمان الغنير وسليمان بن عبد العزيز بن هيشة، الاصطياد الإلكتروني: (الأساليب والإجراءات المضادة)، الطبعة الأولى، مركز التمييز لأمن المعلومات، جامعة الملك سعود، الرياض، 2009، ص ص: 29-30.

والمنتديات، وساحة لتبادل المعارف والخبرات، وآلية لتبادل المعلومات بين عدة أفراد موزعين في أماكن مختلفة من العالم⁽¹⁾، فوجدت فيها التنظيمات الإرهابية بغيتها ومبلغ طموحها فأصبح لهم عدة مواقع تستخدمها كأهم وسيلة في شن هجماتها⁽²⁾.

إن المواقع المختلفة والمنتديات هي الوسيلة الإعلامية البديلة عن وسائل الإعلام التقليدية، فأصبحت بمثابة مقر افتراضي للجماعات الإرهابية، إذ يمكن فيها إنشاء مواقع خاصة بها، أو استغلال مواقع موجهة للنفع العام كوسائل التواصل الاجتماعي التي غدت من أهم الوسائل التي يعتمدونها في نشر التطرف وتجنيد الشباب وإغوائهم للالتحاق بساحات القتال والفتن، وتحريضهم عبر إشاعة الدعايات الكاذبة⁽³⁾.

فطبيعة وسائل التواصل الاجتماعي التي تتسم بالتجمهر الافتراضي في ساحاتها، والتواصل بين حلقاتها المجتمع فيها يشكل نقطة حرجة، إذ تجتمع في استعمالها كل الفئات العمرية وجميع المستويات الاجتماعية وعامة الدرجات الرتب والمقامات العلمية والثقافية⁽⁴⁾، مما يجعلها الوسيلة الأنجع لممارسة كل أصناف التحريض والنشر للكراهية والتطرف، من خلال استغلال ضعف النفوس والمراهقين وذوي الصعوبات الاجتماعية والمادية، واستغلال المضطربين نفسيا ومشاعريا.

ثانيا: الأسلحة الإلكترونية الفعلية:

إن الأسلحة الإلكترونية الفعلية هي أسلحة مبتكرة خصيصا لخوض المعارك وشن الحروب على الساحة الإلكترونية، وهي الآلية المهلكة التي يستخدمها المحترفون من العريقين في الإجرام والإرهاب الإلكترونيين، ويمكن تلخيصها في ما يلي:

1- الفيروسات والبرامج الخبيثة:

الفيروس الإلكتروني هو عبارة عن برنامج إلكتروني صغير يعمل وفق النمط لغة برمجية معينة خصص من أجل أن يحدث نوعا من الفوضى في أنظمة التشغيل، ويعمل على تلويث البيئة

(¹) صليحة محمدي وشفيعة حداد، الإرهاب الإلكتروني والأمن القومي للدول: (نمط جديد وتهديدات مختلفة)، المجلة الجزائرية للأمن والتنمية، المجلد 08، العدد 2، جامعة الحاج لخضر، باتنة، الجزائر، جوان 2019، ص ص: 65-77: <https://www.asjp.cerist.dz/en/article/96164>

(²) سعد عطوة الزنط، الإرهاب الإلكتروني وإعادة صياغة استراتيجيات الأمن القومي، أطروحة مقدمة لمؤتمر الجرائم المستحدثة: كيفية إثباتها ومواجهتها، المنعقد في المركز القومي للبحوث الاجتماعية والجنائية، خلال 15-16 ديسمبر 2010:

<http://www.child-trafficking.org/ar/مؤتمر-الجرائم-المستحدثة>

(³) شفيق حسنين، الإعلام الجديد والجرائم الإلكترونية: (التسريبات، التجسس الإلكتروني، الإرهاب)، دار فكر وفن للطباعة والنشر والتوزيع، مدينة السادس من أكتوبر، 2014، ص 195 وما يليها.

(⁴) وليد غسان سعيد جلعود، المرجع السابق، ص ص: 101-102.

الإلكترونية، وهذا بهدف أحدث فجوة رقمية يمكن من خلالها النفاذ إلى المعلومات، أو استنزاف المخزون الرقمي، كما يمكن أيضا أن تحدث أضرارا بالأجزاء المادية لنظم التشغيل⁽¹⁾، ويمكن تمييز عدة أشكال من الفيروس نذكر منها ما يلي:

أ- حصان طروادة cheval de Troy:

هو برنامج صغير ودقيق يختفي في البرنامج الأصلي وينشط عند تشغيل هذا البرنامج، أو هو جزء من كود يضاف إلى برنامج معين دون أن يكون له أي وظيفة فيه ويقوم بوظيفة تخريبية، وهو برنامج لا يمكن للنظام التفتن إلى وجوده إلى غاية اللحظة التي يؤدي فيها عمله التخريبي، ويستخدم حصان طروادة في عمليات الاختراق والاستيلاء الرقمي وعمليات التجسس الإلكتروني، وينتقل عن طريق البريد الإلكتروني بإرساله ضمن ملف أو برنامج، أو عن طريق تحميل البرامج أو الملفات من المواقع، أو عند الاتصال بالشبكات الداخلية أو العامة، وسمي بحصان طروادة تشبيها له الحصان الخشبي الذي صنعه الإغريق للتمكن من اجتياز حصن طروادة، فهو برنامج مخادع يملك قدرة عالية على التضليل والاختفاء ومن ثم التدمير والتخريب⁽²⁾

ب- الدودة الإلكترونية:

الدودة الإلكترونية برنامج دقيق صغير الحجم وضع من أجل القيام بالأعمال التدميرية، أو من أجل سرقة البيانات المتعلقة بالمستخدم من ألق الأضرار به، أو بالمتصلين به أثناء تصفح الشبكة العالمية للإنترنت، وهو برنامج يملك القدرة على التخفي والتناسخ والمراوغة، وله أن ينتشر بسرعة كبيرة، كما أنه برنامج مستقل بذاته، فلا يحتاج إلى غيره من البرامج⁽³⁾.

ج- فيروس تشيرنوبيل:

هو من ضمن أخطر الفيروسات الإلكترونية، فقد كتبه "شان يتغ هو" في أواخر القرن العشرين، ويقوم بالهجوم على أنظمة التشغيل ويندوز، فيخرب النظام بحيث لن يملك الجهاز القدرة على الإقلاع، كما يحاول هذا الفيروس أيضا القيام بمسح نظام الإدخال والإخراج الأساسي "البيوس"، وهو نظام معقد ضروري في عملية إقلاع الجهاز، فإن حدث وإن استطاع الفيروس

(¹) وليد غسان سعيد جلعود، المرجع السابق، ص 99.

(²) ضرغام جابر عطوش آل مواش، جريمة التجسس الإلكتروني: (دراسة مقارنة)، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2017، ص ص: 53-54.

(³) المرجع نفسه، ص ص: 50-51.

مسحه فإن الأمر يصبح مستعصيا، لإعادة تنصيب " البيوس " أمر معقد وعادة ما يلجأ الناس إلى تغيير اللوحة الأم لجهازهم⁽¹⁾.

د - فيروس الفدية الخبيثة:

يعتبر فيروس الفدية الخبيثة من بين أخطر وأحدث الفيروسات على الإطلاق، فهو فيروس يشفر البيانات ومن ثم يطالب بفدية لفك الشفرة، وبرنامج الفدية يتوفر منه نوعان؛ أحدهما يقوم بتشفير البيانات مع إتاحة القدرة إلى الوصول إليها دون القدرة على فك شفرته وإزالته، وثانيهما يقوم بالحيلولة حيث يثبث الجهاز ويبدأ في عملية التشفير والإغلاق، كما يمكن أيضا أن ينتشر عبر الثغرات الموجودة في نظام الويندوز، بحيث يتم استغلالها لتنشيط البرنامج الخبيث وتفعيله، وهو من أخطر الوسائل باعتبار يحول بين المستخدم وبين البيانات فلا يتمكن من الوصول إليها، وينتشر عادة هذا البرنامج عن طريق البريد الإلكتروني أو وسائل وتطبيقات التواصل الاجتماعي على شكل رابط إلكتروني، وبمجرد الضغط عليه يلوث الجهاز ويفقد المستخدم السيطرة عليه⁽²⁾.

هـ/ القنابل المنطقية:

القنبلة المنطقية صنف من أصناف أحصنة طروادة، صمم بطريقة تتوقف على التلازم الشرطي، فلا يعمل إلا عند حصول الشروط المحددة سلفا فيه، كبلوغ الموظفين عددا معينا، أو رفع اسم معين من كشف الرواتب، أو عن طريق تشغيل البرنامج لعدد معين من المرات، كما يمكن أن يكون عمله مرتبطا بوقت معين محدد سلفا، فيسمى حينها بالقنبلة المؤقتة⁽³⁾.

وتتحدث معظم الفيروسات في أربع خصائص تمنحها الصفة التدميرية والتخريبية ويمكن حصرها في ما يلي:

أ - الاختراق:

إن اللغة البسيطة التي يبرمج بها الفيروس تمكنه من تنفيذ عملية اختراق للنظم المعلوماتية،

⁽¹⁾ ويكيبيديا، تشيرنوبيل (فيروس)، الموسوعة الحرة ويكيبيديا:

[https://ar.wikipedia.org/wiki/%D8%AA%D8%B4%D9%8A%D8%B1%D9%86%D9%88%D8%A8%D9%8A%D9%84 \(%D9%81%D9%8A%D8%B1%D9%88%D8%B3\)](https://ar.wikipedia.org/wiki/%D8%AA%D8%B4%D9%8A%D8%B1%D9%86%D9%88%D8%A8%D9%8A%D9%84 (%D9%81%D9%8A%D8%B1%D9%88%D8%B3))

⁽²⁾ إيهاب خليفة، الهجمات الصفرية: (كيف يمكن الاستعداد لليوم الأسود في الإنترنت؟)، 17 مايو 2017، تم الاطلاع عليه بتاريخ 22 جانفي

2020، على الساعة 03:17، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/2802/>الهجمات-الصفرية-كيف-يمكن-الاستعداد-اليوم-الأسود-في-الإنترنت

⁽³⁾ فائق سعيد بامفلح، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: (دراسة حالة)، الاتجاهات الحديثة في المكتبات والمعلومات،

العدد 18، المكتبة الأكاديمية، القاهرة، مصر، 2002، ص ص: 249-282.

كما يمكن له أيضا أن يخترق المواقع بكل يسر وسهولة ⁽¹⁾، فالفيروسات يتم دعمها وإحاطتها بكافة الوسائل والآليات التي تمكنها من هذا الاختراق، كما توفر لها كل الأساليب لتحقيق الغرض الذي صنعت من أجله، وأكثر الأمثلة شهرة ما يعرف بفيروس حصان طروادة ⁽²⁾.

ب- الاختفاء:

تملك جميع الفيروسات القدرة الكاملة على الاختفاء لضمان عدم التمكن من اكتشافها، فهي تقوم بالتضليل والتمويه إذ تستقر داخل الملف البرمجي للبرنامج، أي في خلفيته الرقمية، فلا يمكن أبدا للمستخدم ملاحظتها، وعندما تتمكن من الدخول إلى الجهاز عن طريق ملفات أو عن طريق تنصيب البرنامج فإنها تدخل في حالة الخمول إلى غاية بلوغ لحظة نشاطها الذي برمجت عليها، فتستقر في أماكن داخل الجهاز من غير الممكن الوصول إليها بوسائل البحث العادية، فهي لا تظهر في الملفات ولا يمكن ملاحظتها إلى غاية ظهور الأعراض الأولى للتلوث أو العدوى هي المرحلة التي يبدأ فيها نشاطها ⁽³⁾.

فالفيروسات كثيرات ما تكون مدعومة بآليات تمكنه من التخفي في النظام لكي لا يتم الكشف عنه، كدخوله إلى النظام على شكل ملف مخفي، كما هو عليه الحال في الفيروسات المنطقية والزمنية ⁽⁴⁾.

ج- الانتشار:

تمتلك الفيروسات الإلكترونية قدرة مذهلة على الانتشار، فتركيبها الرقمية وصغر حجمها يمكنها من الانتشار بشكل سريع جدا سواء عن طريق الشبكات الداخلية أو عن طريق الشبكة العالمية ⁽⁵⁾، كما يمتلك سرعة محولة تمكنه من الانتقال عبر القارات في ثواني قليلة بسبب سرعة تكاثره الكبيرة، وقد ساعد تماثل البرامج المستعملة حول العالم وتطابقها من هذا الانتشار السريع ⁽⁶⁾.

د- التدمير:

يملك الفيروس الإلكتروني القدرة على أحداث آثارا تدميرية جسيمة في نظم المعلومات ونظم التشغيل، بحث يستطيع أن يحطمها كلياً أو جزئياً كما يمكنه أن يغير من شكلها الرقمي، ويستطيع أيضا إحداث آثار تدميرية داخل البنية المادية للجهاز عندما يتعلق الأمر بالماس بأنظمة الإقلاع

⁽¹⁾ حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، المرجع السابق، ص 811.

⁽²⁾ أيمن عبد الله فكري، الجرائم المعلوماتية: (دراسة مقارنة في التشريعات العربية والأجنبية)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2014، ص 172.

⁽³⁾ حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، المرجع السابق، ص 810.

⁽⁴⁾ أيمن عبد الله فكري، المرجع نفسه، ص 172.

⁽⁵⁾ حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، المرجع السابق، ص 811.

⁽⁶⁾ أيمن عبد الله فكري، المرجع السابق، ص 172.

الحساسة⁽¹⁾، فالهـداف الأساسي من الفيروسات هو إحداث هذا الأثر التدميري، وذلك من خلال اتجاهه لمنطقة معينة داخل ذاكرة الجهاز، ومن ثم يضل فيها كامناً إلى غاية توفر الشروط التي برمج عليها للقيام بوظيفتها سواء أكانت أوامر أو حلول الزمن، ومن ثم يبدأ في النشاط التدميري له⁽²⁾.

2- القنابل الكهرومغناطيسية:

تعتبر القنابل الكهرومغناطيسية من أحدث الأسلحة وأشدّها فتكاً، فرغم أنها قنابل غير قاتلة، إلا أنها تحدث دماراً شاملاً أو جزئياً بكل المعدات التقنية والآلات الإلكترونية ومحطات توليد الطاقة، فحين انفجارها تصدر ذبذبات كهرومغناطيسية شديدة، تقوم بالتأثير على الشحنات، فتدمر الوحدات الإلكترونية في أي إدارة أو محطة، مما يفقد قدرتها على العمل⁽³⁾ وأهم أنواعها:

أ- الحقيبة الكهروستاتيكية:

هي أحدث أنواع التكنولوجيا العسكرية، صنعت على شكل حقائب محمولة، صغيرة الحجم، وتقوم بتوليد النبض الكهرومغناطيسي ذو القدرة الفائقة، ومن خلاله يمكن التأثير على الوحدات الإلكترونية، وتدمير أجهزة الإرسال بحيث تفقد كل قدرتها التشغيلية أو الإنتاجية⁽⁴⁾.

ب- قنابل التعقيم الميكروويفية:

هي قنابل صغيرة، تقوم بطرد كمية هائلة من النبضات الكهرومغناطيسية قصيرة الموجة، فتعمل على قطع جميع مصادر الطاقة والمعلومات في المكان المستهدف، ويمكن بها استهداف محطات التزويد بخدمة الإنترنت، ومراكز الاتصالات السلكية واللاسلكية، ومحطات البث الخلوي وغيرها من وسائل التزويد بالمعلومات⁽⁵⁾.

ج- قنبلة الغرافيت (الجرافيت):

تعد قنبلة الغرافيت من بين قنابل التعقيم غير القاتلة، فهي تحدث حين انفجارها سحابة دقيقة جداً من ألياف الكربون المعالج كيميائياً، فتنشر على الآلات الكهربائية مما يسبب ماس كهربائياً،

(1) حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، المرجع نفسه، ص 811.

(2) أيمن عبد الله فكري، المرجع نفسه، ص 173.

(3) حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، المرجع نفسه، ص ص: 816-817.

(4) وليد غسان سعيد جلعود، المرجع السابق، ص 103.

(5) المرجع نفسه، ص 105.

وقد استخدمت لأول مرة في العراق في حرب الخليج الثانية، وتحدث بذلك أضرار على الشبكات وهي تعمل فقط على خطوط الكهرباء غير المعزولة⁽¹⁾.

الفرع الثالث: مظاهر الإرهاب الإلكتروني:

إن تعدد أشكال الأسلحة الرقمية التي يمكن للتنظيمات الإرهابية توظيفها على الساحة الإلكترونية قد نوعت أيضا من مظاهر النشاطات الإرهابية عليها، فالشبكة الإلكترونية توفر عددا كبيرا من الخدمات المختلفة الموجهة للاستغلال الإيجابي في حياة الأفراد، والتي يستغلها الإرهابيون أيضا في دعم نشاطاتهم التقليدية (أولا)، كما أن التوجه الكبير الذي شهدته الدول والأفراد والمؤسسات في استغلال البيئة الإلكترونية في التسيير والإدارة قد عزز من ظهور أشكال جديدة للنشاط الإرهابي ومظاهرة أكثر حداثة وخطورة للهجمات الإرهابية (ثانيا).

أولا: استغلال البيئة الإلكترونية في دعم الإرهاب:

تكتسي البيئة الإلكترونية أهمية بالغة بالنسبة لدعم النشاط الإرهابي عموما والتقليدي منه خصوصا، فهي بيئة ملائمة لتيسير النشاطات التخريبية وجعلها أكثر فعالية وتأثيرا، كما أنها تحفز من انتشارها وتعتبر عن رؤية منفذها، وتتميز بمواردها المادية والبشرية، وقد أدركت التنظيمات الإرهابية هذه الأهمية العظيمة ولذلك نرى الإقبال الشديد عليها والتوافد المتسارع إلى استغلالها، ولعل من أهم صور نشاطاتها فيه ما يلي ذكره:

1- الاتصال والتنسيق:

يحتاج النشاط الإرهابي إلى نوع من الفعالية في الاتصال لبلوغ أهدافه ومراميها، والإنترنت يعد من بين الأدوات الأكثر تأثيرا ونفوذاً في عمليات الاتصال الحديثة، فهو يوفر لهم آليات وتقنيات اتصالية تتسم بالسرعة من جهة، وبالسرية من جهة أخرى، وفي مقدمة تلك التقنيات نجد البريد الإلكتروني وخدمة الاتصالات على الماسنجر، كما نجد أيضا غرف الدردشة والمنديات، والتي يقوم الإرهابيون باستغلالها وتوظيفها في الاتصال والتنسيق بينهم عن طريق وضع رسائل مشفرة تأخذ طابعا برئا، بحيث لا يمكن الكشف عنها أو التفتن إلى محتواها الإرهابي، أو معرفة مغزاها، فهي بذلك الوسيلة الأنسب والأجود للقيام بالاتصال والتنسيق بين أفراد التنظيمات

(1) ويكيبيديا، قبلة غرافيت، الموسوعة الحرة ويكيبيديا:

https://ar.wikipedia.org/wiki/%D9%82%D9%86%D8%A8%D9%84%D8%A9_%D8%BA%D8%B1%D8%A7%D9%81%D9%8A%D8%AA

الإرهابية، فهي لا تلزمهم على كشف هويتهم، وتضمن لهم السرية التامة في معاملاتهم⁽¹⁾، بالإضافة إلى قلة تكاليفها وكثافة المعلومات التي يمكن تبادلها فيها⁽²⁾.

وتكتسي هذه الوسائل الاتصالية على شبكة الإنترنت أهمية خاصة بالنسبة للإرهابيين، فهي آلية كفيلة بضمان التنسيق والتخطيط، إذ أن الأعمال الإرهابية فيها جانب كبير من التعقيد، مما يستدعي التخطيط الشامل لها، والتنسيق التام بين خطواتها، والإنترنت يمكنهم من فعل ذلك بكل يسر وسهولة وفي جو من الراحة والهدوء⁽³⁾.

2- الإعلام الإرهابي:

يعتبر الفضاء الإلكتروني من أكثر وسائل التقنية استعمالاً في العالم، فعدد الذين يرتادونها يقدر بالملايين، مما يجعلها ساحة إعلامية مهمة، يمكن عبرها التأثير الفعال على الرأي العام العالمي باستخدام تقنيات سمعية بصرية وأخرى نصية، وعلى هذا الأساس فإن التنظيمات الإرهابية تقوم بتكوين منابر إعلامية لها على الصفحات الإلكترونية، لتساعد على إيصال أفكارها ونشر كل ما من شأنه أن يدعم قضيتها⁽⁴⁾.

تلجأ التنظيمات الإرهابية إلى الإعلام السيبراني بغية إصدار بياناتهم المختلفة عن طريق المواقع الشبكية أو المنتديات الحوارية والتي تختلف الأهداف المرجوة منها، وما يزيد من تسارع الوتيرة الإعلامية للتنظيمات الإرهابية ما تقوم به وسائل الإعلام التقليدية من نقل لتلك البيانات ونشرها على نطاق أكثر اتساع⁽⁵⁾.

كما يهدف الإرهابيون أيضاً من خلال حملاتهم الإعلامية على الإنترنت إلى نشر ثقافة العنف والكراهية من خلال إصدار التسجيلات والصور والمقاطع المختلفة، كما تعمل أيضاً على توثيق نشاطاتها ونشرها من أجل الترويع والتخويف وشن الجو بمشاعر الرهبة منهم، ويظهر هذا جلياً من خلال ما فعله تنظيم الدولة الإسلامية بتوثيق عملية حرق التيار الأرمني معاذ الكساسبة حياً، ونجح الأسرى الأقباط⁽⁶⁾.

(1) علي بن عبد الله عسيري، الإرهاب والإنترنت، الإرهاب والقرصنة البحرية، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2006، ص: 211-250.

(2) صليحة محمدي وشفيعة حداد، المرجع السابق.

(3) شفيق حسنين، المرجع السابق، ص 193.

(4) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص 126.

(5) صليحة محمدي وشفيعة حداد، المرجع السابق.

(6) مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة العلوم الاقتصادية والإدارية والقانونية، المجلد 02 العدد 07، غزة، فلسطين، مايو 2018، ص: 56-67: <http://www.ajsrp.com/M080318.html>

وهذا التنظيم يعتبر على رأس هرم المستخدمين لتكنولوجيا المعلومات وبطريقة عالية الاحترافية، مبرزة رموزها وشعاراتها بهدف تعزيز مكانتها وتأكيد هيمنتها وإظهار قوتها لتهريب أعدائها، وكذلك لتشجيع الانضمام إليها عبر خلق مشاعر الاعتزاز بمن ينتمي إليها⁽¹⁾، ويعود استعمالها لهذه الفضاء إلى النطاق الذي يشغله هذا الفضاء فضلا عن سهولة الدخول إليه من كافة الناس⁽²⁾.

وتظهر احترافية تنظيم داعش في توظيف هذا الفضاء الإلكتروني لأغراض دعائية من خلال العديد من المظاهر والصور، ولعل أبرز ما تتجلى فيه الاحترافية امتلاك هذا التنظيم ترسانة إعلامية تمثل عمدة جيشها الإلكتروني، فضلا على أنه قد تجنب التقنية التقليدية للإعلام حين تقادي الاعتماد الكلي على الاتصال الجمهوري بل عمل على استغلال خاصية التخصيص التي يتمتع بها هذا الفضاء لممارسة الإقناع المباشر عبر متخصصين في هذا المجال، ناهيك عن كونه يعتمد في دعايته إلى علم النفس في الإقناع⁽³⁾، وهذا ما يبلور خطره، ويجعله يحتل مرتبة متقدمة في توظيف هذا الفضاء توظيفا إعلاميا لأغراض إرهابية.

فالهدف الإعلامي للتنظيمات الإرهابية عموما على الفضاء الإلكتروني هو إرهاب أعدائها من خلال خوض حرب نفسية ضدهم، ومن المعروف أن الحرب النفسية تستعمل فيها العديد من الأساليب ومن أبرزها أسلوب الدعاية سواء أكانت دعائية استراتيجية أو تكتيكية، أو من خلال اللجوء إلى أسلوب الشائعات بأنواعها الثلاث (الزاحفة، العنيفة، الغائصة)، والتي قد تحمل بين طياتها آمالا، أو خوفا، أو كراهية، أو من خلال غسل الدماغ والهيمنة على العقول⁽⁴⁾، والفضاء الإلكتروني يعتبر وسطا أو بيئة مواتية لتوظيف كل هذه الأساليب في أعمال الإرهاب النفسي للجهات المستهدفة.

ليس هذا فحسب، فالناظر في نموذج داعش يجلى الأهداف الإعلامية للتنظيمات الإرهابية على الفضاء الإلكتروني، وهي لا تخرج في إطارها عن خمس ثنائيات متناقضة في جوهرها على

(¹) فاطمة الزهراء عبد الفتاح، سيميوطيقا داعش: (دلائل استخدام الإرهابيين للرموز والشعارات على الإنترنت)، 15 مارس 2017، تم الاطلاع عليه بتاريخ 12 ديسمبر 2019، على الساعة 18:55 سا، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/2575/> سيميوطيقا-داعش-دلائل-استخدام-الإرهابيين-للرموز-والشعارات-على-الإنترنت

(²) سعد محمد خضير، اتجاهات الجمهور العراقي آراء المنطق الدعائي للتنظيمات الإرهابية: (دراسة ميدانية)، مجلة الباحث الإعلامي، المجلد 07، العدد 30، كلية الإعلام، جامعة بغداد، العراق، 2015، ص ص: 146-125:

<https://www.iasj.net/iasj/article/113424>

(³) أحمد عبد المجيد، الأساليب الإقناعية لتنظيم داعش في تجنيد الأفراد: (مقاربة علمية)، مجلة الباحث الإعلامي، المجلد 08، العدد 31، كلية الإعلام، جامعة بغداد، العراق، 2016، ص ص: 106-89:

<https://www.iasj.net/iasj/article/117300>

(⁴) ارجع إلى: فهمي النجار، الحرب النفسية: (أضواء إسلامية)، الطبعة الأولى، دار الفضيلة، السعودية، 2005، ص ص: 156-197.

ما أكده جاك أيلول، وهي؛ دعاية سياسية ودعاية اجتماعية، دعاية تكتيكية ودعاية استراتيجية، دعاية عمودية وأخرى أفقية، دعاية تحريضية ودعاية اندماجية، دعاية عقلانية وأخرى لا عقلانية⁽¹⁾.

3- الحشد والتجنيد:

إن الضمان الوحيد لاستمرارية التنظيمات الإرهابية وفعالية نشاطاتها هو؛ انخراط المزيد من الأفراد فيها، ولذلك تسعى كل التنظيمات الإرهابية إلى الدعاية لنفسها من أجل التغيرير بالبسطاء والسذج في أوساط الشبكة العنكبوتية للانضمام والالتحاق⁽²⁾.

ولا شك أن هذه الطريقة في تجنيد الشباب من أهم وأخطر الطرق على الإطلاق، نظرا لسلاستها وسرعتها وفعاليتها في تكوين القناعات الفكرية المتطرفة لدى مستخدمي الإنترنت، وكل ما يكلفهم في ذلك مجرد حاسوب متصل بشبكة الإنترنت، وشيء من الاحترافية التقنية والسيكولوجية ليتمكنوا من إنشاء جيش افتراضي مترامي الأطراف⁽³⁾.

4- التدريب الإلكتروني:

ليس من السهل الخوض في عمليات إرهابية أو تنفيذها بإتقان دون دراية تامة بها وبأساليب القيام بها، ومن غير الممكن تكوين هذه المعرفة والدراسة دون قسط كبير من التدريب الميداني، وبما أن معسكرات التدريب رغم سريتها تحوى مخاطر كثيرة على التنظيمات الإرهابية، فقد لجئوا إلى الفضاء الإلكتروني الذي تنتوع فيه الآليات التي تعينهم على خلق معسكرات تدريب افتراضية، فيتم التدريب فيها على تقنيات صنع الأسلحة والمتفجرات والمواد الحارقة والاختراق الإلكتروني، عبر منشورات تعليمية وإرشادية يمكن أن تصل بكل يسر وسهولة إلى كل إرهابي في العالم⁽⁴⁾.

5- الحصول على التمويل:

تلجأ التنظيمات الإرهابية في دعمها لنشاطها الإرهابي إلى إطلاق حملات التمويل من خلال الطلب المباشر باستخدام المنصات الاجتماعية على الشبكة الإلكترونية، أو عن طريق مواقع

(1) نقلا عن: علاء الدين أحمد عباس، صناعة الخوف في خطاب الصورة الدعائي لتنظيم "داعش" الإرهابي عبر الإنترنت، مجلة الباحث الإعلامي، المجلد 09، العدد 38، كلية الإعلام، جامعة بغداد، العراق، 2017، ص ص: 67-94:

<https://www.iasj.net/iasj/article/141055>

(2) صليحة محمدي وشفيعة حداد، المردع السابق.

(3) إيمان بن سالم، المرجع السابق، ص 22.

(4) شفيق حسنين، المرجع السابق، ص ص: 195-196.

تعرض بيع الكتب والتسجيلات ويتم تحويل هذه الأموال إلكترونياً إلى الأطراف المعنية بالنشاط الإرهابي عن طريق بطاقات الائتمان⁽¹⁾، ويتم استجداء التبرع من ذوى القلوب الرحيمة والمشاعر الرقيقة بطريقة المخادعة وبنوع من الحنكة والمراوغة لدفعها إلى منظمات صورية تكون واجهة لهؤلاء الإرهابيين⁽²⁾.

ثانياً: الهجوم إلى البيئة الإلكترونية:

لقد تحول الفضاء الإلكتروني بفعل الاعتماد المتزايد عليه في إدارة شؤون الحياة خاصة في الدولة المتقدمة إلى فضاء حيوي، الشيء الذي جعله أيضاً هدفاً حيويًا للهجمات الإرهابية، ومن أهم صور النشاط الإرهابي الذي يستهدف البيئة الإلكترونية نجد:

1- الاختراق:

يمكن تعريف الاختراق على أنه: (القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظم الحماية الخاص بالهدف)⁽³⁾، كما يمكن تعريفه بأنه: (دخول دون تصريح وبطريقة متعمدة إلى الحاسب الآلي، أو موقع إلكتروني على الشبكة العنكبوتية أو نظام معلوماتي، أو شبكة حاسبات آلية)، فالاختراق إذا يعتمد على التواصل الشبكي بين الأنظمة، ولكي يتمكن المخترق من تخطي آليات الحماية ودروع الأمان لا بد أن يكون على قدر عالي من الفطنة والمعرفة والدراية بالأنظمة المتعلقة بالحاسب والشبكات ونظم التشغيل⁽⁴⁾، ويطلق عليهم اسم الهاكرز، وهم على ثلاث أصناف:

أ- الهاكرز الأبيض القبعات:

يعرف الهاكرز الأبيض القبعة بتسمية أخرى هي "القرصان الأخلاقي"، وهو قرصان أو هاكلر لا يسمح له ضميره الأخلاقي من تنفيذ الهجمات ضد أنظمة المعلومات، فهو يعمل على عكس الهاكرز ذوي القبعات السوداء على ضمان الحماية اللازمة للفضاء الإلكتروني، ولذلك فإنه قرصان

(1) فوزية حاج شريف والساجي علام، واقع الإرهاب الإلكتروني وآليات مكافحته، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 03، العدد 01، جامعة عمار تليجي، الأغواط، الجزائر، 2019، ص ص: 158-172: <https://www.asjp.cerist.dz/en/article/93754>

<https://www.asjp.cerist.dz/en/article/93754>

(2) صليحة محمدي وشفيعة حداد، المرجع السابق.

(3) أحمد السيد، تعريف الاختراق وطرقه وأنواعه وكيفية التصدي له، 06 ديسمبر 2013، تم الاطلاع عليه بتاريخ 16 جانفي 2020، على الساعة 11:32، في الموقع:

<https://www.suezbalady.com/index.php/علوم-وتكنولوجيا/11008-تعريف-الاختراق-وطرقه-وانواعه-وكيفية-التصدي-له>

(4) عبد الله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية: (دراسة تطبيقية على المحققين في هيئة التحقيق والادعاء العام بمدينة الرياض)، رسالة ماجستير في قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014، ص 41.

مرخص له باللجوء على ما يحظر من أساليب على غيره بهدف سد الثغرات الأمنية للفضاء الإلكتروني⁽¹⁾، إذا الوازع الخلفي لهذا النوع من الهاكرز يحول بينه وبين أن ينتهك أنظمة الحواسيب الأخرى⁽²⁾.

ب- الهاكرز السود القبعات:

القراصنة أو الهاكرز ذوى القبعات السوداء هو تعبر مجازي عن فئة من القراصنة والهاكرز الذين يقتحمون وينتهكون بنية الفضاء الإلكتروني أو يعملون على بناء فيروسات تساعد على التدمير أو على جني العائدات المادية⁽³⁾.

ج- الهاكرز رمادي القبعة:

هذا النوع من الهاكرز يخلط بين الأعمال المشروعة وغير المشروعة، ففي بعض الأحيان يقوم بأعمال مشروعة سواء بمساعدة أمنية أو من تلقاء نفسه، وفي أحيان أخرى يقوم بأعمال مؤذية، وتسميته بالقبعة الرمادية كونه اللون الذي يمزج بين الأبيض والأسود، فهو خليط بين النوعين الأولين، والغالب أن هذا الهاكرز لا يقوم بالهجوم بدافع خبيث بل يقوم بذلك للزيادة من خبراته وحصوله على معارف جديدة بالثغرات الأمنية⁽⁴⁾.

وجدير بالإشارة هنا أن مصطلح المخترق والهاكرز ليسا مترادفان، فالمخترق ليس مبرمجا في حد ذاته، بل يقوم باستغلال البرامج التي تمت صياغتها لهذا الغرض، وينفذ هجما بها، غير أن الهاكرز هو شخص يهوى علم البرمجيات، بلغاتها وأنظمتها وبرامجها، ودائما ما يعمل على تطويرها، فهو شخص متمرس وخبير في نوع معين من اللغات البرمجية أو نظام من أنظمة التشغيل⁽⁵⁾، لكن في النهاية يبقى المخترق والهاكرز في دائرة واحدة وهي الاختراق.

2- الإغراق أو القصف المعلوماتي:

وهو نوع من الاعتداء على الجهوزية أو قابلية عمل النظام المعلوماتي، ويكون عن طريق إرسال كم هائل من الرسائل الإلكترونية والبيانات بحيث يعجز النظام على استيعابها وتحليلها، فيزيد الضغط عليه مما يؤدي إلى تعطيله وعدم قدرته على استقبال رسائل جديدة، مما ينجر عنه

(1) بشرى حسين الحمداني، القرصنة الإلكترونية: (أسلحة الحرب الحديثة)، الطبعة الأولى، دار أسامة للنشر والتوزيع ونبلأ ناشرون وموزعون، الأردن، 2014، ص 18.

(2) أسامة سمير حسين، الاحتيال الإلكتروني: (الأسباب والحلول)، الطبعة الأولى، الجنادرية للنشر والتوزيع، الأردن، 2011، ص 136.

(3) بشرى حسين الحمداني، المرجع نفسه، ص 19..

(4) أسامة سمير حسين، المرجع نفسه، ص 136.

(5) بشرى حسين الحمداني، المرجع نفسه، ص: 14-15.

ضرر مادي ومعنوي غير محدودة⁽¹⁾، فهو إذا يركز على محدودية القدرة الاستيعابية وضيق مساحة التخزين في البريد الإلكتروني، فيستنزف قدرته ويجبره على التوقف عن أداء وظائفه⁽²⁾.

3- استهداف المعلومات:

يتخذ استهداف المعلومات أربعة أشكال هي:

أ- إتلاف المعلومات:

هو من أخطر أنواع الجرائم التي تستهدف المعلومات وهي تقع من خلال الحواسيب الآلية أو الشبكات العنكبوتية⁽³⁾، ويتم فيها إتلاف البيانات المسجلة داخل الحواسيب وبيانات الشبكات المغلقة أو المفتوحة، وإتلاف ببيانات البرامج الحساسة، وبيانات نظم التحكم والمتابعة، عن طريق اللجوء إلى استخدام البرمجيات الخبيثة من فيروسات وديدان قادرة إلى مسح وإتلاف المعلومات⁽⁴⁾.

ب- تزوير المعلومات:

يتطلب هذا النوع من الصورة الإجرامية نوعاً من معرفة تقنية عالية نظراً لارتباطها بالصياغة التقنية لبرامج معالجة المعلومات⁽⁵⁾، ويستطيع الجاني من خلال تلك التقنيات تغيير مسار الطيران وكل وسائل المواصلات وإحداث تغيير في أنظمة التوجيه، وتزوير محتوى الرسائل الإلكترونية وزرع رسائل كاذبة، ويكون الهدف منها أحداث أضرار بالمعلومات المتداولة بما يحقق الإضعاف والإرباك بالوظائف الحيوية للمراكز المستهدفة وشل حركتها، وقد ينفذ من أجل تحريف معلومات المواقع على شبكة الإنترنت لغرض إرباك وتشهير المواقع خاصة إذا كان مشهوراً بقدرته على ضمان الأمن والحماية⁽⁶⁾.

ج- الإغراض الإلكتروني:

تعتبر الإعاقة بين بين النظم والآليات الإلكترونية المضادة التي يتم الاعتماد عليها في إعاقة نظم العدو وما يمله من آليات إلكترونية، والتي تتأسس على مبدأ شل نظم العدو من خلال التأثير على عملياتها وأدائها⁽⁷⁾.

(1) سعيد عبيدي، المرجع السابق

(2) عبد الله بن حسين آل حنجراف القحطاني، المرجع السابق، ص 42.

(3) المرجع نفسه، ص 42.

(4) حكيم غريب، المرجع السابق، ص ص: 820-821.

(5) أيمن عبد الله فكري، المرجع السابق، ص 448.

(6) حكيم غريب، المرجع نفسه، ص 822.

(7) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي: (رؤية مستقبلية)، مجلة رسالة الحقوق، المجلد 07، العدد 02، كلية القانون، جامعة

كربلاء، العراق، 2015، ص ص: 74-121: <https://www.iasj.net/iasj?func=issueTOC&isId=6335&uiLanguage=ar>

فتعرف الإعاقة أو التشويش على أنها: (عبارة عن إشعاعات كهرومغناطيسية أو هيدروصوتية غير مدمرة، تقوم بخفض نوعية عمل الوسائط الإلكترونية والهيدروصوتية القائمة على توجيه الأسلحة والعتاد العسكري، أو منظومات إنتاج المعلومات...) ⁽¹⁾، وتنقسم الإعاقة إلى نوعين:

• الإعاقة الإلكترونية الإيجابية:

يمكن تعريف الإعاقة الإلكترونية الإيجابية على أنها: (عملية توجيه حزمة من الأشعة الكهرومغناطيسية المتعمدة إلى مستقبلات النظم والوسائل الإلكترونية المعادية، للتأثير على أدائها بتعطيمها، أو خادعها بهدف شل عملها وإرباكها)، وتتم هذه الإعاقة بخمس مراحل، حيث تبدأ بتحديد الهدف ثم بعدها يتم نوجه بيانات الإعاقة إلى القاعدة التي ستنفذها، ثم بعدها تم تنفيذها من قبل هذه الأخيرة، وفي الأخير مرحلة مراقبة مفعولها على العدو ⁽²⁾.

• الإعاقة الإلكتروني السلبية:

تعرف الإعاقة الإلكترونية السلبية على أنها: (هي عملية انعكاس متعمد للموجات الكهرومغناطيسية الصادر من أجهزة إرسال النظم والوسائل الإلكترونية المعادية، وخاصة الرادارية، نتيجة لإجبارها على الاصطدام بأجسام معينة دون سواها، فيرتد الشعاع مرة أخرى نحو مستقبلات هذه النظم والمسائل المعادية، مسببا إرباكها، وتقليل كفاءتها في تنفيذ مهامها) ⁽³⁾، وهذا النوع من الإعاقة يتطلب أمر تنفيذها إلى تطوير الكثر من الأنظمة الإلكترونية ومن ذلك جهاز تشييت الموجات المضادة، أجهزة الإنذار المبكر وما إلى ذلك ⁽⁴⁾.

جدير بالذكر أن تنفيذ هجوم مثل هذا يتطلب كفاءة عالية، إلا أن بعض الباحثين قد أفاد بإمكانية اعتماد الجماعات على هذا الأسلوب، وذلك لإمكانية اقتناء هذه المعدات من السوق السوداء، كما يمكن أيضا أن ينفذ هذا الهجوم من خلال اعتماد الآليات الفيروسية ⁽⁵⁾.

غير أننا نرى أن هذا الاحتمال غير وارد، على الأقل في الفترة الراهنة، أو المستقبل القريب، وذلك لأن استعمال مثل هذا النمط من قبل الجماعات الإرهابية يفترض فيه تمتعهم بالكفاءة اللازمة والحذاقة العالية، فضلا عن علمهم بهذا الأمر من أساسه، ويفترض أيضا أنهم يمكن أن يحصلوا في يوم من الأيام على مثل هذه المعدات حتى من السوق السوداء، وهذا كله أمر غير محتمل بالمرّة.

(1) أ. ي. بالي، ن. ب. مارين، موسوعة الحرب الإلكترونية، ترجمة: (يوسف إبراهيم الجهماني)، الطبعة الأولى، دار الحوار، سورية، 1992، ص 15.

(2) فيصل محمد عبد الغفار، المرجع السابق، ص ص: 38-40.

(3) المرجع نفسه، ص 40.

(4) سامر مؤيد عبد اللطيف، المرجع السابق.

(5) حكيم غريب، المرجع السابق، ص 822.

ونأسس لرأينا هذا بما أشار إليه جاسم محمد البصيلي من حقائق، فقد أشار إلى أن الدول التي تمتلك مثل هذه التقنيات تتفادى تقديم دورات تدريبية حولها، فضلا عن ندرة المراجع التي تتناول موضوعها، بالإضافة أيضا إلى تكلفتها العالية، وبيعها واقف على مجموعة من الضوابط والقيود الشديدة، بل إن بيعها في بعض الأحيان يقابل بالرفض، فضلا عن ذلك كله، هناك من القادة من لا يعرف شيئا عن قواعد هذا المجال⁽¹⁾، هذا كله بالنسبة للدول، فكيف يعقل حينها احتمال توظيف الجماعات الإرهابية لهذه الصورة؟ إنه كمن يحتمل حصول الجماعات الإرهابية على أسلحة نووية.

ثم إن القول بأن مثل هذا الهجوم يمكن تنفيذه بالاعتماد على الوسائل الفيروسية قول مجاني للصواب، لأننا حينها لا نكون أمام إعاقة أو تشويش، بل أمام هجمة فيروسية يمكن أن ينفذها آخر البلهاء في مجال البرمجيات، في حين أن الاعتراض أو التشويش هو عملية معقدة تحتاج إلى كفاءة ومعدات خاصة غير متاحة للجماعات الإرهابية، ومع ذلك تبقى متاحة للدول، وهذا الذي أملى علينا إدراجها ضمن صور الإرهاب الإلكتروني الذين يمكن أن تمارسه الدولة.

4- التجسس الإلكتروني:

تعتبر المعلومات من أثمن ما يمكن أن يمتلكه الإنسان ويحافظ عليه، نظرا لما لها من أهمية قصوى في الكثير من المجالات الحيوية، وقد سعى إلى جمعها وتوثيقها منذ العصور الأولى وصولا إلى عصر المعلومات، أين اكتسبت فيه كيانا جديدا وبعدا استراتيجيا مهما، الأمر الذي جعل حمايتها وحماية سريتها بشتى الطرق القانونية والتقنية أمر في قمة هرم المسؤوليات الأمنية⁽²⁾.

ومع ظهور تقنيات المعلومات الحديثة أصبحت المعلومات المتداولة على الشبكات الإلكترونية تمتلك بعدا حيويا جدا، بحيث اعتبرها البعض " نפט العصر " كونها المورد الجيوسياسي الأكثر أهمية لما تملكه من قدرة كبيرة على التأثير في صياغة القرارات وإعادة تشكيل الأمم والإمارات⁽³⁾.

(1) جاسم محمد البصيلي، الحرب الإلكترونية: (أسسها وأثرها في الحروب)، الطبعة الثانية، المؤسسة العربية للدراسات والنشر، بيروت، 1989، ص 35.

(2) عزيزة راجحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2017-2018، ص 23.

(3) إريك روزنباخ وكاثارين مانستد، رأسمالية البيانات: (تحولات الصراع بين القوى الكبرى على قوة المعلومات)، المستقبل للأبحاث والدراسات المتقدمة، 12 يونيو 2019، تم الإطلاع عليه بتاريخ 17 جانفي 2020، على الساعة 17:36 سا، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/4794/> رأسمالية البيانات-تحولات-الصراع-بين-القوى-الكبرى-على-قوة-المعلومات

لذلك تكاثرت الزخم عليها بالمحاولات المتكررة للاستيلاء عليها عبر برامج التجسس الإلكترونية، فبرعت الدول في استغلال التقنيات المعلوماتية المتطورة لممارسة التجسس الإلكتروني الذين يمكن تعرفه على أنه اختراق يهدف إلى التعرف على المعلومات التي يتضمنها الحاسوب دون ممارسة أي شكل من أشكال الهجمات التي تؤدي إلى تلفها⁽¹⁾.

تضلع الدول بشكل أساسي في الاستعانة بتقنيات التجسس الإلكتروني عبر أجهزة الاستخبارات التابعة لها وهذا بهدف الحصول على معلومات سرية حساسة ليتم إفشائها لدول معادية أو بهدف استغلالها بما يضر بالمصالح الوطنية للدولة المستهدفة⁽²⁾، وغالبا ما يتم التركيز على المعلومات الاقتصادية نظرا لما لها من أهمية كبرى، وقد أشار المرشح الأمريكي لرئاسة وكالات المخابرات الأمريكية إلى هذه الأهمية في معرض جوابه عن سؤال وجه إليه من قبل لجنة الكونجرس، عما ينوي التركيز عليه في حالة قبول ترشحه فكان جوابه: (التجسس الاقتصادي)⁽³⁾.

كما قد يتعدى التجسس الإلكتروني القطاعات المدنية إلى المساس بالقطاعات الخاصة بالقوات المسلحة نظرا لطبيعة وأهمية المعلومات التي تحويها تلك القطاعات، وهذا ما يفسر الاهتمام الكبير المنصب على الجاسوسة العسكرية⁽⁴⁾، إذ يهدف المتجسس من خلالها الحصول على خطط الدفاع العسكري وأسرار عسكرية حيوية، ومعلومات استخباراتية، وقد يمتد ذلك إلى مدى بعيد كرسم خرائط لشبكات الحاسوب واستخدامها في ما بعد من أجل شن هجمات إلكترونية فاعلة⁽⁵⁾.

وتعتبر أسلحة التجسس السيبراني من بين الأسلحة الأكثر سرية لدرجة أنه حتى وجودها لا يعرف به سوى عدد ضئيل من الناس وهم القادة العسكريين⁽⁶⁾.

لا تقتصر عمليات التجسس الإلكتروني على المعلومات التي تحوزها الدول والشركات الاقتصادية، بل يتم التجسس أيضا على طلبات البحث في بنوك المعلومات الخارجية، إذ يمكن استغلالها من قبل

(1) سامر مؤيد عبد اللطيف، المرجع السابق.

(2) فتيحة رصاع، المرجع السابق، ص 77.

(3) نبيل علي، العرب وعصر المعلومات، عالم المعرفة، الإصدار رقم الإصدار 184، المجلس الوطني للثقافة والفنون والآداب، الكويت، أبريل 1994، ص ص: 218-219.

(4) نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012-2013، ص 64.

(5) نسرین الشحات الصباحي، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول/ (دراسة حالة إسرائيل)، المركز العربي الديمقراطي، 29 أبريل 2016، تم الاطلاع عليه بتاريخ 28 ديسمبر 2019، على الساعة 19:07 سا، في الموقع:

<https://democraticac.de/?p=30962>

(6) فرد كابلان، المنطقة المعتمدة: (التاريخ السري للحرب السيبرانية)، ترجمة (لؤي عبد المجيد)، عالم المعرفة، رقم الإصدار 470، المجلس الوطني للثقافة والفنون والآداب، الكويت، مارس 2019، ص 177

أجهزة التجسس المختلفة من أجل تحديد بروفایل دقيق لاحتياجات النخب العلمية في الدول أو المجتمعات الأمر الذي يعرضها لاكتشاف المخططات السياسية والمشاريع المتنوعة التي تريد أن تبقىها سرية⁽¹⁾.

ويمكن أن نمثل لمثل هذه الجوسسة بما تقوم به إيران على الفضاء الإلكتروني من اقتحامات وهجمات من أجل التجسس على المعلومات وجمعها ولاسيما تلك المتعلقة بالاتصالات والسفر وبيانات الملكية وعملاء الشركات ورصد وتتبع عمليات أفراد مخصصين، من أجل جمع المعلومات والإضرار بخصومها، وتستعين على ذلك بإمكانياتها وبمجموعات من الهاكرز الذين يمتلك بعضهم انتماءات مختلف⁽²⁾.

وقد أعلن الاتحاد الأوروبي عن إدراج إدارة الأمن الداخلي للاستخبارات الإيرانية على قائمة الإرهاب الخاصة بها⁽³⁾، وبالتالي فإن الهجمات الإلكترونية التي تهدف إلى ممارسة التجسس والتي ينفذها هذا الجهاز والحرس الثوري الإيراني يعتبر من قبيل الهجمات الإرهابية السيبرانية من وجهة نظر الدول الغربية.

5- تدمير المواقع:

يقصد بتدمير المواقع الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام (pc-server) أو مجموعة نظم متصلة شبكياً بهدف تخريب نقطة الاتصال أو النظام⁽⁴⁾.

المطلب الثاني:

تداعيات الإرهاب الإلكتروني:

لقد صنع الإرهاب الإلكتروني اتجاهات جديدة وقاسية من العنف والترويع، وتأثيرات سلبية على الأمن والاستقرار، وآليات جديدة لدعم الكراهية والتطرف والبغضاء، فأصبح هاجساً مقلقاً على المدنيين فرادى وجماعات (الفرع الأول) وبرزت على الدول تحديات سياسية وأمنية متزامنة مع تصاعد التهديدات الاستثنائية والمجهولة والتي تهدد أمنها القومي وتضع عقبات مضنية أمام

(1) نبيل علي، المرجع السابق، ص 216.

(2) صباح عبد الصبور، تكتيكات مضادة: (حدود قدرة إيران على توظيف الاختراقات السيبرانية)، المستقبل للأبحاث والدراسات المتقدمة، 02 أبريل 2019، تم الاطلاع عليه بتاريخ 25 جانفي 2020، على الساعة 21:31 سا، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/4645/> تكتيكات مضادة-حدود قدرة إيران-على توظيف الاختراقات-السيبرانية

(3) مروة الأسدي، سباق التجسس الإلكتروني وزعزعة النظام العالمي، 20 ديسمبر 2017، تم الاطلاع عليها بتاريخ 18 جانفي 2020، على الساعة 23:12 سا، في الموقع: <https://m.annabaa.org/arabic/informatics/13571>

(4) مصطفى يوسف كافي، الإدارة الإلكترونية: (إدارة بلا أوراق-إدارة بلا مكان-إدارة بلا زمان-إدارة بلا تنظيمات جامدة)، المرجع السابق، ص 444.

مصالحتها وتطلعاتها (الفرع الثاني) الأمر الذي أدخل المجتمع الدولي في دوامة من التهديدات والأخطار غير المسبوقة، والصراعات غير المعهودة، التي تستعص سيادة القانون الدولي عن ردعها وتسويتها نظرا لطبيعتها وتعقيدها وانعدام النظم الأساسية التي تكفل الحقوق وتحدد المسؤوليات (الفرع الثالث).

الفرع: تداعيات الإرهاب الإلكتروني على الأفراد:

تعتبر الثورة المعلوماتية الهائلة نقطة تحول مفصلية في مفاهيم الحقوق والحريات، فقد ظهر في كنفها شكل جديد من أشكال الحقوق الإنسانية والحريات الأساسية، وبرزت خلالها أساليب حديثة ومتطورة لآليات ممارستها والتمتع بها غير أن هذه القفزة العظيمة في ميدان حقوق الإنسان لحقتها تبعات خطيرة تهددها وتنتهكها على أيدي الجماعات المتطرفة والأنظمة الشمولية والاستبدادية (أولا)، فضلا عما ترتب عن هذا التطور من تمكين المتطرفين عبر منصاته من تزيف وعي الأفراد وتهديد أمنهم الفكري والثقافي (ثانيا).

أولا: تداعيات الإرهاب الإلكتروني على حقوق الإنسان الرقمية:

"إن حقوق الإنسان هي حقوق طبيعية متأصلة في كل البشر مهما كانت أوضاعهم وصفاتهم وأعرافهم ولغاتهم، ولكل البشر الحق في الحصول على تلك الحقوق الإنسانية التي لا تقبل التجزئة على قدم المساواة دون أي شكل من أشكال التمييز" (1).

وقد جاءت العديد من الأطر القانونية الدولية التي تدعم حقوق الإنسان وتمنع أي شكل من أشكال الاعتداء عليها، ومن أبرزها الإعلان العالمي لحقوق الإنسان والعهد الدولي المتعلقين بالحقوق المدنية والسياسية والحقوق الاقتصادية والاجتماعية والثقافية، وتتبعها سلسلة كبيرة من التشريعات الدولية التي تمنع التمييز العنصري وحرية الصحافة وغيرها من الحقوق الأساسية للإنسان، ومع التطور التكنولوجي الكبير الذي يشهده العصر الحديث برز الفضاء الإلكتروني بشكل جديد من أشكال حقوق الإنسان المتعلقة بحرية استخدام تكنولوجيا المعلومات، وعلى صعيد آخر، أدى الترابط الكبير بين المرافق الأساسية للدولة مع هذا الفضاء الحديث إلى نشوء ترابط وظيفي بين العالم الرقمي والحصول على الحقوق الطبيعية للإنسان (2).

(1) هيئة الأمم المتحدة، حقوق الإنسان، (د.ت.ن)، تم الاطلاع عليها بتاريخ 15 جانفي 2020، على الساعة 22:23، على موقع:

<https://www.un.org/ar/sections/issues-depth/human-rights/>

(2) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص ص: 316-317.

أطلق الإعلان الإفريقي لحقوق وحرّيات الإنترنت، مجموعة متكاملة من الحقوق والحرّيات الأساسية التي يجب على الدول العمل على تنميتها وتعزيزها والحفاظ عليها، ومن أبرز هذه الحقوق التي تضمنها، نجد حق الوصول إلى الإنترنت بتكاليف مقبولة، ضمان حرية التعبير، الحق في المعلومات، حرية التجمع والتنظيم على الإنترنت، الخصوصية، الأمان على الإنترنت وغيرها ، وهذه الحقوق التي تضمنها هذا الإعلان لا تخرج في محتواها عن الإطار التشريعي لحقوق الإنسان المعلنة في الأحكام والمواثيق الدولية، وقد كرست الجمعية العامة أحكاما متعلقة بالاستخدام السلمي لتكنولوجيا المعلومات، وضمان حقوق الإنسان المتعلقة بها⁽¹⁾، ومن أهم القرارات التي صادقت عليها الجمعية العامة للأمم المتحدة، القرار الذي اعتمدته مجلس حقوق الإنسان في دورته الثانية والأربعون والمتعلق بالحق في الخصوصية في العصر الرقمي الصادر بتاريخ 26 سبتمبر 2019.

إن هذه الحقوق المشار والتي تكرسها وتحميها الأعراف والقوانين الدولية أصبحت أكثر عرضة للانتهاكات الإلكترونية في الساحة السيبرانية، إذ أن استخدام هذه الساحة في القيام بارتكاب نشاطات وأعمال إرهابية مختلفة، ينعكس سلبا على هذه الحقوق التي تعتبر بين الركائز الأساسية لحقوق الإنسان الدولية، فلبث الرعب في السكان وانتهاك الخصوصية، وتعرض معلوماتهم للسرقة أو التلف، أو تعريض الخدمات التي تقدمها المرافق الحكومية لهم، يشكل جزءا لهم عن ممارسة حياتهم الطبيعية بسلام واطمئنان، ويحرمهم من الراحة والسكينة ويحول دونهم ودون حقوقهم الأساسية⁽²⁾، وليس هذا فحسب، بل هناك مخاطر كبرى تهدد حقوق الإنسان الأساسية وهذا من خلال استعمال هذه الساحة العالمية في الدواعي الإرهابية ويمكن أن نبين منها ما يلي:

1- خطاب الكراهية والتحريض على العنف:

إن منصات ومنظمات الشبكات الاجتماعية التي صيغت من أجل الوقوف أصاد الخطاب التطرفي العدائي لاحظت أن معظم تفاعلات الكراهية على الشبكة العنكبوتية أصبحت تنتشر بشكل متسارع، وحسب " قاعدة الكراهية " ⁽³⁾، التي تجمع وتحلل خطابات الكراهية على الإنترنت

⁽¹⁾ voir: la Déclaration Africaine des Droits et Libertés de l'Internet dernière mise à jour 28 août 2014, sur le site suivant:

https://www.2idhp.eu/images/declaration-africaine-des-droits-et-libertes-de-l-internet_170314.pdf

⁽²⁾ عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص 319.

⁽³⁾ قاعدة الكراهية (Hatebase): مشروع مشترك يتمثل في مستودع رقمي لخطاب الكراهية المنظم متعدد اللغات والذي يعتمد أساسا على المستخدمين، ويعتمد على ما يتم توظيفه من نصوص وكلمات بأي صيغة كانت وعلى أساسها يتحدد نمط خطاب الكراهية، أنظر الموسوعة الحرة:

- <https://en.wikipedia.org/wiki/Hatebase>

فإن كافة أغلب خطابات الكراهية تستهدف أفراداً بناءً على انتماءاتهم العرقية والوطنية والدينية والاجتماعية⁽¹⁾.

يعد خطاب الكراهية الذي تنتهجه التنظيمات الإرهابية يعد أكثر خطراً وأبلغ أثراً، فقد اثبت الواقع والحال أثره الشديد في قطع أواصر المجتمعات والتحريض على اعتماد العنف كلغة للحوار، عنف قد تتجر عنه أعتى العمليات الإرهابية التقليدية، ويتجلى مثال هذا الأثر الناجم عن الخطابات المسمومة ما انجر عن خطاب الكراهية الغربي ضد المسلمين التي أنتجت مجزرة مسجدني نيوزلندا⁽²⁾، وكذلك من خلال تعرض الشاب اليمني عمر باطويل في محافظة عدن اليمنية إلى عملية اغتيال جراء اتهامه بالإلحاد على شبكة التواصل الاجتماعي فيسبوك والدعوة إلى اغتياله، كما تتجلى أيضاً من خلال الإرهاب الطائفي في الشرق الأوسط بين السنة والشيعة.

2- إرهاب الدولة للمعارضين:

ترمي كل الأنظمة التي ترتكز على تكريس مبدأ الديمقراطية في بلدانها إلى ضمان الكثير من الحقوق والحريات لمواطنيها، كرحية الرأي والتعبير، وحريةهم في تكوين صروح لممارسة ذلك من خلال منحهم الحق والحرية في إنشاء الجمعيات وتنظيم التجمعات دون أن ينتابهم خوف أو وجل من تعرضهم لأنواع من التنكيل بهم كالاقتال غير القانوني والزج بهم في السجون⁽³⁾.

وتعتبر ساحة الفضاء الإلكتروني أداة ذات قيمة عالية في تفعيل هذه الديمقراطية وهذا من خلال توظيف هذه الآليات التقنية المتعلقة بمجال المعلومات والاتصال الرقمية في توليد وجمع وتصنيف وتحليل ومعالجة ونقل وتداول المعلومات والبيانات والمعارف المتعلقة بممارسة الديمقراطية وآلياتها المختلفة، وقد عملت بشكل كبير في دعم التحول الديمقراطي وتكريس المشاركة الفعلية في السياسة وضمان الحق في حرية الرأي والتعبير والمساهمة في إدارة شؤون الدولة والمجتمع⁽⁴⁾.

(1) إغنيو كاكاياردون وآخرون، مكافحة خطاب الكراهية في الإنترنت، ترجمة (صابر طروات)، سلسلة اليونسكو حول حرية الإنترنت، فرنسا، 2015، ص 13: https://unesdoc.unesco.org/ark:/48223/pf0000233231_ara

(2) جمانة حمدي، الفضاء الإلكتروني يدين خطاب الكراهية المسبب لهجوم نيوزلندا، 15 مارس 2019، تم الاطلاع عليه بتاريخ 28 نوفمبر 2019، على الساعة 19:25، في الموقع: <https://m.arabi21.com/Story/1166783>

(3) جيدرور حاج بشير، أثر وسائل التواصل الاجتماعي في عملية التحول الديمقراطي في الدول العربية: (دراسة مقارنة)، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، السنة الجامعية 2016-2017، ص 57.

(4) منال قدواح، الإعلام الجديد: (خطوات وأعدة نحو بروز مفهوم جديد للديمقراطية وآليات ممارستها الرقمية)، مجلة العلوم الإنسانية، المجلد "ب"، العدد 43، جامعة منتوري، قسنطينة، الجزائر، جوان 2015، ص ص: 75-88:

<http://revue.umc.edu.dz/index.php/h/article/view/2082>

ورغم أن ظهور مثل هذا الفضاء قد عكر الجو على الأنظمة الشمولية والاستبدادية حين قلص من قدرتهم على السيطرة على المجتمع المدني⁽¹⁾، إلا أن الكثير من الدول تقوم بتوظيف هذا الفضاء في قمع المعارضين وبسط الرقابة على المواطنين. فقد أدرج المجلس الأعلى السيبراني في إيران ضمن قائمة مؤسسة مراسلون بلا حدود كأسوأ 20 مؤسسة تقمع حرية الإعلام في 2020، وذلك بمناسبة اليوم العالمي لمناهضة الرقابة الإلكترونية⁽²⁾، وعملت على إسكات الاحتجاجات عبر إجراءات قمع فريدة تركز على حضر التجوال الإلكتروني وقطع الإنترنت⁽³⁾.

كما أكد تقرير استقصائي لميدل إيست البريطانية أن السلطات الإماراتية تتبع سياسة التجسس على مواطنيها والمقيمين بالإمارات، وملاحقة أي رأي يعارض سياستها الداخلية أو الخارجية وقمع حرية الرأي والتعبير⁽⁴⁾، أما في الجزائر فهناك مثال شاهد لقمع حرية الرأي والتعبير، فقد تعرض الصحفي محمد تامالت⁽⁵⁾ إلى المتابعة القضائية والحبس الذي توفي إثره في ظروف مشبوهة وغامضة، وهناك مخاوف فعلية من تزايد التضييق على حرية التعبير والرأي الذي تقدم عليه السلطات الجزائرية على النشطاء والمدونين⁽⁶⁾.

وأفاد أيضا بحث نشر على موقع حملة المركز العربي لتطوير الإعلام الاجتماعي بأن الشباب الفلسطيني يخشى من ممارسه حقه في إبداء الرأي وحرية التعبير نظرا للمضايقات

(¹) يانشيا بنكلر، ثورة الشبكات: (كيف يغير الإنتاج الاجتماعي الأسواق والحریات)، ترجمة (فريج سعيد العويضي)، الطبعة العربية الأولى، مكتبة العبيكان، الرياض، المملكة العربية السعودية، 2012، ص 368

(²) صالح حميد، المجلس السيبراني في إيران.. يد إلكترونية لقمع الحريات، 12 مارس 2020، تم الاطلاع عليها بتاريخ 22 مارس 2020 على الساعة 08:06 سا، في الموقع:

<https://www.alarabiya.net/ar/iran/2020/03/12/> المجلس السيبراني في إيران يد إلكترونية لقمع الحريات

(³) أنظر: موقع قناة الجزيرة، ليبيراسيون: (كيف أسكتت السلطات الإيرانية صوت الاحتجاجات)، 20 نوفمبر 2019، تم الاطلاع عليها بتاريخ 18 فيفري 2020 على الساعة 19:23 سا، في الموقع:

<https://www.aljazeera.net/news/politics/2019/11/20/> إيران-الاحتجاج-القمع-الإنترنت-البنزين-خامنتي

(⁴) صحيفة الشرق، تقارير عالمية: (أبوظبي تمارس الإرهاب الإلكتروني وتهدد الأمن السيبراني الإقليمي)، 22 مايو 2019، تم الاطلاع عليه بتاريخ 12 جانفي 2020، على الساعة 18:53 سا، في الموقع:

<https://m.al-sharq.com/article/22/05/2019/> تقارير عالمية-أبوظبي تمارس الإرهاب الإلكتروني وتهدد الأمن السيبراني الإقليمي

(⁵) محمد تامالت: "صحفي جزائري بريطاني، سجن في يوليو 2016 بتهمة الإساءة إلى الرئيس عبد العزيز بوتفليقة وإهانة هيئة نظامية، توفي وهو في الحجز في 11 ديسمبر 2016 بعد بضع أشهر من حبسه، ويعتبر كأول صحفي توفي في الحبس في عهد الجزائر المستقلة". نقلا عن الموسوعة الحرة:

- https://ar.wikipedia.org/wiki/%D9%85%D8%AD%D9%85%D8%AF_%D8%AA%D8%A7%D9%85%D8%A7%D9%84%D8%AA

(⁶) عبد المجيد رمضان، الديمقراطية الرقمية كآلية لتفعيل الديمقراطية التشاركية: (حالة الجزائر)، دفاتر السياسة والقانون، المجلد 09، العدد 16، جامعة قصدي مرياح، ورقلة، الجزائر، جانفي 2017، ص ص: 75-88:

<https://www.asjp.cerist.dz/en/article/28349>

والاستجابات والاعتقالات التي يتعرض إليها على خلفية ذلك⁽¹⁾، وهذا ما أثبتته دراسة كما أفاد وثائقي "أسلحة المراقبة الشاملة" أن بعض الحكومات العربية تلجأ إلى الغرب من أجل اقتناء أنظمة متطورة لفرض الرقابة، فكل عملية شراء أو كل زيارة لموقع، أو كل رسالة نصية خارجة أو واردة أو كل مكالمة تجريها يتم تتبعها، وقد كشف هذا الوثائقي أن أحمد منصور قد قضى اعتقال لمدة 8 أشهر بعد أن أنفقت حكومة بلده أموالاً طائلة لتعقبه، لمجردة تغريده عن تجاوزات ارتكبتها الحكومة الإماراتية⁽²⁾.

كما تثير الرقابة على الفضاء الإلكتروني أيضاً هجسا كبيرا بالنسبة للصحافيين الذين تخشى مصادرهم من التواصل معهم خوفا من الملاحقات والإدانات، ويمتد هذا الخوف أيضاً إلى بعض المحامين الذين يتبعهم هاجس وصول محادثاتهم من موكليهم إلى جهات الادعاء العام، فضلا عن هواجس الخوف التي تطارد رواد السياسة القدماء أو الناشطون المتمردون أو دعاة التغيير الاجتماعي⁽³⁾.

ثانيا: تداعيات الإرهاب الإلكتروني على الأمن الفكري:

لن ننظر في هذا المقام إلى المجندين في صفوف التنظيمات الإرهابية عبر الإنترنت باعتبارهم مجرمين ومخربين، ولكن سننظر إليهم باعتبارهم ضحايا ضمن ضحايا الهجمات الإرهابية الدعائية الجذابة التي يمارسها المتطرفون والإرهابيون على الساحة الإلكترونية.

يتميز الخطاب المتطرف عموماً بنوع من الجاذبية والقدرة على استمالة الشباب وتأجيح أحاسيسهم، فيجد الشباب أنفسهم في وسط من الصراع الفكري وفي معركة دائمة يصور له فيها رواد الشبكات والناشطين فيها أنه في قلب معركة وصراع بين الحق الذي هم أهله وممثلوه، ووباطل يقيمه ويدعمه من خالف لهم الأمر والرأي، ومع هذا الخطاب الجذاب والضغط التي تحاصر الشباب يصبح الفضاء الإلكتروني أكبر داعم معنوي وفكري للمتطرفين والغلاة⁽⁴⁾، وأصبح

(1) حملة المركز العربي لتطوير الإعلام الاجتماعي، شبكة مسكتة: (تلقى الشباب الفلسطيني لا يشعرون بالأمان للمشاركة السياسية عبر الإنترنت)، 20 أكتوبر 2019، تم الإطلاع عليه بتاريخ 18 أكتوبر 2019، على الساعة 18:33 سا، على موقع:

<https://7amleh.org/2019/10/20/%D8%A7%D8%B3%D8%AA%D8%B7%D9%84%D8%A7%D8%B9-%D8%AD%D9%85%D9%84%D8%A9.pdf>

العنوان الإلكتروني للبحث:

<https://7amleh.org/wp-content/uploads/2019/10/%D8%A7%D8%B3%D8%AA%D8%B7%D9%84%D8%A7%D8%B9-%D8%AD%D9%85%D9%84%D8%A9.pdf>

(2) أنظر: الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، أسلحة المراقبة الشاملة، 17 جوان 2019، تم الإطلاع عليه بتاريخ 18 أكتوبر 2019، على الساعة 20:30 سا، على موقع: <https://www.politics-dz.com/> أسلحة-المراقبة-الشاملة

(3) بروس شنابير، المعلومات وجالوت: (المعارك الخفية لتجميع بياناتك والسيطرة على عالمك)، ترجمة: (أحمد مغربي)، الطبعة الأولى، منتدى العلاقات العربية والدولية، قطر، 2017، ص ص: 152-154.

(4) فايز بن عبد الله الشهري، الخطاب الفكري على شبكة الإنترنت: (رؤية تحليلية لخصائص وسمات التطرف الإلكتروني)، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن الفكري، جامعة الملك سعود، الرياض، 1429 هجرية، ص 37.

بديلا عن الوسائل التقليدية من فضائيات ووسائل إعلام في الغزو الثقافي لما له من تأثير فعال على تغيير وجهات النظر المختلفة والتحكم في السلوكيات والقيم في المجتمع المتصفح له مما يشكل خطرا كبيرا على الأمن الفكري للأفراد⁽¹⁾.

إن ما يتم تداوله والترويج له من مفاهيم منحرفة في مواقع التواصل الاجتماعي التي تحظى بالاهتمام والإقبال الشديدين خاصة من فئتي الشباب والمراهقين الذين لا يملكون خلفية فكرية واعية، أو تحصين ثقافي أو ديني ممن يندفعون بانفعال خلف الأحداث، وخلف كل جديد يشكل خطرا كبيرا على الأمن الفكري للأفراد، إذ بعد الدراسة والتحليل ثبت يقينا أن محتوى المعلومات التي يتم تداولها في صفحات ومواقع التواصل الاجتماعي نتج عنه أثر مريب، حيث تشابكت المفاهيم وتداخلت الكثير من المدلولات للعديد من المصطلحات الثابتة في يقين المجتمعات المختلفة فينشأ عنها فكر مختلط تركب من خلال تلاقي المفاهيم المختلفة التي أصبحت مع تكرارها وتداولها من المسلمات، الأمر الذي انعكس سلبا على التوجه الثقافي المتوارث لدى الشباب، ويتم تبنيه وقبولها مسايرة لهم لهذا المجتمع الافتراضي فينشأ فيهم السلوك العدواني الذي يتم صياغته في قالب عملي عبر انتهاج العنف والإرهاب⁽²⁾.

تلجأ التنظيمات الإرهابية والمتطرفة في عملية التحشيد والتجنيد إلى الخلط بين الفكر المغلق المنحرف من جهة وبين دغدغة مشاعر الشباب من جهة أخرى، فيقدون النساء البارعات المتمنقات ليلعبن بعواطف الشباب على وتر المظلومة والاستبداد والقهر الذي تمارسه الأنظمة والحكومات حتى يقتنعوا بأن الإرهاب هو الحل الذي يدفع به الظلم وترد به الحقوق⁽³⁾.

وليست فئة المراهقين والشباب هم فقط من يتم استهدافهم من خلال الترويج الإعلامي التطرفي على الإنترنت، فالأطفال أيضا يعتبرون من ضمن ضحايا هذا الفكر المنحرف، إذ تسعى التنظيمات الإرهابية إلى ضمهم إلى صفوفها وزرع بذرة السلوك العدواني فيهم، لتخلق بعدها جيلا من المتطرفين العدوانيين الذين سلبوا هويتهم ومفاهيمهم الثقافية والدينية، فالجماعات الناشطة على ساحات الإنترنت تستغل مواطن الضعف لدى الأطفال وتقوم بعدها بتعبئتهم لتغير نمط تفكيرهم

(1) أيمن حسن، دور مواقع التواصل الاجتماعي في نشر الفكر المتطرف، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، 30 سبتمبر 2017، تم الاطلاع عليه بتاريخ 22 جانفي 2020، على الساعة 19:40 سا، في الموقع:

<https://www.europarabct.com/دور-مواقع-التواصل-الاجتماعي-في-نشر-الف/>

(2) أيمن حسن، المرجع السابق.

(3) أنظر: عربية سكاى نيوز، نساء داعش " الوديعات " .. " الأقوى " في تجنيد الإرهابيين، 10 ديسمبر 2018، تم الاطلاع عليه بتاريخ 22 جانفي 2020، على الساعة 20:00 سا، في الموقع: <https://www.skynewsarabia.com/world/1207068-نساء-داعش-الوديعات-الأقوى-تجنيد-الإرهابيين>

وتبديل توجههم، كما تستهدف أيضا الفئات ذات الاحتياجات الخاصة فيشركونهم في نشاطاتهم لاستقطابهم ومن ثم يتم سحبهم لخدمة مصالحهم⁽¹⁾.

الفرع الثاني: تداعيات الإرهاب الإلكتروني على الأمن القومي للدول:

يشكل الإرهاب الإلكتروني خطورة كبيرة نظرا لضعف البيئة الإلكترونية وقابليتها للاختراق من جهة، ونظرا لحيوية الفضاء الإلكتروني جهة أخرى، فتزايد الدول وإقبالها الكثيف على تكنولوجيا المعلومات وأنظمة الحواسيب الآلية في تسير وإدارة وتشغيل البنية التحتية الحرجة يجعل من تداعيات الهجمات الإرهابية تهديدا صارخا للأمن القومي للدول (أولا)، كما أن ظهور الحكومة والإدارة الإلكترونية التي تقوم بتخزين مجمل معلوماتها في أنظمة آلية يمكن الوصول إليها عبر الشبكات من أي مكان يزيد من خطورة الإتلاف أو الاطلاع على أكثر المعلومات سرية حرجا (ثانيا).

أولا: تداعيات الإرهاب الإلكتروني على البنية التحتية الحرجة:

ترتبط الكثير من البنية التحتية الحرجة والحيوية للدول بالأنظمة المعلوماتية في تسيرها وتشغيلها، وأي انقطاع أو هجوم على أنظمتها بأي شكل من الأشكال سيؤدي حتما إلى كارثة على المؤسسات الخدماتية الأكثر حيوية واستراتيجية في الدول⁽²⁾، كلما تزايد الإقبال على مثل هذا الربط، وتكاثر الاعتماد على تكنولوجيا المعلومات، كلما تزايد وتفاقم الخطر على الأمن القومي للدول⁽³⁾، وتبرز أخطار وتداعيات الإرهاب الإلكتروني على البنية التحتية الحرجة من خلال الأمثلة التالية:

1- تدمير الاقتصاد:

إن عامل الخطورة الذي يحدق باقتصاديات البلدان يقف وراءه هذا الانفتاح الكبير على عالم المعلوماتية والحوكمة الإلكترونية، والتعاطي مع تكنولوجيا المعلومات كبديل عن أنماط التشغيل التقليدية نظرا لسرعتها وإيجازها ودقة عملها⁽⁴⁾، فيمكن للهجمات الإرهابية استهداف أنظمة التصنيع بإجراء تعديلات طفيفة وخفية عليها بحيث يصبح المنتج النهائي معيبا لا يصلح

(1) هناء الكلوت، الطفل أكبر ضحايا "إرهاب" الإنترنت.. كيف يستدرج؟، 10 مارس 2017، تم الاطلاع عليه بتاريخ 25 جانفي 2020، على الساعة 00:21 سا، في الموقع: <https://alkhaleejonline.net/> مجتمع-الطفل-أكبر-ضحايا-إرهاب-الإنترنت-كيف-يُستدرج؟

(2) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص 155.

(3) أشرف محمد كشك، الأمن الإستراتيجي والأمن الوطني: (رؤية مستقبلية)، سبتمبر 2019، تم الاطلاع عليه بتاريخ 15 جانفي 2020، على الساعة 15:36 سا، في الموقع: <http://www.akhbar-alkhaleej.com/news/article/1182104>

(4) مهدي سلمان الرسام، الإرهاب الرقمي الإلكتروني ناقوس الخطر القادم، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، 12 جوان 2019، تم الاطلاع عليه بتاريخ 16 أكتوبر 2019، على الساعة 19:44 سا، على الموقع: <https://www.politics-dz.com/> إرهاب-الرقمي-الإلكتروني-ناقوس-الخط

استعماله، كما يمكن لهذه الهجمات استهداف مصانع الأغذية والأدوية بنفس هذه الطريقة أو عن طريق استهداف سلاسل التوريد فيها بغية ابتزازها⁽¹⁾، أو بهدف تعطيمها وتحطيم الاقتصاد العام.

ليس هذا فحسب، بل إن ارتباط أسواق المال والبورصة والبنوك بالشبكات المتصلة التي تتحكم بسريراتها يشكل خطورة بالغة على النظام المالي للدول، إذ يمكن تسديد هجمات عالية المستوى إليها مما يحدث فوضى عارمة في الصفقات التجارية وتحولات البورصة، كما يمكن أيضا أن يحدث توقفا جزئيا أو كليا في أنظمتها مما يحدث شللا في نشاطها الأمر الذي يكابدها خسائر اقتصادية كبرى⁽²⁾.

علاوة على ذلك، يمكن للهجمات الإرهابية إحداث خلال كبير على السوق المالية الافتراضية، وقد كشف باحثون من الإنترنت في مجال مكافحة التهديدات السيبرانية عن خطر يهدد سجل الحسابات المتعلقة بالمعاملات المالية الافتراضية، إذ يمكن اختراقها بسهولة تامة من خلال البرمجيات الخبيثة⁽³⁾.

وقد أكدت شركة الأمن المعلوماتي (Kaspersky) أن مجموعة من الهاكرز قد تمكنوا باستخدام تقنيات معقدة، وباستغلال الثغرات الأمنية التي تعيب أنظمة أجهزة الحواسيب المصرفية، من اختراق حسابات مصرفية عالمية والسيطرة عليها ومن ثم نهبها وسرقتها، فقد كابدوا العالم خسائر مالية تقدر بنحو مليار دولار، ولم تستغرق العملية كلها إلا مدة قصيرة جدا من الاختراق وحتى تحويل تلك الأموال وسرقتها⁽⁴⁾.

يمكن للرقابة التي تفرضها الدولة على الفضاء الإلكتروني أن يشكل في حد ذاته إرهابا إلكترونيا ذو آثار فتاكة بالاقتصاد القومي، وقد أشار بروس شناير إلى ثلاثة أساليب يمكن للرقابة على الفضاء الإلكتروني أن تحدث بها آثار اقتصادية كبيرة ومزعجة بالاقتصاد في معرض حديثه عن الرقابة التي تقوم بها وكالة الأمن القومي الأمريكية، وهي؛ تجنب المصادر الأمريكية

(1) مروان صالح، مخاطر سيبرانية: (أشكال الابتزاز الإلكتروني من سرقة الهويات إلى اختراق الصناعات)، المستقبل للأبحاث والدراسات المتقدمة، 07 مايو 2018، تم الاطلاع عليه بتاريخ 16 أكتوبر 2019، على الساعة 19:40، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/3897/مخاطر-سيبرانية-أشكال-الابتزاز-الإلكتروني-من-سرقة-الهويات-إلى-اختراق-الصناعات>

(2) شفيق حسنين، المرجع السابق، ص 202.

(3) أنظر؛ الإنترنت، بحث الإنترنت في المجال السيبراني تكشف عن تهديد تشكله البرمجيات الخبيثة على العملات الافتراضية، 26 مارس 2015، تم الاطلاع عليه بتاريخ 16 أكتوبر 2019، على الساعة 19:30، في موقع: <https://www.interpol.int/ar/1/1/2015/4>

(4) نقلا عن: هاجر حسونة، الإرهاب الإلكتروني.. هل يتحول لمصدر التهديد الأول للعالم؟، 04 ماي 2015، تم الاطلاع عليه بتاريخ 17 أكتوبر 2019، على الساعة 18:21 سا، في الموقع: <https://alkhaleejonline.net/علوم-وتكنولوجيا/الإرهاب-الإلكتروني-هل-يتحول-لمصدر-التهديد-الأول-للعالم؟>

للمعلومات، تدني نسبة المبيعات للمنتجات الأمريكية المتعلقة بالفضاء الإلكتروني، كالحواسيب وما إلى ذلك، وفقدان الثقة في الشركات الأمريكية، وقد أوضح تعقياً على ذلك حجم الخسائر التي تكابدها الشركات الأمريكية جراء ذلك كله⁽¹⁾.

2- تدمير نظم توليد وتوزيع الطاقة والمياه:

يعتبر استهداف منشآت كبرى بحجم محطات توليد الطاقة والمياه وتوزيعهما أمر سينجر عنه بما لا يدع مجالاً للشك آثاراً كارثية على الأمن القومي للدولة، فمعظم المؤسسات والمرافق داخل الدولة تعتمد اعتماداً كلياً على الطاقة الكهربائية، وأي هجوم على أنظمة التشغيل للمولدات أو لنظم تشغيل التوزيع سيزعزع أمن التهوي في أنظمة الفوضى والشلل المرفقي والخدمات، وهذا لا يختلف كثيراً عما قد يحصل بالسدود وشبكات توزيع المياه⁽²⁾.

تمتلك الولايات المتحدة الأمريكية لوحدها اعتباراً من 31 ديسمبر 2019 عدد كبيراً من المولدات الكهربائية والتي يبلغ عددها 22.731 مولداً كهربائياً مقسمة على حوالي 10346 محطة طاقة كهربائية حسب المرفق⁽³⁾، ولذلك فإن أي هجوم على مثل هذا المرفق سيحدث شللاً كاملاً للحياة، ذلك أن غالبيتها يتم تسييره وإدارته عبر التقنيات الحديثة.

وتقريباً لحجم التهديد الذي يمكن أن يصوب إلى مثل هذا المرفق والتداعيات الخطيرة التي يمكن أن تنتج عنه، قام باحثون في مختبرات أيداهو الوطنية بتجربة تحت عنوان " اختبار مولد أورورا" لإظهار نتائج محاكاة هجوم إلكتروني على شبكة طاقة، ففي مقطع مصور أصدرته وزارة الأمن الداخلي، تم إجبار توربينات مولدة للطاقة على رفع درجة حرارتها وإحكام غلقها بعد تلقي أوامر خبيثة من أحد المتسللين، كان الباحثون من خلال هذه المحاكاة يحققون في نتائج هجوم إلكتروني محتمل موجه ضد ثغرة تم إصلاحها منذ ذلك الحين، لكن التسجيل المصور أفاد بأن مولدات الطاقة المتعددة الأخرى التي تشترك في نقاط ضعف إلكترونية مماثلة يمكن تعطيلها بنفس الطريقة⁽⁴⁾.

(¹) بروس شناير، المرجع السابق، ص: 188-189.

(²) شفيق حسنين، المرجع السابق، ص: 201-202.

(³) How many power plants are there in the United States?, Frequently asked questions, U.S. Energy Information Administration, Last updated: November 18, 2020, Accessed on 24/11/2020 At 00:93 in: <https://www.eia.gov/tools/faqs/faq.php?id=65&t=2#:~:text=As%20of%20December%2031%2C%202019,plants%20in%20the%20United%20States.>

(⁴) Clay WILSON, Botnets, cybercrime, and cyberterrorism: (vulnerabilities and policy issues for congress), Congressional research service, January 29, 2008, PP.16-17: <https://www.everycrsreport.com/reports/RL32114.html>

3- المساس بالأنظمة العسكرية والمفاعلات النووية:

يعتبر الهجوم على الأهداف العسكرية أمر نادر الحصول، فهو يحتاج إلى دراسة ومعرفة عالية بالنظام العسكري وآلياته وطبيعته عمله، خاصة وأن معظم الأهداف العسكرية تتمتع بالسرية عبر سلسلة من الأرقام السرية التي لا يمكن الحصول عليها، والتي لا تطلع عليها حتى أجهزة الأخرى للدولة، ومع هذا يبقى احتمال تعرضها لهجمات إرهابية أمر وارد⁽¹⁾، فقد يتسنى للجماعات الإرهابية الحصول على تلك الشفرات السرية فيتم التحكم من خلالها بتشغيل منصات إطلاق الصواريخ والأسلحة الفتاكة الأخرى مما يقود إلى كارثة كبرى⁽²⁾.

وتجدر الإشارة إلى أن احتمالية تنفيذ الهجمات التي تستهدف المفاعلات النووية ومنصات إطلاقها أمر وارد أيضا، فقد تم استهداف البرنامج النووي الإيراني عن طريق استخدام دودة " ستاكسنت " والتي تعتبر حينها أخطر سلاح سبيرياني على الإطلاق، وقد تم اكتشافها في 2009 عندما تمكنت من أحاق الضرر بأجهزة الطرد المركزي لمنشأة (ناتانز) الإيرانية لتخصيب اليورانيوم، وتسببت في تعطيل عدد كبير منها⁽³⁾.

ولعل الهجمات الإرهابية الإلكترونية على الأنظمة العسكرية هي التي تظهر فيها الفوارق بين إرهاب الأفراد والجماعات وبين إرهاب الدولة، فالأفراد والجماعات الإرهابية تعتبر كأصل عام غير قادرة على استهداف هذه الأنظمة، فهم لا يملكون القدرات الفنية والتقنية التي تمكنهم من تنفيذ هجوم ناجح عليها، في حين أن الدولة يمكنها أن تفعل ذلك، نظرا لما تحتكره من قوة سيبرانية يمكن أن تنفذ بها هجوما ناجحا يخلف آثار كبيرة، وهذا ما دلّ عليه المثال المشار إليه آنفا.

4/ المساس بأنظمة المواصلات:

ليس من المستبعد مطلقا على الإرهابيين اللجوء إلى شن هجمات إلكترونية على أنظمة إدارة وتسيير المواصلات البرية والملاحة البحرية وكذلك نظم النقل الجوي عن طريق إحداث خلل في برامج إقلاع وهبوط الطائرات مما قد يترتب عنه التصادم والتداخل في ما بينها مما يسقط العدد من الضحايا، كما يمكن أيضا الإقدام على اختراق نظم القطارات وشبكات ميترو الأنفاق والعبث في

(1) مهدي سلمان الرسام، المرجع السابق.

(2) شفيق حسنين، المرجع السابق، ص 201.

(3) إيهاب خليفة، تهديدات سيبرانية: (هل يستطيع القراصنة اختراق المنشأة النووية؟)، المستقبل للأبحاث والدراسات المتقدمة، 07 يناير 2020، تم الاطلاع عليه بتاريخ 28 جانفي 2020، على الساعة 18:55 سا، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/5191/> تهديدات سيبرانية-هل يستطيع القراصنة-اختراق المنشآت النووية

مواعيدها، الأمر الذي ينجم عنه فوضى وتصادم فيما بينها، وهذه المخاطر والتداعيات تنطبق أيضا على السفن والباريجات والنقلات والغواصات البحرية⁽¹⁾.

و هناك عدد من الأمثلة التي يمكن الاستشهاد بها في بيان خطورة تمكن الإرهابيين من التلاعب بأنظمة تسيير وسائل النقل والمواصلات المختلفة، وأبرزها العملية التي قام بها القرصان " كريس روبرت " لعشرات الرحلات الجوية والذي تم إلقاء القبض عليه من قبل السلطات الأمريكية سنة 2015، وتعرضت أيضا ست منشآت سعودية لهجمات القرصنة والاختراق وعلى رأسها الهيئة العامة للطيران المدني السعودي، وقد استهدفت الهجمات تعطيل الأنظمة الخدمانية ومحاولة زرع برامج خبيثة فيها⁽²⁾.

ثانيا: تداعيات الإرهاب الإلكتروني على أمان المعلومات وسريتها:

تعتبر المعلومات عنصرا هاما في حياة البشر، وتلعب دورا هاما في حياة الأفراد والجماعات منذ ظهور الإنسان على وجه الأرض، أخذ تطور المنظومة المعلوماتية يتنامي مع تنامي تطور الإنسان وبدأ احتكارها مع ظهور الثورة الصناعية في الغرب حيث كان الحرص شديدا على عدم اطلاق الدول على معلومات بعضها البعض، ومع الزمن أصبحت المعلومات هي الركيزة الأساسية التي تبني عليها القوة الإنتاجية القومية في الدول، فتكون بذلك مصدر القوة وعماد السلطة⁽³⁾.

تطور الأمر حتى ظهور الشبكات العالمية للإنترنت، فأصبحت الدول تخزن معلوماتها وتدير أسرار مشاريعها باستخدام تكنولوجيا الاتصال، فغدي الفضاء الإلكتروني بعدها مكتب أرشيف للوثائق والأسرار الحكومية، فانصرفت إليها أنظار الجواسيس التقليديين، محاولين الاطلاع على مكنونها عن طريق استخدام نظام تجسسي حديث يعتمد على تقنيات الاختراق المختلفة التي تتحدى بها الأجهزة الأمنية والقضائية، ففتح المجال بعدها للجماعات الإرهابية التي تسعى حثيثا إلى الاطلاع على المعلومات الحساسة للدول والتي تتضمنها المزودات السرية على هيئة رقمية⁽⁴⁾.

إن الثغرات التي تم التوصل إلى إيجادها في عالم تكنولوجيا المعلومات تم توظيفها في ميادين الاستخبارات العامة، - سواء أكانت من الدول أو من غيرها - من خلال اختراق الحواسيب

(1) شفيق حسنين، المرجع السابق، ص 202.

(2) محمد عزت هلال، آليات المواجهة: (تهديدات الأمن الإلكتروني في قطاع الطيران المدني)، المستقبل للأبحاث والدراسات المتقدمة، 25 مايو 2017، تم الاطلاع عليه بتاريخ 15 جانفي 2020، على الساعة 21:14 سا، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/2827/> آليات المواجهة-تهديدات-الأمن-الإلكتروني-في-قطاع-الطيران-المدني

(3) طويي بحري ودلال بحري، المرجع السابق.

(4) حكيم غريب، المرجع السابق، ص ص: 833-834.

والأجهزة باستعمال الفيروسات أو الديدان وغيرها من أساليب الاختراق التي تسهل بلوغ المعلومات والاستيلاء عليها⁽¹⁾، وتعتبر منظمة ويكيليكس أخطر مظهر للتسريبات والجوسسة الإعلامية في العالم، والتي لاقت نشاطاتها ردود أفعال متباينة.

إن هجوم التنظيمات الإرهابية على مخازن المعلومات المتعلقة بالجوانب الاستراتيجية للدول يعتبر من بين أخطر الهجمات التي من شأنها أن تحدث انعكاسات خطيرة على الأمن الدولي، فاطلاع الإرهابيين على المعلومات العسكرية والاقتصادية والسياسية يمنح لهم إمكانية توظيفها في المساس بالأمن القومي للدول، وليست الجوسسة والاستطلاع فقط من يشكل خطورة على أمن المعلومات، فهناك آليات قد سلف وأن أشرنا إليها تمكن الإرهابيين من إتلافها أو تزوير محتواها ولا يخفي على أحد ما يمكن أن يترتب من سلبات وأضرار جمة جراء هذا التصرف التخريبي.

الفرع الثالث: تداعيات الإرهاب الإلكتروني على العلاقات الدولية:

لقد ساهم ظهور النظام الدولي الجديد في تغيير موازين القوى وظهور مفاهيم قانونية وسياسية جديدة وصياغات متعددة للرؤى والتوجهات السياسية في العلاقات بين الدول، وأصبحت العلاقات الدولية قائمة على استراتيجية القوة وفرض النفوذ والسيطرة، ومع ظهور الفضاء الإلكتروني أصبحت القوة، ذات بعد إلكتروني وأصبحت الإلكترونية آلية على قدر كبير من الفعالية في الصراع العنيف بين الدول (أولاً) كما أفضى إلى تشكل أنماط جديدة من القوى الناعمة التي توظفها الدول لتحقيق مصالحها ورؤاها الاستراتيجية (ثانياً).

أولاً: التوظيف الصلب للإرهاب الإلكتروني في الصراع الدولي:

لقد كان الإرهاب بمفهومه اللغوي في كثير من الأحيان سلاحاً في يد المستضعفين ضد الأقوياء والمستعمرين ضد المستعمرين، ثم بعد ذلك تم توظيفه لأهداف سياسية للخط بين الإرهاب كظاهرة إجرامية وبين حق الشعوب في المقاومة والتحرر وتقرير المصير، ثم بقي مصطلحاً حملاً للأوجه، يتم توظيفه تبعاً للمصالح السياسية التي يقتضيها الحال، ولم يتوقف حد التوظيف السياسي للإرهاب عند هذا الحد فقط، بل أصبحت الدول المهيمنة أو تلك المدعومة من الدول المهيمنة توظف الإرهاب بنفسها من أجل فرض نفوذها وسطوتها والتأثير في المنظمات الإقليمية والعالمية، فتحول بذلك إلى بديل للحروب التقليدية، وأصبح آلية وقوة ذات فعالية كبرى في الصراع السياسي

(1) خالد محمد غازي، الأصابع الخفية: (التوظيف الإعلامي السياسي لشخصية الجاسوس)، وكالة الصحافة العربية، الجزيرة، مصر، 2015، ص

الدولي، تفرض بها الدول نفوذها، وتضعف به خصومها، عبر تحريك أجندها خارج حدودها لارتكاب الأفعال الإرهابية⁽¹⁾.

فبعد ما كان الإرهاب السياسي يعد حتى أواخر الستينات من القرن الماضي من قضايا السياسة الداخلية للدول، والتي يتم فيها توظيف الإرهاب على نطاق محلي ضيق، أصبح تدريجياً ظاهرة دولية خطيرة بسبب تورط الدول بشكل أو بآخر في التخطيط له وتمويله وتنفيذه، فأصبح بذلك من الظواهر الدولية الخطيرة التي ينتج عنها تهديد فعلي لأمن الدول واستقرارها⁽²⁾.

ليس التخطيط والتنفيذ فقط هما صورتان اللتان يظهر فيهما التوظيف الدولي للظاهرة الإرهابية، بيد أن ردود الأفعال نحوه تشكل توظيفاً بحد ذاته، ففوة الإدانة وشكله ضد الجرائم الموصوفة بالإرهاب، يختلف تبعاً للمصلحة الاستراتيجية المشتركة، إذ لا تنطلق فيها الجهات الفاعلة على أسس قانونية وأخلاقية، بل على أسس المصلحة والغاية، فعندما وقعت أعمال إرهابية في السنوات الماضية في دول أوربية، توحد العالم كله في إدانتها، وأظهروا المساندة والدعم للدول المنكوبة باعتبارها ضحايا إرهاب، لكن في المقابل عندما تعلق الأمر بالهجمات الإرهابية التي استهدفت مسجد الروضة بجمهورية مصر العربية، والتي راح ضحيتها مئات المصلين الأبرياء، نجد تفاعلاً دولياً غريباً، إذ من المفترض بالدول أن تقف بجوار مصر وتساندها باعتبارها ضحية إرهاب، وتدعمها في حربها ضده، لكن العكس هو الذي حصل، فقد تعرضت مصر لعقوبات قاسية، واتهمت الدولة المصرية بالتقصير وعدم حماية المدنيين، وهذا الأمر يعكس ازدواجية المعايير والخطاب من جهة⁽³⁾، والتوظيف السياسي للأحداث الإرهابية من جهة أخرى.

ومع بروز الثورة غير العادية للتكنولوجيا والتي شهدتها القرن العشرين ظهرت تغيرات خطيرة في مجالات عدة⁽⁴⁾، وأصبح الفضاء الإلكتروني وتكنولوجيا الاتصال والمعلومات هو الصورة المعبرة عن هذه الصراعات التفاعلية بين الدول، بل وتحولت هي نفسها ساحة صراع، بحيث

(1) حسام أبو حامد، المرجع السابق.

(2) محمد شوقي عبد العال، رؤية سياسية قانونية: (التطورات المعاصرة في ظاهرة الإرهاب الدولي 1-2)، المركز العربي للبحوث والدراسات، 10 ديسمبر 2015، تم الاطلاع عليه بتاريخ 26 أكتوبر 2019، على الساعة 15:12 ساء، في الموقع: <http://www.acrseg.org/39685>

(3) أحمد صلاح الدين، ازدواجية المعايير والتوظيف السياسي، 25 مارس 2019، تم الاطلاع عليه بتاريخ 15 جانفي 2020، في الموقع: <https://www.omandaily.om/?p=684570>

(4) لقد طرأ تغيير جذري في نمط ممارسة التوظيف السياسي للإرهاب بسبب هذه الطفرة العلمية الكبرى في مجال المعلومات والاتصالات، وأثر ذلك بشكل كبير على التفاعلات الدولية في السلم كما في الحرب، فإن كان التوظيف التقليدي للإرهاب يقتضي تدخلاً عسكرياً مباشراً أو عن طريق ميليشيات مسلحة تخدم مصالحها خارج نطاق حدود سيادتها. فإن الوضع أصبح مختلفاً، إذ يمكنها توظيفه بشكل أكثر سهولة ومرونة وبآليات أكثر تأثيراً وفعالية، وفي غالبية الأحيان دون أن تترتب عنها مسؤولية دولية لطبيعة الفضاء الذي تستغله الذي يتسم بالمجهولية وخفاء الهوية.

أصبح الصراع التقني هو الأكثر ظهوراً، والأشد تميزاً، إذ ساهم في خلق طرق جديدة بديلة عن الحرب التقليدية في الصراعات الدولية مما أدى إلى تغيير شكل الحرب وطبيعتها وطبيعة الفاعلين فيها واختلاف أنماط التهديد والنتائج المترتبة عنه، لقد أصبح الفضاء الإلكتروني وسطاً وبيئة للقيام بالأنشطة المدنية والعسكرية، كما تحول إلى أكبر ساحة إعلامية وآليات اتصال دولية بالإضافة إلى ارتباط البنى التحتية الأكثر حيوية بها، مما يجعل أي تهديد لها أكثر تدميراً وأشد خطراً⁽¹⁾.

إن الدول المتصارعة فيما بينها كثيراً ما تصف أعمال بعضها البعض في إطار تنازعها بأنها من قبيل الأعمال الإرهابية⁽²⁾، وعلى هذا الأساس فإن استخدام الهجمات الإلكترونية في صراع روسيا وإستونيا في عام 2007 واستخدامها في الحرب الجورجية الروسية عام 2008، واستخدام الولايات المتحدة الأمريكية وإسرائيل للهجمات الإلكترونية ضد المنشآت النووية الإيرانية باستعمال فيروس ساكسنت، وقيامها أيضاً بشن 231 هجوماً إلكترونياً ضد روسيا وإيران والصين⁽³⁾، يعتبراً من قبيل الإرهاب الإلكتروني الدولي.

عملت إيران أيضاً بدورها على شن هجمات إلكترونية عالية المستوى على أهداف اقتصادية وعسكرية للولايات المتحدة، إذ شنت هجوماً قوياً على نادي القمار بفندق بلاس فيغاس كلفها عشرين ألف حاسوب بتكلفة 40 مليون دولار، وكان هذا الهجوم على خلفية التصريحات غير المهدبة، والتي أطلقها بشأن تدمير إبرتان بالقنبلة النووية، كما شنت مجموعة من القراصنة تدعى " حراس السلام " هجمة إلكترونية هائلة على شركة سوني الأمر الذي أفضى إلى دمار ثلاثة آلاف حاسوب، وثمانمائة مخدم حاسوبي، وسرقة ما يعادل مئة تيرا بيت من البيانات، كما تعرضت إلى هجمتين قبل ذلك في 2011 ترتب عنها إيقاف شبكة بلاي ستايشن لمدة ثلاثة وعشرون يوماً، وثبت بعد ذلك أن تلك الهجمات كانت من قبل مجموعة من القراصنة وتدعى " دارك سيول " التي غالباً ما تخدم مهاماً سيبرانية موكلة إليها من قبل حكومة كوريا الشمالية، ويرجح بعض المحللين أن تلك الهجمات كانت على خلفية فيلم كوميدي عزمت شركة سوني إطلاقه والذي يتضمن إساءة للقيادة العليا في كوريا الشمالية⁽⁴⁾.

(1) ريهام عبد الرحمن رشاد العباسي، أثر الإرهاب الإلكتروني على تغيير مفهوم القوة في العلاقات الدولية: (دراسة حالة تنظيم داعش "الدولة الإسلامية")، المركز الديمقراطي العربي، 24 يوليو 2016، تم الاطلاع عليه بتاريخ 27 جانفي 2020، على الساعة 22:19، في الموقع: <https://democraticac.de/?p=34528>

(2) محمد شوقي عبد العال، المرجع السابق.

(3) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المرجع السابق، ص 64.

(4) فرد كابلان، المرجع السابق، ص ص: 307-310.

يلاحظ أن أهم الأهداف التي يسعى مرتكبي الهجمات الإرهابية الإلكترونية تحقيقها تتمثل في امتلاك قوة إلكترونية كبيرة قادرة على أحداث أضرار جسيمة في البنية الاقتصادية والسلوكيات النفسية لخدمة مصالحهم الاستراتيجية أو مصالح حلفائهم، فقد قامت وزارة الدفاع الأمريكية عام 1999 بتنفيذ هجمات إلكترونية عالية ضد أجهزة الكمبيوتر التابعة للدولة الصربية بغية إفشال خططها وعملياتها العسكرية وإخلال بنيتها التحتية المدنية الحرجة، وهذا من أجل دعم قوات التحالف⁽¹⁾.

ولهذا أصبح السباق نحو التسلح الإلكتروني يكتسي أهمية استراتيجية كبيرة في توازن القوى وعملية بسط النفوذ والهيمنة، فسعت الدول في إطار عسكرة الفضاء الإلكتروني إلى تحقيق التفوق التقني لبناء منظمة إلكترونية هجومية وأخرى دفاعية لتعزيز أمنها ضد الأخطار التي قد تتعرض لها من جراء الهجمات الإرهابية الإلكترونية⁽²⁾.

دون أن ننسى بطبيعة الحال دور التنظيمات الإرهابية التي أصبحت من بين اللاعبين غير الشرعيين في العلاقات الدولية، فمنذ هجمات الحادي عشر من سبتمبر 2001، أصبحت الأعمال الدراسية للتنظيمات الإرهابية من بين أولويات الأشغال المتعلقة والمرتبطة بالعلاقات الدولية، وهذا الأمر راجع إلى المرامي والغايات التي تهدف هذه التنظيمات إليها، والتي أصبحت ذات بعد دولي⁽³⁾.

ثانياً: التوظيف الناعم للإرهاب الإلكتروني في العلاقات الدولية:

تلجأ بعض الدول والتنظيمات في إرهابها الإلكتروني إلى استخدام أساليب الاختراق للتجسس الإلكترونية من أجل حيازة الوثائق والمعلومات الحرجة المتعلقة بخصومها وحلفائها على حد سواء، فقد أثارة التسريبات التي نشرتها المنظمة الدولية " ويكيليكس " موجة من ردود الأفعال الدولية الغاضبة، لكشفها عما يعادل 76900 وثيقة سرية حول الحرب في أفغانستان، كما نشرت بعدها 400000 وثيقة متعلقة بكواليس الحرب الأمريكية على العراق، وأتبعها بسلسلة من البرقيات الدبلوماسية للخارجية الأمريكية⁽⁴⁾ وغيرها من الدول.

(1) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، المرجع السابق، ص: 246-248.

(2) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المرجع السابق، ص: 64-66.

(3) جوانيتا إلياس وبيتر ستش، أساسيات العلاقات الدولية، ترجمة: (محيي الدين حميدي)، الطبعة الأولى، دار الفرق للكتابة والنشر والتوزيع، سورية، 2016، ص: 131-132.

(4) حكيم غريب، المرجع السابق، 835.

ورغم أن معظم تلك التسريبات لم تكن ذات أهمية كبيرة ولا تشكل أي خطورة على الأمن القومي الأمريكي، إلا أنها تداعياتها كانت قوية، فقد أصيبت العديد من الدول بالدهشة والذهول وارتباكات في أعمالها بما في ذلك الولايات المتحدة الأمريكية التي سارعت إلى تدارك الأمر عبر المسائل الدبلوماسية لامتناع ردود الفعل، فقد كشفت التسريبات عن وثائق أخرجت الولايات المتحدة الأمريكية أمام بعض الدول كتركيا وروسيا لاحتوائها على توصيفات غير لائقة عن الوضع السياسي والقادة الروس (1).

كما شكلت تلك التسريبات أيضا سببا في الفوضى والتناحر والاحتجاجات التي سادت في الشرق الأوسط وشمال إفريقيا وخلق موجة جديدة من الإرهاب الدولي (2).

يرى الدكتور **حكيم غريب** (3) أن الغرض المراد والمقصود من مثل هذه التسريبات ليس بلوغ الحقيقة وتحقيق الشفافية في العمل السياسي بل الغاية منها هو تنفيذ أجندة سياسية مخالفة أو تشكيل نقاط في الصراع داخل المؤسسة (4).

ويكون هذا بتشويه الشخصيات أو المؤسسات السياسية واستنزاف طاقاتها ووقتها في الدفاع السياسي عن نفسها وإشغال معارك جانبية لرفع من قيمة الخسائر المعنوية خاصة عندما تكون تلك التسريبات موجهة كضربة استباقية في معارك سياسية أو انتخابية، وبالتالي أضعاف فرصها في إدارة المشهد السياسي وتسييره على الوجه الأكمل، وقد كانت المرشحة الأمريكية **هيلاري كلينتون** النموذج الأمثل لمثل هذا التأثير، حيث تراجعت شعبيتها في معركتها الانتخابية ضد خصمها السياسي **دونالد ترامب** بانشغالها في الدفاع عن نفسها، وهذا كله بسبب هجمة إلكترونية استباقية استهدفت بريدها الإلكتروني والاستيلاء على محتواه ومن ثم نشره على موقع **ويكيليكس**،

(1) محمد عاكف جمال، تداعيات الدفعة الثالثة من وثائق ويكيليكس، 10 ديسمبر 2010، تم الاطلاع عليه بتاريخ 12 أكتوبر 2019، على الساعة 12:55، في الموقع: <https://www.albayan.ae/opinions/2010-12-10-1.595130>

(2) حكيم غريب، المرجع السابق، ص 837.

(3) حكيم غريب: (أستاذ محاضر بالمدرسة الوطنية للعلوم السياسية الجزائر العاصمة وخبير في الشؤون الأمنية والاستراتيجية واطار سامي سابق في جهاز الأمن الوطني الجزائري، القيام بتدريس المواد المقررة: في برنامج دكتوراه في الدراسات الاستراتيجية، وبرنامج الماجستير في العلوم السياسية، متخصص في ملف مكافحة الإرهاب بكل أشكاله الجديدة له العديد من المقالات المنشورة في العديد من المجلات المتخصصة في الشؤون الأمنية والسياسية والدراسات الاستراتيجية وحاصل على درجات الدكتوراه في العلاقات الدولية، والاستراتيجية وأشرف ويشرف على الرسائل العلمية لدرجتي الماجستير والدكتوراه. كما شارك في ندوات ومؤتمرات وورش عمل دولية علمية واستراتيجية، وأجرى العديد من اللقاءات الإذاعية والتلفزيونية العربية حول الأحداث الجارية وتطوراتها المستقبلية وأستاذ متعاقد مع عدة مدارس العسكرية العليا لوزارة الدفاع الوطني كما شارك في عمليات مكافحة الإرهاب خلال العشرية السوداء التي عرفتها الجزائر)، نقلا عن:

- <https://alarabiahunion.org/%D8%AD%D9%83%D9%8A%D9%85-%D8%BA%D8%B1%D9%8A%D8%A8/>

(4) حكيم غريب، المرجع نفسه، ص 836.

وتستعمل أيضا مثل هذه التسريبات لتقديم الدعم السياسي للحلفاء أو الحلفاء المحتملين عبر تقوية مواقفهم السياسية وتعزيز فرصهم الانتخابية، فقد كشف البيت الأبيض الأمريكي على لسان متحدته الرسمي بأن جهاز الاستخبارات الأمريكي توصل إلى اكتشاف تورط روسيا في عملية قرصنة إلكترونية لأنظمة الحاسب التابعة للحزب الديمقراطي لدعم الحليف المحتمل الذي نزل كمرشح ضدهم في الانتخابات الأمريكية⁽¹⁾.

وقد أشارت تقرير أخرى أيضا تورط جهات روسية في هجمات إلكترونية لتقويض التحالفات الديمقراطية من خلال اختراق الانتخابات الفرنسية باستهداف حملة المرشح إيمانويل ماكرون واختراق شبكتها والاستيلاء على المعلومات الحقيقية واستبدالها بمستندات مضللة⁽²⁾.

توظف بعض الدول أيضا الإرهاب الإلكتروني بحجة حقوق الإنسان وتكريس الديمقراطية من خلال دعمها لأنظمة الفساد في بعض الدول، وقد أشرنا سابقا إلى تقديم بعض الدول الغربية تقنيات إلكترونية عالية الدقة إلى بعض الدول العربية وهي تعرف جيدا نطاق الاستغلال الذي ستوظف فيه فبدلا من أن يساعد الغرب على خلق الشروط الموضوعية لانتشار حقوق الإنسان في تلك الدول نجدها تستمر بكل صفاقة في دعمها لتلك الأنظمة التي تدوس على الحقوق برجليها كل يوم⁽³⁾.

وعلى ضوء ما سبق، يمكن القول بأن توصيف العمليات والهجمات الإلكترونية التي تقوم بها الدول في الفضاء الإلكتروني بالأعمال الإرهابية أقرب من توصيفها بالحرب الإلكترونية، ذلك بأنها عمليات تهدف في أصلها إلى الترويع والتخويف من جهة، ولأنها مجهولة المصدر من جهة ثانية، فهي عمليات غير متكافئة كون الذي يبادر بها هو الطرف الأقوى فيها، الأمر الذي يؤثر بشكل واضح على نظرية الردع الاستراتيجي، وكونها مجهولة الأهداف والآثار يُصعب على من تشكيل آلية دولية لضمان الحماية منها، فمصطلح الإرهاب السيبراني مصطلح فضفاض يتم استغلاله تبعا للنوازل والمصالح السياسية، فالهجمات التي شنتها الولايات الأمريكية على المفاعل النووي الإيراني

(1) عمرو صلاح، قرصنة الديمقراطية: (الأنماط المتعددة للاختراق الإلكتروني للسياسات الداخلية للدول)، المستقبل للأبحاث والدراسات المتقدمة، 02 فبراير 2017، تم الاطلاع عليه بتاريخ 13 فيفري 2020، على الساعة 15:30 سا، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/2439/> قرصنة الديمقراطية-الأنماط المتعددة للاختراق الإلكتروني للسياسات الداخلية للدول

(2) كارولين سايج، حرب الأفكار الجديدة: (تأثيرات "التضليل الرقمي" في مكافحة الغرب للإرهاب)، المستقبل للأبحاث والدراسات المتقدمة، 08 يوليو 2019، تم الاطلاع عليه بتاريخ 13 فيفري 2020، على الساعة 16:02 سا، في الموقع:

<https://futureuae.com/ar/Mainpage/Item/4838/> حرب الأفكار الجديدة-تأثيرات-التضليل الرقمي-في مكافحة الغرب للإرهاب

(3) محمد أركون، أين هو الفكر الإسلامي المعاصر، ترجمة (هاشم صالح)، الطبعة الثانية، دار الساق، بيروت، لبنان، 1995، ص 27.

هو إرهاب وليست حرباً من وجهة نظر إيران بينما الهجمات التي تعرضت لها شركة سوني فهي إرهاب من وجهة نظر الولايات المتحدة الأمريكية وليست حرباً⁽¹⁾.

توظيف الإرهاب الإلكتروني الصراعات الدولية وخدمة المصالح الاستراتيجية إذا، يشكل خطراً محدقاً بالعلاقات الدولية، وتأثير خطيراً على المسارات الديمقراطية، مما ينعكس سلباً على الأمن والاستقرار الدوليين، وما يزيد من خطورته أكثر هو عدم وجود مفاهيم قانونية تأطر مجال الفضاء الإلكتروني، فالمسؤولية الدولية عن أعمال الإرهاب الإلكتروني لا تزال تسري وفق القواعد العامة التي تحكم العلاقات بين الدول كتحريم التدخل في الشؤون الداخلية، واحترام سيادة الدول، ومبدأ حظر استخدام القوة في العلاقات الدولية، ورغم صدور قرارات من الجمعية العامة التي تمنع استخدام مصادر أو تكنولوجيا المعلومات في تحقيق أغراض إرهابية، إلا أن طبيعة الإرهاب الإلكتروني وتعلقه بفضاء تقني معقد يستدعي وضع أطر قانونية واضحة ومحددة تمكن من بلورة المسؤولية الدولية عن أعمال الإرهاب الإلكتروني من جهة، وعلاقة توظيف الإرهاب الإلكتروني بالقوانين الدولية المختلفة.

(1) الموسوعة الجزائرية للدراسات الاستراتيجية والسياسية، قوة الفضاء السيبراني: (الثقافة والسياسة في الفضاء الإلكتروني والإنترنت)، 27 نوفمبر 2019، تم الاطلاع عليه بتاريخ 15 فيفري 2020، على الساعة 19:17 سا، في الموقع: <https://www.politics-dz.com/> -الفضاء-السيبراني-الثقافة-والسياس/

الباب الثاني:

المواجهة الدولية لظاهرة الإرهاب الإلكتروني

تعد الأهمية التي ترسخت للفضاء الإلكتروني بفعل ما أشرنا إليه من توظيفات واستخدامات وما ينعكس عليه من مفاهيم وتصورات وكذلك الأخطار والتهديدات التي يشكلها الإرهاب الإلكتروني على هذه البيئة الحيوية مصدر قلق للعالم أجمع، ومن منطلق حرص الدول وأصحاب المصلحة في الفضاء الإلكتروني على أمن وسلامة هذه البيئة، انطلقت علميات واسعة النطاق من أجل صونها وحمايتها من التهديدات التي تتربص بها الدوائر ولاسيما الإرهاب الإلكتروني الذي أشرنا إلى جزء يسير من تداعياته.

ولما كانت الطبقات التكوينية لهذا الفضاء متعددة ومنقسمة على عدة فواعل فإن التشكيلة الأمنية لحمايتها لا بد أن تكون على قدر كبير من التنسيق والترابط فيما بينها، ويجب أن يكون الفاعلون الرئيسيون وأصحاب المصلحة العمل سويا وفق استراتيجية ذات أبعاد محددة تتحدد على أساسها المسؤوليات وتتعين وفقها الأدوار، في جو من الشفافية وتبادل الثقة والائتمان، ولا يتحقق هذا الأمر إلا من خلال تفعيل مبادئ الحوكمة، غير أن الحوكمة بمفردها كأسلوب تنظيمي لن يكون على قدر مرضي من الحماية لضمان أمن هذا الفضاء، إذ يتعين من أجل إحاطة الفضاء الإلكتروني بضمانات أمنية صارمة أن تشمل أيضا هيكلة تنظيمية تُعنى بتهديدات الإرهاب الإلكتروني وسائر الأخطار الأخرى حال وبعد وقوعها، ويكون ذلك من خلال تكوين أو إحداث هيئة أو جهاز يركز بشكل دقيق على جمع الأدلة الرقمية التي يخلفها الإرهاب على الوسط السيبراني، ويناط بها دور تحليلها وتقديمها كأدلة ذات قوة ثبوتية يعتد بها أمام الجهات القضائية المختصة، وهذا الأمر ليس الهدف منه هو تقديم الجناة أمام العدالة لنيل الجزاء العادل جراء ما كسبت أيديهم فقط، بل إن هذا الأمر يشكل قاعدة معرفية على قدر كبير من الثراء والتنوع فيما يتعلق بأنواع الهجمات المستجدة والآليات التي يمكن بواسطتها التصدي لها في المستقبل، وهذا من شأنه أن يدعم الآليات التقنية التي يتطلبها هذا الوسط لمجابهة مثل هذا النوع من التهديدات، إذ لكل فضاء أسلحة يتم توظيفها للتصدي للتهديدات التي تحول حوله، وأسلحة الدفاع في الفضاء الإلكتروني يجب أن تكون من نفس الطبيعة الافتراضية لهذا الفضاء، دون إهمال الحماية لجميع الأصول أو البنى التحتية المادية له (الفصل الأول).

إن الأساليب الوقائية التي يتم اعتمادها في الوقت الحاضر على الصعيدين الوطني والدولي ليست ضمانا ناجعة لحماية الفضاء الإلكتروني من مخاطر الهجمات الإرهابية، فكثير ما تفشل في التصدي لها نظرا لكثرة الفجوات والثغرات الأمنية التي تشوب الفضاء الإلكتروني، ولذلك يتعين على الدول سواء على المستوى المحلي أو الإقليمي أو الدولي العمل على صياغة نماذج تشريعية

متكاملة الأركان بحيث تتحدد فيها الجوانب الموضوعية لجرائم الفضاء الإلكتروني ولاسيما جريمة الإرهاب الإلكتروني، وتتجلى فيها النواحي الإجرائية التي تضمن المحاكمة السليمة والعادلة للمتورطين في جريمة الإرهاب السيبراني، ليس هذا فحسب، بل يتعين أيضا أن تعمل الدول جنبا إلى جنب بمختلف الآليات القانونية المتاحة من اتفاقيات جماعية أو ثنائية أو وفق الاعتبارات الدبلوماسية من أجل تعزيز التعاون القضائي والدفع بعجلة التنسيق بين الفواعل الدولية بما يضمن السلم والأمن الدوليين على الفضاء السيبراني، وهذا بطبيعة الحال يحتاج إلى مادية تشريعية ملزمة لضمان المسائلة والزامية الوفاء بالالتزامات الدولية في مجال التعاون القضائي في التصدي للإرهاب السيبراني، وخلق منافذ خاصة تتناسب وطبيعة هذه الجريمة (الفصل الثاني).

الفصل الأول:

الجهود الأمنية الدولية لمواجهة الإرهاب الإلكتروني

تخلص دراستنا من خلال مباحثها السابقة أن عملية تأمين الفضاء الإلكتروني من تداعيات جريمة بحجم الإرهاب الإلكتروني واستراتيجيات الوقاية منها يجب أن تكون على قدر كبير من التنظيم والهيكلية، فليس من الصواب ولا من المستساغ أن نعمل على مواجهة هذا النوع من الجرائم المعقدة دون أن تكون لنا رؤية استراتيجية واضحة للقيام بذلك، كما لا يعقل أن نواجه إرهابا يعمل وينشط في فضاء إلكتروني يتقاسم تسيره عدة كتل وقطاعات، ويلعب فيه المجتمع المدني دورا محوريا سواء أكان ذلك سلبا أو إيجابا، لا يعقل أن يواجه في وسط كل هذا إلا بجمع كل هذه الفواعل الرئيسية وهؤلاء اللاعبين الأساسيين في جبهة واحدة متسقة ومتجانسة ضمن سياسية أمنية تتحدد مسؤولياتها ضمن إطار مبادئ الحوكمة، كما تقتضي أيضا نظرية الردع العام أن ينشأ هيكل تنظيمي واختصاص علمي يعنى بقضية الإثبات الجنائي في الجرائم الماسة بالفضاء الإلكتروني وبصفة خاصة وحرارة ما يتعلق منها بظاهرة الإرهاب السيبراني، الذي غدى ساريا في عصرنا كالنار في الهشيم (المبحث الأول)، كما يجب أيضا أن تشمل السياسات الأمنية التي نعنى بحماية هذا الفضاء على تطبيقات وتكتيكات وقائية تحول دون بلوغ الإرهابيين لأهدافهم الإجرامية عبر الفضاء الإلكتروني، والعمل على تأمين جميع الطبقات التكوينية له بدأ بالمعلومات والبيانات وصولا إلى الأصول المادية له.

ولا يعدم العلم الحديث والتقنيات الإلكترونية والبرمجية الوسيلة لتحقيق ذلك، فقد قدم لنا المتخصصون نماذج رائعة من المعدات التي إن لم تؤمن الفضاء الإلكتروني بشكل كامل، فإنها تعمل على التخفيف من حدة التداعيات والآثار التي تخلفها هجمات الإرهاب الإلكتروني، ويعمل أيضا المبرمجون في مجال علم الحواسيب والشبكات على وضع برامج فاعلة تتمتع بالديناميكية من أجل للتصدي لأي تهديد أو هجوم يستهدف الفضاء السيبراني، كما أن لمهندسي الأمن دورا كبيرا في صياغة نماذج فاعلة ومؤثرة في حماية النطاقات التي تحمل داخلها منظمة متكاملة للمعلومات، بأجهزتها وشبكتها ومعلوماتها وموظفيها، ومن خلال كل هذه الأدوار التي تلعبها الفواعل وذوى المصلحة بالإضافة إلى الأساليب التقنية والفنية تتكون سياسة أمنية شاملة لكل الثغرات التي يمكن أن يتم استغلالها لشن أي شكل من أشكال الهجمات التي تهدد أمن وسلامة الفضاء السيبراني (المبحث الثاني).

المبحث الأول:

التنظيم الوظيفي لدحر الإرهاب الإلكتروني

سعت الدول لبذل جهود كبيرة على الصعيدين الوطني والدولي من أجل تنسيق العمل بين القطاعين العام والخاص وتحديد المسؤوليات والأدوار التي يتعين على القطاع الخاص لعبها من أجل المساهمة الفعالة في تأمين الفضاء السيبراني من التهديدات المحدقة به، كما نشطت على الوتيرة ذاتها مساهمة المجتمع المدني في التصدي لجرائم الإرهاب الإلكتروني، ودعم دورها الحيوي في ذلك، وهذا في إطار تنظيم وإدارة رشيدة تتكافل فيها جهود القطاعات ومنظمات المجتمع الدولي مع الحكومة والقطاع العام لصياغة نموذج متكامل للوقاية والتصدي لظاهر استغلال الفضاء الإلكتروني لأغراض إرهابية (المطلب الأول)، كما عملت أيضا على استحداث أجهزة وتخصصها الطب الشرعي التي تعنى بالتحقيق الرقمي في الإرهاب الإلكتروني وغيرها من جرائم تقنيات المعلومات، بغية الحصول على أدلة موثوقة تقطع دابر الاعتقاد السائد بأن المجرم السيبراني مجرم متخفي لا يمكن الوصول إليه ويتعسر إقامة الدليل على الجرائم التي يقوم بارتكابها أو الأنشطة التي يمارسها على الفضاء الإلكتروني، وبذلك يكون الطب الشرعي الرقمي قد رفع التحدي رغم كل العقبات والعثرات التي تواجهه للقيام بالاستدلال على ما يرتكب في الفضاء السيبراني من إجرام محققا بذلك أبعاد ومقتضيات العدالة والغابة من العقاب (المطلب الثاني).

المطلب الأول:

حوكمة الأمن السيبراني

يشخص الفقهاء والباحثون الإرهاب الإلكتروني بأنه ظاهرة عالمية عابرة للحدود السيادية، وأنها ظاهرة تهدد كل مستخدم للفضاء الإلكتروني، وهذا ما يضاعف من قوتها ويضعف في المقابل أساليب مواجهتها، غير أن العمل بشكل جماعي منسق ومرتب وفق مبادئ الحوكمة، سيكون له الأثر الطيب في قمعها أو التخفيف من أثرها، فحوكمة الأمن السيبراني بما تتضمنه من مفهوم وما ترمي إليه من أبعاد (الفرع الأول)، بما في ذلك العمل المرتب والمنسق مع القطاع الخاص الذي يعتبر من بين أهم القطاعات التي تتعرض للهجمات السيبرانية، ومن بين أبرز الفواعل على الصعيدين الوطني والدولي، ومن بين أولى المصلحة في تأمين الفضاء الإلكتروني، تشكل آلية حاسمة لضمان السلم والأمن على هذا الفضاء (الفرع الثاني)، ومن المهم أيضا إشراك المجتمع المدني الذي يلعب دور أساسي في وضع وتفعيل استراتيجيات وأطر الأمن السيبراني من أجل ضمان بيئة إلكترونية آمنة (الفرع الثالث).

الفرع الأول: مفهوم حوكمة الأمن السيبراني:

تحتل القضايا الأمنية مرتبة عالية في سلم أولويات عمل الحكومات والدولي على المستوى الوطني والدولي، غير أن مفهوم الأمن مع ظهور الوسط الإلكتروني والفضاء السيبراني قد فتح على الدول تحديات جديدة تحاول رفعها من خلال تبني حوكمة أمن هذا المجال، ولما كان مصطلح الحوكمة من المصطلحات الحديثة فإنه من الضرورة بمكان العمل على تحديد مفهومها بوضع تعريف يجلي معالمها (أولا) ويبرز الأبعاد المتعددة التي ترمي إليها (ثانيا).

أولا: تعريف الحوكمة الأمنية في مجال الفضاء الإلكتروني:

تعد عملية القيام بتطبيق أو إعمال السياسة العامة من بين العمليات التي تتسم بالصعوبة والعسر، وهذا اعتبارا لكون مثل هذه السياسات والبرامج العامة تستوجب نوعا من التكاتف والتشارك والتعاقد بين عدة فواعل، فهو في أغلب الأحيان يتطلب مساهمة أكثر من منظومتين، وأنه في الغالب الأعم يستوجب أكثر من حكومة وطنية، ويتطلب إسهاما من الميادين والمجالات (القطاعات) الربحية وغير الربحية، والمشاع في التعبير عن هذه الدلالة من الأشكال والأساليب المتسعة من الدور الجمعي هو مصطلح الحوكمة⁽¹⁾.

وتعتبر الحوكمة من المصطلحات المستجدة والحديثة، والهدف منه هو وصل المواضيع السياسية وتسيير وتوجيه المسائل المتعلقة بشؤون الدولة بالفواعل الأخرى التي تملك تأثيرا وفاعلية في صياغة السياسات التي تعمل على تنظيم الحياة العامة، سواء أكانت فواعل سياسية أو اجتماعية، فهي بهذه الدلالة تصيغ نمطا محورا ومبدلا للأسلوب التقليدي في المباحث الدراسية السياسية، من اعتبارها ثمرة لمؤسسات الدولة الرسمية، إلى أسلوب جديد يضع نصب عينيه على الجماعات الأهلية والفواعل الاجتماعية في تنمية السياسات وتطويرها، مستقصيا وباحثا عن شكل التفاعل بينها بمظهر متسق مع مؤسسات الدولة ومؤسسات القطاع الخاص والمجتمع المدني⁽²⁾، فهذه المقاربة إذًا، تضع الحوكمة أمام نقطتين مفهومتين مهمتين هما؛ الحكم والتنظيم.

أما الحكم فكما أشرنا إليه، وهو أن المقاربة السياسية الحديثة قد أبعدت الطبيعة المترابطة للعلاقة بين الدولة والمجتمع والسوق عن الهيكل الهرمي التقليدي حيث كانت الدولة تحتكر السلطة، إلى هيكل الشبكة

(1) لورانس أوتول وكينيث ماثير، كتاب كامبردج في الإدارة العامة: (المنظمات والحوكمة والأداء)، ترجمة: (عبد الحكم أحمد الخزامي)، الطبعة العربية الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2013، ص 20.

(2) عنتر مرزوق وعبد المؤمن سي حمدي، الإنتقال إلى الحوكمة المحلية في الجزائر: (دراسة فب التحديات والآليات)، مجلة التراث، المجلد 07، العدد 05، جامعة زيان عاشور، الجلفة، جوان 2018، ص ص: 214-230: <https://www.asjp.cerist.dz/en/article/60109>

الذي يشمل أصنافا من الفواعل الجدد، وظهر بعد ذلك تمييز بين العلاقة المتبادلة فيما يعرف بالعلاقة الأفقية والرأسيّة. ومن الضروري فهم هذه العلاقات كلها، فهذه العلاقات ذات أهمية بالغة في المجال السيبراني، وفهماها يفضي إلى تحديد هياكل الحوكمة الجديدة في مجال الأمن السيبراني أفقيا ورأسيا⁽¹⁾.

أما عن التنظيم، فقد أثار التحول في الفكر المفاهيمي من الحكومة إلى الحوكمة والبحث عن فهم آليات التنسيق الناشئة بين الدولة والمجتمع، عدة أسئلة تتعلق بالدور الجديد والمتغير للآليات التنظيمية والتنسيقية بين الدولة والمجتمع، وأدى هذا الفكر المفهومي بعد ذلك إلى محاولات للتمييز بين الحوكمة والتنظيم، حيث برز أهم تفسير يجلي ذلك من خلال اعتبار الحوكمة أكثر اتساعا من التنظيم الذي يعتبر مفهوما مقيدا بالسيطرة المستمرة والمركزة التي تمارس من قبل وكالة عامة مستقلة على الأنشطة الخاصة، فالحوكمة تشير إلى أنظمة التنسيق والجهات الفاعلة المتعددة، كما أن مصطلح الحوكمة في نفس يجلي الفاعلين من جهة والتفاعلات التي تقع بينهم من جهة أخرى، كما يحمل بين طياته أسس هذه التفاعلات فيجب حين دراسة الحوكمة، الجمع بين الجهات الفاعلة والهياكل والعمليات، بالإضافة إلى العلاقات القائمة بينهم والأفكار الكامنة في تفاعلاتهم⁽²⁾.

ومصطلح الحوكمة في اللغة العربية هو ترجمة موجزة لما يعرف في اللغة الإنجليزية بـ (Corporate Governance)⁽³⁾، ويعرف مصطلح (governance) في اللغة الإنجليزية على أنه: (نشاط إدارة بلد أو التحكم في شركة أو مؤسسة؛ الطريقة التي يتم بها تنظيم بلد أو مراقبة شركة أو مؤسسة)⁽⁴⁾، أما القاموس الفرنسي لاروس، فيعرفها لغة على أنها: (طريقة التسيير والإدارة) وبحيننا بعد ذلك إلى المعنى المعتمد في اللغة الإنجليزية فيصرح على أنه: (من الإنجليزية، الحوكمة، فن الحكم المستقل علت سلطة الدولة، تهتم بالمرونة والتأديب، واحترام قضايا البيئة، وتستند إلى مشاركة مختلف الجهات الفاعلة في المجتمع المدني)⁽⁵⁾.

(1) Samantha A. Adams, Marlou Brokx, Lorenzo Dalla Corte, Maša Galič, Kaspar Kala, Bert-Jaap Koops, Ronald Leenes, Maurice Schellekens, Karine e Silva, Ivan Škorvák, The Governance of Cybersecurity: (A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK), TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, The Netherlands, November 2015, PP.27-28.

(2) Ibid..PP.28-29.

(3) العياشي زرار، من الحوكمة المحلية إلى الحوكمة الإلكترونية للإدارات المحلية، مجلة القانون والمجتمع، المجلد 03، العدد 01، جامعة أحمد دراية، أدار، جوان 2015، ص ص: 84-112. <https://www.asjp.cerist.dz/en/Articles/133>

(4) oxford learner's dictionaries; governance: " the activity of governing a country or controlling a company or an organization; the way in which a country is governed or a company or institution is controlled "

<https://www.oxfordlearnersdictionaries.com/definition/english/governance?q=governance>

(5) larousse; gouvernance; " Manière de gérer, d'administrer ", " De l'anglais governance, art de gouverner indépendant de l'autorité étatique. (Soucieuse de souplesse, de transdisciplinarité et du respect des enjeux environnementaux, elle repose sur la participation de différents acteurs de la société civile.):

<https://www.larousse.fr/dictionnaires/francais/gouvernance/37692?q=gouvernance#431601>

أما اصطلاحاً فقد تعددت التعاريف وتباينت فيما بينها، إذ تم تعريفها من قبل منظمة التعاون الاقتصادي على أنها: (مجموعة من العلاقات فيما بين القائمين على إدارة الشركة ومجلس الإدارة وحملة الأسهم وغيرهم من المساهمين)، أما عن منظمة التمويل الدولية فقد عرفت على أنها: (هي النظام الذي يتم من خلاله إدارة الشركات والتحكم في أعمالها) ⁽¹⁾.

يوجد ممن الباحثين والدارسين من يطرح فكرة حوكمة الأمن السيبراني كجزء من حوكمة الإنترنت وعلى رأسهم (Laura DeNardis) التي ذهبت هذا المذهب ⁽²⁾، غير أن حوكمة الإنترنت في بعض الأحيان تعدها مسألة ثانوية، ولذلك يتعين على ذوى المصالح أن يعملوا على تمديد تعريف الحوكمة من أجل أن تتطوي تحته كل المسائل التي يقوم على أساسها تصميم واستخدام الإنترنت، وما يترتب عنه من آثار اجتماعية، وأن يعملوا على جعلها من بين أولوياتهم ⁽³⁾.

برز مفهوم حوكمة الإنترنت إلى الوجود لأول مرة على الصعيد العالمي في "القمة العالمية لمجتمع المعلومات" والتي بدأت فعاليتها بناءً على قرار اتخذته الجمعية العامة للأمم المتحدة تحت رقم 56/183 ⁽⁴⁾⁽⁵⁾، والتي عرفت على أنها: (تطور وتطبيق المبادئ والمعايير والقواعد وإجراءات اتخاذ القرار والبرامج المشتركة بواسطة الحكومات، القطاع الخاص، المجتمع المدني في أدوارهم الخاصة بهم (In their respective roles)، التي تشكل تطور واستخدام الإنترنت) ⁽⁶⁾.

والملاحظ من هذا التعريف أنه يقدم بشكل صريح إقراراً بأن العناصر التكوينية لعمل الفضاء الإلكتروني، أو بالأحرى تعدد الأدوار الوظيفية التي تلعبها عناصره، والذي ترتب عنه دخول الكثير من الفواعل المختلفة وغير المتجانسة فيه، وجعلت في المقابل من عملية تنظيمه عملية متعددة

(1) العياشي زرزار، المرجع السابق.

(2) Tatiana Nascimento HEIM, and Ramses A. WESSEL, The Global Regulation of Cybersecurity: A Fragmentation of Actors, Definitions and Norms, Draft contribution to be published in Lucía Millán Moro (dir.) and Gloria Fernández Ciberataques Arribas (ed.), y Ciberseguridad en la Escena Internacional, 2020. <https://pdfs.semanticscholar.org/ecf5/4154cfb07634324b4d62107b0c7b7600d3e1.pdf>

(3) ولیم هـ داتن، آنا دوباتكا، مايكل هيلز، غينيت لو، فيكتوريا ناش، حرية الإتصال حرية التعبير: (تغيير البيئة القانونية والتنظيمية الداعمة

للإنترنت، منظمة الأمم المتحدة التربية والعلم والثقافة، فرنسا، 2013، ص 79.

(4) قرار الجمعية العامة رقم 56/183 الصادر بتاريخ 31 جانفي 2002، المتضمن مؤتمر القمة العالمي لمجتمع المعلومات.

(5) رضوى الخولي، حوكمة الإنترنت، سلسلة أوراق الحق في المعرفة، مركز دعم لتقنية المعلومات، القاهرة، (د.س.ن)، ص 03.

(6) محمد فرحات، دور البرلمان في حوكمة الإنترنت، مجلة اتجاهات سياسية، تحليلات سياسية، المركز الديمقراطي العربي، المجلد 03، العدد

11، برلين، ألمانيا، يونيو 2020، ص ص: 137-152.

الفواعل، فمسألة تنظيم الفضاء الإلكتروني ليست حكرا على فاعل واحد، بل يتشارك فيه كل من له دور وظيفي⁽¹⁾.

يلاحظ من جهة أخرى أن هذا التعريف يؤثر بشكل كبير على النهج والبرامج والاستراتيجيات المتعلقة بحوكمة الفضاء الإلكتروني، إذ أن ما يتمخض من هذا التعريف من مناهج وبرامج لا تخرج في مجملها عن حالتين؛ فإنما أن تكون ساذجة إذا كانت قائمة على تصور أن مجرد حوار بسيط يمكن أن يكون الحل للنزاعات المختلفة، ويكون هزليا إذا كانت مضامين البرامج والاستراتيجية مجرد مطالبات غير مهمورة بضمانات تحقيقها ودون أن تكون مصحوبة بمسؤوليات تقع على أطرافها⁽²⁾.

وتجدر الإشارة هنا أن حوكمة الإنترنت لا يرادفها مصطلح الحوكمة الإلكترونية، إذ أن هذه الأخيرة هي: (استخدام سلطات الإدارة العامة لتطبيقات تكنولوجيا المعلومات وتكنولوجيا الاتصالات من أجل الحصول على كفاءة وفعالية وشفافية تبادل المعلومات بين: الحكومة - الحكومة (المعاملات الداخلية) أو الحكومة - الوكالات الوطنية أو الولائية أو البلدية أو المحلية ؛ الحكومة - المواطنون والحكومة - الشركات، مما يتيح الوصول إلى المعلومات واستخدامها)⁽³⁾، فهي إذا تشر إلى: (استخدام تكنولوجيا المعلومات والاتصالات لتحسين كفاءة الحكومة وفعاليتها وشفافيتها ومساءلتها)⁽⁴⁾.

فالحوكمة الإلكترونية بهذا المعنى تختلف كلياً عن حوكمة الإنترنت أو حوكمة الفضاء الإلكتروني، فالحوكمة الأولى يكون موضوع الحوكمة فيها أو محلها هو المؤسسات والإدارات والشركات وما إلى ذلك من القطاعات بحيث يتم اللجوء إلى مزايا وخصائص الفضاء الإلكتروني في إدارتها وتسييرها، أما الحوكمة الثانية فهي حوكمة يكون موضوعها أو محلها الفضاء الإلكتروني نفس.

وتجدر الإشارة في هذا الموضوع أيضاً، إلى أن مسألة حوكمة الإنترنت لم تكن محط إجماع بين الدول، فالخلافات فيها كثيرة بين مختلف الفواعل الدولية، ولاسيما بين الولايات المتحدة الأمريكية وبين

(1) Ahmed DAHMANI, Jose DO-NASCIMENTO, Jean-Michel LEDJOU, Jean-Jacques GABAS, la démocratie à l'épreuve de la société numérique, Editions Karthala, PARIS, 2007, P.131.

(2) Geneviève VIDAL, la sociologie des usages: (continuités et transformations), LAVOISIER, 2012, P.168.

(3) Mariua ERBANA, Raluca-Mariana TEFANB, Eduard-Ionel IONECUL, Information Protection – Security, Clustering and E-governance, 21st International Economic Conference 2014, IECS 2014, 16-17 May 2014, Sibiu, Romania, Procedia Economics and Finance, Volume 16, Elsevier B.V, 2014, PP. 288-292:

<https://www.sciencedirect.com/science/article/pii/S221256711400803X>

(4) Satyabrata DASHA, Subhendu Kumar PANIB, E-Governance Paradigm Using Cloud Infrastructure: Benefits and Challenges, International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science, Volume 85, Elsevier B.V, 2016, Pages 843-855:

<https://www.sciencedirect.com/science/article/pii/S187705091630624X>

روسيا والصين، إذ أن كل جهة من هاتين الجهتين تحاول أن تمارس نوعاً من النفوذ والهيمنة على النظم التي تسري على الإنترنت بما يحقق مصالحها، والعمل في الوقت ذاته على منع الطرف الآخر من ذلك، ويتجلى هذا الصراع من خلال سياسة الرفض التي تنتهجها روسيا والصين إزاء النموذج الحالي لحوكمة الإنترنت، خاصة ما يتعلق منها بوجود فواعل من غير الدول، كما أن هناك نوعاً من المواجهة الروسية الصينية لهيمنة الولايات المتحدة الأمريكية على آيكان⁽¹⁾.

ليست الهيمنة والسيطرة وحدهما من يقف وراء تباين وجهات نظر حول حوكمة الفضاء السيبراني، بل لأن هذا الموضوع نفسه يطرح العديد من المسائل المعقدة، كحرية التعبير، ومبدأ الخصوصية، والأمن، وإنفاذ التشريعات، والسيادة الوطنية، ومن المعروف أن هذه القضايا داخلية ضمن المسائل الجدلية الحساسة التي تتباين فيها وجهات نظر الدول⁽²⁾.

وعلى هذا الأساس فإن تصور منهج أو برنامج عالمي لحوكمة الأمن السيبراني يعد أمر غاية في الصعوبة، وذلك أن الحوكمة تعني الإدارة والتنظيم معاً، واختلاف نهج ذلك بين الدول، وأسبقية المصالح الداخلية للدول على حساب المصلحة العالمية، وسعي كل دولة إلى توظيف هذا الفضاء فيما يخدم مصالحها، كل هذه تعد عوائق جدية تحول دون صياغة خارطة طريق نحو حوكمة هذا الفضاء العالمي.

وإذا كانت الدول باختلافاتها وصراعتها عاجزة عن خلق نموذج عالمي للحوكمة، فمن هي الجهة التي يمكن أن يخول إليها أمر حوكمته؟، ترى الباحثة (Laura DeNardis) أن هذا تساؤل لا معنى له مطلقاً، إنما التساؤل الذي يجب أن يكون دائماً محور البحث عن جوابه يتجلى في تحديد الشكل الأكثر فعالية وتأثير للحوكمة⁽³⁾، إذ أن حوكمة الأمن السيبراني لا يملك زمامه أحد، فهو ليس نظاماً أحاديثاً بمفاتيح يمكن أن يتم إعطاؤها وتسليمها من مجموعة لأخرى، إنه نظام متعدد المستويات والطبقات⁽⁴⁾.

وعلى ضوء ما تقدم من طرح يمكن تعريف حوكمة الأمن السيبراني على أنه: (الأساليب التي يستخدمها العديد من أصحاب المصلحة لتحديد وتأطير وتنسيق الاستجابات الاستباقية والتفاعلية للتهديدات المحتملة لسرية وتكامل وتوافر أجهزة الكمبيوتر والشبكات، والمعلومات التي تشكل معاً

(1) شفيق نوران، حوكمة الإنترنت: (أبعاد الصراع على إدارة الفضاء الإلكتروني)، موقع المستقبل للأبحاث والدراسات المتقدمة، 12 يوليو 2014،

تم الاطلاع عليه بتاريخ 15 جويلية 2020، على الساعة 15:22 سا، مختصر الرابط: <https://n9.cl/9wkq>

(2) منى الأشقر جبور، السيبرانية: (هاجس العصر)، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول

العربية، (د.م.ن)، (د.ت.ن)، ص 14، متوفر على موقع جامعة الدول العربية: <https://carj.org/node/4644>

(3) Tatiana Nascimento HEIM, and Ramses A. WESSEL, Op.Cit

(4) Laura DENARDIS, The Global War for Internet Governance, Yale University Press, usa, 2014, P.226.

الفضاء الإلكتروني... وهذا لا يشمل فقط مناهج قصيرة المدى ولملموسة لمواجهة التهديدات المعروفة، ولكن أيضاً على وجه الخصوص تطوير وتنفيذ الهياكل والعمليات للحد من عدم اليقين وتمكين الاستجابة للتهديدات من الأحداث غير المتوقعة على المدى الطويل⁽¹⁾.

ويمكن لنا أن نعرفه أيضاً على أنه: "مجموع القواعد والمعايير التي تستند إلى مبادئ الشفافية والمسؤولية والعدالة التي يجب أن يتقيد بها أصحاب المصلحة من القطاع العام والخاص ومنظمات المجتمع المدني لتوفير بيئة آمنة على الفضاء الإلكتروني والتصدي لمختلف التهديدات التي يمكن أن تأتي من خلاله مع تكريس أسس الديمقراطية وضمان الحريات والحقوق الرقمية ومراعاة مقتضيات الحكم الرشيد"

وتبرز اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي كاتفاقية وحيدة من بين كل الاتفاقيات المتعلقة بالأمن السيبراني التي تنص بشكل صريح على تفعيل مبدأ الحوكمة في تأمين الفضاء السيبراني في المادة 27 الفقرة الأولى الآتي نصها: (1- حوكمة أمن الفضاء الإلكتروني: أ) تقوم كل دولة طرف باتخاذ الإجراءات الكفيلة لإنشاء آلية مؤسسية ملائمة مسؤولة عن حوكمة أمن الفضاء الإلكتروني، ب) ويجب أن تؤدي التدابير المتخذة وفقاً للفقرة 1 من هذه المادة إلى إنشاء قيادة قوية والالتزام في جميع جوانب أمن الفضاء الإلكتروني للمؤسسات والمجموعات المعنية في كل دولة طرف...⁽²⁾.

ثانياً: مرتكزات حوكمة الأمن السيبراني:

تقوم حوكمة الأمن السيبراني على العديد من المرتكزات التي تضمن فاعلية الأمن السيبراني وتأثره في حماية الفضاء الإلكتروني من التهديدات المختلفة التي تحقق به، وهذه المرتكزات هي:

1- الوعي:

تتطلب الجهود الرامية إلى تحقيق الأمن السيبراني إلى رفع مستوى الوعي لدى ذوى المصلحة من مستخدمي الفضاء الإلكتروني أياً كانوا وأياً كانت المصالح التي تربطهم بالفضاء الإلكتروني، ويجب أن ينصب هذا الوعي بصفة خاصة على إدراك ما يتهدد مصالحهم على الفضاء

(1) Samantha A. Adams, Marlou Brokx, Lorenzo Dalla Corte, Maša Galič, Kaspar Kala, Bert-Jaap Koops, Ronald Leenes, Maurice Schellekens, Karine e Silva, Ivan Škorvánek, Op.Cit. PP.31-32.

(2) المادة 27 من اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المعتمدة في الدورة العادية 23 لقمّة رؤساء دول وحكومات الاتحاد الأفريقي، غينيا الاستوائية، بتاريخ 27 يونيو 2014.

الإلكتروني، وإحاطتهم الكاملة بالدور الذي يجب أن يلعبوه في التعاطي مع مثل هذه التهديدات والمخاطر المحدقة بهم وبمصالحتهم المختلفة⁽¹⁾.

كما يجب أيضا أن ينصب هذا الوعي في تكوين الإدراكات والمعارف المتعلقة بالأسباب والدوافع والمحفزات التي تجعل من بعض المنظومات عرضة لمثل هذه التهديدات والهجمات الإلكترونية، كما يجب أيضا أن تتكون معارف لدى ذوي المصلحة من المستخدمين والموظفين للفضاء الإلكتروني عن التداعيات التي قد تنجر عن الهجمات التي تستهدفهم والطريق التي تأثر بها عليهم، ويجب أن يكون هذا الوعي والإدراك ذو شمولية، فلا يقتصر على حدود المنظمة المعنية فحسب، بل يجب أن يكون عاما وشاملا حتى للعلاقات والروابط الخارجية التي قد تأثر على أمن المنظمة السيبراني⁽²⁾.

وقد نصت اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي في هذا الصدد بالتزام الدول الطرف فيها بالعمل على الدفع بثقافة أمن الفضاء السيبراني نحو الأمام بين الحكومات والقطاع الخاص والمجتمع المدني على حد سواء، كما دعت أيضا إلى ضرورة تركيز هذه الثقافة على الأمن حال القيام بتنمية وتحديث أنظمة وشبكات المعلومات، كما يجب أيضا إبداع أساليب جديدة للتفكير والتصرف حال توظيف هذه الأنظمة وعند القيام بالاتصال أو إجراء المعاملات عبر هذا الفضاء⁽³⁾. كما أجازت الاتفاقية أيضا في سياق الترويج لهذه الثقافة بما يلي: (إنشاء خطة تأمين فضاء إلكتروني للأنظمة التي تديرها حكومات هذه الدول؛ إعداد وتنفيذ برامج ومبادرات للتوعية بالأمن لمستخدمي الأنظمة والشبكات؛ التشجيع على تطوير ثقافة أمن الفضاء الإلكتروني في المؤسسات...)⁽⁴⁾.

2- التصميم:

يكون التصميم كمرتكز من مرتكزات حوكمة الأمن السيبراني من خلال إنتاج ووضع الأطر والاستراتيجيات والمواصفات التي من خلالها يتم التصدي للتهديدات الأمنية، والمخاطر المختلفة التي تحدث بالفضاء الإلكتروني، وكذلك المتطلبات الواجب توفرها لتأمين هذه البيئة، إضافة إلى الامتثال للقواعد والسياسات التي يتعين انتهاجها وتطبيقها⁽⁵⁾.

(1) Information Technology Industry Council, The IT Industry's Cybersecurity Principles for Industry and Government, Information Technology Industry Council (ITI), Washington, Version 3.0, 2011, P.09.

<https://www.itic.org/dotAsset/0e3b41c2-587a-48a8-b376-9cb493be36ec.pdf>

(2) Richard HORNE, Governing cyber security risk: It's time to take it seriously: (Seven principles for Boards and Investors), PricewaterhouseCoopers LLP, January 2007, P.04.

(3) المادة 1/26 من اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

(4) المادة 1/26 ب.

(5) Janne J. KORHONR, Kari HIEKKANEN, Juha MYKKANEN, Information Security Governance, Strategic and Practical Approaches for Information Security Governance: (Technologies and Applied Solutions), IGI Global, 2012: PP.1-16. https://www.researchgate.net/publication/274007219_Information_Security_Governance

وتهدف الاستراتيجية والبرامج والسياسيات المتعلقة بالأمن السيبراني إلى توصيف وتعيين الأساليب والنهج التي تسير عليها الإدارة، وكذلك تقليص المخاطر والتهديدات السيبرانية بصورة فاعلة وبطريقة متكاملة وشاملة، وهذا ما يفرض على نوى المصلحة تكوين وإنشاء استراتيجية ونهج عام للأمن السيبراني بحيث تكون الدرع الواقي والسد المانع أمام المخاطر والتهديدات التي يمكن أن تنفذ من خلال الفضاء السيبراني، مستندة في ذلك ومستتيرة بما تم تحديده من معايير وقواعد توجيهية، سواء أكانت صياغتها وطنية أو دولية أو صناعية⁽¹⁾.

ويتعين أيضا لهذه الاستراتيجيات والبرامج أن تتضمن فقه التوقعات، أو فقه الاحتماليات، وذلك من خلال اشتغالها على أساليب وآليات وطرق الاستجابة للتهديدات المفترضة افتراضا مرجحا، كما يتعين أيضا أن تدرج فيها آليات وطرق تكفل التعافي منها إذا ما حدثت⁽²⁾.

كما يتعين أيضا أن تأخذ بعين الاعتبار الأصول العامة والعناصر الأساسية التي تقوم عليها الاستراتيجيات بعمومها، فتكون خططا وتصميمات تتحدد فيها الأهداف والغايات المستقبلية والآليات التي تمكن من بلوغها، ومرورها بمراحل ثلاث بداية من تحديد الأهداف وصولا إلى صياغة الاستراتيجية، فضلا تحقق البعد الفلسفي فيها ناهيك عن هيكلتها⁽³⁾.

وعليه يمكن تعرف الاستراتيجية من منظور الأمن السيبراني على أنها: (بيان بتصميم أصحاب المصلحة في الأمن السيبراني على اتخاذ تدابير في مجالات مسؤوليتهم الخاصة، والتعاون مع أصحاب المصلحة الآخرين وتبادل المعلومات اللازمة)⁽⁴⁾.

3- التنمية:

يتعلق هذا المرتكز بشكل أساسي في تطوير حلول وخدمات أمن المعلومات، والعمل على تطبيق معايير ومميزات الأمان التي يتعين توفرها على الأنظمة والنهج سارية المفعول، والحديث منها بشكل خاص⁽⁵⁾. وقد استجبت الكثير من الاستعدادات في الآونة الأخيرة وهذا يؤكد على ضرورة توفير استراتيجية أمن سيبراني تتسم بالاستمرارية والنشاط، إذ على أساسها يتم تحديد الحدود الفاصلة بين النجاح والفشل في ما يختص بحماية أصول الفضاء الإلكتروني أيما كان نوعها⁽⁶⁾.

(1) U.S. DEPARTMENT OF THE TREASURY, G7 fundamental elements of cybersecurity for the financial sector, , Treasury and Federal Reserve, U.S. DEPARTMENT OF THE TREASURY, 10/nov/2016:

<https://www.treasury.gov/press-center/press-releases/Pages/jl0570.aspx>

(2) Richard HORNE, Op.cit. P.04

(3) أنظر في ذلك: محمد جمال عبد الله، التخطيط الاستراتيجي، الطبعة الأولى، دار المعتر للنشر والتوزيع، الأردن، 2016، ص 259.

(4) Galinec DARKO, Moznik DARKO, Boris Guberina, Cybersecurity and cyber defence: national level strategic approach, Automatika Journal for Control, Measurement, Electronics, Computing and Communications, volume 58, Issue 3, PP.273-286 : <https://www.tandfonline.com/doi/full/10.1080/00051144.2017.1407022>

(5) Janne J. KORHONR, Kari HIEKKANEN, Juha MYKKANEN, Op.cit.

(6) Alina ANDRONACHE, ALIGNING CYBERSECURITY MANAGEMENT WITH ENTERPRISE RISK MANAGEMENTIN THE FINANCIAL INDUSTRY, A thesis submitted for the degree of Doctor of Philosophy, Brunel Business School, Brunel University, London, 2019, P.46.

ومن بين أهم مقتضيات التطور، القيام بتحضير ووضع دورات تدريبية بما في ذلك تلك المتعلقة بتكنولوجيا المعلومات من أجل الإحاطة والاطلاع على أحدث التطورات ومسايرتها، ويتعين أن تشمل تلك الدورات أيضا الإحاطة الكاملة بالجرائم المتوقعة ذات الصلة بهذه التطورات الجديدة، ووضع الطرف لمواجهتها من جهة ومن أجل مواكبة التطورات المتتابعة فيما يخص المعايير الدولية لأمن المعلومات من جهة ثانية (1).

كما ويتطلب الأمر أيضا القيام بالتنسيق وتعيين أولويات وأسبقيات البحث والتطوير في مجال الأمن السيبراني، ومد أفق مجتمع الأبحاث والدراسات في هذا المجال، وتنمية وتسويق الملكية الفكرية والتكنولوجية والإبداع بدعم البحوث التخصصية والتطويرية، والعلم على تعزيز السوق المحلي والصناعات في ميدان الأمن السيبراني، والعمل أيضا على وضع تخصص جامعي يعني بالأمن السيبراني القائم على المعايير المتعلقة بذلك وتخصص في مجال العلم الجنائي الرقمي واستحداث مناهج متعلقة بالجرائم المعلوماتية في كليات دراسة القانون ومعاهد القضاة (2).

يجب أن يكون التعليم والتدريب دؤوبين فيما يتعلق بالمسائل المرتبطة بالأمن السيبراني، ويتعين أن يتكون هذه المسؤولية مشتركة جنبا إلى جنب مع القاطعين العام والخاص - شأنها شأن الاستراتيجيات الأخرى - (3)، كالعامل مثلا على تأهيل القوى العسكرية السيبرانية وتدريبها من خلال ممارسة قتال افتراضي على الساحة السيبرانية تأهبا لأي تهديد جديد (4).

4- العمليات:

يتعلق هذا المرتكز أو البعد، بوضع سياسات الأمن موضع التنفيذ والتطبيق والإنفاذ في العمل التشغيلي اليومي (5)، فالخطط والتصاميم إنما جعلت في أصلها لتوضع موضع التنفيذ " فعندما يتم وضع خطة فمن الضروري أن ينتبه أحد ما إلى تطبيقها" (6)، إذ لا جدوى من التصميم والتخطيط ما لم يتم إنزالها موضع التطبيق والتنفيذ.

(1) فيصل محمد عسيري، الأمن السيبراني وحماية أمن المعلومات، ص 27، متوفر على الموقع:

<https://www.kutub.info/library/book/21854>

(2) مستشارية الأمن الوطني، أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، استراتيجية الأمن السيبراني العراقي، ص 09.

(3) Michal Tonhauser, Jozef Ristvej, Disruptive acts in cyberspace, steps to improve cyber resilience at National Level, 13th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM 2019), High Tatras, Novy Smokovec – Grand Hotel Bellevue, Slovak Republic, May 29-31, 2019, Transportation Research Procedia, Volume 40, Elsevier B.V, 2019, PP. 1591-1596
<https://www.sciencedirect.com/science/article/pii/S2352146519303916>

(4) عنتر بن مرزوق ومحي الدين حرشاي، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، المنشورات العلمية لجامعة قسدي مرياح، ورقلة، 2017، ص ص 65 - 80: <https://dspace.univ-ouargla.dz/jspui/handle/123456789/14052>

(5) Janne J. KORHONR, Kari HIEKKANEN, Juha MYKKANEN, Op.Cit.

(6) مايكل ج. دوريس، جون م. كيلي، جيمس ف. ترينر، التخطيط الاستراتيجي الناجح، ترجمة سمة عبدربه، الطبعة العربية الأولى، مكتبات ونشر العبيكان، المملكة العربية السعودية، 2006، ص 145.

وإنزال الاستراتيجيات والتصاميم والخطط في عمومها يحتاج إلى بعض المسائل والآليات الجوهرية، إذا يجب أولاً أن تتسم تلك الاستراتيجيات الموضوعية بالملئمة سواء أكان ذلك مع السياسات العامة سارية المفعول أو مع الأنظمة المعمول بها حال تطبيق الاستراتيجية، فضلاً عن إلزامية بناء هياكل تنظيمية تعمل على تطبيقها، وتأخذ بعين الاعتبار الاستراتيجيات الوظيفية في تحديد أبعاد أهمية الاستراتيجية المصممة⁽¹⁾.

وإذا أردنا أن ننزل هذه المتطلبات على مسألة تنفيذ استراتيجيات الأمن السيبراني فإننا سنقرر بأن عملية تنفيذها لا بد أن تراعي ملائمتها مع التشريعات المعمول بها، فلا يمكن أن نقبل باستراتيجية تأمن الفضاء الإلكتروني وفي نفس الوقت تنتهك خصوصية الأفراد، أو الأسرار التجارية للشركات وما إلى ذلك، فلا عن ملائمتها أيضاً مع ما استجد من تقنيات ونظم في مجال الفضاء الإلكترونيين إذ من غير المتصور تنفيذ خريطة طريق وليس هناك أي طريق أصلاً، فلا يمكن التحدث عن تأمين حواسيب قديمة خارج الخدمة، ولا تأمين أنظمة وبرامج سقطت في خبر كان.

كما يجب أيضاً توفير الهياكل التنظيمية التي تباشر عملية تنفيذ هذه الاستراتيجية، خاصة وأن الفضاء الإلكتروني وما يتعلق به من مسائل الأمن تتسم بالتعقيد وبالطابع التقني، فمفاد هذا المطلب هو إسناد الأمر إلى أهله، وتنفيذها بشكل تخصصي مهيكّل ومنظم، وفي الأخير لابد من النظر في مدى جدوها من خلال تتبع السياسات والاستراتيجية الوظيفية، إذ لا يعقل تنفيذ استراتيجية أمن سيبراني لا تتوافق مع استراتيجيات التجارة الإلكترونية أو الإدارة الإلكترونية أو الحكومة الإلكترونية وما إلى ذلك.

ويمكن أن نشير إلى بعض النقاط الأساسية التي يمكن من خلالها فهم الآليات التي تنفيذ في إطارها استراتيجيات الأمن السيبراني، وسنوقها على النحو الآتي:

أ- المراقبة:

تكون المراقبة كمرتكز لحوكمة الأمن السيبراني من خلال إنشاء هيكلية مراقبة ممنهجة تعمل على الكشف السريع عن أي حادث يطرأ على الفضاء الإلكتروني⁽²⁾، أو من أجل الكشف عن الجرائم المرتبطة بالنشاطات الإرهابية والتخريبية أو تلك التي تتال من أمن الدولة على ساحة الفضاء الإلكتروني⁽³⁾.

(1) أنظر: عبد القادر محمد الأسطة، أساسيات الإدارة الاستراتيجية الحديثة، الطبعة الأولى، الأكاديميون للنشر والتوزيع، الأردن، 2016، ص 13.

(2) U.S. DEPARTMENT OF THE TREASURY, G7 fundamental elements of cybersecurity for the financial sector, Op.cit.

(3) عنتر بن مرزوق ومحي الدين حرشاي، المرجع السابق.

تتجلى لنا صور المراقبة من خلال العديد من الأنشطة المستمرة ضمن الاستراتيجية المصممة لأمن الفضاء الإلكتروني، ومن ذلك؛ مراقبة الشبكات والاختبار والتدقيق بالإضافة إلى التدريبات المشتركة بين القطاعين العام والخاص التي تقضي إلى فهم وإدراك أفضل لطبيعة التهديدات ومواطن الضعف السيبرانية⁽¹⁾.

ب- الاستجابة:

يجب العمل على تطوير إقامة هياكل ومباشرة عمليات تمكين الاستجابة للتهديدات⁽²⁾، ويعد إنشاء فرق الاستجابة لحوادث أمن الكمبيوتر جزءاً أساسياً من هذه العملية⁽³⁾، كما يجب التعاون بين القطاعين العام والخاص من أجل تدريب هذه الفرق وتأهيلها⁽⁴⁾، ويتعين أيضاً للاستجابة أن تتضمن النقاط التالية:

- تقييم طبيعة ونطاق وتأثير الحادث السيبراني في الوقت المناسب؛
- احتواء الحادث وتخفيف أثره؛
- إبلاغ أصحاب المصلحة الداخليين والخارجيين؛
- تنسيق أنشطة الاستجابة المشتركة حسب الحاجة⁽⁵⁾.

ج- التعافي:

ويكون ذلك من خلال النقاط التالية:

- القضاء على المخلفات الضارة للحادث
- إعادة النظم والبيانات إلى وضعها الطبيعي وتأكيد وضعها الطبيعي
- تحديد وتخفيف جميع نقاط الضعف التي تم استغلالها
- معالجة نقاط الضعف لمنع وقوع حوادث مماثلة
- التواصل بشكل مناسب داخلياً وخارجياً⁽⁶⁾.

(1) U.S. DEPARTMENT OF THE TREASURY G7 fundamental elements of cybersecurity for the financial sector, Ibid.

(2) Samantha A. Adams, Marlou Brokx, Lorenzo Dalla Corte, Maša Galič, Kaspar Kala, Bert-Jaap Koops, Ronald Leenes, Maurice Schellekens, Karine e Silva, Ivan Škorvánek, Op.Cit. P.32.

(3) Michal Tonhauser, Jozef Ristvej, Op.cit.

(4) Louise Marie HUREL, Luisa Cruz LOBATO, A Strategy for Cybersecurity Governance in Brazil, INSTITUTO IGARAPÉa think and dotank, strategic note 30, Rio de Janeiro, Brasil, SEPTEMBER 2018, P.17:<https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf>

(5) U.S. DEPARTMENT OF THE TREASURY, G7 fundamental elements of cybersecurity for the financial sector, Ibid.

(6) U.S. DEPARTMENT OF THE TREASURY, G7 fundamental elements of cybersecurity for the financial sector, Op.cit.

5- المراقبة:

وتختص المراقبة هنا بمتابعة ورصد عملية تنفيذ الإجراءات الأمنية التي دخلت حيز التنفيذ، ومن خلالها يتم حشد وتجميع البيانات من أجل العمل على دعم وتعزيز عمليتي التصميم وتطوير التصميم الجديد وتعزيز عملية التطوير، ويتعين أيضاً مشاركة هذه المعلومات وتبادلها مع تبادل الخبرات من أجل التصدي لتحديات التكنولوجيا⁽¹⁾.

الفرع الثاني: تفعيل دور المجتمع المدني في الوقاية من الإرهاب الإلكتروني:

تعددت الدراسات التي ناقشت موضوع دور المجتمع المدني ومؤسساته في مكافحة الظاهرة الإرهابية بكل أشكالها، ومعظمها قد حصرت هذا الدور في التعليم والتثقيف والتوعية، غير أننا آثارها أن نوسع بعض الشيء في الأدوار التي يلعبها في هذا المجال، مبينين ثقل المجتمع المدني وفعالية دوره على الصعيدين الوطني والدولي (أولاً)، ومظهرين الأساليب والتكتيكات التي يقوم بها في تثبيت دوره داخل منظمة المواجهة التي تستهدف قمع ظاهرة الإرهاب الإلكتروني وتحقيق الأمن السيبراني (ثانياً).

أولاً: لمحة عامة عن المجتمع المدني ودوره في تحقيق الأمن والسلم العالميين:

بادئ ذي بدء، يتعين علينا أن نقدم تعريفاً ولو مقتضباً عن المجتمع المدني، الذي يمكن تعريفه على أنه: (جملة المؤسسات السياسية والاقتصادية والاجتماعية والثقافية، ومختلف التنظيمات التطوعية التي تنشأ بمقتضى الإرادة الحرة لأعضائها قصد حماية مصالحهم والدفاع عنها، ومنها على سبيل المثال: الأحزاب السياسية والتنظيمات الثقافية والاتحادات المهنية وجماعات المصالح والجمعيات الأهلية والمنظمات الحكومية)⁽²⁾، ويمكن تعريفه أيضاً على أنه: (مجموعة من التنظيمات الطوعية الحرة التي تملأ المجال العام بين الأسرة والدولة لتحقيق مصالح أعضائها ملتزمة في ذلك بقيم ومعايير الاحترام والتراضي والتسامح والإدارة السلمية للصراع وقبول التنوع والاختلاف)⁽³⁾.

(1) جان فرنسوا لانسو، دور الجامعات الفرنكوفونية في مواجهة الجرائم السيبرانية، مداخلة في الجلسة الأولى من مؤتمر الأمن السيبراني والدفاع السيبراني: (تحديات وآفاق)، الجامعة اللبنانية والوكالة الجامعية الفرنكوفونية AUF، تحت إشراف جنان الخوري ومحمود رمال، مركز المعلوماتية القانونية في الجامعة اللبنانية، سن الفيل، ص 26: <https://ul.edu.lb/common/news.aspx?newsId=1191>

(2) وداد غزلاني، واقع المجتمع المدني في الجزائر ودوره في تحقيق الرشادة، مجلة القانون، المجتمع والسلطة، المجلد 04، العدد 01، جامعة محمد بن أحمد، وهران 2، فيفري 2015، ص ص: 31-60: <https://www.asjp.cerist.dz/en/article/7167>

(3) محمد عبد الكريم الحوراني، المجتمع المدني ضرورة وظيفة للدولة، مجلة علوم الإنسان والمجتمع، المجلد 02، العدد 08، جامعة محمد خيذر، بسكرة، ديسمبر 2013، ص ص: 43-78: <https://www.asjp.cerist.dz/en/article/48119>

أما على الصعيد العالمي، فإن المجتمع المدني: (هو قطاع من منظمة المجتمع المدني في بلد معين أو إقليم محدد، يتخطى الحدود الجغرافية، ليتضامن أو يتسابق مع منظمات أخرى في مختلف دول العالم، حيث يكون هناك توافق حول قضية معينة مثل محاربة الفقر، أو مجموعة من المبادئ المشتركة كاحترام حقوق الإنسان مثلا، ويهدف إلى التأثير على السياسات العالمية، والتأثير على الرأي العام العالمي...) (1).

يعبر المجتمع المدني عن إسهام كبير ودور حيوي في التصدي لجميع المعضلات والآفات والمآزق التي يتعرض لها المجتمع وهذا بالمناقشة والتعامل معها بما يدرؤها ويعالجها، ويكون دوره كبيرا وحاسما وأكثر نجاحا وإثمارا كلما كان دوره يتسم بالفاعلية والديناميكية، ومن هنا فإن للمجتمع المدني القدرة والاستطاعة والتمكين للعمل على الوقوف أصدا جريمة الإرهاب ولاسيما في دوره التوعوي (2).

فالمجتمع المدني إذا، يلعب دورا مهما وفعالا في مجال السلم والأمن الدوليين التقليديين، إذ أن له دور كبير في تطوير المعايير وتطبيقها، ولا شك أن هذا الدور يلعبه أيضا في إطار الأمن السيبراني، إذ أن له دورا هاما وحيويا في القضايا المتعلقة بالإنترنت (3)، بما في ذلك تأمين الفضاء الإلكتروني من الأخطار الجسيمة التي تتهدده من جرائم الإرهاب الإلكتروني.

وهذا الدور الذي يلعبه المجتمع المدني على المستوى الدولي إنما كان نتاج للضغوطات التي كانت تمارس من قبله لحيازة مكانة وثقل في عمليات صنع القرار فيما يتعلق بالعديد من المسائل والقضايا، وهذا الدور الذي يلعبه المجتمع المدني قد وصفه البعض على أنه أحد أهم الأحداث التي حدثت في العصر الحديث، فالمجتمع المدني يلعب أدورا حيوية على الصعيد الدولي في العديد من الاتجاهات والمسائل والقضايا الدولية التي يعتبر القانون الدولي الإنساني أكثرها انتفاعا به، فضلا عن انتفاع العلاقات الدولية بها من خلال مساهمتها في بناء الثقة سواء أكان ذلك على المستوى الداخلي للدول أو على المستوى الخارجي (4).

وقد شددت العديد من الوثائق الدولية وقرارات هيئة الأمم المتحدة على هذا الدور حين أشارت إلى ضرورة انخراط وانضمام المجتمع المدني إلى عملية التصدي للظاهرة الإرهابية، ومن بين

(1) إكرام بلباي، آليات المجتمع المدني العالمي في رصد وتوثيق وقمع انتهاكات حقوق الإنسان، مجلة حقوق الإنسان والحريات العامة، المجلد 02، العدد 01، جامعة بن باديس، مستغانم، جانفي 2017، ص: 173-202: <https://www.asjp.cerist.dz/en/article/68398>

(2) محمد مسعود قيراط، الإرهاب: (دراسة في البرامج الوطنية واستراتيجيات مكافحته -مقاربة إعلامية-)، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2011، ص 275.

(3) Andrijana GAVRILOVIC, [Webinar summary] What is the role of civil society and communities towards a peaceful cyberspace?, Posted on 11 Dec 2018, Accessed on 30 July 2020, at 19:14h, In: <https://www.diplomacy.edu/blog/webinar-what-role-civil-society-and-communities-towards-peaceful-cyberspace>

(4) Camino KAVANAGH, Daniel STAUFFACHER, A role for civil society, ICTs norms and confidence building measures in the context of international security, ICT4 Peace Foundation, GENEVA, 2014, P.8

نماذج ذلك، نجد أن الجمعية العامة لهيئة الأمم المتحدة قد شجعت وحفزت الدول الأعضاء في مضمون قرارها المتعلق باعتماد استراتيجية مكافحة الإرهاب الصادر بتاريخ 8 سبتمبر 2006، على الاستمرار في تحفيز المنظمات غير الحكومية والمجتمع المدني من أجل الإسهام في تقوية وتوطيد المبادرات التي تهدف إلى تطبيق وإنجاز هذه الاستراتيجيات المتعلقة بمكافحة الإرهاب⁽¹⁾.

وأكدت أيضا في قرارها رقم 272/62 المؤرخ بتاريخ 15 سبتمبر 2008، أن مسؤولية وضع الاستراتيجيات يقع بشكل أصيل على كاهل الدول الأعضاء، ومع ذلك فقد حثت المجتمع المدني والمنظمات غير الحكومية على المساهمة قدر الحاجة في المبادرات التي تهدف إلى تطبيق هذه الاستراتيجية⁽²⁾.

وهذا الدور إنما تؤكدونه وتعززه جمعيات المجتمع المدني نفسها، فقد برهنت في الكثر من الدول سواء في العالم العربي وجمعيات أخرى في الجزائر والمملكة العربية السعودية على قدرتها في نشر الوعي وتعزيز قيم الوسطية والاعتدال والتسامح، وسعيها في تأصيل الوعي المناهض للعنف والطرف والغلو⁽³⁾.

لكن ورغم هذه الأهمية الكبيرة التي تحتلها منظمات المجتمع المدني ورغم ما تحصل عليه من دعم من قبل الأمم المتحدة، ورغم أيضا ما تحتله منظمات المجتمع المدني من مكانة في بناء منظومة الفضاء الإلكتروني إلا أن دورها فيما يتعلق بصياغة سياسات الأمن الإلكتروني ومختلف التدابير والتنسيقات الاستشارية والتشاركية في غاية المحدودية، فضلا عن دورها الهزيل في بناء السياسات والاستراتيجية والمعايير المتعلقة بالأمن الإلكتروني وبناء الثقة⁽⁴⁾.

ويعود هذا الأمر من جهة نظرنا إلى حادثة موضوع الأمن السيبراني والجرائم الإرهابية المرتكبة على هذا الفضاء المستجد، كما يمكن إرجاع ذلك إلى نقص وعي المجتمع المدني بخطورة التهديدات التي تواجه السلم والأمن العالميين جراء الإرهاب الإلكتروني، خاصة إذا علما أن هناك أطراف لا تزال تتناقل في الاعتراف بوجود إرهاب إلكتروني أصلا.

(1) عبد الحفيظ سعيد مقدم، تقرير عن ندوة: دور مؤسسات المجتمع المدني في التصدي للإرهاب، المجلة العربية للدراسات الأمنية والتدريب، المجلد 30، العدد 60، جامعة نايف العربية للعلوم الأمنية، الرياض، أغسطس 2014، ص ص: 319-330.

<https://repository.nauss.edu.sa/handle/123456789/59418>

(2) علي لونيبي، آليات مكافحة الإرهاب الدولي بين فعالية القانون الدولي وواقع الممارسات الدولية الانفرادية، رسالة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 04 جويلية 2012، ص 264.

(3) عبد الحفيظ سعيد مقدم، المرجع نفسه.

(4) Camino KAVANAGH, Daniel STAUFFACHER Op.cit., P.09.

يختلف الدور الذي يلعبه المجتمع المدني وتتباين أيضا نشاطاته عن تلك التي يقوم بها القطاع العام والخاص، والسبب في ذلك راجع إلى الاختلاف القائم في مهام كل منها، والقيم الجوهرية التي تنطلق منها، كما أن هناك فارق كبير في آليات تمويل كل جهة من تلك الجهات، فمنظمات المجتمع المدني هي منظمات تسعى على خدمة الفئات المهمشة، وبما أنها لا تعد منظمات ربحية فإن موردها يقوم على التبرعات المختلفة، ولاسيما المساعدات الأجنبية، وأمام ما يطرأ من تغيرات على الصعيد الدولي، والارتياح من التأثير الأجنبي عليها يتقل كاهلها ويعيق نشاطها، كما أن هناك من الدول المنغلقة من تمنع مثل هذه التبرعات التي يكون مصدرها طرف أجنبي، وتحول دون وصولها إلى منظمات المجتمع المدني المحلية⁽¹⁾.

تجدر الإشارة في هذا الطرح إلى أن الجوهر الكامل وراء سياسة الاعتماد والتركيز على المجتمع المدني يعود إلى المدرك والمستعاب من شأن الأفراد، إذ أن الأكثرية والسواد الأعظم من المواطنين يملكون قدرات خفية ومضمرة وتوق شديد للعمل على تحسين أحوالهم في مجالات متعددة، فالأشخاص يمثلون في حد ذاتهم عنصرا جوهريا في التنمية البشرية في هذا العصر⁽²⁾.

فهذه السياسة المبتكرة تعي جيدا أطر المؤسسات البعيدة في هذا الجو الذي يطغى عليه الترابط الإلكتروني والتحول المتسارعة، وتسعى إلى تحقيق فائدة مما يملكه المعدومين والمعوزين من موارد، وهذا بلا شك يصير آمال هؤلاء المعدومين والمعوزين وطاقتهم إلى قوة تصوب نحو المجال التنموي⁽³⁾، كما تصوب على نفس الوتير لمحاربة أشكال الإرهاب المختلفة، تقليدية كانت أم سيبرانية.

ثانيا: إسهامات المجتمع المدني في مكافحة الإرهاب الإلكتروني وتحقيق الأمن السيبراني:

لقد ذكرنا في ما سبق من بحثنا، أن للظاهرة الإرهابية أيا كان نوعها وشكلها، أسباب تقف وراء ظهورها واستفحالها، وحصرنا بعض هذه الأسباب في ما يحيط بالفرد من ظروف اقتصادية واجتماعية وسياسية وإيديولوجية، ورأينا أن لهذه الظروف دورا محوريا في نشوء بذرة الإرهاب ونموها واستفحالها في المجتمع، ولهذا فإنه من الحيف أن نحصر دور المجتمع المدني في مجرد

(1) Pavan K. JAGALUR, Peter L. LEVIN, Kate BRITTAIN, Matthew DUBINSKY, Kristine Landau JAGALUR, Charlotte LATHROP, Cybersecurity for Civil Society, IEEE International Symposium on Technology in Society (ISTAS) Proceedings Miriam Cunningham and Paul Cunningham (Eds), 2018:

<https://amida.com/wp-content/uploads/2019/07/article3.pdf>

(2) دون إيبيرلي، نهوض المجتمع المدني العالمي: (بناء المجتمعات والدول من أسفل إلى أعلى)، ترجمة: (لميس فؤاد يحيى)، الطبعة العربية

الأولى، الأهلية للنشر والتوزيع، الأردن، 2011، ص 89.

(3) دون إيبيرلي، المرجع السابق، ص 92.

التوعية والتتقيف دون أن نشير إلى ما يمكن له ولمؤسساته القيام به على صعيد تغيير هذه الأوضاع والظروف التي تعتبر الحاضنة الأولى للإرهاب والمغذية له، وانطلاقاً من هذا الإطار النظري يمكن القول بأن للمجتمع المدني الاستطاعة والقدرة الكافية لإحداث تغييرات اقتصادية واجتماعية وسياسة كبرى والحيلولة بما ينتج عن هذه التغييرات من انتشار الظاهرة الإرهابية، وفيما يلي بعضاً من الأدوار الحيوية التي يمكن له من خلالها إحداث تغييرات في بيئة تعشعش الظاهرة الإرهابية.

يعتبر مصطلح المجتمع المدني العالمي وعاء يحوى بين طياته استطاعة كبيرة على المساهمة الإيجابية من كل جهات المجتمع المدني العالمي، كما تكمن فيه أيضاً استطاعة وقدرة على تشكيل مستقبل العالم، كما أن مفهومه أيضاً يتصادم مع فكرة تحكم أو سيطرة قوى كبرى على أحداث أو مجريات الأمور في العالم، ثم أنه يقوم بإضعاف حدة سطوتها وتحكمها فيها، كما يمكن أيضاً أن ننظر إلى هذا المصطلح كونه صورة من مزاولة حقيقية لقيمة العدالة أو المساواة الإنسانية في بيئة تكتنفها صور الضيم والبغي⁽¹⁾.

فلا ريب حينها أن يكون للمجتمع المدني دوراً اقتصادياً ذو أهمية بالغة، كما يمكنه أيضاً أن يمثل آلية محورية في التأسيس للتحوّل الديمقراطي الظاهر، فإطار العلاقة بين المجتمع المدني والتنمية قد بلورته أبحاث ودراسات يزخر بها الأدب السياسي النظري، ويتعين من أجل بلورة هذا الدور وتكريسه أن يكون ضمن صورة متكاملة تتادي لبناء مشروع مجتمعي وتنموي تتضافر فيه قوى المجتمع المدني مع الدور الأصيل للدولة ضمن أسس وقواعد الحكم الرشيد، التي تمثل الرقابة والتوصية والتدبير والمحاسبة جزء منها، وبها تتلاقى الرقابة من أعلى بالرقبة من أسفل مشكلة بذلك سدا منيعاً أمام ما يطلق عليه اسم تنمية الفقر والتخلف⁽²⁾.

فالتحوّل الديمقراطي الظاهر من وجهة نظرنا يمثل القوة الناعمة التي تقوض بنيان الفكر الراديكالي الذي يعتبر الحاضنة الأولى للإرهاب، ويضيق الخناق على أجواء التطرف الشاذة بدلاً من السماح لها بالانتشار والتمدد بين اللبّات الأساسية المكونة للمجتمعات، فضمن الحريات وتحقيق المساواة بين مختلف أطياف الشعب ومكوناته، وفتح المجال للتمثيل والعمل السياسي لكافة عناصر المجتمع،

(1) طلعت مصطفى السروجي، رأس المال الاجتماعي، الطبعة الأولى، مكتبة الإنجلو المصرية، القاهرة، مصر، 2009، ص 85.

(2) صالح زيان، موقع مؤسسات المجتمع المدني في إطار التنمية المحلية في الجزائر، مجلة العلوم الاجتماعية والإنسانية، المجلد 08، العدد

16، جامعة باتنة 1 حاج لخضر، الجزائر، جوان 2007، ص ص: 255-274: <https://www.asjp.cerist.dz/en/article/37798>

سيكون له وقع كبير في إرساء دولة الحق والقانون التي من الصعب جدا أن يعيش فيها التطرف والإرهاب.

ذلك فإن غياب الديمقراطية وشعور الأفراد بالحرمان من حقهم في التعبير عن آرائهم، وما يتعرضون إليه من إهدار لحقوقهم، وانتشار الفساد سيرتب حتما كبتا وتطرفا وعنفا يفضي إلى النشاط المستتر والسري وبالتالي السقوط في بؤرة ووحل التنظيمات الإرهابية التي تتغذى أساسا من إقصاء الشباب عن المشاركة السياسية وتجميد الدور الذي تلعبه منظمات المجتمع المدني في ردم هذه الفجوة، فتفعيل وإتاحة العمل السياسي الديمقراطي للشباب وتكريس حقوق الإنسان والحريات يعتبر من بين أهم الآليات وأكثرها ضرورة لضمان التوطن السياسي والتطور الاقتصادي والاجتماعي ومن ثم خلق النشاطات الإرهابية واجتثاثها⁽¹⁾.

ولذلك فإن تكريس الديمقراطية والابتعاد عن الشمولية في الحكم والديكتاتورية والتسلط في تسيير قضايا الأوطان هي التي ستتيح الجو الملائم للتفاعل مع سياسات مكافحة الإرهاب، وهي الضامن لعدم نشوء خلايا جديدة والقاطعة لدابر التعاطف الشعبي مع تلك الخلايا المتطرفة، وللمجتمع المدني الدور الكبير في ذلك، من خلال تأطير الشباب في عمل سياسي منظم من جهة، وفي نفس الوقت الدفاع عن حقوقهم أمام السلطات الحاكمة من جهة ثانية.

يبرز أيضا دور المجتمع المدني الحاسم في تحقيق الأمن السيبراني، في فرض رقابته على قطاع الأمن الذي من خلاله يكمل العمل الرقابي الذي أنيط بالسلطة التشريعية وأجهزة القضاء، فالمجتمع المدني يمكنه أن يعمل على منح توجيهات سياسية كما يمكنه أيضا أن يساهم بالخبرة التقنية كجزء من دوره العام في الدفاع عن مصالح الأفراد، ويمكن أن يكون طرفا مساهما في تسيير عملية الحوار في هذا الباب⁽²⁾.

فالمجتمع المدني من خلال ما سقناه من تعاريف يعتبر شديد الاتساع في نطاق عمله وفي عدد أفراداه وفي تنوع أغراضه ومشاربه، هو أكثر بكثير من نطاق القطاعين العام والخاص، ومن هنا يمكن القول أن مساهمته من ناحية الخبرة التقنية ودوره في الحوارات المتعلقة بحوكمة الأمن السيبراني يعد أمر بالغ الضرورة، وعظيم الأهمية، وعلى الدول أن تشجع هذا الدور، وأن تفتح له منافذه، وتأطره تأطيرا قانونيا يضمن له الفعالية والتأثير.

(1) عبد الرحمن خلف العنزي، دور مؤسسات المجتمع المدني في مكافحة التطرف والإرهاب، متوفر على الموقع المندوبية السامية للتخطيط،

المملكة المغربية، مختصر رابط موقع نشر الوثيقة: <https://cutt.us/f4ZAw>

(2) Guide pour la bonne gouvernance de la cybersécurité, Le Centre pour la gouvernance du secteur de la sécurité, Genève, 2019, P.20

ترى الباحثة أيضا أن للمجتمع المدني دورا مهما في الحماية من كل أشكال الإرهاب بما فيها الإرهاب الإلكتروني عبر الحشد والتعبئة ضد الحركات الاستعمارية والتدخلات الأجنبية التي كما اشرنا إليها سابقا تعتبر من بين الأسباب الرئيسة التي تقف وراء الظاهرة الإرهابية، وقطع السبب هو قطع لما يترتب عنه من حاصل وناتج.

وقد عبر المجتمع المدني فعلا عن رفضه للحركات الاستعمارية الحديثة من خلال الحركة الإنسانية الكبيرة التي شهدتها الأشهر الأولى من عام 2003، والتي شبعتها جريدة نيويورك تايمز بأنها القوة العالمية الثانية المعادية لأمريكا وأن التاريخ لم يعش نشاطا معارضا ومحتجا بهذا الشكل، إذ انطلقت سلسلة من المظاهرات الجماهيرية الضخمة التي حوت ما يقارب احدى عشر مليون شخص في أكثر من ثمانمائة مدينة على الصعيد العالمي، بتعدد جنسياتهم وأعمارهم وأجيالهم، الذين أجمعوا على رفضهم للحرب المعلنة على العراق⁽¹⁾.

كما ذكر أيضا اليمين زرواطي حادثة يمكن أن نستوحي منها الدور الذي يمكن أن يلعبه المجتمع المدني في رفض التدخلات الأجنبية والوقوف أصدا بواورها الأولى، فقد وجه الوزير الداخلية الجزائري السابق نور الدين يزيد زرهوني تعليمات للمنظمات الجماهيرية وفعاليات المجتمع المدني والنقابات، بمقاطعة اللقاءات والندوات التي تنظمها السفارة الأمريكية بالجزائر على اثر عزم الولايات المتحدة إنشاء فرع آف بي أي في بمقر سفارتها بالجزائر⁽²⁾.

تلعب أيضا منظمات المجتمع المدني ولاسيما الأسرة والمؤسسات التربوية دورا حاسما في مواجهة الظاهرة الإرهابية من خلال جهودها في توعية الجيل الصاعد وتربيتهم على القيم الأصيلة ومكافحة الانحرافات، وما تقوم به أيضا المؤسسات الأهلية لتحقيق ذلك في ميدان نشر الوعي الأمني باعتماد أسلوب تنظيم المحاضرات والندوات العلمية، مع ما تقوم به المؤسسات الدينية والإعلامية من توعية بمخاطر هذه الظاهرة والعمل على مجابقتها⁽³⁾.

فيمكن لمؤسسات المجتمع المدني أن تلعب دورا كبيرا في تطوير الحس الأمني للأفراد، ولها أيضا إمكانية القيام بإعداد بحوث ودراسات عن العوامل التي تقف وراء هذه الجرائم ذات الطابع الدولي التي تتطلب حولا علمية قائمة على أبحاث علمية، بالإضافة إلى أنه يمكن أن يلعب دورا

(1) طلعت مصطفى السروجي، المرجع السابق، ص 84.

(2) اليمين زرواطي، التجربة الجزائرية في مكافحة الإرهاب: (1978-2008)، مطبوعات إي-كتب، لندن، 2014، ص 121 (ترقيم إلكتروني).

(3) عمر بن خزام بن ناصر بن عمر بن قمرلة، دور مؤسسات المجتمع المدني في الوقاية من الإرهاب، رسالة ماجستير في العدالة الجنائية، السياسة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 10 جوان 2007، ص ص: 157-158.

مهما في مكافحتها حتى ولو بعد وقوعها من خلال العمل على مساندة ضحاياها بشتى الطرق الممكنة⁽¹⁾.

يمكن للمجتمع المدني أيضا أن يلعب دورا كبيرا في السياسة التشريعية المتعلقة بالفضاء الإلكتروني أمام هذا الإحجام الدولي عن توضيح وبيان أساليب تطبيق القانون الدولي على الفضاء السيبراني، حيث ذهبت بعض الجهات غير الحكومية ولاسيما منظمات المجتمع المدني وشركات تكنولوجيا المعلومات والاتصال إلى العمل من أجل سد هذا الفراغ التشريعي من خلال مقترحات المعايير المتعلقة باحترام حقوق الإنسان على الفضاء السيبراني ومن ثم بلوغ بيئة إلكترونية آمنة وموثوقة⁽²⁾.

ومن أمثلة ذلك دعم الكثير من المنظمات غير الحكومية لمبادئ كامدان المتعلقة بحرية التعبير والمساواة على الساحة السيبرانية، كما اعتمدت أيضا صكوك قانونية غير ملزمة كما هو واضح من خلال مبادئ مانيلا المتعلقة بمسؤولية الوسطاء⁽³⁾.

أما فيما يتعلق بالوقاية من التطرف والريديكالية وتجنييد الإرهابيين، فإن مشاركة المجتمع المدني وبشكل خاص المنظمات الشبابية، ستكون ذات دور حاسم، ومثالها تلك الدعوة التي أطلقتها الشبكة الأوروبية للتوعية ضد التطرف (شبكة التوعية بالتطرف التابعة للاتحاد الأوروبي) (RSR) ومركز الامتياز ليلعب المجتمع المدني دورا مهما في هذا الموضوع⁽⁴⁾.

وقد دعا المشرع الجزائري أيضا في الأشهر القليلة الماضية لهذا الغرض؛ إشراك المجتمع المدني والقطاع الخاص من خلال نص المادة 07 من قانون الوقاية من التمييز وخطاب الكراهية ومكافحتها والتي تنص على أنه: (يتم إشراك المجتمع المدني والقطاع الخاص في إعداد وتنفيذ الاستراتيجية الوطنية للوقاية من التمييز وخطاب الكراهية)⁽⁵⁾.

يمكن لمنظمات المجتمع المدني أن تلعب دورا في مكافحة إرهاب الدولة، فمنظمات المجتمع المدني كثيرا ما تستعين في ذلك بالفضاء الإلكتروني لجمع المعلومات أو لنشر الوعي أو لانتقاد القمع والتطرف الذي تمارسه الدولة، غير أن هذه الآليات في الحقيقة يمكن أن يكون نفسها هي

(1) سميرة ناصري ويسمة ترغيني، دور المجتمع المدني في مكافحة الجريمة المنظمة، مجلة الحقوق والعلوم السياسية، المجلد 01، العدد 02،

جامعة عباس لغرور، خنشلة، أكتوبر 2014، ص ص: 159-171: <https://www.asjp.cerist.dz/en/article/10151>

(2) Guide pour la bonne gouvernance de la cybersécurité, Op.cit. P.57

(3) Ibid. P.59

(4) Joaquin PUEYO, Marie-Louise FORT, rapport d'information déposé par la commission des affaires européennes sur la nouvelle politique européenne de voisinage, assemblée nationale, No3364, 16 décembre 2015, France, PP. 21-22.

(5) المادة 07 من القانون رقم 05-20 المؤرخ بتاريخ 28 أبريل 2020 يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج.ر عدد 25 لسنة 2020.

الآلية التي تقمع بها الدولة معارضيها، أو تراقب بها حركة المعلومات أو العمل على التستر عليها وحجبها، ووضع ترتيبات لتصغير حجم ونضج الدور الذي يمكن أن تلعبه منظمات المجتمع المدني⁽¹⁾، فالفضاء الإلكتروني بذلك يكون سلاحا في يد الطرفين، الطرف الذي يرهب والطرف الذي يقاوم الإرهاب.

وفي الأخير، ننوه إلى أن مساهمة المجتمع المدني في مكافحة التطرف والإرهاب وفعالية الدور المنوط به مرهون بمتغيرات كثيرة، ومن أهم هذه المتغيرات وأكثرها بروزا مسألة الطاقات البشرية والمالية لها، بالإضافة إلى نطاقها القانوني الذي تمارسه به دورها، والتصور الأمني الذي تتصرف به الدولة حيال هذا الدور، بالإضافة إلى جوهر القادة والصفوة في منظمات المجتمع المدني، كما أن الاعتماد على هذا الدور الذي تلعبه مرهون أيضا بطاقات هذه المنظمات في الانسجام مع الأفراد وتبني السياسة الجماهيرية بدلا من الاقتصار على الصفوة والنخبة، وذلك من خلال اعتماد رسالة سياسية سلسلة ووسائل وأنساق مختلفة⁽²⁾.

ولعل هذا العنصر الأخير هو الذي يضع فجوة عميقة بين الدول الديمقراطية وسعيها الحثيث نحو تأمين الفضاء الإلكتروني من خلال استغلال دور المجتمع المدني، وبين الدول المتتطعة والدكتاتورية التي لا تزال تعاني من مختلف الولايات داخليا وخارجيا، فالدول الديمقراطية تركز هذا الدور الكبير للمجتمع المدني ومنظّماته، وتعزز من آليات إشراكه في اتخاذ القرار عموما، والقرار في شأن الأمن السيبراني خصوصا، وعلى النقيض فإن دور المجتمع المدني في الدول الشمولية والأنظمة اليعقوبية المركزية والسلطات الاستبدادية منكش جدا، ولاسيما في عمليات اتخاذ القرار، وهذا ما يجعل دورها في تأمين الفضاء الإلكتروني ومواجهة ظاهرة الإرهاب فيه منحصر وهزيل.

الفرع الثالث: التعاون بين القطاع العام والخاص:

يتعين من أجل صياغة استراتيجية متكاملة لمكافحة الإرهاب السيبراني وتأمين الفضاء الإلكتروني إشراك القطاع الخاص فيها، لما له من مكانة مهمة في إدارة وتسيير الفضاء الإلكتروني، ولتحقيق هذا النوع من الشراكة يجب أولا أن تتحدد الأطر العامة التي تؤثر في عملية فيها وضبط الخطوات الهامة في إنشاء مثل هكذا علاقة (أولا)، ثم بعد ذلك يجب أيضا تحديد المحاور الأساسية التي تشكل محل هذه الشراكة (ثانيا).

(1) Pavan K. JAGALUR, Peter L. LEVIN, Kate BRITTAİN, Matthew DUBINSKY, Kristine Landau JAGALUR, Charlotte LATHROP, Op.cit.

(2) عبد الرحمن خلف العنزي، المرجع السابق.

أولاً: إطار بناء الشراكة بين القطاع العام والخاص في الأمن السيبراني:

يكتسي القطاع الخاص أهمية كبرى في دعم حوكمة الأمن السيبراني وضمان بيئة آمنة على الفضاء الإلكتروني، فالولايات المتحدة الأمريكية تتجه إلى القطاع الخاص الجهة الأكثر ملاءمة في توجيه هذا الفضاء⁽¹⁾، وقد أشار بيان الرياض للأمن السيبراني أيضاً إلى هذه الأهمية من خلال تسليط الضوء على دوره في تطوير صناعة الأمن السيبراني على الصعيد الدولي، وأهمية الاستثمارات التي تنشأ في هذا المجال⁽²⁾، والتعاون بين القطاع العام والخاص في هذا المجال لا يأتي إلا من خلال خطوات جادة وممنهجة يمكن أن نأطرها على النحو الآتي:

أ- ضروريات بناء الشراكة بين القطاع العام والخاص:

إن بناء الشراكة بين القطاع العام والقطاع الخاص في مجال الأمن السيبراني تتطلب خطوتين أساسيتين وضرورتين في الوقت نفسه وهما:

1- بناء الثقة وتعزيزها:

يشكل المستوى العالي من الثقة بين جميع الأطراف الخطوة الأولى والأساسية والعامل الأول لإنجاح الشراكة بين القطاع العام والخاص، والحديث عن الثقة لا يكفي فيه مجرد الخطاب المعزز لها، بل لا بد أن تكون هناك مؤشرات حقيقية وفعالية تعمل على بناء الثقة في نموذج إجريائي، فالمعلومات على سبيل المثال - ولأهميتها في الأمن السيبراني - لا يمكن أن تتدفق طواعية إلا بوجود عامل الثقة ما لم يكن هناك قانون أو عقد يلزم الأطراف بذلك، والثقة يمكن استكمال بنائها من خلال الكيانات الخاصة والعامة من خلال جهود صغيرة تؤدي في البداية لتصل بعد ذلك إلى تحقيق هدف مشترك ناجح وبناء علاقة موثوقة في نهاية المطاف⁽³⁾.

فطبيعة العديد من المخاطر تتطلب تعاوناً وتنسيقاً وتقاهما وثقة متبادلة بين أصحاب المصلحة الذين بالإضافة إلى كون مصالحهم متباينة، يملكون تصورات متباينة للمخاطر التي تنطوي عليها هذه الجهات⁽⁴⁾.

والثقة ورغم أهميتها الحاسمة في مجال التعامل مع المعلومات والبيانات إلا أنها في الوقت ذاته تتسم بالهشاشة والقابلية للتحطيم، فإذا حدث وأن تحطمت الثقة وفقدت فإن ذلك من شأنه أن

(1) اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، حوكمة الإنترنت: (تحديات وفرص للبلدان الأعضاء في الإسكوا)، الأمم المتحدة، نيويورك، 2009، ص 21.

(2) بيان الرياض للأمن السيبراني، المنتدى الدولي للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، الرياض، 05 فبراير 2020، ص 02.

(3) Max MANLEY, Cyberspace's Dynamic Duo: (Forging a Cybersecurity Public-Private Partnership), Journal of Strategic Security, Vol. 8, No. 3, University of South Florida Board of Trustees, Supplement: Eleventh Annual IAFIE Conference (Fall 2015), pp. 85-98: <https://www.jstor.org/stable/10.2307/26465248>

(4) Samantha A. Adams, Marlou Brokx, Lorenzo Dalla Corte, Maša Galič, Kaspar Kala, Bert-Jaap Koops, Ronald Leenes, Maurice Schellekens, Karine e Silva, Ivan Škorvánek Op.Cit. P.30

يرتب طامات جسام على جميع الأطراف المعنية⁽¹⁾.

2- إنشاء توجه قانوني واضح:

تتبنى هذه الخطوة على بناء توجه قانوني أساسي واضح لتعزيز علاقة الثقة بين الأطراف المعنية، والتي من الممكن أن تتخذ شكلين أو صورتين أساسيتين أحدهما تتمثل في الاتفاقيات التعاونية غير الملزمة، وثانيهما القيام بإبرام اتفاقيات تعاقدية ملزمة، والشراكة الأكثر ملائمة بطبيعة الحال لهذا العمل الجماعي والتواصلي هو الشكل التعاوني، غير أنه يبقى غير ملزم، ولذلك فإن الحديث عن الشكل الأنسب للتعاون أو الشراكة بين القطاعين العام والخاص سيكون ذاك الشكل الذي يتخذ صورة التشريع، وبذلك يكون ملزم وليس تعاونيا بسيطا⁽²⁾.

يمكن العمل على تكوين منظومة قانونية وتشريعية متعلقة بالثقة، غير أن فاعليتها تبقى مستحيلة على رأي بعض الباحثين، فرغم أن مثل هذه التشريعات من الممكن لها أن تلعب دورا في إجبار القطاع الخاص على التبليغ عن الحوادث السيبرانية، وتقديم مختلف المعلومات، إلا أن دورها يتوقف هنا، فلا يمكن لهذه التشريعات أن تضاعف من الثقة بين أصحاب المصلحة ولا يمكنها أن تزيد من التعاون فضلا عن عدم قدرتها في التقليل من تلك الحوادث والتهديدات، لذلك فإن مسألة الوقاية من سائر التهديدات السيبرانية يتطلب بناء وتكوين علاقة تعاون فعلية لتبادل المعلومات بين أصحاب المصلحة⁽³⁾، أو في مجال وضع الخطط المستقبلية أو الاستجابة للطوارئ، وفي كل الأحوال تعتبر الثقة فوق كل قيمة تقديرية في تعزيز النتائج الفعالة بالنسبة لذوى المصلحة⁽⁴⁾، وقد قيل: (الثقة المرتفعة لا تنقذ الاستراتيجية الضعيفة بالضرورة، أما الثقة المنخفضة فدائما تفسد الاستراتيجية الجيدة)⁽⁵⁾.

ثانيا: اتجاهات التعاون بين القطاع العام والخاص:

إن المحاور الأساسية التي ينظر من خلالها إلى هذا التعاون بين القطاعين العام والخاص من خلال ما طرحته مجموعة من دول مجموعة العشرين والتي شملت أمريكا وبريطانيا ودول الاتحاد الأوروبي، وكندا وأستراليا وجنوب إفريقيا والمملكة العربية السعودية وتركيا فيما يلي؛

(1) Cristin GOODWIN, J. Paul NICHOLAS, A framework for cybersecurity information sharing and risk reduction, Microsoft Corporation, 2015, P.3: <https://www.microsoft.com/en-us/download/details.aspx?id=45516>

(2) Max MANLEY, Op.cit.

(3) Cristin GOODWIN, J. Paul NICHOLAS, Op.cit., P.3.

(4) Nathan E. BUSCH, Austen D. GIVENS, Public-Private Partnerships in Homeland Security Opportunities and Challenges, Faculty and Researcher Publications, Homeland Security Affairs (Journal), v.8, article 18, Naval Postgraduate School, October 2012, PP.1-24: <https://calhoun.nps.edu/handle/10945/25017>

(5) ستيفن إم. آر. كوفي، ريبكا آلا. ميريل، سرعة الثقة: (الشيء الذي يغير كل شيء)، ترجمة (نشوى ماهر كرم الله)، الطبعة العربية الأولى،

مكتبة العبيكان، المملكة العربية السعودية، 2014، ص 43.

1- بنية الشراكة:

وتتضمن إنشاء هيئة مشتركة للأمن السيبراني، من أجل أن تحوى هذا التعاضد بين القطاعين العام والخاص، كما تحوى أيضا مركزا للتنسيق المشترك للطوارئ الحاسوبية، وبناء فرق عمل جماعية وموحدة، وبناء مركز للتوعية والتعليم والتدريب، وهذا من شأنه أن يكون طبقة من الخبراء والمستخدمين الملائمين لهذا الفضاء، ضم إلى ذلك تركيب فرق بحثية متخصصة تعنى بكل المشاكل السيبرانية، كما تضم أيضا صياغة لقواعد قانونية وأخرى للممارسة الآمنة في الفضاء الإلكتروني⁽¹⁾.

ويلاحظ في هذا المجال، أن لدى الاتحاد الأوروبي مركزان مهمان يمكنهما المشاركة في الجوانب الإدارية أو التشغيلية للأمن السيبراني والمتمثلتان في؛ الوكالة الأوروبية لأمن معلومات الشبكة (ENISA) والتي تعمل على بناء وإنشاء شراكات لتحسين الموثوقية التقنية ومرونة الفضاء الإلكتروني أو البنية التحتية للمعلومات الحيوية الموجودة في أيدي القطاع الخاص، ومركز (EC3) للجرائم الإلكترونية في يوروبول، والتي تبحث في موضوع شراكات الأمن السيبراني للتعامل مع التهديدات السيبرانية المعقدة، كما تحاول أيضا مع اليوروبول توسيع نطاق الآليات الطوعية مع القطاع الخاص للتحكم في محتوى الإنترنت⁽²⁾.

2- نشاطات الشراكة بين القطاع العام والقطاع الخاص:

والذي يضم هدفين اثنين؛ أحدهما متعلق بالتهيئة من أجل تأمين حمى هذا الفضاء وما يرتبط به من إمكانيات وقدرات، والثاني مرتبط بالقيام بتفعيل هذا التأمين وأن يكون قادرا على تلبية المتطلبات العامة والطارئة⁽³⁾.

يتعين أن يكون هناك تعاون كبير بين القطاع العام والقطاع الخاص من أجل العمل على تعزيز الأمن السيبراني من خلال مشاركة المعلومات والمساهمة الفعالة في تحمل الأعباء المادية مشاركة بين القطاعين، والتعاضد عمليا في تأمين هذا الفضاء، والعمل أيضا على تكوين وترتيب الحلول في مجال التقنية، ورفع وتكثيف الاستثمارات، وبما أن عملية تزويد خدمات الاتصال

(1) سعيد علي الحاج بكري، الأمن السيبراني ..و الشراكة بين القطاعين العام والخاص، جريدة العرب الاقتصادية الدولية، 11 أكتوبر 2018، تم الاطلاع عليه بتاريخ 02 أوت 2020 على الساعة 16:26 في الموقع: https://www.aleqt.com/2018/10/11/article_1468696.html

(2) Pradipta Nindyan SAPUTRA, Arfin SUDIRMAN, Obsatar SINGA, Wahyu WARDHANA, Nurul HAYANA, Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP), Central European Journal of International & Security Studies, Vol. 13, N° 4, CEJISS, Metropolitan University Prague, (2019), PP.104-120

<https://search.proquest.com/openview/0bf39f077ccf7cb9128df299fba78a1e/1?pq-origsite=gscholar&cbl=2069611>

(3) سعيد علي الحاج بكري، المرجع نفسه.

والخدمات الشبكية في داخله في مجال القطاع الخاص فإن لهذا القطاع الدور الكبير في تأمين الفضاء السيبراني تقنيا من كل المخاطر التي تهدده، بالإضافة إلى تعاونها مع الحكومة في تزويدها بالبيانات اللازمة في عملية التحقيق والإسهام أيضا مع الحكومة في التثقيف والإرشاد بالإضافة إلى التزامها بالإرشادات الوطنية المتعلقة بآليات التعامل مع بيانات المستفيدين، والعمل على ضمان أمن هذا الفضاء وفقا للمعايير المطلوبة⁽¹⁾.

يجب في إطار هذا التعاون بين القطاعين أن تعمل الشركات المزودة بخدمات الاتصال والإنترنت للعمل على حجب المواقع التي تشتمل على نشاطات غير قانونية، أو الحيلولة دون وصول البيانات التي تأتي من عناوين إلكترونية مريبة، كما يمكن أن تساهم أيضا في حظر المحتويات غير القانونية وتقديم يد العون للمتعاملين معها في تشخيص أجهزة الحواسيب المهددة أو تلك التي تعرضت للتلوث وإبلاغهم بذلك، والعلم على تأمين الاتصالات وتثقيف البيانات، كما يمكن لمقدمي خدمة "استضافة الويب" التي تستضيف المواقع أن يمارسوا نوعا من الرقابة عليها، وحظر أي استخدام غير قانوني⁽²⁾.

وفي إطار مكافحة الإرهاب الإلكتروني فإن للقطاع الخاص دورا مهما في تمويل الجهود الرامية إلى مكافحته، أيا كان الوسيلة والطريقة التي تتخذها لذلك، فالثابت من هذا التحالف الدولي القائم على مجابهة الظاهرة الإرهابية أن القسط الكبير من مصادر تمويل جهوده حازته من موارد غير حكومية بما في ذلك القطاع الخاص، كما يمكن أيضا للأجهزة التشريعية العمل على حث القطاع الخاص على اعتماد سياسة تهدف إلى ضمان مصالح المجتمع ومكافأتها على ذلك بتقديم حوافر ومزايا، ولا شك أن تمويل جهود مكافحة الإرهاب الإلكتروني من بين أهم المصالح المتعلقة بمصالح المجتمع⁽³⁾.

3- أولوية الحماية:

تجمع تلك الدول على أن الأولوية في هذا العمل يجب أن يكون خاصا بالبنية الوطنية الحرجة والتي تضم العديد من البنى الأساسية والتي تشمل الأصول الحيوية لتمكين المجتمع والاقتصاد من أداء ما أسند إليه من وظائف، ومن الملائم ههنا أن نشير إلى أن الاتحاد الأوروبي قد أقام أولوية

(1) الأمن في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: (توصيات سياسية)، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، الأمم المتحدة، نيويورك، 2015، ص(IX).

(2) المرجع نفسه، ص 23.

(3) عيسى تركي خلف، تمويل جهود مكافحة الإرهاب الإلكتروني، مجلة الجامعة العراقية، المجلد 34، العدد 03، مركز البحوث والدراسات

الإسلامية الجامعة العراقية، 2015، ص ص: 471-498: <https://www.iasj.net/iasj/article/128576>

للتعاون بين دوله في مسألة أمن البنية الوطنية الأساسية، إذ أنه قام بالدعوة إلى تأسيس مركز متخصص في ذلك، والمتمثل في المركز الأوروبي للشراكة الفاعلة بين القطاعين العام والخاص⁽¹⁾. وقد أشار مطلع توجيه مجلس الاتحاد الأوروبي في اعتباراته المتعلق بتحديد وتعيين البنى التحتية الأوروبية الحيوية وتقييم الحاجة إلى تحسين حمايتها إلى ضرورة إشراك القطاع الخاص في تأمين البنى التحتية إذ ينص على أنه: (نظرًا لأن القطاعات المختلفة لديها تجربة وخبرة ومتطلبات خاصة في حماية البنية التحتية الحيوية، يجب تطوير وتنفيذ نهج مجتمعي في هذا المجال، مع الأخذ في الاعتبار الخصوصيات والتدابير القطاعية القائمة، ولا سيما تلك المعمول بها على المستوى المجتمعي أو الوطني أو الإقليمي، ختصة حينما توجد بالفعل اتفاقيات مساعدة متبادلة عبر الحدود بين مالكي / مشغلي البنية التحتية الحيوية، نظرًا للدور المهم للغاية الذي يلعبه القطاع الخاص في المراقبة وإدارة المخاطر وتخطيط استمرارية الأعمال والتعافي من الكوارث، يجب أن يشجع نهج المجتمع على المشاركة الكاملة من هذا القطاع)⁽²⁾.

أما في الولايات المتحدة الأمريكية فقد أنشئت سنة 1996 لجنة رئاسية لحماية البنية التحتية الحيوية، وأنيطت بها عمليات دراسة البنية التحتية الحيوية التي تمثل عصب الحياة في البلد، كما أنيط بها أيضا تحديد أبعاد ضعفها ووضع استراتيجيات مقترحة لحمايتها، وقد أكدت هذه اللجنة على أن حماية البنية التحتية الحيوية هي مسؤولية واقعة على القاطعين العام والخاص على حد سواء⁽³⁾، خاصة إذا علمنا أن 85-90 بالمئة من البنية التحتية الحرجة في الولايات المتحدة الأمريكية هي تابعة للملكية الخاصة للقطاع الخاص⁽⁴⁾.

(1) سعيد علي الحاج بكري، الأمن السيبراني ..و الشراكة بين القطاعين العام والخاص، جريدة العرب الاقتصادية الدولية، 11 أكتوبر 2018، تم الاطلاع عليه بتاريخ 02 أوت 2020 على الساعة 16:26 في الموقع: https://www.aleqt.com/2018/10/11/article_1468696.html

(2) (08), Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (Texte présentant de l'intérêt pour l'EEE), 23 décembre 2008:

<https://op.europa.eu/fr/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/>

" Dans la mesure où différents secteurs possèdent une expérience, une expertise et des exigences particulières en matière de protection des infrastructures critiques, il convient d'élaborer et de mettre en œuvre une approche communautaire dans ce domaine, en tenant compte des spécificités et des mesures sectorielles existantes, notamment celles en vigueur au niveau communautaire, national ou régional, y compris où il existe déjà des accords transfrontaliers d'assistance mutuelle entre propriétaires/opérateurs d'infrastructures critiques. Compte tenu du rôle très important joué par le secteur privé dans la surveillance et la gestion des risques, la planification de la continuité de l'exploitation et la reprise d'activité après une catastrophe, l'approche communautaire doit encourager une participation pleine et entière de ce secteur"

(3) Jean-François DAGUZAN, La protection des infrastructures critiques: (l'enjeu stratégique du XXIe siècle), AFRI, Volume XI, Centre Thucydide, Université Panthéon-Assas, paris, 2010, PP.1001-1015: <https://www.afri-ct.org/afri/tous-les-volumes/>

(4) Mubarak BANISAKHER, Marwan OMAR, Wade CLARE, Critical Infrastructure - Perspectives on the Role of Government in Cybersecurity, Journal of Computer Sciences and Applications, Vol.7, No.1, Science and Education Publishing, US, 2019, PP.37-42; <http://pubs.sciepub.com/jcsa/7/1/6/>

تفرض علينا أهمية الأولوية الممنوحة لحماية البنية التحتية الحيوية والدرجة في إطار الأمن عموماً والسيبراني منه خصوصاً أن نستقصي عن المراد بالبنية التحتية الدرجة، ومن أجل ذلك نورد بعض التعاريف التي تم تقديمها لرفع اللبس عن مفهومها وبيان مضمونها.

تعرف دول مجلس الاتحاد الأوروبي هذه البنى على أنها: (الأصول أو عناصر الأصول الضرورية للحفاظ على الوظائف المجتمعية الحيوية، بما في ذلك سلسلة التوريد والصحة والسلامة والرفاه الاقتصادي أو الاجتماعي للمواطنين؛)⁽¹⁾.

وتعرف البنى التحتية الدرجة الأوروبية على أنها: (البنى التحتية الحيوية التي سيؤثر إغلاقها أو تدميرها بشكل كبير على العديد من الدول الأعضاء أو دولة واحدة فقط، إذا كانت دولة عضو غير تلك التي توجد فيها البنية التحتية الحيوية. وهذا يشمل الآثار الناشئة عن التبعية عبر القطاعات على أنواع أخرى من البنية التحتية؛)⁽²⁾.

أما على مستوى الولايات المتحدة الأمريكية فيعرفها الأمر التنفيذي الذي أصدره مؤخراً الرئيس الأمريكي دونالد ترامب بشأن تعزيز المرونة الوطنية من خلال الاستخدام المسؤول لخدمات تحديد المواقع والملاحة والتوقيت، المنشور على موقع البيت الأبيض الأمريكي على أنها: (الأنظمة والأصول، سواء كانت مادية أو افتراضية، وهي حيوية جداً للولايات المتحدة بحيث يكون لعجز أو تدمير هذه الأنظمة والأصول تأثير مدمر على الأمن القومي أو الأمن الاقتصادي القومي أو الصحة العامة الوطنية أو السلامة، أو على أي مجموعة من تلك الأمور)⁽³⁾.

وعلى الصعيد الإفريقي نصت المادة 4/25 من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي على وجوب التزام الدول الأطراف فيها (باعتقاد إجراءات تشريعية و/أو تنظيمية تراها ضرورية لتحديد القطاعات الحساسة لأمنها الوطني

(1) Article 02/A, Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, Op.Cit.

"«infrastructures critiques»: les actifs ou éléments d'actif qui sont indispensables au maintien des fonctions sociétales critiques, notamment la chaîne d'approvisionnement, la santé, la sécurité et le bien-être économique ou social des citoyens;"

(2) Article 02/B, Ibid.: " «infrastructures critiques européennes»: les infrastructures critiques dont l'arrêt ou la destruction affecterait sensiblement plusieurs États membres ou un seul, s'il s'agit d'un État membre autre que celui dans lequel l'infrastructure critique est située. Cela inclut les effets découlant de liens de dépendance intersectoriels sur d'autres types d'infrastructures;"

(3) Sec. 2/ C, Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services, issued on: February 12, 2020:

<https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/>

"«Critical infrastructure» means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or on any combination of those matters."

وازدهار اقتصادها بالإضافة إلى أنظمة تكنولوجيا المعلومات والاتصالات المصممة للعمل في هذه القطاعات الحساسة باعتبارها تشكل بنية تحتية حيوية للمعلومات، مع القيام في هذا الخصوص باقتراح فرض عقوبات أكثر صرامة على الأعمال الإجرامية ضد أنظمة تكنولوجيا المعلومات والاتصالات في هذه القطاعات، واتخاذ إجراءات وتدابير لتحسين اليقظة والتأمين والإدارة⁽¹⁾.

ومن الواضح أن هذه التعريفات ليست متسقة في تحديد البنية التحتية الحرجة، وذلك عائد إلى اختلاف مصالح الجهات التي أصدرت هذه التعريفات، كما وأنها تجاهلت في الوقت نفسه البنية التحتية الإلكترونية الحرجة ما عدا المرسوم الذي أصدره الرئيس الأمريكي دونالد ترامب، أما تعريف الاتحاد الأفريقي فقد ترك أمر تحديد هذه البنى للتشريع والتنظيم الداخلي للدول.

ومع ذلك فإن التعريفات كلها توضح طبيعة الحرج في هذه البنى التحتية، وهي تعلقها بقطاعات حساسة يؤثر توقفها أو المساس بها بعناصر دستورية غاية في الحيوية، ومن أهمها الأمن، الاقتصاد، الصحة، وما إلى ذلك من القطاعات التي تؤثر سلامتها على وظائف ذات أبعاد مجتمعية أو سيادية.

المطلب الثاني:

الطب الشرعي الرقمي

تعاني المنظمة القضائية والأجهزة الأمنية وجميع منظومات إنفاذ القانون من صعوبات وتعقيدات كبيرة من أجل الوصول إلى الكشف عن جريمة الإرهاب الإلكتروني أو الاستدلال عليها بأدلة جنائية يمكن للقضاء أن يعول عليها في إسناد الأفعال الإرهابية السيبرانية إلى مرتكبيها نظرا لافتراضية هذا الفضاء الذي تقع فيه، وطبيعة الأدلة التي يمكن الحصول عليها منه، ولذلك فإنه من الضروري إنشاء هيكلية أو نظام خاص يعنى بهذه المسائل المعقدة مسابقة لما هو متعارف عليه في مجال البحث والتحقيق الجنائي، فكان بذلك أن ظهر مفهوم الطب الشرعي الرقمي (الفرع الأول)، الذي يعمل على جمع وتحليل وتقديم الأدلة التي يتم استخلاصها من الفضاء الإلكتروني لتعمل على تكوين قناعة القضاء في جرائم الإرهاب الإلكتروني (الفرع الثاني)، غير أن هذا النوع من الطب الشرعي تعترض طريق عمله تحديات تقنية وفنية وقانونية متعددة تقلل من كفاءته وحجية تقاريره (الفرع الثالث).

(1) المادة 4/25 من اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

الفرع الأول: الإطار المفاهيمي للطب الشرعي الرقمي:

يعد الطب الشرعي الرقمي من بين الأساليب الأكثر حداثة وتطوراً في حماية الفضاء الإلكتروني من التهديدات والأخطار المختلفة وعلى رأس قائمتها خطر جريمة الإرهاب الإلكتروني، إن أهمية هذا العلم الجنائي تقتضي الإحاطة بمفهومه ومضامينه، ووضعه في إطار تعريف واضح وجلي (أولاً)، كما يتعين أيضاً إدراك ما له من مكانة علمية وعملية، وتحديد الأشكال والصور التي يتجلى فيها (ثاني).

أولاً: تعريف الطب الشرعي الرقمي:

يمتلك الطب الشرعي كوظيفة أو مهنة مفهوماً ذو جوهر تخصصي، ذلك أنه يقوم بدور غاية في الأهمية في تحقيق العدالة، وبشكل خاص فيما يرتبط برفع اللبس من الناحية الطبية في المسائل المعروضة، فجسم الضحية هو محل عمل الطب الشرعي ومنه تستخرج الأدلة وتستخلص، وبها تثبت الجريمة في حق جانيها، وبها أيضاً تثبت طبيعة وحقيقة النشاط الذي تم القيام به ضد المجني عليه⁽¹⁾.

فالطب الشرعي إذاً هي وظيفة تقع بين مهنة الطب من جهة وبين الهيئة الاجتماعية من جهة ثانية، فهي تصل بين الطب والقانون، ولذلك فإن تعريفه قد تصدى له ذوى الاختصاص من أهل الطب والقانون معاً، وقد ذهبوا في صياغته أشكالاً عدة، مع أنها في جوهرها لا تعبر إلا على معنى واحد، إذ عرفه بعض الباحثين على أنه: (العلم الذي يمثل العلاقة بين الطب والقانون، وترتكز هذه العلاقة على ما يحتاج إليه القانون من الطب وما يحتاج إليه الطب من القانون)⁽²⁾.

وللطب والقانون علاقة ترابط وثيقة، وتكامل وتلازم وظيفي مهم، فالقانون كثيراً ما يتطلب أن يقتزن بالطب، فهو ضروري في منح العدالة الأدلة والحجج والإثباتات التي تتطلبها بعض الظروف والصور من الجرائم التي لا يمكن إقامة الدليل فيها وإثباتها إلى بناءً على حجج وأدلة طبية، والطب بدوره أيضاً كثيراً ما يكون مقتضياً للقانون، وهذا من خلال صور د تنظيمات ونصوص قانونية تقوم بتنظيم هذه المهنة وأخلاقياتها⁽³⁾، فالعلاقة بين الطب والقانون هي علاقة تلازم وتكامل، بحيث يكون عمل أحدهما مقتضياً للآخر، حتى وإن كان ذلك بصفة عرضية في بعض الأحيان.

(1) سميرة بيطام، حجية الدليل البيولوجي أمام القاضي الجنائي، أمواج للنشر والتوزيع، عمان، الأردن، 2015، ص 79.

(2) المرجع نفسه، ص ص: 79-80.

(3) منصور عمر المعاينة، الطب الشرعي في خدمة الأمن والقضاء، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2007، ص 16.

هذا إذا ما عرف عليه الطب الشرعي في الأدبيات القانونية التقليدية، أما الطب الشرعي محل الدراسة فهو لا يتعلق بالبحث عن الأدلة في جسد الضحية، بل هو طب يعمل على استخلاص الأدلة في مسرح جريمة افتراضي والمتمثل في الفضاء الإلكتروني أو السيبراني، فهو بذلك علم من علوم التحقيقات الجنائية التي تلعب دورا مهما في الوقاية من جرائم الحاسب الآلي وردعها، وبشكل خاص جريمة الإرهاب الإلكتروني التي أصبحت هاجسا يؤرق العالم كله.

يرجع مصطلح الطب الشرعي الرقمي إلى الأدب القانوني الغربي، فمن الناحية اللغوية نجد أنه مركب في اللغة الإنجليزية من مصطلحين أولهما هو مصطلح "Digital" الذي يعرف على أنه: (تسجيل أو تخزين المعلومات على شكل سلسلة من الأرقام 1 و 0 لتوضيح وجود إشارة أو غيابها) أو هو: (عرض المعلومات على شكل صورة إلكترونية) ⁽¹⁾، ويقابل هذا المصطلح في اللغة الفرنسية كلمة "numérique" أما في اللغة العربية فيقابلها مصطلح "رقمي".

وثانيهما هو مصطلح: "Fronsacs" والذي يقصد به: (الأساليب العلمية لمعالجة الجرائم التي تنطوي على فحص الأشياء أو المواد المتعلقة بالجريمة)، أو هي: (الأشياء أو المواد المتعلقة بالجريمة، والتي يتم فحصها علميا للمساعدة في معرفة مرتكبها وكيفية ارتكابها) ⁽²⁾ فيقابلها في اللغة الفرنسية عبارة "médecine légale" أما في اللغة العربية فتقابلها عبارة "الطب الشرعي".

أما من الناحية الاصطلاحية، فالطب الشرعي الرقمي هو علم متعلق ومرتببط بضبط وجمع الأدلة من مختلف الوسائط الرقمية وحفظها وتوثيقها من أجهزة التخزين الإلكترونية المتنوعة، مثل أجهزة الكمبيوتر، وأجهزة المساعد الرقمي الشخصي، ومختلف أجهزة ذاكرة التخزين، بحيث يتم ذلك بطريقة خاصة واستثنائية تضمن الحفاظ للأدلة الرقمية القيمة الإثباتية لها وضمان قبولها عند تقديمها وعرضها في إطار إجراء قانوني معين ⁽³⁾.

ويعرف الطب الشرعي الرقمي أيضا على أنه: (ممارسة ضبط وتحليل وإعداد التقارير حول البيانات الرقمية بالطريقة المقبولة قانونيا، ويمكن استخدامه في كشف عن الجريمة والوقاية منها، وفي أي نزاع تكون فيه الأدلة مخزنة رقميا، وهو استخدام تقنيات متخصصة لاستعادة

(1) oxford dictionary, Digital: "recording or storing information as a series of the numbers 1 and 0, to show that a signal is present or absent", "showing information in the form of an electronic image":

<https://dictionary.cambridge.org/fr/dictionnaire/anglais/digital>

(2) oxford dictionary, forensics: "Scientific methods of solving crimes, that involve examining objects or substances to a crime", "objects of substances related to a crime, that are scientifically examined to help find out who committed it and how": <https://dictionary.cambridge.org/fr/dictionnaire/anglais/forensics>

(3) ISFS, Computer Forensics, Part 1: (An Introduction to Computer Forensics), Information Security and Forensics Society (ISFS), April 2004, P.03

البيانات الإلكترونية وتوثيقا وتحليلها عندما تنطوي القضية مسائل تتعلق بإعادة بناء استخدام الكمبيوتر وفحص البيانات المتبقية وتوثيق البيانات عن طريق التحليل الفني أو شرح الميزات التقنية للبيانات واستخدام الكمبيوتر⁽¹⁾.

ويعرف أيضا على أنه: (تحديد وفحص وإعادة بناء الأدلة المستخرجة من أي عنصر من عناصر أنظمة الكمبيوتر وشبكات الحواسيب ووسائطها، والأجهزة الطرفية للحواسيب التي تسمح لمحلي الطب الشرعي بحل الجرائم المتعلقة بالكمبيوتر)، فهو يشير إلى تحليل الأدلة وأنظمة الحواسيب، بكل أجزائها مهما صغرت، وغرضه هو الاستدلال عن الجرائم المرتكبة من خلال الحواسيب، والإرهاب بمساعدة الحاسب، والإرهاب السيبراني، وغيرها من الجرائم⁽²⁾.

جدير بالذكر أن هناك تشويش وارتباك في استعمال مصطلح الطب الشرعي، فبالنسبة الباحثين فإن مصطلح علوم الطب الشرعي (Forensic Sciences) كثيرا ما يكون محلا للخلط والتشويش بينه وبين مصطلح التحاليل الجنائية (criminalistique)، غير أن المصطلحان لا يعبران عن حقيقة واحدة، فالطب الشرعي يحمل بين طياته معنى (البحث والاستغلال للأدلة من أجل إظهار الحقيقة)، أما التحليل الجنائي فهو من بين العلوم المعقدة، التي تحمل في طياتها اجتماعا للعديد من التخصصات والأساليب التي توظفها أجهزة التحقيق ومعاهد الطب الشرعي للتوصل إلى تحديد الظروف والملابسات الدقيقة التي تكتنف الجريمة وتعمل في الوقت ذاته على تحديد الجاني فيها، ويذهب فريق من الباحثين إلى التأكيد بأن نطاق توظيف التحليل الجنائي أضيق مما هو عليه في الطب الشرعي⁽³⁾.

وهذا الأمر يسرى أيضا على الطب الشرعي الرقمي باعتباره تخصصا، فقد وجدنا في خضم بحثنا أن هناك مصطلحات تستعمل على وجه المرادفة أو الترجمة لمصطلح (Digital Forensic)، كاستعمال القاموس الإلكتروني "ترجمان" عبارة التشريح الرقمي⁽⁴⁾ للدلالة على مصطلح (Digital Forensic).

(1) Jeetendra Pande, Ajay Prasad, Digital Forensics, Post-Graduate Diploma in Cyber Security Digital Forensics, Uttarakhand Open University, Haldwani, 2016, P.01

(2) Jonathan A. MATUSITZ, Cyberterrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them, thesis Doctor of Philosophy, GRADUATE COLLEGE, Graduate college, University of OKLAHOMA, Norman, Oklahoma, 2006, P.149.

(3) Yves SCHULIAR, La coordination scientifique dans les investigations criminelles. Proposition d'organisation, aspects éthiques, ou de la de la nécessité d'un nouveau métier, thèse pour obtenir le grade de docteur, Ecole des Sciences Criminelles, UNIVERSITÉ PARIS DESCARTES, Paris, 23 novembre 2009, PP.10-11.

(4) قاموس ترجمان: Digital Forensic : <https://torjoman.com/dictionary/search/2-1/Digital+Forensic>

يجب التمييز أيضا بين الأمن السيبراني والطب الشرعي، فعلى الرغم من ارتباط الطب الشرعي الرقمي وصلته بالأمن السيبراني إلا أنهما مختلفان في جوهرهما، فالطب الشرعي للكمبيوتر معني في المقام الأول بالحصول على الأدلة الرقمية الصحيحة وحفظها وتحليلها ويكون ذلك عادة بعد حدوث الجرم، أما عن الأمن السيبراني فينصب تركيزه على منع الجرم وكذلك الحفاظ على السرية والتكامل في أنظمة الكمبيوتر، ومع ذلك، فإن الطب الشرعي يكمل الأمن السيبراني، وذلك من خلال زيادة الوعي بشكل كبير بأهمية الأمن في هذا المجال، بالإضافة إلى أنه يساهم في تطوير الأسس والضوابط الإجرائية المناسبة التي تحكم الوصول واستخدام الطبقة المادية للفضاء الإلكتروني، كما أن من شأن الطب الشرعي أن يقدم الكثير من الفوائد حال جمع البيانات الرقمية، فهذه المعارف كلها يمكن أن تكون آلية لتحسين الضوابط الإجرائية للنظم والعمليات وقدرات الموظفين⁽¹⁾.

ونحن إذ أدرجنا الطب الشرعي الرقمي في باب الإجراءات الوقائية فليس ذلك لأننا نتجاهل دوره الكبير في ردع الإرهاب الإلكتروني أو غيره من الجرائم السيبرانية، ولكن اعتقادنا منا أن الطب الشرعي الرقمي يلعب دورا وقائيا فعليا أكثر منه ردعيا، فما تجرأ الجناة من الإرهابيين على جعل الفضاء الإلكتروني كسلاح أو كساحة للأعمال والنشاطات الإرهابية إلا لما أمنوا العقاب، وقد درجت العرب في أمثالها على القول أن من أمن العقوبة أساء الأدب، فالإرهابيون وغيرهم ممن سولت لهم أنفسهم على توظيف هذه الساحة لأغراض إجرامية كان سببه كما أشرنا إليه في سابق بحثنا؛ هو طبيعة هذه الساحة التي تتميز بالمجهولية والغفلية وصعوبة الاستدلال أمام المحاكم على يقع فيها من جرائم، فبمجرد أن يعلم المجرمون أن هذه الساحة أيضا خاضعة لسلطة القانون، وأن التحقيق في الجرائم التي تقع فيها ليس عصية بالشكل الذي يتوقعونه فإن ذلك يعد عاملا نفسيا لمنع حدوثها خوفا من المتابعة القضائية، كما أن هناك ما يعرف في أوساط المختصين بالطب الشرعي الرقمي بالإستباقي، ودوره وقائي أكثر منه ردعي.

ثانيا: الطب الشرعي الرقمي: المكانة والأنواع:

1- مكانة الطب الشرعي الرقمي:

يعتبر موضوع الطب الشرعي الرقمي من بين أهم الموضوعات الدراسية والبحثية في أمن الفضاء الإلكتروني، فقد كان محطة للكثير من الأبحاث والدراسات والتي يتمحور مضمونها وجوهرها على مناقشة وتحليل عملية الطب الشرعي، ومختلف الجزئيات والتفاصيل المتعلقة

(1) ISFS, Computer Forensics, Op.cit., P.03

والمرتبطة بعملية الحصول على الأدلة الرقمية وتحليلها في وسط لا تشوبه شائبة، ضم إلى ذلك دراسة مختلف العناصر المرتبطة بأنظمة التشغيل المختلفة، وآليات استخدامها لتكون صالحة لتحليل الطب الشرعي الرقمي⁽¹⁾.

وتظهر أهمية الطب الشرعي الرقمي من خلال المحاولات المتعددة التي قامت بها الولايات المتحدة الأمريكية لإدراج الطب الشرعي الرقمي وإدماجه بأمن المعلومات، ومن بين أهم تلك المحاولات هي: "دليل دمج تقنيات الطب الشرعي في الاستجابة للحوادث" الذي قام بنشره المعهد الوطني للمعايير والتكنولوجيا، الذي تتجلى فيه ضرورة وأهمية تنفيذ مهارات الطب الشرعي الرقمي في الاستجابة لمختلف الحوادث، حيث يتم توظيفه في العديد من المسائل المتعلقة بالأمن الإلكتروني، كما تظهر الأهمية أيضا من خلال قانون ("Sarbanes-Oxley "SOX") الذي يتضمن العديد من القواعد والضوابط ذات الصلة بالأدلة الرقمية، وواجبات الشركات والموظفين فيما يتعلق بمختلف السجلات وحفظها⁽²⁾.

وترى الباحثة أيضا أن أهمية الطب الشرعي الرقمي تتجلى بصفة خاصة وفي صورة جلية من خلال تنوع المساهمين في هذا العلم المستجد، وتعدد الشبكات المشاركة فيه. فوفقا لمختبر الطب الشرعي الرقمي في جامعة بورديو، هناك أربع شبكات مشاركة في الطب الشرعي السيبراني أوردتها الباحثة (Jonathan A. MATUSITZ) على الشكل الآتي:

- **شبكة إنفاذ القانون:** حيث تم تشجيع الضباط على تعلم فنون الطب الشرعي الرقمي، إذ من المهم بالنسبة لهم أن يكونوا قادرين على تجميع الأدلة وضبطها بأسرع وقت ممكن، كما تمكنهم برامج الطب الشرعي الرقمي من حماية الأدلة الرقمية لاستخدامها في التحقيقات؛

- **الجيش:** يشارك الجيش أيضا في شبكة واسعة من نشاطات الأمن الإلكتروني والتي تهدف إلى تطهير الفضاء الإلكتروني من الإرهابيين الإلكترونيين؛

- **القطاع الخاص:** يشارك القطاع الخاص بشكل جدي في الشبكة المناهضة للإرهابيين السيبرانيين، والسبب في ذلك هو أن الإرهابيين السيبرانيين قد قاموا بالفعل بشن هجمات على البنى

(1) Ayman Shaaban, Nashwa Abdelbaki, Comparison Study of Digital Forensics Analysis Techniques; Findings versus Resources, The 5th International Workshop on Privacy and Security in Health Care (PSCare 2018), Procedia Computer Science, Volume 141, Elsevier B.V, 2018, Pages 545-551:

<https://www.sciencedirect.com/science/article/pii/S1877050918317769>

(2) Sungmi Park, Nikolay Akatyev, Yunsik Jang, Jisoo Hwang, Donghyun Kim, Woonseon Yu, Hyunwoo Shin,, Changhee Han, Jonghyun Kim, A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement, Digital Investigation, Volume 24, Supplement, Elsevier Ltd, March 2018, Pages S93-S100: <https://www.sciencedirect.com/science/article/pii/S1742287618300446>

التحتية للقطاع الخاص عبر العديد من الوسائل، ولهذا نجد هذه الشركات تعمل على التواصل مع المنظومات التي تضمن السلامة على الإنترنت؛

- الأوساط الأكاديمية: يوجد أقسام مخصصة لمختبرات الطب الشرعي الرقمي في الجامعات، ولمختبراتها هذه دور مهم في التعاون مع وكالات إنفاذ القانون⁽¹⁾.

2- أنواع الطب الشرعي الرقمي:

للطب الشرعي أنواع وأقسام عدة، وسنقوم في بحثنا هذا بإدراجها على النحو الآتي ذكره:

أ- الطب الشرعي الرقمي من حيث المحل: وينقسم إلى ثلاث أقسام أساسية وهي:

• الطب الشرعي الرقمي للكمبيوتر وملحقاته:

يعرف موجز قاموس أكسفورد الجديد الطب الشرعي للكمبيوتر على أنه: (تطبيق تقنية علم الطب الشرعي على مرتكزات الكمبيوتر المادية)، فهو بذلك يعبر في مضمونه عن عملية ضبط وتحديد الأدلة الرقمية وحفظها وتحليلها وتقديمها بطريقة يمكن على أساسها أن تقبل في إطار إجراء قضائي معين⁽²⁾، فمحله جهاز الكمبيوتر وما يخلق ويحموم به من أجهزة، إذ يعمل على البحث والتحري عن الأدلة وتحليلها على أجهزة الحواسيب لتقديمها كأدلة أمام الجهات القضائية.

• الطب الشرعي الرقمي للهاتف الخليوي:

يتكون الطب الشرعي للهاتف الخليوي من جملة العمليات التي تستهدف فحص الهاتف الخليوي بالإضافة إلى السجلات التي تم إنشاؤها بواسطة موفري خدمة الهاتف الخليوي مثل معلومات فواتير الهاتف الخليوي وسجلات تفاصيل المكالمات⁽³⁾، ويعرف على أنه: (...علم استرداد الأدلة الرقمية من الهاتف المحمول في ظل ظروف سليمة للطب الشرعي باستخدام طرق مقبولة) وتعتبر عملية الطب الشرعي الرقمي من بين المظاهر الحديثة للطب الشرعي، ويتم التعامل فيها علناغالب الأعم بتقنيات الطب الشرعي الرقمي التقليدي الخاص بالكمبيوتر⁽⁴⁾.

(1) Jonathan A. MATUSITZ, Op.cit. PP.150-152.

(2) Michael G. SOLOMON, Diane BARRET, Neil BROOM, Computer Forensics: (JumpStartTM), SYBEX, london, 2005, P.02.

(3) Larry DANIEL, Lars DANIEL, Digital Forensics for legal professionals: (understanding digital evidence from the warrant to the courtroom), Elsevier, USA, 2011, P.19

(4) Wayne SANSEN, Rick AYERS, Guidelines on Cell Phone Forensics: (Recommendations of the National Institute of Standards and Technology), Technology Administration, National Institute of Standards and Technology, Sponsored by the Department of Homeland Security, USA, May 2007, P.ES1.

• الطب الشرعي الرقمي للتلفاز الذكي:

لقد أضحى التلفزيون الذكي شائع الاستعمال عند الكثير من الناس، فشعبيته تتزايد يوما بعد يوم، فكثير من المستخدمين منهم يوظفونه من أجل الوصول السريع إلى شبكة الإنترنت، بما في ذلك الحصول على فيديوهات الموقفة على الطلب، وشبكات التواصل الاجتماعي، وكذلك الرسائل الفورية، وتوفر هذه الأجهزة الذكية إمكانية ربطها بأجهزة أخرى خارجية، فكل هذه المميزات والسمات التي يتسم بها هذا الجهاز تجعله مصدرا غنيا وازخرا بالمعلومات لأغراض الطب الشرعي، خاصة وأن شيوع استخدامه قد أتاح الفرصة لإساءة الاستعمال، وعليه فإنه من الضروري دراسة الطب الشرعي الرقمي للتلفاز الذكي في مجال تقنيات الطب الشرعي الرقمي⁽¹⁾.

ب- الطب الشرعي الرقمي من حيث المكون:

• الطب الشرعي الرقمي الاستباقي (Proactive Forensics):

يعتبر الطب الشرعي الرقمي الاستباقي ذو قدرة وإمكانية على إجراء جمع البيانات والأدلة بشكل مسبق لارتكاب الجريمة، ويمكن له أيضا حفظها والعمل على الكشف عن الحثيات والأحداث المشبوهة التي تجري على الفضاء الإلكتروني، ويعمل أيضا على جمع الأدلة وإجراء التحاليل وبناء أسانيد القضايا الجنائية وإقامتها ضد مرتكبي الأنشطة المريبة، ضم على ذلك، يمكن للطب الشرعي الرقمي الاستباقي أن يعمل على بناء أو إنشاء تقارير آلية من أجل استخدامها لاحقا، في الطب الشرعي التفاعلي⁽²⁾.

وأول نظام تم إنشاؤه لغرض الطب الشرعي الرقمي الاستباقي هو نظام (PROOFS) الذي يعمل على توضيح الأسئلة المتعلقة بإجراءات وعمليات المستخدم⁽³⁾.

يسير الطب الشرعي الرقمي الاستباقي وفق مراحل متعددة، فهو أولا يعمل على جميع استباقي للبيانات المحددة مسبقا حسب درجة التقلب والأولوية، ووفق متطلبات معينة لمنظمة ما، ثم عملية تشغيل المهمة، وتكون بتشغيل أي مهمة مريبة من خلال البيانات التي تم تجميعها، ثم بعد ذلك تليها مرحلة الحفظ الاستباقي، وهي عملية حفظ آلي للأدلة المتعلقة بالمهمة المشبوهة، وتأتي

(1) A. BOZTAS, A.R.J. Riethoven, M. Roeloffs, Smart TV forensics: Digital traces on televisions, DFRWS 2015 Europe, Digital Investigation, Volume 12, Supplement 1, March 2015, Pages S72-S80:

<https://www.sciencedirect.com/science/article/pii/S1742287615000134>

(2) UKESSAYS, Proactive and Reactive Cyber Forensics Investigation Process, 12th Mar 2018 Accessed on 02 August 2020, at 04:41H, in:

<https://www.ukessays.com/essays/computer-science/proactive-reactive-cyber-forensics-investigation-1756.php>

(3) Clay SHIELDS, Ophir FRIEDER, Mark MALOOF, A system for the proactive, continuous, and efficient collection of digital forensic evidence, Digital Investigation, Volume 8, Elsevier Ltd, Supplement, August 2011, Pages S3-S13: <https://www.sciencedirect.com/science/article/pii/S1742287611000260>

بعدها مرحلة التحليل الإستباقي، أين تحلل الأدلة بشكل مباشر وفق تقنيات الطب الشرعي الرقمي، وتنتهي العملية بتقرير آلي أولي للمكون الإستباقي (1).

• الطب الشرعي الرقمي التفاعلي: (Reactive Forensics):

الطب الشرعي الرقمي التفاعلي هو أسلوب أو نهج من النهج التقليدية الذي يتم بمقتضاه التحقيق في الجريمة الرقمية بعد وقوعها، وفي هذا الإطار يتم جمع نوعين من الأدلة الرقمية؛ أولهما هو الدليل النشط وهو جمع لكل الأدلة الديناميكية المتواجدة بعد الحادث، وثانيهما هي الأدلة المتفاعلة وهي الأدلة الثابتة المتبقية بعد الحادث (2).

فالطب الشرعي الرقمي التفاعلي إذا، يكون لاحقا لوقوع الجريمة أو أي حادث آخر، حيث يعمل على التحري عليها بجمع الأدلة وتحليلها وإعداد التقارير عليها، وهو أشبه بإجراءات التحقيق التقليدية التي لا تكون إلا بعد وقوع الجريمة، ولا تحقق إلا فيما خلفته من آثار، وتكون الإدانة أو البراءة مرهونة بما يتوصل إليه خبير الطب الشرعي الرقمي من تحليل ودراسة.

وخلاصة لما سبق، فإننا يمكن أن نعتبر الطب الشرعي من بين أهم الآليات والوسائل الحديثة التي يمكن بها العمل على تأمين الفضاء السيبراني من أي تهديد أو خطر داهم، سواء أكان ذلك الخطر إرهابا إلكترونيا، أو أي جريمة أخرى تقع على الفضاء الإلكتروني أو بواسطة، فهو يشكل إجراء محوري من أجل تحقيق العدالة الجنائية وتقديم الجناة في الجرائم الرقمية أمام الجهات القضائية، ضامنا بذلك عدم الانفلات من العقاب، وفي الوقت ذاته يحول دون إقدام المجرمين والإرهابيين على توظيف الفضاء الإلكتروني كهدف أو وسيلة لأغراضهم الإجرامية.

الفرع الثاني: الأدلة الرقمية في الطب الشرعي الرقمي:

إن الهدف الأساسي لعلوم الطب الشرعي الرقمي هي الوصول إلى إثبات الجرائم الإلكترونية كلها بما في ذلك الإرهاب الإلكتروني ونسبتها إلى جناتها درءاً لإنكار العدالة وتحقيقاً للأمن السيبراني وضماناً لتحقيق مبادئ العدالة وعدم الإفلات من العقاب، والدليل الرقمي من الأدلة التي تحمل مفهوما خاصا (أولا) بل إن الحصول عليها أيضا يتعين أن يسير وفق منهج محدد وخاصة ضمانا لأصالتها وموثوقيتها لما تتمتع به من خواص تفرقها عن غيرها من الأدلة (ثانيا).

(1) Soltan ALHARBI, Jens WEBER-JAHNKE, Issa TRAORE, The Proactive and Reactive Digital Forensics Investigation Process: (A Systematic Literature Review), international Journal of Security and Its Applications, Vol 05, No 04,, October, 2011, PP.59-72.

<https://www.uvic.ca/engineering/ece/isot/assets/docs/IJSIA.pdf>

(2) Ibid.

أولاً: مفهوم الدليل الرقمي:

1- تعريف الدليل الرقمي:

يعرف الدليل الرقمي على أنه: (الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون)⁽¹⁾.

ويعرف أيضاً على أنه: (أي عنصر موجود في شكل إلكتروني، سواء أكان مؤقتاً وعابراً أم كان على غير ذلك، ويمكن أن تكون ملفات الكمبيوتر أو عمليات الإرسال أو البيانات أو البيانات الوصفية أو بيانات شبكات الاتصال)⁽²⁾.

أورد الباحث شهزاد سليم (Shahzad Saleem) ثلاث تعريفات للدليل الرقمي، وهي تعريفات كما سنلاحظها تختلف في أبعاد شموليتها، فالتعريف الأول يعرف الدليل الرقمي على أنه: (المعلومات ذات القيمة الإثباتية المخزنة أو المرسل في شكل رقمي)، أما التعريف الثاني فيعرفه على أنه: (المعلومات المخزنة أو المنقولة في شكل ثنائي والتي يمكن الاعتماد عليها في المحكمة)، أما التعريف الثالث فيعرفه على أنه: (أي بيانات مخزنة أو مرسل باستخدام جهاز كمبيوتر يدعم أو يدحض نظرية ما عن كيفية حدوث جريمة أو تتناول العناصر الحاسمة للجريمة مثل النية أو الذريعة)، وقد فضل الباحث شهزاد سليم التعريف الأخير الذي ينسب لكيسي (casey) لاعتبارين؛ أولهما لأن التعريفين السابقين يتجاهلان المعلومات التي يتم جمعها إذا لم تكن قابلة لتوظيفها كأدلة إثباتية، حتى ولو كانت أدلة على قدر كبير من القوة لتعزيز عمليات التحقيق، فالتعرفان يحصران الأدلة الرقمية في تلك الأدلة التي تمتلك القوة الثبوتية أمام الجهات القضائية، أما الاعتبار الثاني فيتحدّث في مصطلح بيانات بدلا من معلومات، فالبيانات أكثر تجريدا من المعلومات وهذا ما يضيف عليها البعد الشمولي أو العمومي⁽³⁾.

(1) نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، المجلد 04، العدد 02، جامعة باتنة 01، الحج لخضر، جوان 2017، ص ص: 908-926: <https://www.asjp.cerist.dz/en/article/24925>

(2) Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, Vienne, 25-28 février 2013, UNODC/CCPCJ/EG.4/2013/2, 23 janvier 2013, P.10.

(3) Saleem SHAHZAD, Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics, Academic dissertation for the Degree of Doctor of Philosophy in Computer and Systems Sciences, Department of Computer and Systems Sciences, Stockholm University, Sweden, 2015, P.22.

وذهب اللواء محمد الأمين البشري⁽¹⁾ في تعريفها على أنها: (معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحاسوبية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه)⁽²⁾.

ونذهب إلى ما ذهب إليه الباحث شهزاد سليم في تفصيل تعريف (casey) لشموليته على كل أصناف الأدلة سواء أكانت تلك التي يحتج بها أمام الجهات القضائية أو تلك التي تعزز وتقوى من نتائج التحقيق وتدعم تصور من التصورات التي تم منحها لواقعة إجرامية على الفضاء السيبراني، بالإضافة إلى ما ذهب إليه في تفصيل مصطلح البيانات عن المعلومات، وفضلا عما ذهب إليه الباحث شهزاد سليم فإن هذا التعريف يقدم صورة شاملة عن الأبعاد التي يمكن للدليل الرقمي أن يوضحها ويجلها في الجريمة، وذلك حينما أشار إلى القصد الجنائي، فالدليل الرقمي بالإضافة إلى أنه يمنح صورة عن العناصر المادية للجريمة فهو في الوقت نفسه يمنح صورة عن القصد الجنائي، فالدليل الرقمي هو الذي سيكون أداة لتكييف الواقعة على أنها جريمة إلكترونية عادية، أو جريمة إرهاب إلكتروني.

2- خصائص الدليل الرقمي:

تميز الأدلة الرقمية عن غيرها من الأدلة ولاسيما الأدلة المادية كونها:

- **أدلة علمية:** ذلك أنها أدلة تتركب من معلومات وبيانات إلكترونية تقنية غير ملموسة، إذ لا يمكن إدراكها إلا من خلال اللجوء إلى استعمال أدوات خاصة سواء أكانت أجهزة ومعدات أم كانت برمجيات حاسوبية⁽³⁾، وبناءً على هذا فإن الدليل الرقمي تسرى عليه القواعد التي تنطبق على سائر الأدلة العلمية إذ يتم استبعاده في حالة تضاربه من الأسس العلمية الصحيحة⁽⁴⁾.

(1) مستشار مكتب مفتش عام وزارة الداخلية بدولة الإمارات العربية المتحدة.

(2) محمد الأمين البشري، الأدلة الجنائية الرقمية: (مفهومها ودورها في الإثبات)، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد

33، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، نوفمبر 2000، ص: 91-147:

<https://repository.nauss.edu.sa/handle/123456789/54802>

(3) لا تتطلب كل الأدلة الرقمية معدات وبرامج لإدراكها، فالأدلة الرقمية المادية يكفي مجرد فحص بسيط لأجهزة الحاسوب أو الهاتف المحمول لإدراكها، كحيازة أفلام أو صور خلاعة متعلقة بالأطفال، أو حيازة ملفات متعلقة بالنشاطات الإرهابية كأسماء المجندين على الفضاء الإلكتروني، إما الذي يتطلب ويستلزم معدات وبرامج لإدراكها هي الأدلة الرقمية المنطقية، فهي أدلة لا يمكن إدراكها في شكل مادي كالصورة أو الفيديو إنما يتم إدراكها من خلال تحليل الطبقة المنطقية سواء للحاسب الآلي أو الموبايل أو الشبكات.

(4) إلهام شهزاد روايح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، المجلد 05،

العدد 02، جامعة لونييسي علي، البليدة 02، جوان 2016، ص: 184-198: <https://www.asjp.cerist.dz/en/article/30452>

- **أدلة حديثة:** الدليل الرقمي يتصف كونه دليلاً حديثاً نشأ، إذ أنه من الأدلة الناتجة عن أشكال التقدم في المجالات التقنية، وهو أيضاً تمتع بالخصوصية في كونه ينشأ ويظهر بيئة خاصة، كما أنه يتميز بطبيعة خاصة فيما يتعلق بالهيئة أو الصورة التي يظهر فيها كما أن الدليل الرقمي لا يرتبط نشوؤه بإرادة الجاني، فهو دليل خارج عن نطاق سيطرته⁽¹⁾، فالوسائل الفنية المميزة هي التي تتيح عملية الحصول هذا الدليل الذي يطلق عليه اسم بالبصمة الرقمية أو الأثر المعلوماتي الذي يخلفه الجاني وراءه في حالة تسخير الأجهزة الإلكترونية⁽²⁾.

- **أدلة ديناميكية:** تظهر هذه الخاصية بشكل واضح من خلال الجرائم المعلوماتية كجريمة بث أحد الفيروسات وغيرها⁽³⁾، فهي أدلة تتسم بالسرعة في انتقالها من جهة من لأخرى، متخطية حدود الزمان والمكان، هذا ما يجعل من عملية الاستدلال تستغرق وقتاً أطول إذا ما قورنت بالأدلة المادية⁽⁴⁾.

- **أدلة يصعب التخلص منها**⁽⁵⁾: إذ أنه حتى لو كان هناك تعليمات أو أوامر صادرة من الجاني للقيام بمحوها وإزالتها ومع ذلك يمكن استرجاعها باستعمال برامج مخصصة لذلك⁽⁶⁾.

- **أدلة قابلة للنسخ:** يكون ذلك من خلال إنشاء نسخة مطابقة للأصل من الأدلة الرقمية والاحتفاظ بها بطريقة تتضاءل معها فرصة إتلافها أو فقدانها⁽⁷⁾.

3- أنواع الأدلة الرقمية:

أ- الإنترنت:

تعتبر مواقع التواصل الاجتماعي ولوحات الرسائل وغرف الدردشة على وجه الخصوص المصدر الأول للأدلة الرقمية، وتعد المجهولية التي تتمتع بها هذه المواقع والعناوين الإلكترونية من

(1) لا يعتبر هذا الأمر كقاعدة عامة، فرغم أن الغالب في الأدلة الرقمية أنها تنشأ بغير إرادة الفاعل إلا أنها يمكن أن تنشأ بإدارته أيضاً، نرى أن المؤلف قد ركز في هذه الخاصية على الأدلة الرقمية المنطقية التي تنشأ في الطبقة المنطقية للقضاء الإلكتروني، غير أن هذا لا ينطبق على الأدلة التي يتم ضبطها في شكلها الحقيقي من صور وأفلام وملفات غير مشفرة وغير ذلك من الأدلة التي يمكن تحسسها دون اللجوء إلى معارف تقنية أو فنية.

(2) سميرة بيطام، المرجع السابق، ص 153.

(3) طارق عفيفي صادق أحمد، نظرية الحق، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2016، ص 310.

(4) إلهام شهرزاد رواج، المرجع السابق.

(5) من الخطأ تعميم هذه الخاصية على جميع الأدلة الرقمية، فهناك من الأدلة الرقمية ما يسهل إتلافها ومحوها أو على الأقل تعميمها من خلال التشفير أو الإخفاء، وسنتطرق إلى هذه النقطة بشيء من التفصيل فيما سيأتي من فروع بحثنا، لذلك نحن ندعم رأي الباحثة إلهام شهرزاد رواج حين وصفت هذه الصعوبة بالنسبية.

(6) محمد بن فريدة، الدليل الجنائي الرقمي وحجته أما القضاء الجزائي: (دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني، المجلد 05، العدد

01، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، جوان 2014، ص ص: 276-286:

<https://www.asjp.cerist.dz/en/article/55437>

(7) المرجع نفسه.

أكبر التحديات التي توجه المحققون، وعليه فإن أول خطوة يتعين القيام بها هو العثور على هذه المواقع، كما تمثل شبكة مشاركة الملفات المصدر الرئيسي الآخر الذي يتم استخدامه أثناء التحقيقات، وقد تم غلق الكثير من نشاطات هذه الشبكات ولاسما تلك المتعلقة بانتهاكات حقوق النشر وتبادل المواد غير القانونية⁽¹⁾.

كما أن عالمية الإنترنت يثير إشكالية الاختصاص، فحتى بعد الكشف عن هوية الشخص تبقى هناك إشكالية خروجه عن دائرة اختصاص المحقق، ومع هذا يمكن للطب أن يكون للأدلة الرقمية قيمة استخباراتية⁽²⁾.

ويتمثل أحد أكبر التحديات في جرائم الإنترنت أيضا في بقاء الخبراء والمنوط بها عملية التحقيق على نفس نمط القدرة على فهمهم لكيفية سير العمليات -سواء تلك المرتبة بالجرائم الإلكترونية أو عمليات التحقيق والتحليل الجنائي الرقمي-، بالإضافة أيضا بقائهم في وسط متابعة ما يستجد في هذا المجال من برمجيات وتقنيات مختلفة⁽³⁾، وهذا لا يعد أمر يسيرا نظرا للطبيعة المتطورة لهذا المجال وتعقيده أيضا.

ب- أجهزة الكمبيوتر:

يمكن الحصول على الكثير والعديد من هذه العناصر الاستدلالية من خلال عملية استخلاص يدوية أو منطقية للأدلة على جهاز الحاسب الآلي التي كثيرا ما ندجها متداخلة مع الأدلة الموجودة على الإنترنت، فعند تصفح الويب تحتفظ البرامج بملفات الإنترنت المؤقتة وملفات تعريف الارتباط ومحفوظات الاستعراض، وكل هذه العناصر من الممكن توظيفها لتحديد نشاط المستخدم، كما أنه يمكن العثور على البريد الإلكتروني والرسائل الأخرى على جهاز الحاسب الآلي أيضا⁽⁴⁾.

يمكن أن يحتوي جهاز كمبيوتر على دليل يفيد حدوث نشاط إجرامي على الويب، أو يمكن أن يحتوي الكمبيوتر نفسه على أدلة تفيد وجود نشاطات إجرامية، فيكون في الجهاز مواد وأدلة تثبت وقوع جريمة معينة، مثل المواد الإباحية وانتهاك حقوق النشر والابتزاز والتزوير وغير ذلك الكثير. وتوجد الأدلة الرقمية على محرك الأقراص الثابتة بجهاز الكمبيوتر والأجهزة الطرفية، بما في ذلك الوسائط القابلة للإزالة مثل محركات الأقراص الثابتة وأقراص CD-ROM⁽⁵⁾.

(1) Sean E. GOODISON, Robert C. DAVIS, Brian A. JACKSON, Digital Evidence and the U.S. Criminal Justice System: (Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence), Priority criminal justice, NEEDS INITIATIVE, RAND Corporation, 2015, PP.03-04: https://www.rand.org/pubs/research_reports/RR890.html

(2) ibid. P.04.

(3) A Simplified Guide To Digital Evidence, National Forensic Science Technology Center, under a cooperative agreement from the Bureau of Justice Assistance (BJA), Florida, 2009: <http://www.forensicsciencesimplified.org/digital/DigitalEvidence.pdf>

(4) Sean E. GOODISON, Robert C. DAVIS, Brian A. JACKSON, Ibid. P.04.

(5) A Simplified Guide To Digital Evidence, National Forensic Science Technology Center, Op.cit.

ج- الأجهزة المحمولة:

تعتبر الهواتف المحمولة محطة للأدلة الرقمية الأكثر شيوعاً، ولا غرابة في ذلك أمام انتشار هذه الأجهزة وسعة استخدامها في مجتمعاتنا المعاصرة، وهذا من شأنه أن يطرح تحديات قانونية جديدة، ومثاله ما حكمت به المحكمة العليا الأمريكية مؤخراً بأن هناك حاجة إلى مذكرة تفتيش لمعظم عمليات البحث عن الهواتف المحمولة، فما تملكه من خواص وميزات تجعلها مصدراً وفيراً للأدلة الرقمية، كما أصبح الهاتف الخليوي مركزاً للإنترنت وآلية إدخال وإخراج وهذا ما يزيد من كمية البيانات التي يحويها (1).

وعلى أي حال فإن الإلكترونيات المحمولة تسمح للمجرمين إمكانية المشاركة والإسهام في مجموعة متنوعة ومتعددة ومتنامية من الأنشطة الإجرامية، ومع ذلك يمكن تتابع الأجهزة المحمولة، وهذه القدرة على التتبع هي التي تحول الأجهزة المحمولة إلى دليل رئيس في كثير من حالات الإجرام الإلكتروني المختلفة (2).

وفي الأخير، تجدر الإشارة إلى أن هناك تقسيمات أخرى للأدلة الرقمية، إذ يمكن تقسيمها أيضاً إلى على إثر طبيعة المعلومات التي يتشكل منها الدليل، والتي يمكن أن تكون صوراً إلكترونية أو تسجيلات صوتية أو نصوصاً مكتوبة، كما ذهب بعض الفقه إلى تصنيفها على أساس طبيعة المخرجات وقسمها إلى ثلاث أقسام وهي المخرجات الورقية، والمخرجات الإلكترونية ومخرجات معالجة البيانات المعروضة بواسطة الشاشة أو وحدات العرض المرئي (3).

كما أن هناك من قسمها إلى أدلة يمكن إنشاؤها كما هو الحال بملفات التسجيل وملفات تعريف الارتباط، وبيانات التعريف والعناوين الإلكترونية، وأدلة مخزنة في أجهزة الحاسب مثل الصور الرقمية وملفات وورد وبرامج العرض وما إلى ذلك (4)، وهناك نوع ثالث بين هذين النوعين فجزء منه محفوظ عن طريق الإدخال، والجزء الآخر منه تم إنشاؤه باستخدام الحواسيب (5).

(1) Sean E. GOODISON, Robert C. DAVIS, Brian A. JACKSON Op.cit. PP.04-05.

(2) A Simplified Guide To Digital Evidence, National Forensic Science Technology Center, Ibid.

(3) بصائر علي محمد ومروى عبد الواحد حسن، الدليل الإلكتروني في مجال الإثبات الجنائي، مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية، المجلد

03، العدد 27، جامعة واسط، 2017، ص ص: 271-285: <https://lark.uowasit.edu.iq/index.php/lark/article/view/374>

(4) مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: (دراسة مقارنة)، دراسات، علوم الشريعة والقانون، المجلد 45،

العدد 04، ملحق 02، عمادة البحث العلمي وضمان الجودة، الجامعة الأردنية، 2018، ص ص: 284-299:

<https://fada.birzeit.edu/handle/20.500.11889/5731>

(5) عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: (دراسة

تطبيقية مقارنة)، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض 12-14 نوفمبر 2007.

ثانيا: إجراءات بناء وتكوين الدليل الرقمي:

1- الجمع والحرز:

يتعلق هذا الإجراء برفع الأدلة التي سيتم نقلها إلى المختبرات المتخصصة في العلوم الجنائية وحرزها بأسلوب يمكن معه ضمان عدم تعرضها لأي ضرر ينجم عنه تأثير على قيمتها الاستدلالية، ففي الجرائم المعلوماتية يتم أخذ الصور لمخلفات الجريمة ورفع كل ما يطاله المحقق من أدلة يمكن أن تكون نبراسا للحقيقة، كما أن المحقق في هذه المرحلة يقوم بصون النظام الرقمي وكل الأصول الرقمية من أجل العمل على تحديدها في وقت لاحق، كما يتعين أيضا القيام بنسخ جميع البيانات الموجودة في الجهاز محل الجريمة ونقلها إلى جهاز خاص بالمعمل الجنائي الرقمي ⁽¹⁾، وتنتقل بذلك من نطاق السيطرة المادية أو الإدارية للمحقق إلى موقع خاضع للرقابة وهو ما يطلق عليه مرحلة المسح ⁽²⁾.

يهدف هذا الإجراء إلى الوصول لغايات محددة، ويهدف بشكل أساسي إلى الإحاطة بجميع الأشياء التي كان لها يدا في الوقائع المتصلة بالحادث أو تكوين الفرضيات والنظريات حول الحادث، كما يمكن أن يهدف هذا الإجراء أيضا إلى التثبت والتحقق من وجود أي شكل من أشكال الحوادث المختلفة، أو من أجل الحصول على أدلة تثبت وجوع حادث أو واقعة معينة، ويمكن أيضا أن يرمي هذا الإجراء إلى اختبار فرضية تم وضعها فيما سبق، والتحقق من مدى صحتها ⁽³⁾.

تتطلب حساسية الأدلة الرقمية الدقة في ممارسة جمع وحرز الأدلة، وقد طورت منظمات مثل (SWGDE) و (NIJ) ممارسات وأساليب للقيام بذلك، فبعد أن يتم تأمين المسرح يمكن بعدها جمع الأجهزة وجمع كل كلمات المرور أو أي رموز أو أرقام من الأفراد المعنيين إن كان ذلك متاحا، كما يتم أيضا رفع كل الأدلة المرتبطة بها، ويجب توخي الحذر الشديد مع تلك الأجهزة، وتوخي الحيلة مع إجراءات جمع الأدلة لمنع تعرضها لأي ضرر ⁽⁴⁾ محتمل ذلك أن الأدلة الرقمية أدلة هشة من اليسير جدا أن تتعرض للتلف أو للتغير، وهذا بطبيعة الحال سيكون له تأثير كبير على مصداقيتها وموثوقيتها أمام الجهات القضائية المختصة.

(1) سيدي محمد لبشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية: (دراسة تحليلية تطبيقية)، رسالة ماجستير في العلوم الشرطية، كلية

الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص ص: 73-74.

(2) Ravneet KAUR, Amandeep KAUR, Digital Forensics, International Journal of Computer Applications, Volume 50 – No.5, Foundation of Computer Science, USA, July 2012, PP.5-9.

<https://www.ijcaonline.org/archives/volume50/number5>

(3) Brian D. CARRIER, Eugene H. SPAFFORD, Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence, Digital Forensic Research Workshop (DFRWS), 2005:

<https://dfrws.org/presentation/automated-digital-evidence-target-definition-using-outlier-analysis-and-existing-evidence/>

(4) A Simplified Guide To Digital Evidence, National Forensic Science Technology Center, Op.cit

2- مرحلة التحليل:

يتولى المتخصص أو محلل الطب الشرعي الرقمي في هذا الإجراء فحص وتحليل الأدلة التي تم تجميعها من مسرح الجريمة والتي تضم الأصول الرقمية من أجل ضبط صنف الدليل ويضم فحص مضمون الملفات والمسارات، والعمل على استرداد ما تمت إزالته من محتوى (1).

يتعين قبل البدء في عملية التحليل عزل الأجهزة اللاسلكية ويجب فحصها مبدئياً في غرفة العزل إذا كانت متوفرة، فهذا من شأنه أن يحول دون الاتصال بالشبكة، ويحافظ على الأدلة قدر الإمكان، كما يقوم المحلل بتثبيت برنامج حظر الكتابة لمنع إحداث أي تغيير في البيانات الموجودة على الأجهزة والوسائط، وبمجرد إنشاء نسخة العمل سيقوم المحلل بتحديد طراز الجهاز ويعمل أيضاً على اختيار برنامج الاستخراج المصمم من أجل تحليل البيانات أو عرض ما تتضمنه، ثم يقوم المحلل بعد أن يزيل البيانات بإرسال الأجهزة والوسائط الأصلية للتعرض للفحص الجنائي وفق المعايير التقليدية للتحقيقات الجنائية، وبعدها يقوم المحلل بتثبيت برامج عرض البيانات التي تمكنه من رؤية البيانات، كما يمكن أن يعمل على استعادة البيانات المحذوفة، ويمكن أيضاً للمحقق أن يلجأ إلى الإنترنت للبحث عن الأدلة، ويمكن أن يجمع سلاسل من التفاعلات التي توفر صورة واضحة عن النشاطات والممارسات التي تمت على الفضاء الإلكتروني (2)، وفئات التحليل بالجوء إلى طبقات التجريد يمكن اختزالها في النطاقات التالية:

"- **تحليل الوسائط المادية:** تحليل طبقة الوسائط المادية للتجريد، يتضمن تحليل هذه الطبقة معالجة أو ترجمة تخطيط التخزين ومحتوياته إلى واجهة قياسية، وحتى استعادة البيانات المحذوفة بعد الكتابة فوقها؛

- **تحليل إدارة الوسائط:** تحليل طبقة إدارة الوسائط التجريدية التي تنظم وسائط التخزين، غير أن هذه الطبقة لا تكون متوفرة في جميع الوسائط؛

- **تحليل نظام الملفات:** تحليل طبقة نظام الملفات التجريدية، والتي تترجم وحدات البايت وقطاعات القسم إلى أدلة وملفات، يتم عرض مضمون ومحتوى الملفات والأدلة واستعادة الملفات المحذوفة من خلال البحث في الطبقة الحدودية؛

- **تحليل التطبيق:** وتكون بتحليل طبقة التطبيق التجريدية التي تترجم البيانات والتي يتم استرجاعها في الغالب من نظام الملفات، إلى التنسيق المخصص الذي يحتاجه التطبيق. يتضمن

(1) سيدي محمد ليشير، المرجع السابق، ص 74.

(2) A Simplified Guide To Digital Evidence, National Forensic Science Technology Center, Op.cit.

التحليل في هذه الطبقة عرض ملفات السجل وملفات التكوين والصور والمستندات والملفات التنفيذية للهندسة العكسية؛

- **تحليل الشبكة:** تحليل طبقة الشبكة التجريدية، التي تترجم بيانات أدنى مستوى من شبكة فعلية أو شبكة لاسلكية إلى البيانات التي يستخدمها أحد التطبيقات. يتضمن التحليل في هذه الطبقة تحليل حزم الشبكة وتنبيهات؛

- **تحليل الذاكرة:** تحليل طبقة الذاكرة التجريدية، والتي تترجم ببايتات وسائط الذاكرة إلى العمليات وبيانات النظام. يتضمن التحليل في هذا المجال تحديد الكود الذي كان قيد التشغيل واستخراج البيانات الحساسة التي لم يتم تخزينها في مكان آخر " (1).

يتعين أن تكون عملية الفحص من قبل أولئك المدربين خصيصا لهذا الغرض (2)، وهم محلي الطب الشرعي الرقمي الذين يمكن تعريفهم على أنهم: (مجموعة خبراء يتمتعون بمهارات تقنية عالية)، ف خبراء الطب الشرعي الرقمي عادة ما يكون لديهم معرفة قوية في مجموعة واسعة من أجهزة الكمبيوتر والشبكات والبرامج وأنظمة التشغيل (3)، كما عليهم أيضا أن يكون على دراية كافية بالمعارف القانونية وأن يكون في الوقت نفسه على قدر من الإلمام والبراعة في التحقيق ومعرفة مستفيضة في مجال تقنية المعلومات (4).

لكن مع هذا التطور المهيول في مجال الأجهزة الإلكترونية فإنه من الصعب مواكبتها، إذ أن الكثير من الوكالات لا تمتلك خبيرا في الأدلة الرقمية، وإن وجد فإنه يكون متخصصا في الهواتف المحمولة لا في غيرها، وقد يكون قادرا على تسجيل الدخول والبحث ولكنه مع ذلك لا يملك القدرة على النقاط سجلات الرسائل النصية للهاتف الخليوي ويمكن أن يدمر الأدلة بمجرد المحاولة، أما المعتمدين منهم فرغم أنهم محققون يملكون الكفاءة والخبرة المواتية والملائمة في مجال التحقيق الرقمي ولاسيما في استخلاص الأدلة الحساسة بشكل صائب وملائم، إلا أنه لا يوجد هيئة تصديق واحدة تصادق على كفاءتهم (5).

وعدم التصديق على الكفاءة يثير العديد من الإشكاليات القانونية، إذ يمكن رد نتائج التحليلات الجنائية الرقمية من قبل المتهم متعللا بعدم وجود وثيقة أو تصديق على مدى كفاءة المحلل أو الطبيب الشرعي الرقمي، كما يمكن للمتهم أيضا طلب خبرة مضادة، أو دعنا نسمة هنا طلب

(1) Brian CARRIER, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence, Volume 1, Issue 4, UTICA COLLAEGE, Winter 2003, PP.01-12: <https://www.utica.edu/search-results?q=International%20Journal%20of%20Digital%20Evidence>

(2) A Simplified Guide To Digital Evidence, National Forensic Science Technology Center, Ibid.

(3) Jonathan A. MATUSITZ, Op.cit. P.149.

(4) محمد الأمين البشري، المرجع السابق.

(5) A Simplified Guide To Digital Evidence, National Forensic Science Technology Cente, Op.cit.

تحليل رقمي مضاد، وهذا سيكون له أثر كبير على مسار الدعوى، لأن معايير المحللين الرقميين مختلفة، والترجيح بين محللين على أساس الكفاءة أمر صعب في غياب جهاز أو هيئة تصديق.

3- مرحلة العرض:

يختصر مضمون هذا الإجراء في استعراض وإحالة ما تمخض عن عملية التحقيق والفحص والتحليل من نتائج أمام الجهات القضائية المختصة، والتي يجب أن تكون وفق القواعد الجنائية التي يملها النظام الجنائي المعمول به في الولاية القضائية المعنية، وفي ذلك، يجب أن تكون الأدلة المقدمة موثوقة ومصادقة وبنفي عنها الشوائب والعيوب، فالتوثيق يسمح من التأكد من مصداقية الأدلة ويمنح أيضا المصادقية في إعادة تشكيل مسرح الجريمة، فالتوثيق هو جانب من جوانب إجراءات حفظ الأدلة إلى غاية نهاية المحاكمة⁽¹⁾، فالأدلة الرقمية تكون موثوقة إذا كان بالإمكان إقناع المحكمة بأن الأدلة الرقمية:

- " لم تتعرض للتبديل أو التغيير في محتواها ومضمونها.
- كل المعلومات الواردة فيها من المصدر المدعى.
- وجود بيانات وصفية مترابطة، كأن تكون الطوابع الزمنية (timestamps)⁽²⁾ دقيقة ومضبوطة وغير متغيرة.
- إذا كان ممن الممكن معها تحقيق مستوى ضروري من المصادقة من خلال الأدلة الشفوية أو أي ظرف آخر، أو من خلال ميزات تكنولوجيا أخرى يمتاز بها النظام أو السجل"⁽³⁾.
- "كما يمكن أيضا تطبيق معايير دوبيرت ومضمون القاعدة 702 المتعلقة بشهادة الشهود الخبراء في هذا الشأن، وتتضمن الأجزاء الأربعة من اختبار موثوقية دوبيرت؛
- إجراء قابل للتكرار؛
- معدل الخطأ معروف أو قابل للمعرفة في الإجراء؛
- نشر الإجراء بعد استعراضه؛

(1) سيدي محمد لبشير، المرجع السابق، ص 74.

(2) الطوابع الزمنية: تعرف في اللغة الإنجليزية بـ (timestamps) أما في اللغة الفرنسية فيطلق عليها اسم (Horodatage): وهي: (آلية تتكون من ربط تاريخ ووقت بحدث أو معلومات أو بيانات، الغرض منه بشكل عام هو تسجيل اللحظة التي أجريت فيها العملية): الموسوعة الحرة، ويكيبيديا: Horodatage: <https://fr.wikipedia.org/wiki/Horodatage#:~:text=La%20valeur%20repr%C3%A9sentant%20la%20date,ou%20tout%20s%20impl%C3%A9ment%C2%AB%20horodatage%20%C2%BB>.

(3) Saleem SHAHZAD, Op.cit. P.24.

- قبول الزملاء للإجراء العلمي المستخدم ولتقديم الأدلة أو كشفها " (1).
أما القاعدة 702 من قواعد الإثبات الفيدرالية فتتضمن ما يلي: (يجوز للشاهد المؤهل كخبير من خلال المعرفة أو المهارة أو الخبرة أو التدريب أو التعليم أن يدلي بشهادته في شكل رأي أو غير ذلك إذا:

- أ- المعرفة العلمية أو التقنية أو غيرها من المعرفة المتخصصة للخبير ستساعد في إظهار الحقيقة لفهم الأدلة أو لتحديد الحقيقة في قضية
- ب- تستند الشهادة إلى حقائق أو بيانات كافية؛
- ج- كانت الشهادة نتاج مبادئ وأساليب موثوقة؛ و
- د- قام الخبير بتطبيق المبادئ والأساليب بشكل موثوق على وقائع القضية (2).

الفرع الثالث: تحديات الطب الشرعي الرقمي:

تعد علوم الطب الشرعي الرقمي من العلوم التقنية المعقدة مما ينتج عنه إشكاليات وتحديات مختلفة متعلقة بطبيعته التقنية كما أن جدته وحدائته وطبيعته الساحات التي يتم وظيفه بالإضافة إلى الموارد المالية التي يتطلبها فيه قد ترتب عنه العديد من الإشكالات والتحديات الوظيفية (أولاً)، ولا شك في أن كل هذه الخصائص والميزات والتحديات التي تحوم حول هذا التخصص الجنائي الحديث قد أربك جهاز القضاء ودوائر التحقيق وأثار العديد من الإشكالات القانونية (ثانياً).

أولاً: التحديات التقنية والتنظيمية:

يوجه خبراء الطب الشرعي الرقمي تعقيدات وتحديات تقنية حين قيامهم بما أنيط لهم من مهام التحقيق في الجرائم الإلكترونية، كما أن الطب الشرعي عموماً يعاني من العديد من التحديات التنظيمية من نقص للموارد والمعارف والخبراء في مجال الطب الشرعي الرقمي:

(1) Gary Craig KESSLER, Judges' Awareness, Understanding, and Application of Digital Evidence, A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, Graduate School of Computer and Information Sciences, Nova Southeastern University, Florida, 2010, P.17.

(2) Federal Rules of Evidence Rule 702. Testimony by Expert Witnesses, legal i,formation institute, cornelle law school, Accessed on 09/08/2020 at 15:55h, in: https://www.law.cornell.edu/rules/fre/rule_702:

(A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if: (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the expert has reliably applied the principles and methods to the facts of the case.)

أ- التحديات التقنية: مكافحة الطب الشرعي الرقمي (Anti-digital Fronsacs):

إن عملية الحصول على أدلة من الشبكات الاجتماعية عبر الإنترنت تعتبر عملية مثقلة بالتحديات، فالمجرمون يلجؤون إلى استخدام تقنيات مضادة للطب الشرعي الرقمي من أجل العمل على إخفاء الأدلة وحجبها، أو لإلهاء عملية التحقيق⁽¹⁾.

وتعرف مكافحة الطب الشرعي الرقمي على أنها: (محاولات للتأثير سلبيًا على وجود، وكمية، و/ أو جودة الأدلة من مسرح الجريمة، أو تجعل فحص الأدلة صعبًا أو مستحيلًا)⁽²⁾، مكافحة الطب الشرعي الرقمي إذن يتجلى في تلك الأساليب الفنية أو التقنية التي يمكن من خلالها إحداث تأثير في الأدلة الرقمية بحيث تكون غير قادرة على الاحتفاظ بإصالتها وبذلك حجبتها كأدلة موثوقة أمام الجهات القضائية.

تتنوع الطرق التي يتم من خلالها استهداف عمليات تحقيق الطب الشرعي الرقمي ويمكن اختصارها في الآليات الأساسية التالية:

أ- إخفاء البيانات:

ويكون ذلك من خلال عملية التشفير، والتشفير -كما أشرنا إليه سابقاً- هو عملية ترميز المعلومات، وتعتبر عملية فك التشفير من العمليات التي تحتاج الكثير من الوقت، وفي بعض الأحيان تعد عملية مستحيلة وغير مجدية⁽³⁾، فالمجرمون يلجؤون إلى العديد من طرق التشفير المختلفة، ومن أجل العمل على جعل البيانات قابلة للاستخدام والاستدلال يتعين على المحققين وخبراء الطب الشرعي الرقمي أن يفكوا التشفير عنها، وهذه العملية قد تستغرق وقتًا طويلاً وفي بعض الأحيان قد تكون غير مجدية بالمرّة كما ذكرنا⁽⁴⁾.

ولأن أشكال التشفير متعددة ومتفرعة فإنها يمكن أن تقع على النظام أو على الأجهزة الطرفية للنظام، أو على البيانات المختلفة، ويعتبر التشفير الواقع على القرص من أهم الفئات وأكثرها حيوية، بحيث يمكن تشفير الحجم الكامل لمحركات الأقراص الثابتة، كما أن النمو الكبير في

(1) Bandr FAKIHA, Digital Forensics: (Crimes and Challenges in Online Social Networks Forensics), Journal of the Arab American University, volume 06, issue 01, American University-Jenin, Palestine 2020, PP: 15-33:

<https://www.aaup.edu/Research/Journals/journal-arab-american-university/Archive/Volume-6/Issue-1/2020/digital-forensics-crimes-and-challenges-online-social-networks-forensics>

(2) Gary C. KESSLER, Anti-Forensics and the Digital Investigator, 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western, Australia, December 3rd 2007: <https://ro.ecu.edu.au/adf/1/>

(3) Bandr FAKIHA, Ibid.

(4) David MUGISHA, digital forensics: (Digital Evidence in judicial System), International Journal of Cyber Criminology, volume 04, march 2019:

https://www.researchgate.net/publication/332245703_DIGITAL_FORENSICS_Digital_Evidence_In_Judicial_System

البيانات التي ينتجها المستخدم قد ينتج عنها نمو في زيادة اللجوء إلى استعمال قواعد البيانات لتخزينها، وبالتالي فإن تشفير هذه القاعدة يعد مظهر من مظاهر إخفاء البيانات، كما يمكن أن نضم في دائرة التصنيف الموسع لإخفاء البيانات؛ عمليات تشفير المجلدات والملفات وتشفير البريد الإلكتروني والتطبيقات والخدمات السحابية والقرص المحمول وجهاز المحمول⁽¹⁾، وما إلى ذلك.

هناك آليات أخرى لإخفاء البيانات، إذ يمكن إخفاؤها في مساحة الركود والمساحات غير المخصصة على محركات الأقراص الثابتة، بالإضافة إلى البيانات الوصفية للعديد من أنواع الملفات، كما يعتبر أيضا سجل التمهيد الرئيسي (MBR)، وسجلات وجدول برامج تشغيل الجهاز المخصصة غير المستخدمة، ومناطق النظام المحمية، والأقسام المخفية، على محركات الأقراص الثابتة أماكن أخرى يمكن إخفاء المعلومات فيها، وهناك غيرها من الأماكن الأخرى التي لا يسع المقام بذكرها، ومع ذلك هناك إمكانية العثور على كل هذه البيانات بواسطة أدوات الطب الشرعي وتوفر محلل ماهر ومتقن، ولكن يعد ذلك أمر صعب، ويصعب معها أمر شرحها لغير المتخصصين في المجالات التقنية⁽²⁾.

ب- مسح وإتلاف الآثار:

وهو التدمير الكلي والكامل للبيانات التي يمكن الاستناد إليها واستخدامها كأدلة، وهناك كميات هائلة وعدد كبير من البرامج التي يمكن أن يتم توظيفها من أجل العمل على مسح أشكال وصور متعددة من البيانات، وقد ثبت أن هناك عدد كبير من الأدوات والآليات التي أدت إلى أكثر من شكل واحد من أشكال المسح⁽³⁾.

وهذه الأدوات كانت أدوات موجودة من ذي قبل، وهي تعمل من خلال إجراء عمليات الكتابة المتعددة التي تجعل أي استرجاع غير ممكن إن لم يكن مستحيلا، فهذه الأدوات يمكنها أن تصعب أكثر عملية التحليل على فاحصي الطب الشرعي الرقمي، غير أن هذه البرامج ليست عظيمة ونموذجية، فمعظمها كثيرا ما يخلف وراءه آثارا هو الآخر، وغالبا ما تترك وراءها بقايا الأشياء التي من المفترض حذفها⁽⁴⁾، وقد تخلق عملية التدمير نفسها دليلا، إذا يمكن أن تؤدي عملية الكتابة

(1) Kevin CONLAN , Ibrahim BAGGILI, Frank BREITINGER, Anti-forensics: (Furthering digital forensic science through a new extended, granular taxonomy), DFRWS USA 2016 d Proceedings of the 16th Annual USA Digital Forensics Research Conference, Digital Investigation, Volume 18, Supplément, 7 août 2016, Pages S66-S75: <https://www.sciencedirect.com/science/article/pii/S1742287616300378>

(2) Gary C. KESSLER, Op.cit.

(3) Kevin CONLAN , Ibrahim BAGGILI, Frank BREITINGER, Ibid.

(4) Gary C. KESSLER, Op.cit.

فوق الملف إلى محو الملف كلياً أو جزئياً، ولكن البرنامج المستخدم لإجراء المسح قد يؤدي إلى إنشاء أدلة إضافية⁽¹⁾.

ج- تشويش المسار:

التشويش على المسار هو نشاط مقصود لإرباك التحقيق الجنائي على نظام رقمي أو شبكة إلكترونية محددة⁽²⁾ من خلال التعطيم، أو هجمات رفض الخدمة وغيرها، وترمي مثل هذه الهجمات في الغالب إلى هدم موثوقية الأدلة التي تم تجميعها أو لتدميرها كلياً⁽³⁾، ومن المحتمل جداً أن تزداد أنشطة التعطيم على المسار أو التشويش عليها مع تزايد النشاطات الإجرامية على ساحة الفضاء الإلكتروني، ومرد ذلك إلى محاولة أصحاب تلك الأنشطة غير المشروعة والإجرامية التخفيف من البصمات والآثار التي يخلّفونها والتي توفر أدلة تدينهم على جرائمهم، وقد يتم اللجوء إلى الأدوات والتقنيات المتاحة لهم لإرباك المحققين وتضليلهم⁽⁴⁾.

د- الهجمات ضد أدوات الطب الشرعي الرقمي:

تعد الهجمات المباشرة على سير عمليات التحليل الجنائية الحاسوبية من أكثر الهجمات حداثة وأكثرها تهديداً للطب الشرعي الرقمي⁽⁵⁾، فالهجوم المباشر على البرامج التي يتم استخدامها في التحقيق الجنائي الرقمي وكذلك تلك التي تستهدف العمليات التي يتم إجراؤها خلال عملية التحقيق الجنائي تمثل أكثر النشاطات تدميراً للتحقيق والأدلة التي تتمخض عنه، حيث يتم استخدام حزم البرامج لإعاقة عملية الطب الشرعي، واللجوء أيضاً إلى الهندسة العكسية لتشتيت محاولات المحللين لاستخراج الأدلة من المخلفات التي تركها المجرمون والإرهابيون خلفهم، كما تستهدف عمليات الهجوم ضد أدوات الطب الشرعي الرقمي نزاهة المحققين أو المنظمات التي أنيط بها التحقيق القانوني في مثل هذه المسائل والقضايا المتعلقة بمجال الفضاء الإلكتروني⁽⁶⁾.

ومع ذلك يمكن التقليل من هذه الهجمات، وذلك من خلال تقادي استخدام برنامج واحد فقط من برامج الطب الشرعي الرقمي، فيتعين إذا الاعتماد على مجموعة متنوعة ومتعددة من البرامج التي يتم اعتمادها في عمليات التحقيق الجنائي الرقمي، لكن الصعوبة هنا أنه من غير اليسير

(1) Ryan HARRIS, Arriving at an anti-forensics consensus: (Examining how to define and control the anti-forensics problem), Digital Investigation, Volume 3, Supplement, September 2006, PP. 44-49:

<https://www.sciencedirect.com/science/article/pii/S1742287606000673>

(2) Kevin CONLAN , Ibrahim BAGGILI, Frank BREITINGER, Op.cit.

(3) Bandr FAKIHA, Op.cit.

(4) Kevin CONLAN , Ibrahim BAGGILI, Frank BREITINGER, Ibid.

(5) Gary C. KESSLER, Ibid.

(6) Kevin CONLAN , Ibrahim BAGGILI, Frank BREITINGER, Op.cit.

تشجيع الإدارات على هذا الاستخدام المتنوع، ذلك أنها برامج باهظة الثمن، ونقص التمويل يحول دون ذلك، كما يمكن التخفيف من هذه الظاهرة التي تستهدف أدوات الطب الشرعي الرقمي من خلال جعل هذه الأدوات أكثر فاعلية وأحسن دقة حل استخلاص الأدلة الرقمية (1).

1- التحديات التنظيمية:

تعاني الدول من نقص كبير في خبراء الطب الشرعي الرقمي إذ من النادر أن تجد تعادلا بين الدول وتكافؤا في توفر المتخصصين والخبراء في هذا المجال، بل قد يصل عدم التكافؤ إلى داخل البلد الواحد، كما هو الحال في الدول الفيدرالية التي فوارق كبيرة بين المقاطعات الفيدرالية وبين الدولة المركزية، وإضافة إلى نقص الخبراء فإن هناك أيضا نقصا في مستلزمات وأدوات وعتاد الطب الشرعي الرقمي، وإذا نظرنا إلى الوقت فإن التأخر سمة بارزة في التحديات التي تواجه هذا المجال نظرا الحجم الهائل للبيانات التي يجب تحليلها (2).

ثانيا: التحديات القانونية:

تشكل القواعد القانونية المتعلقة بالاختصاص الإقليمي تحديا وعائقا كبيرا أمام أجهزة التحقيق التي تعمل على بناء الأدلة الإلكترونية على الجرائم التي ترتكب على الساحة السيبرانية، كما يمثل التباين في القوانين والتشريعات القائم بين مختلف الدول وما تتطلبه من شروط للموافقة والتصديق على الأدلة وبعض الإجراءات المتعلقة بالتفتيش عبر الحدود عقبة وعرقلة كبيرة لضبط مثل الصنف من الجرائم التي تتخطى حدود الدول (3).

تثير الأدلة الرقمية مشكلات كبيرة حول السلطة التقديرية لقبولها أمام القضاء الجنائي كأدلة يمكن التعويل عليها لتكوين قناعة القاضي الجنائي، فبلوغ اليقين القضائي في وقوع الجريمة الإلكترونية وإسنادها إلى المتهم ليست كما هي عليه في الأدلة التقليدية، ففي مثل هذه الأدلة يتطلب الأمر معرفة علمية خاصة للقاضي بما يتعلق بالمجال المعلوماتي، وجهل القاضي بمثل هذه العلوم والمعارف قد يفضي تبعا إلى التشكيك في القيمة الثبوتية للدليل الرقمي مما يربط إفلات المجرمين من العقاب (4)، ولا يتطلب الأمر أن يصبح القضاة خبراء في الطب الشرعي للكمبيوتر

(1) Ryan HARRIS, Op.cit.

(2) voir: Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, Op.cit.

(3) أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، جامعة نايف

العربية للعلوم الأمنية، نوفمبر-ديسمبر 2013، ص: 85-132: <https://repository.nauss.edu.sa/handle/123456789/53578>

(4) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي: (دراسة مقارنة)، رسالة ماجستير في الحقوق، كلية الحقوق،

جامعة الإسكندرية، 2009، ص 181.

وتكنولوجيا المعلومات والاتصالات ولكن الأمر يحتاج فعلا إلى معرفة عامة كافية حتى يفهموا التفاصيل الدقيقة وفروقاتها عندما تقدم أمامهم الأدلة الرقمية (1).

تشكل الطبيعة المتقلبة للأدلة الرقمية مشكلة كبيرة قادحة في أصالتها، فإذا تمت استعادة دليل رقمي معين من ذاكرة الوصول العشوائي -على سبيل المثال- فإن ذلك سيكون مجرد شكل سريع للنظام يتم التقاطه في ظرف زمني محدد، فالمحتوى الموجود في ذاكرة الوصول العشوائي لا يتسم بالثبات بل بالاستمرارية، ولن تترك شيئا أصليا يمكن مقارنة الأدلة المستعادة به للتأكد من صحتها، والأصالة التي نتحدث عليها هنا هي توافق البيانات المسترجعة مع البيانات الأصلية (2).

تبرز أيضا مشكلة أخرى تتعلق بالتقارير التي تتمخض عن عمليات التحقيق في الفضاء الإلكتروني لغياب المعايير التي تكون ضابطا لإعداد التقارير حول الأدلة وأدوات توثيقها، فيمكن أن تكون تلك التقارير على قدر كبير من الاختلاف فيما بينها، ويعود هذا الأمر إلى أن خبراء الطب الشرعي الرقمي كثيرا ما يستعملون أثناء أداء مهامهم العديد من الوسائل والأساليب والتقنيات المختلفة، وبشكل خاص عندما يرمون التحقق من النتائج التي توصلوا إليها، وهذا ما ينتج عنه اختلاف في تحديد عناصر الأدلة الرقمية، فعدم وجود معايير في وظيفة إعداد التقارير الخاصة بأدوات الطب الشرعي الرقمي قد يؤدي إلى إعاقة عملية التحقيق في جهاز الكمبيوتر إذا كانت الأدوات المستعملة مختلفة، قد توجه صعوبات في دمج عناصر الأدلة التي تولدت عن تقارير البرامج في التقرير الرسمي للتحقيق الذي سيقدم للمحامين أو للعملاء (3).

(1) Gary Craig KESSLER, Op.cit. P.131.

(2) Saleem SHAHZAD, Op.cit. P.23.

(3) Hamda BARIKI, Mariam HASHMI, and Ibrahim BAGGILI, Defining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools, Digital Forensics and Cyber Crime: (Second International ICST Conference Abu Dhabi, United Arab Emirates, October 4-6, 2010) Volume Editor: Ibrahim Baggili, Springer Heidelberg Dordrecht London NewYork, 2011, PP.78-95.

المبحث الثاني:

الاستراتيجية الوقائية لحماية الفضاء الإلكتروني

تتقاطع صور وأشكال الإجرام السيبراني في نقطة محورية واحدة، وهي الأسلحة التي يتم اللجوء إليها وتوظيفها لتنفيذ هجمات على الفضاء الإلكتروني وتشكيل تهديد بأمنه وسلامته، لذلك نجد أن غالبية الأساليب المعتمدة والمعمول عليها في مواجهتها تكون على قدر كبير من التماثل، فما يصلح لمواجهة الجرائم السيبرانية العادية يكون كذلك صالحا لمواجهة الإرهاب الإلكتروني كونه مندرجا في دائرتها، فهو يتضمن تعاملًا بالجانب الفني والتقني واللجوء إلى استعمال أسلحة مضادة تقارع بها وتجاله تلك التي يستعملها المهاجمون (المطلب الأول).

كما يتقاطع الإرهاب الإلكتروني مع الإرهاب التقليدي في إمكانية اللجوء إلى عمليات وأنشطة إرهابية تقليدية يتم من خلالها استهداف الأصول المادية التكوينية للفضاء الإلكتروني وذلك بغية الإيقاع به في بؤرة من انعدام الأمان وبث الرعب والترهيب من خلال ذلك، وفي هذه الحالة فإن حماية الأصول المادية تعد جانباً مهماً وأساسياً من جوانب عمليات وخطط تأمين الفضاء الإلكتروني، وعادة ما تكون هذه الخطط مترامنة مع الحماية التقنية والفنية لهذا الفضاء، ومطابقة إلى حد كبير للخطط والاستراتيجية والسياسات الأمنية التي يضعها مهندسو الأمن لحماية المنشآت الاستراتيجية والحيوية الأخرى (المطلب الثاني).

المطلب الأول:

ديناميكيات التأمين التقني للفضاء الإلكتروني

سلف في موضوع بحثنا التطرق إلى الطبقة التكوينية للفضاء الإلكتروني، وبرز لنا من خلالها أن أهم طبقة مكونة منها تتسم بطابعها العلمي والتقني والفني، وأن الهجمات الإرهابية عليه أو من خلاله تكتسي إلى حد كبير نفس الطبيعة التي يكتسها هذا الفضاء، ومن أجل ذلك، فقد تضمن معظم السياسات والاستراتيجية المتعلقة بتأمين الفضاء الإلكتروني إلى ضرورة تطوير الجانب التقني في التصدي لمثل تلك الهجمات والتهديدات، فكان التشفير من بين أهم تلك التقنيات التي طورت لحماية الفضاء الإلكتروني (الفرع الأول)، كما تلعب جدران الحماية بمرافقة برامج مكافحة الفيروسات دوراً مهماً في تفصيد وغل يد الإرهابيين عن بلوغ منيتهم من وراء هجماتهم على الفضاء الإلكتروني (الفرع الثاني)، ليس هذا فحسب، بل وضعت آليات الحجب والمراقبة الإلكترونية للبيانات لمنع ورصد التهديدات التي تحوم حول هذا الفضاء (الفرع الثالث).

الفرع الأول: التشفير:

منح التشفير أو علم الكريبتولوجيا أهمية كبيرة منذ زمن بعيد، فتاريخ التشفير ضارب في أعماق التاريخ، إذ كان يمثل الآلية المثالية التي تتبرقع تحتها المعلومات لضمان سريتها وسلامتها، وفي ظل المجتمع حرب المعاصر الذي يطغى عليه الطابع المعلوماتي والتقني في آن واحد أصبح من الضروري أن يكون التشفير من بين الأدوات الأساسية التي تضمن حماية الفضاء الإلكتروني من الهجمات الإرهابية (أولا)، وهذا ما دعا إلى تطويره واختلاق عدة أنواع منه ليكون أكثر كفاءة وفاعلية (ثانيا).

أولا: تعريف عملية التشفير:

تعود عملية التشفير من الأساليب القديمة التي يعود تاريخها إلى ألفي سنة قبل الميلاد، حيث تم استخدامها من قبل الفراعنة إذا تم العثور على كتابات سرية بالخط الهيروغليفي، كما تم توظيفها أيضا من قبل يوليوس قيصر في رسائله الموجهة إلى شيشرون، كما كتب جزء دليل "استواء الكواكب" لصاحبه جيفري تشوسر بشكل مشفر، كما استعمل أيضا من قبل الملكة ماري الإسكتلندية (1).

تعاظم شأن التشفير مع ظهور النزاعات والملاحم التي سعي فيها كل طرف من أطرافها إلى حماية سرية الاتصالات والمراسلات العسكرية، ولعل ظهور الحاسب الآلي كان يعتبر بمثابة الآلية الحديثة للاتصالات الآمنة، ولهذا استأثرت الدول في الستينات بحقوق التشفير وفكه، ومع أواخر الستينات قامت شركة (IBM) بتكوين فريق بحث متخصص في مجال التشفير والذي وصل إلى تطوير أنظمة التشفير مستحدثة، الأمر الذي أبرز أهمية توفر معايير لعملية التشفير، ثم بعد ذلك، وفي سنة 1973 قام المعهد الوطني للمعايير والتكنولوجيا بتطوير المعيار الذي يعتمد على مفتاح تشفير بطول (56 Bits) ثم تم تطوير نظام آخر وهذا سنة 1986، ويتسم هذا النظام بالكفاءة العالية واستعصائه عن الاختراق، ولما كان الفضاء الإلكتروني في أيامنا هذه الآلية التي يتم من خلالها تناقل المعلومات، فإنه يتعين القيام بذلك بالصيغ المشفرة خاصة فيما يتعلق بالمعلومات الحرجة ضمانا لسلامتها وحمايتها ممن يستهدفها (2).

(1) أنظر في ذلك: هال أبلسون، هاري لويس، كين ليدين، الطوفان الرقمي: (كيف يؤثر على حياتنا وحررتنا وسعادتنا)، ترجمة: (أشرف عامر)، مؤسسة هنداوي للتعليم والثقافة، مصر، 2014، ص ص: 232-237.

(2) سعيدي عزو وخالد رامول، الأمن التقني للدفع الإلكتروني أي فعالية؟، مجلة معالم للدراسات القانونية والسياسية، المجلد 01، العدد 02، المركز الجامعي، تندوف، ديسمبر 2017، ص ص: 112-129: <https://www.asjp.cerist.dz/en/article/69283>

يدور معنى أي نوع من أنواع أنظمة التشفير حول مفهوم ستر وتعتيم وحجب المعلومات التي تتسم بالسرية بشكل يمكنها من الظهور في صورة لا يمكن معها فهم ما تتضمنه لكل من لا يملك إذنا بالاطلاع عليها، ويتمثل الاستعمال الأكثر ذيوعا وانتشارا لها في عمليتين؛ العملية الأولى تتمثل في حفظ المعلومات بشكل آمن ضمن ملفات داخل الحاسب الآلي، وأما العملية الثانية فتتضمن في نقل وتحويل هذه المعلومات من خلال قنوات غير آمنة كالإنترنت، والجدير بالإشارة إليه، أن عملية التشفير لا تقوم بحظر بلوغ الأشخاص الذين لا يملكون تصريحاً إلى تلك المعلومات، وإنما تقم بتعميتها بحيث لا يمكن إدراك مضمونها⁽¹⁾، فحتى عند وصول أي شخص لتلك المعلومات فإنه لن يتمكن من إدراك معنى ومضمون الرسالة إلا بعد فك شفرتها التي لا تكون متاحة له.

ويتكون التشفير كنظام متكامل من عدة عناصر، أولها "النص الأصلي" وهو النص المفهوم والذي يراد تعتيمة لحفظ سرية، وعنصر "التشفير" والذي هو الوسيلة أو الآلية التي يتم من خلالها تعتيمة النص الأصلي، ثم يأتي العنصر الثالث والمعروف باسم "النص المشفر" أو "بيان التشفير"، وهو النص الذي تم تعتيمة من النص الأصلي، أما العنصر الرابع فيطلق عليها اسم "خوارزمية التشفير" وهو الوسيلة أو الصيغة المنطقية التي يتم اعتمادها في عملية التشفير، وفي الغالب يتم تركيب الخوارزمية بالشكل الذي تتضمن فيه مفتاحاً للتشفير والذي يشكل المعبر، وتتضمن أيضاً الرسالة، كما تتضمن الخوارزمية أيضاً على مفتاح لفك التشفير الذي من خلاله يتم رفع العتمة على هذه الرسالة المشفرة وهذا متى كان مناسباً لذلك⁽²⁾.

يعرف التشفير في علم اللغة على أنه: (... اللغة التي نستعملها حتى نتواصل مع الآخرين، لنتعرف على نظام اتفاقي من قوانين تسمح بالإنتاجية وفهم النص، إذ التشفير هو جرد للرموز متبوعة بمجموعة من القواعد التي تخص نظام الكلمات المشفرة، وغالبا تكون موضوعية بموازاة القاموس... بينما إن كانت اصطلاحية مشتقة فإنها تتجاوز القاموسية إلى مرحلة إيحائية)⁽³⁾.

أما اصطلاحاً فتعرف عملية التشفير على أنها: (تكنولوجيا استعمال خوارزميات رياضية معقدة لتشفير وفك تشفير البيانات وهذا بهدف ضمانا لسرية التي تستلزمها المعلومات بقصد

(1) فريد بابير وشون ميرفي، علم التشفير: (مقدمة قصيرة جدا)، ترجمة (محمد سعد طنطاوي)، الطبعة الأولى، مؤسسة هندواي للتعليم والثقافة، القاهرة، مصر، 2016، ص 15.

(2) المرجع نفسه، ص 15.

(3) عائدة حوشي، التشفير والما وراء لسانية في رواية: (التفكيك) - رشيد بوجدر، الملتقى الوطني الأول حول: النقد الأدبي الجزائري، 21-22 ماي 2006، موقع جامعة المسيلة: <http://dspace.univ-msila.dz:8080/xmlui/handle/123456789/13643>

تأمين المعاملات بين الزبون على الخط والتاجر أو البنك بقصد حصر قراءتها والاطلاع عليها على المعنيين الشرعيين لهذه العملية⁽¹⁾.

كما يعرف التشفير أيضا على أنه: (عملية دمج المعلومات في شفرة سرية غير مفهومة ثم فك هذه الشفرة بعد وصولها إلى وحدة الويب الآمنة، أي أن الشفرة هو استبدال مستند أو رسالة باستخدام برنامج معين، ولهذا تنطوي عملية التشفير على تحويل النصوص البسيطة إلى رموز (حروف، أرقام، إشارات) قبل إرسالها إلى مستقبلها شريطة أن يكون لهذا الأخير القدرة على حل الشفرة وتحويل الرسالة إلى صيغتها الأصلية باستخدام مفتاح التشفير)⁽²⁾.

وذهب بعض الفقه في تعريف التشفير على أنه: (عملية تحويل النص إلى رموز وإشارات غير مفهومة تبدو ذات غير معنى لمنع الغير من الاطلاع عليها إلا الأشخاص المرخص لهم بالاطلاع على النص المشفر وفهمه، فتتصب عملية التشفير على القيام بتحويل النصوص العامة إلى نصوص مشفرة مع إمكانية إعادة النص المشفر إلى نص عادي بعد فك التشفير بمفتاح التشفير الذي تم إنشاؤه للتشفير وفكه)، كما ذهب البعض الآخر إلى النظر إلى التشفير من زاويته التقنية فتم تعريفه على أنه: (أن التشفير أو الترميز أو الكتابة المشفرة هو تقنية قوامها خوارزمية رياضية ذكية، تسمح لمن يمتلك مفتاحا سريا بأن يحول رسالة مقروءة إلى رسالة غير مقروءة وبالعكس، أي أن يستخدم المفتاح السري بفك الشفرة وإعادة الرسالة المشفرة إلى وضعيتها الأصلية)⁽³⁾.

وعرفه البعض الآخر على أنه: (عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز، بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء، لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف، ويهدف التشفير إلى منع الغير من التقاط الرسائل أو المعلومات ومن ثم منع وصولها مشوهة للطرف الآخر في المعاملة التجارية على نحو يعرقل هذه التجارة)⁽⁴⁾.

(1) سعيدي عزو وخالد رامول، المرجع hgshfr.

(2) مصطفى بوعقل، آليات وقاية المعاملات الإلكترونية في ظل حوكمة تكنولوجيا المعلومات، مجلة دفاتر MECAS، المجلد 12، العدد 01،

جامعة أو بكر بلقايد، تلمسان، جوان 2016، ص ص: 380-396: <https://www.asjp.cerist.dz/en/article/8799>

(3) محمد عقوني وإبراهيم بلمهدي، الآليات التقنية والقانونية لحماية التوقيع الإلكتروني، مجلة الفكر، المجلد 14، العدد 01، جامعة محمد خيضر،

بسكرة، فيفري 2019، ص ص: 300-313: <https://www.asjp.cerist.dz/en/article/76577>

(4) حكيم نشاد، المستهلك الإلكتروني وآليات حمايته في عصر الاقتصاد الرقمي، مجلة البحوث القانونية والاقتصادية، المجلد 01، العدد 02،

المركز الجامعي، أفلو، جوان 2018، ص ص: 209-223: <https://www.asjp.cerist.dz/en/article/71955>

أما من الناحية التشريعية، فقد عرفه المشرع التونسي في المادة 05/02 من قانون المبادلات الإلكترونية على أنه: (التشفير: إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تميرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها) ⁽¹⁾.

أما المشرع العماني فيعرف التشفير على أنه: (عملية تحويل نص بسيط أو وثيقة نصية أو رسالة إلكترونية إلى رموز غير معروفة أو مبعثرة يستحيل قراءتها أو معرفتها بدون إعادتها إلى هيئتها الأصلية) ⁽²⁾.

في حين يعرفه المشرع السوداني على أنه: ("التشفير" يقصد به استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إليها من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها) ⁽³⁾.

أما المشرع الفرنسي فيرى أن التشفير يقصد به: (...جميع الخدمات التي تهدف من خلال استعمال اصطلاحات سرية إلى تحويل معلومات أو إشارات واضحة إلى معلومات أو إشارات غير مفهومة لطرف ثالث، أو تنفيذ عملية معاكسة، من خلال استخدام وسائل مادية أو برامج مصممة لهذا الغرض، يقصد بوسيلة التشفير كل وسيلة جهاز أو برنامج تم تصميمه أو تعديله لنفس الغرض) ⁽⁴⁾.

وخلاصة لذلك؛ فإن التشفير لا يعبر في جوهره ومعناه إلا على كونه كتابة باستعمال الرموز، وسهولة أو صعوبة اختراق التشفير تقف بشكل أساسي على مدى تعقيد هذه الرموز، وقد ثبت جليا ما للتشفير من فوائد جمة وأهمية بالغة في تأمين مواقع الإنترنت التي تتسم بالحساسية، كتلك

(1) المادة 05/02 من القانون عدد 83 لسنة 2000، مؤرخ في 09 أوت 2000، يتعلق بالمبادلات والتجارة الإلكترونية، ر.ر.ج.ت عدد 64، 11 أوت 2000، ص 2084.

(2) المادة 26/01 من مرسوم سلطاني رقم 2008/69، بإصدار قانون المعاملات الإلكترونية، صدر ب 17 مايو 2008، ج.ر. عدد 864 لسنة 2008.

(3) المادة 03/02 من القانون رقم 11 لسنة 2007، يتعلق بقانون المعاملات الإلكترونية، صدر بتاريخ 14 جوان 2007.

(4) Article 28/01 de la Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, Modifié par [Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 \(V\) JORF 22 septembre 2000 en vigueur le 1er janvier 2002](#), Abrogé par [Loi n°2004-575 du 21 juin 2004 - art. 40 \(V\) JORF 22 juin 2004](#): " On entend par prestations de cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet. On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié dans le même objectif. "

المتعلقة بالأمن القومي أو ذات التخصص في التجارة والمعاملات المالية ذات الطابع الإلكتروني، ومما يكد عليه الواقع العملي أن هذه الآلية تعمل على ضمان درجة شديدة من الأمن الإلكتروني، وهذا ما يرسحها لتكون الآلية المثلى للوقوف أصاد القراصنة (1).

صلابة تقنية التشفير تتحدد من خلال الخوارزمية التي تم العمل بها لصياغته وبطول المفتاح الذي تم التشفير به، والمقصود بطول المفتاح هو عدد البتات التي يتضمنها مفتاح التشفير، فأمانها مرهون بعددها فيتضاعف أمانها كلما تضاعفت أعدادها، وإذا أردنا تقريب هذا المعنى فإننا يمكن التمثيل لها بأسنان مفتاح الباب، إذ أنه كلما تضاعفت أعدادها كلما عسر أمر تقليدها أو اقتحامها قفلها، وعلمية التشفير عادة تتراوح أطوال مفاتيحها بين 40 إلى 2048 بت، ولا يعد المفتاح على قدر من الأمان ما لم يكن مفتاحه قد بلغ 128 بت أو زاد عنها، وبذلك فإن تخمين مفتاح التشفير بهذه القوة يحتاج إلى 02 ترليون سنة من أجل فكها، ولهذا لم يسمع عن عملية فك تشفير بهذه القوة مما يجعله تشفيراً على قدر كبير من الكفاءة في حماية أمن المعلومات (2).

ثانياً: أنواع التشفير:

1- التشفير المتماثل (symétrique):

يعتمد في كثير من الأحيان في هذا النوع من التشفير على شفرة القيصير (chiffre de César) التي تتأسس على قاعدة تعويض النص بأحرف تقابلية وهذا من خلال السير وفق عدد من المراحل من أجل بلوغ النص المشفر، ويتعين في ذلك أن تكون اللغة والخوارزمية التي يتم السير عليها معروفة وهذا من أجل تيسير عملية فك التشفير، ويعتبر تشفير الرسالة هو نفسه كلمة السر المترتبة جعل عن إعادة تشكيل الحروف أو الأرقام أو الرموز إلى عدد ثنائي وإدراج رموز أخرى لها (3)، ومن بين الأمثلة على هذا الأسلوب نجد:

✓ معيار تشفير البيانات (DES): يعتبر هذا المعيار كأول معيار تم توظيفه على مستوى المؤسسات، حيث التمس والمكتب الوطني الأمريكي للمعايير (National Bureau Of Standard) تقديم عروض خاصة بنظام تشفير يتضمن ثلة من المميزات أبرزها: علو مستوى

(1) أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 09، العدد 01، جامعة عبد الرحمان ميرة، بجاية، جويلية 2018، ص ص: 721-744: <https://www.asjp.cerist.dz/en/article/57745>

(2) ندى بدر جراح، تقنيات التشفير في التبادل التجاري الإلكتروني، مجلة ميسان للدراسات الأكاديمية، المجلد 07، العدد 14، جامعة ميسان، العراق، 2009، ص ص: 193-210: <https://www.iasj.net/iasj?func=article&aId=23696>

(3) سراح حليتهم، خصوصية التوقيع الرقمي في توثيق العقود الإلكترونية، مجلة الباحث للدراسات الأكاديمية، المجلد 05، العدد 02، جامعة باتنة 01، الحاج لخضر، باتنة، جويلية 2018، ص ص: 737-752: <https://www.asjp.cerist.dz/en/article/59702>

الأمن ويسر الاستعمال، ومن بين كل العروض التي تم تقديمها وقع الخيار على النظام الخاص بشركة (IBM)، وفي عام 1981 وضعت المؤسسة المحلية الأمريكية لتوحيد المعايير معياراً لتشفير البيانات وعملت على إدراجه وإعماله في الكثير من التطبيقات خاصة فيما يتعلق بالتطبيقات البنكية، إذ عملت البنوك على توظيفه من أجل تشغيل الصرافات الآلية، ومع أن مفتاح التشفير الخاص بمعيار (DES) يتكون من (56 Bits) غير أنه من السهل العمل على اختراقه وتدمير النظام الخاص به بمجرد امتلاك الحد الأدنى من التجهيزات⁽¹⁾.

✓ **معيار التشفير (IDEA):** كان يطلق على هذا النظام إسم (Proposed PES Encryption Standard) ثم (Imprived Proposed Encryption Standard) IPES وبعد ذلك تمت تسميته تشفير البيانات الدولي (IDEA) ويقوم هذا التشفير على استخدام مفتاحاً يتكون من 128 بيت، وهو مماثل لنظام (DES) الذي يقوم بتشفير الرسائل من خلال تجزئتها إلى فئتين مركبة من 64 بيت. يعد نظام (IDEA) نظاماً عصياً عن الاختراق والتعطيم، إلا أن ثغرتة تتجلى في استعمال مفتاح واحد فقط في عملية التشفير وفي فكّه أيضاً⁽²⁾. وينقسم التشفير المتماثل أو المتناظر إلى:

✓ **التشفير الكتلي: (Block Ciphers):** يقوم هذا الصنف من أصناف التشفير على أساس تقسم النص الأصلي إلى كتل بأحجام متعادلة، وبعدها يتم تنفيذ خوارزمية التشفير على كل كتلة من الكتل لتصبح بدورها كتلات مشفرة ويعتبر التشفير الكتلي من بين الأصناف الحديثة للتشفير إلى جانب التشفير الانسيابي⁽³⁾.

✓ **التشفير الانسيابي:** يقوم هذا النظام على استعمال مفتاح سري في عملية التشفير وفي فكّه أيضاً، تتمتع هذه الأنظمة بكثرة وكثافة استعمالها وعلى نطاق واسع في ميدان التشفير حالياً، ذلك أنها أنظمة لها من المميزات والخصائص المهمة، ومن بين هذه الخصائص نجد أنها أنظمة يتضاءل معها الخطأ، كما أنها أنظمة يسيرة الاستعمال في التطبيقات العلمية، كما تتسم بالخفة

(1) إيمان العاني، البنوك التجارية وتحديات التجارة الإلكترونية، مذكرة ماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، السنة الجامعية 2006-2007، ص 108.

(2) المرجع نفسه، ص 108.

(3) حيدر محمد عبد النبي ورعد عبد الحسن مهجر ونهلة عباس فليح، تشفير الملفات النصية باستعمال المفتاح المتناظر ومفتاح مستتب من معلومات النص الصريح، مجلة أبحاث البصرة، المجلد 32، العدد 3B، جامعة البصرة، العراق، ص ص: 25-33.

<https://www.iasj.net/iasj?func=article&Id=57994>

حال التنفيذ ويعد من بين الأصناف الحديثة والمهمة لأنظمة التشفير⁽¹⁾، "و يتم في التشفير الانسيابي معالجة عناصر الإدخال بصورة مستمرة، ناتج عن عنصر واحد كل مرة وهكذا تتم معالجة جميع العناصر"⁽²⁾ ويتكون من جزأين أساسيين هما:

● خوارزمية توليد المتتابعة شبه العشوائية؛

● المازج: تقوم خوارزمية هذا النظام بتوليد متتابعة شبه عشوائية اعتمادا على مفتاح يغذيها ثم تدمج هذه المتتابعة المتولدة مع متتابعة النص الصريح بواسطة المازج لتوليد متتابعة النص المشفر⁽³⁾.

2- التشفير غير المتماثل:

يقوم التشفير غير المتماثل على استخدام مفتاحي تشفير، أولهما من يعمل على قفل النص المراد تشفيره ويدعي هذا المفتاح بالمفتاح العام، أما المفتاح الثاني فهو مفتاح يتم استعماله من أجل فتح الملف وإعادته إلى الحالة التي كان عليها قبل عملية التشفير ويدعي بالمفتاح الخاص، ومن غير الممكن أن العمل على استخدام المفتاح العام من أجل استرجاع المفتاح الخاص على الرغم من الارتباط الحسابي القائم بينهما، وهو ما يعرف بمبدأ عدم القابلية للعكس، وللعمل على تركيب هذين المفتاحين يستوجب القيام بعمليات أسية بالغة التعقيد، ويدعي هذا النظام بنظام (RSA) وهذا نسبة إلى مبتكره (RIVEST SHAMIRET ADLEMAN)⁽⁴⁾.

إن الفتح العام في مثل هذا النظام لا يمكنه أن فتح شفرة الملف المشفر بالمفتاح العام، ولعل هذا الأمر هو السبيل إلى التثبت من هوية المواقع الإلكترونية وتشفير ما يرسل من رسائل من خلال توظيف القاعدة البرمجية الحاسوبية المتخصصة، وتجدر الإشارة إلى أنه إذا ما أراد المرسل إليه أن يرسل ردا على الرسالة أو الملف أن يقوم بتشفيره أولا عنده باستعمال المفتاح العام الخاص به والذي لا يمكن فك تشفيره بعد ذلك إلا بالمفتاح الخاص⁽⁵⁾.

(1) حميد عبد الكريم يونس وأنور صالح سليمان، تطور السرية في نظام التشفير الانسيابي اللاخطي من نوع (J-K)، مجلة البصرة للعلوم، المجلد 25، العدد 1/أ، جامعة البصرة، 2007، ص: 44-55: <https://www.iasj.net/iasj/article/54386>

(2) إلهام حسن عزيز ووفاء محمود جاسم، تصميم خوارزمية تشفير باستخدام الأرقام السومرية، مجلة جامعة كركوك، المجلد 12، العدد 03، جامعة كركوك، العراق، 2017، ص: 40-63: <https://www.iasj.net/iasj/article/131305>

(3) لهيب محمد الزبيدي وريا جاسم العطوي، تطبيق أسلوب التشفير الانسيابي المبني على الشبكة العصبية الاصطناعية، مجلة علوم الرافدين، المجلد 17، العدد 02/أ، جامعة الموصل، 2006، ص: 105-123: <https://www.iasj.net/iasj?func=article&aId=42823>

(4) منيرة عبيزة، التوقيع الإلكتروني كضمانة قانونية لحماية المستهلك الإلكتروني، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 02، العدد 1، كلية الحقوق والعلوم السياسية، جامعة عمار نليجي، الأغواط، مارس 2018، ص: 181-202: <https://www.asjp.cerist.dz/en/article/70372>

(5) سراج حليتيتم، المرجع السابق.

3- المزج بين التشفير المتماثل والتشفير اللامتماثل:

يبدو أن للمرسل والمرسل إليه إمكانية استعمال النظام المتماثل والنظام غير المتماثل معا في عملية التشفير، ويكون ذلك بإجراء عملية تشفير بالمعيار المتماثل، وبعدها يتم تشفير هذا المفتاح نفسه بالمفتاح العام بالنسبة للمرسل، ويبعث بالمفتاح الخاص إلى المرسل إليه من أجل أن يقوم بفتح الشفرة من أجل إسترجاع المفتاح المتماثل الذي كان الأسلوب المعتمد في تشفير الملف الأصلي⁽¹⁾.

وفي الأخير، تجدر الإشارة إلى أن نظام التشفير ليسا نظاما خاليا من أي ثغرة، فكما أن له العديد من الفوائد والمميزات كذلك له العدد من الفجوات والثغرات ومن أبرزها:

✓ "إن غالبية التطبيقات تستند على أسلوب واحد من أساليب التشفير، ولمدة زمنية مطولة، وهذا من شأنه أن يفتح المجال لتصويب الجهد عليه والتركيز عليه بالتحليل وهذا يمنح إمكانية التعرف على مفتاح التشفير، أو إمكانية ابتكار أسلوب يمكن من معرفة المفتاح في كل مرة يتم تبديلها فيها؛

✓ نظرا لتشابك مؤشرات الإدارة وتوزيع المفاتيح فإن عملية تبديل المفاتيح تعتبر عملية معقدة، وبالأخص عندما تزداد أعداد المستفيدين من العلمية (المستخدمين) بشكل كبير، وبعد ذلك تستمر بعض الأقسام في استعمال المفتاح لمدة طويلة، وهذه المدة تمكن من الكشف عن المفتاح؛

✓ وحتى في حالة تغيير المفتاح وتبديله، يبقى هنا تهديد باعتراضه من قبل من قبل المهددين والأعداء عند توزيعه على شبكات الاتصال؛

✓ نظرا لزيادة وارتفاع الهجمات على أنظمة التشفير فإن قصورها وهشاشتها تزداد هي الأخرى، وقد تبرهن تجريبيا أن أساليب وآليات التشفير التي كانت في وقت سابق تعد من الأساليب والآليات القوية قد تبين ضعفها في وقت لاحق " (2).

كما أن نظام التشفير ليس حكرا على الجهات الحامية فقط، أي تلك الجهات التي تضمن الحماية للفضاء الإلكتروني، بل يمكن أن تكون أيضا بيد الإرهابيين الذين يستغلونها لتبادل مختلف المعلومات والبيانات، لذلك هناك مناداة إلى ضرورة تمكين الحكومات من فتح الملفات المشفرة، وذلك من قبل منتجيها من القطاع الخاص، وهذا بالفعل ما اقترحه السيناتور جود جريج، غير أنه

(1) سراج حليثيم، المرجع السابق.

(2) أيمن محمد فارس الدنف، واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، رسالة ماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية، غزة، 2013، ص 90.

تخلى بعد ذلك عن مشروع قانونه، ومن ثم لم يكن للرقابة عن التشفير أي تأطير قانوني جاد في الولايات المتحدة الأمريكية⁽¹⁾.

ومع ذلك فإن هناك الكثير من الدول قد عملت على تأطيره وضبط وتنظيم عملية اللجوء إلى التشفير على الساحة الاتصالية بجملة من الضوابط والشروط والإجراءات، حيث نصت المادة 09 من مجلة الاتصالات التونسية على أنه: (تضبط بأمر شروط وإجراءات استعمال وسائل أو خدمات التشفير عبر شبكات الاتصالات وكذلك شروط تعاطي الأنشطة ذات العلاقة)، أما المشرع الفرنسي جعل عملية التشفير واقفة على شرط الترخيص الإداري المسبق أو بالتصريح لذلك للإدارة، وهذه الضوابط من شأنها أن تحول دون توظيف هذه التقنية في ارتكاب الجرائم⁽²⁾.

الفرع الثاني: الجدران النارية وبرامج مكافحة الفيروسات:

يفتح الاتصال القائم بين الأجهزة والشبكات ثغرات أمنية يمكن من خلالها أن ينفذ الإرهابيون إلى داخلها واختراقها والاعتداء عليها بالشتى الصور المعروفة، ولذلك عمل المتخصصون على إدراك هذه الثغرات بأدوات وبرمجيات تمثل حائطا يحول دون التمكن من هذا النفاذ (أولا)، وتم تصميم برمجيات معقدة لتقرع أي برمجة خبيثة تنفذ إلى داخل الأجهزة أو الشبكات، وتثبطها عن القيام بنشاطها التدميري أو الجوسسي في الفضاء السيبراني (ثانيا).

أولا: الجدران النارية:

1- تعريف الجدران النارية:

كانت الحصون والقلاع في الأزمنة والقرون الخالية الآلية التي يتم الاعتماد عليها من أجل حماية المدن والدفاع عنها ضد ما قد تتعرض إليه من هجمات واعتداءات، وعلى نفس الشاكلة ولتحقيق الهدف عينه، وضعت الجدران النارية أو ما يطلق عليه بجدار الحماية، وسميت بهذا الاسم لتشابهها بما هو معروف في الأزمنة القادمة حيث أن الفتحات الموجودة بحيطان القلاع والحصون كانت تسمح بإطلاق النار إلى الخارج دون أن يتمكن من بخارجها من تمريرها عبر تلك الفتحات، وكذلك الحال فيما يتعلق بالجدران النارية في الاصطلاح الإلكتروني، حيث أنها تمكن صاحب الجهاز من الخروج إلى شبكة الإنترنت في حين أنها لا تسمح بمن في الخارج من الدخول إلى الجهاز⁽³⁾.

(1) أنظر في ذلك: هال أبلسون، هاري لويس، كين ليدين، المرجع السابق، ص ص: 227-228.

(2) أنيس العذار، المرجع السابق.

(3) أيمن محمد فارس الدنف، المرجع السابق، ص 91.

فالطريقة المثلى التي من خلالها يمكن حماية الشبكات الآمنة من الشبكات التي لا تتوفر فيها عناصر الأمان تتمثل في توظيف أو استخدام جدار الحماية، التي تحول دون أن يتمكن المستخدم للشبكة غير الآمنة من الدخول إلى الشبكة الآمنة، فجدار الحماية من شأنه أن عمل على تحقيق عوامل الأمان من خلال تثبيت فواصل تفصل بين الشبكات الآمنة وغير الآمنة من كفالة الحماية لها، فهي أشبه ما تكون بالعازل النارية التي يتم تثبيتها بين جدران الغرف درءاً لخطر انتقال النار بينها، كما تعمل أيضا هذه الجدران على الحيلولة دون إمكانية الدخول إلى الشبكات الداخلية⁽¹⁾.

يعرف الجدار الناري على أنه: (كل آلة موضوعة في شبكة معلوماتية وقادرة على تحقيق غربة على التوصلات الداخلية والخارجية) وتعرف أيضا كونها: (جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب، ويكون أداة مخصصة أو برنامج على جهاز حاسوب آخر الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يقرر أحقية المرور ضمن قواعد معينة)⁽²⁾.

وتعرف أيضا على أنها: (هي عبارة عن برمجيات هدفها الأساسي تأمين الحماية الكافية لمعلومات الشركة والقضاء على عمليات الاختراق والتدمير التي تتعرض لها ملفات خوادم الويب، من خلال إقامة حاجز بين شبكة الإنترنت والشبكة الداخلية للمؤسسة ليقوم هذا الحاجز بتصفية وفحص كل عمليات الدخول والخروج إلى الشبكة لمنع دخول المستخدمين غير المصرح لهم وغير المسجلين ولتجنب خطر الفيروسات والبرامج الدخيلة)⁽³⁾.

ويقصد منها أيضا: (مجموعة من الأنظمة، والتي توفر سياسات أمنية ما بين الإنترنت وشبكة المؤسسة، للتحكم بجميع عمليات المرور إلى الشبكة، والتصدي للقرصنة والمتلصقين، فهو بمثابة حاجز وجسر إلكتروني بين الإنترنت وشبكة المؤسسات، هدفه حماية المتعاملين والتحقق من المتعامل المحلي أو الخارجي، بعبارة أخرى، تقوم الأنظمة بعملية مراقبة لكل تعاملات وعمليات الدخول إلى شبكة المؤسسة)⁽⁴⁾.

(1) عبد القادر بن عبد الله الفتوخ، الإنترنت: (للمستخدم العربي)، الطبعة الأولى، مكتبة العبيكان، الرياض، 2001، ص 226.

(2) أسماء فيلاي، عبد اللطيف شليل، تهديدات أمن المعلومات وسبل التصدي لها، مجلة البشائر الاقتصادية، المجلد 04. العدد 03، كلية العلوم

الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة طاهري محمد، بشار، فيفري 2019، ص ص: 163-177:

<https://www.asjp.cerist.dz/en/article/79099>

(3) سيمية ديميش، التجارة الإلكترونية: (حقيقتها وواقعها في الجزائر)، مذكرة ماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم

التسيير، جامعة منتوري، قسنطينة، السنة الجامعية 2010-2011، ص 94.

(4) إيلاف فاخر كاظم علي، مخاطر العمليات المصرفية الإلكترونية: (دراسة مقارنة)، الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية

للنشر والتوزيع، القاهرة، مصر، 2019، ص 122.

ويعرف البعض جدار النار بصيغة أكثر شمولاً على أنه: (عبارة عن مجموعة من البرمجيات والأجهزة التي يتم إعدادها لتشكيل حدود فاصلة بين شبكة المؤسسة الخاصة وشبكة الإنترنت، والهدف منه هو التغلب على أكبر قدر ممكن من الثغرات الأمنية من خلال بناء قناة اتصالات توجه إليها المعلومات المرسلة والمتبادلة مع شبكة الإنترنت لمراقبة والسيطرة على خروجها ودخولها من وإلى شبكة المؤسسة الخاصة، وذلك وفق أسس وقواعد يتم تحديدها وبنائها في جدار النار وبالتالي يقوم جدار النار بدور المرشح حيث يراقب تدفقات البيانات التي تمر عبره دخولا وخروجاً، ويقوم بتحليلها ومن ثم السماح بمرورها إذا كانت تحقق الشروط، أو منعها في حالة العكس)⁽¹⁾.

تنقسم الجدران النارية إلى نوعان، النوع الأول هو الجدران النارية المؤسسية وتعمل هذه الجدران على ضمان الحماية للتطبيقات التي تعمل عليها المؤسسات وهذا على نطاق الأجهزة المانحة أو المقدمة للخدمة، وبعدها على نطاق الأجهزة المتصلة بنظم تقديم الخدمات إن استمرت في الاتصال بالشبكة، والنوع الثاني هو الجدران النارية الشخصية التي ظهرت مع ظهور المستخدمين المتنقلين والقيام بأعمال خارج نطاق المؤسسة حيث لا يوجد هناك جدران نارية وأنظمة تزويد، فهي جدران نارية بالغة الأهمية لدورها المهم والفريد في حماية تلك الأجهزة التي تستعمل خارج المؤسسة أو المنظومة، ففي الآونة الأخيرة شرع رواء التقنية في الدول الغربية في تنصيب هذه الجدران على الأجهزة المحمولة المستعملة من قبل المشتغلين في المنظومات أو المؤسسات⁽²⁾، وهذا درء للخطر الذي يترتب عن بعدهم عن المزودات المحمية بجدران النار المؤسسية.

وتنقسم الجدران النارية أيضاً إلى نوعين بحسب طبيعتها. فهي إما أن تكون برمجية تستعمل في الغالب على الأجهزة المستقلة وأو تلك الأجهزة أو الحواسيب المتصلة بالشبكة أو الخادم، وإما أن تكون أجهزة وبتعبير آخر جدران نارية ذات طبيعة مادية، والتي يطلق عليها أيضاً اسم العلب السوداء ويتم استخدامها في حماية السيرفر وتعتبر هذه الجدران أكثر فعالية في ضمان الحماية مقارنة بالجدران النارية ذات الطبيعة البرمجية ذلك لأنها لا ترتبط بأنظمة التشغيل وبذلك فهي لا تخضع لما يمكن أن يحتويه من ثغرات وعيوب⁽³⁾، ويطلق على هذه الأخيرة أيضاً اسم الأبواب، الأقفال، المفاتيح، الجدران، حراس الأمن، وأسهل وسيلة للسيطرة على الأجهزة هو القيام بالسيطرة

(1) حديد نوفيل وحنان كريبط، أمن المعلومات ودورها في مواجهة الاعتداءات الإلكترونية على نظام معلومات المؤسسة، مجلة المؤسسة، المجلد 03، العدد

03، جامعة الجزائر 03، الجزائر، سبتمبر 2014، ص ص: 186-207: <https://www.asjp.cerist.dz/en/article/18359>

(2) سامر مؤيد عبد اللطيف، الإرهاب الإلكتروني وسبل مواجهته، مجلة جامعة كربلاء العلمية، المجلد 14، العدد 03، جامعة كربلاء، العراق،

2016، ص ص: 57-72: <https://www.iasj.net/iasj/article/114792>

(3) هاجر بوعوة وأمال مونزفي، واقع إدارة أمن المعلومات في مؤسسة السويدي إلكترونيك الجزائر، مجلة الريادة لاقتصاديات الأعمال، المجلد 06، العدد 02،

جامعة حسيبة بن بوعلي، الشلف، الجزائر، جانفي 2020، ص ص: 199-217: <https://www.asjp.cerist.dz/en/article/108307>

على هذه الجدران، وبالتالي فإنه يجب حمايتها، وأفضل حماية لها تكون من خلال الاستراتيجيات والمعايير المتبعة في حماية الأجهزة المادية عموماً (1).

ومن أشهر الجدران النارية ذات الطبيعة البرمجية نجد: (Zone Alarm Pro, eSafe)
(Desktop, Comodo Watch) أما عن أشهر الجدران النارية ذات الطبيعة المادية فنجد: (Guard, Watch Guard SOHO) (2).

2- عمل الجدران النارية:

تمكن الجدران النارية من رصد كل ما ينتهي إلى السيرفرات أو الخوادم من معطيات وبيانات، فهي آلية تعمل على ضمان حماية كل البيانات التي يتم الاحتفاظ بها داخل السيرفر مما قد يهددها، فحينما تكون هنا عملية إصدار الأوامر من جهة غير مرخص لها فإنه من شأن هذا الجدار أن ينذر المستخدم وينبئه بوجود عملية اختراق، وهذا الأمر ينطبق أيضاً في حالة ولوج المستخدم إلى بيانات من خلال الشبكة العنكبوتية، إذ يعمل جدار النار على تنبيه وتحذير المستخدم بعدم أمان المعطيات التي ولج إليها أو الموقع الذي يقوم بتصفحه، وتحذيره بأنه قد يكون ضحية نشاط اختراقية، ويتعين استعمال هذه التقنية على كل الحواسيب التي تمتلئها المنظمة أياً كان حجمها (3) تقاديا للوقوع في مغبات التطفل والاختراق، ودرء لأي اقتحام أو تهديد أو هجوم سيبراني.

توظف الجدران النارية أيضاً من أجل التأكد من صحة هوية المستخدمين، وذلك من خلال آليات وأساليب أكثر قوة من مجرد التأكد من أسماء المستخدمين وكلماتهم السرية، وذلك بالاعتماد على التشفير أو برامج حساب الشفرات الخاصة، كما توظف الجدران النارية أيضاً في مراقبة المحتوى على شبكات الفضاء الإلكتروني (4).

يتعين علينا أيضاً في هذا النطاق أن نشير إلى أن هناك توصيات شديدة الحدة تقضي باستعمال جدران الحماية مقترنة مع برامج مكافحة الفيروسات التي يجب أن تكون قد تمت تهيئتها بشكل صحيح وجيد، حتى وإن كانت هناك حقا تقنيات معروفة أو قيد الدراسة يمكن من خلالها تجاوزها (5).

(1) جلاء أحمد يس، الحوسبة السحابية للمكتبات: (حلول وتطبيقات)، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2014، ص 88.

(2) حديد نوفيل وحنان كريبط، المرجع السابق.

(3) كريمة صراع، واقع وآفاق التجارة الإلكترونية في الجزائر، مذكرة ماجستير في العلوم التجارية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، وهران، الجزائر، السنة الجامعية 2013-2014، ص 83.

(4) أيمن عبد الله فكري، المرجع السابق، ص ص: 181-182.

(5) Eric FILIOL, les virus informatiques: (théorie, pratique et applications), deuxième édition, Springer, FRANCE, 2009, P.129.

كما يجب أن تشير أيضا في نطاق أهمية الجدران النارية. فيما يتعلق بالكشف عن أنواع أخرى من الإصابات العدوى التي تصيب أجهزة الحواسيب مثل أحصنة طروادة والقنابل المنطقية وما إلى ذلك، فإن برامج المضادة للفيروسات أقل كفاءة في مواجهتها، إذ أنه لا يكشف هناك بشكل يمكن العويل عليه والثقة فيه، وبشكل خاص فيما يتعلق بالأصناف الجديدة من تلك الإصابات، ففي هذه الحالة يرجح أن يكون جدار النار أكثر فعالية في بعض الأحيان، وبشكل مكمل أساسيا لمكافحة الفيروسات بجانب برامج مكافحة الفيروسات، على شريطة أن تكون جدران الحماية قد تمت تهيئتها بشكل جيد وأن تكون قواعد وتعليمات التصفية خاضعة لعملية تدقيق بشكل متكرر مع إعادة تقييمها (1).

3- صور الحماية باستخدام الجدران النارية:

تعمل الجدران النارية بتسيير عمليات الدخول إلى المواقع أو الشبكات من خلال الآليات التالية:

1- **أسلوب سنج ومنع الخاص:** في هذا الأسلوب من أساليب الحماية بالجدران النارية نجد أن مستخدمه يبدأ في العمل به بتجزئة وتشطير معلوماته وبياناته إلى صنفين، صنف عام وآخر خاص، أما الصنف العام فيتم إدراجه في سيرفر يستقر خارج نطاق جدار الحماية، وهذا من أجل أن تبلغ كل الأفراد وتمنح لهم إمكانية الاطلاع عليها، أما الصنف الخاص فهو صنف يتمتع بالسرية الكاملة فهي بذلك تدرج في سيرفر ينتهي به المستقر بين طيات جدار النار وتضم فيه وتواري للوقوف والحيلولة دون بلوغها (2).

2- **أسلوب جدران النار المزدوجة:** يعد الجدر الناري المزدوج عامل وقف وحجر وحيلولة دون إدراك وبلوغ التعليمات والأوامر المرئية المنبثقة من الشبكة غير الآمنة إلى الخادم العام والخاص بشكل مباشر، وحينها يتم وضع الخادم الذي تستقر عليه الملفات العامة بعد جدار النار الأول، ويوضع خادم الذي يتضمن الملفات الخاصة بعد جدار النار الثاني، وهذا من أجل غرلة كل المجموعات والرمز الصادرة والواردة من وإلى الشبكة، وهذا من شأنه أن يمنح حماية تامة لكي صنف معلومات المؤسسة، سواء أكانت عامة متاحة أو خاصة مضمرة (3).

3- **أسلوب التفريق الكامل للخدمات:** يعتمد هذا الأسلوب على الفصل المطلق والكامل بين الخوادم، بحث يتم فيه اللجوء إلى استعمال حواسيب منفصلة عن بعضها البعض، فيخصص

(1) Eric FILIOL, Op.cit. P.182

(2) سيمة دميش، المرجع السابق، ص 94.

(3) المرجع نفسه، ص 94.

حاسب آلي مستقل متعلق بالخادم الذي يحمل بين طياته الملفات الخاصة ويعمل وفق نظام يتسم بأمان يضمن الحيلولة دون الوصول إلى الملفات الخاصة بالمؤسسة⁽¹⁾.

يعد الجدر الناري مصفاة تقوم بتتقية مجموعات البيانات الصادر والوارد من وإلى الشبكة، فهي تنشأ طبقة تقوم بعزل وتحديد شبكة المنظمة عن الشبكة الخارجية، فكل البيانات والتعليمات سواء تكل التي ترد عن المنظومة أو تلك التي ترد إليها لا تعبر إلا من خلال هذا الجدار الذي يعمل على تنقيتها بحيث يحول دون دخول أي مجموعة تعليمات أو أعمال لم يرخص لها بالاجتياز، وتتخذ هذه العملية عدة صور، وتتأسس على عدة قواعد منها ما يتعلق بفئة البيانات نفسها، ومنها ما يتعلق بالنوع والتاريخ والوقت، فهي تستند حين قيامها بعملية التنقية على جداول تم وضعها وحفظها في بنية الجدار الناري، ووفقا لهذه الجداول يتم السماح أو المنع لرزم البيانات من العبور، وهذه العملية تتخذ صورة الإيجابية، حيث تجيز للبيانات التي تستوفي الشروط التي تتضمنها قوائم التنقية وتحول دون عبور غيرها من البيانات، وصورة السلبية، بحيث تكون البيانات الموافقة للشروط التي تم تضمينها في قوائم التنقية هي التي لا يجوز لها العبور، بينما تسمح وتجزز لغيرها العبور⁽²⁾.

4- بعض أساليب عملية التصفية:

1- التصفية باستعمال العناوين (Address filtering): يعتمد هذا الأسلوب في التصفية على العناوين الإلكترونية، وهذا من خلال تضمينها جداول التصفية التي يجوز الإرسال إليها أو بالتلقي منها، والتي تستخدمها البيانات حال عبورها، غير أن هذا الأسلوب لا يعد بمفردها كافية لضمان الحماية المناسبة وهذا نظرا لوجود قدر كبير من العناوين التي يتعين حفظها في الجداول، كما يتعين أن تكون محل تحديث مضطرد ومتجدد⁽³⁾.

2- التصفية باستعمال المنافذ (Port filtering): يعتبر هذا الأسلوب من أكثر الأساليب استخداما وأذيعها صيتا، وتعتمد هذه الطريقة على تحليل نوع المنفذ، فتجزز لمجموعات البيانات بالعبور على أساس رقم منفذها، بحيث يمكن التحكم في هذه البيانات من خلال سد تلك المنافذ وبالتالي لا يمكن للملفات أن تنفذ من خلالها⁽⁴⁾، فبروتكول مكتب البريد (POP3) الوارد

(1) سيمية ديمش، المرجع السابق، ص 94.

(2) ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، المملكة العربية السعودية، 2015، ص ص: 253-255.

(3) المرجع نفسه، ص 256.

(4) المرجع نفسه، ص 256.

يعمل على منفذ تي سي بي 110، وبروتوكول البريد البسيط الصادر (SMTP) يعمل على منفذ تي سي بي 25⁽¹⁾، فبمجرد أن يتم السيطرة على هذه المنافذ لا يمكن لأي ملف أن ينفذ من خلالها، فمجال العمل في مثل هذه التصفية ومحلها يكون وارد على مقاطع المنفذ سواء أكان البروتوكول متعلق بالإرسال (TCP) أو بروتوكول حزم بيانات المستخدم (UDP)⁽²⁾.

3- التصفية باستعمال النطاق (Domain filtering): يعمل هذا الأسلوب على التحكم في النطاقات، بحيث يتم حظرها والحيلولة دون وصولها إلى الشبكات الداخلية⁽³⁾ وبالتالي منع الملفات غير المسموح بها من بلوغ الشبكات الآمنة.

ترى الباحثة أن الفرق بين هذه الصور أو الأساليب الثلاثة في التصفية والتنقية لا يتمحور فقط في درجة الحماية والأمان التي تضمنها للشبكات الداخلية للمنظومة فقط، بل في شمولية نطاقه أيضا استنادا إلى ما أدركناه من مفاهيم، فالعنوان الإلكتروني (IP) يعد أكثر شمولاً من المنفذ، والمنفذ يتكون من رزم النطاقات، وبذلك يمكن القول أن منع عنوان إلكتروني معين أكثر شمولاً رغم أنه يثقل على القوائم ويضخم حجمها لكثرة العناوين، ومنع منفذ من المنافذ أكثر شمولاً من منع النطاق.

وأخيرا يجدر بنا الإشارة إلى أن جدار الحماية لا يمثل حماية مطلقة من الهجمات التي يمكن أن تتعرض لها البيئة الإلكترونية خاصة هجمات فيروسات المستندات. فقد أثبتت تجارب مخبرية التي تدعمها مواقف واقعية أن ورقة برنامج إكسال (EXCEL) بسيطة يمكنها التسلل إلى أي شبكة من الشبكات، حتى تلك الشبكات التي يعتقد أصحابها أنها أكثر حماية وأماناً، إذ أنه في حالة الفيروسات المضمنة في المستندات فإن الهجوم يكون مصحوباً ببراعة اجتماعية مناسبة من غير الممكن إيقافها، والتجربة تثبت وتوضح أنه من مضادات الفيروسات والجدران النارية تبقى عاجزة عن الكشف عن أي شيء، ليس إلا الوقاية الشديدة مع الحذر الشديد من يمكن لها ربما أن تجنب مثل هذه الهجمات⁽⁴⁾.

ثانياً: برامج مكافحة الفيروسات:

تصدى العلم الحديث للفيروسات الإلكترونية ولم يبق مكتوف الأيدي حيالها، فقد عمل على تصميم برامج خاصة لمقومتها ومحوها من الأنظمة⁽⁵⁾، وتعرف هذه البرامج على أنها: (مجموعة

(1) الموسوعة الحرة، ويكيبيديا: منفذ شبكات.

(2) الغرض من قوائم (ACL)، (د.ت.ن)، تم الاطلاع عليه بتاريخ 19 جويلية 2020 على الساعة 03:24 سا، في الموقع:

<http://static-course-assets.s3.amazonaws.com/RSE50AR/course/module9/9.1.1.3/9.1.1.3.html>

(3) ذيب بن عايض القحطاني، المرجع نفسه، ص 256.

(4) Eric FILIOL, Op.Cit. PP: 395-396

(5) أشرف عبد المحسن الشريف، أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية، مجلة اعلم، الاتحاد العربي للمكتبات

والمعلومات بالتعاون مع مكتبة الملك عبد العزيز العامة بالرياض، يناير 2016، ص ص: 87-114:

http://www.arab-afli.org/media-library/Journal%20Issues/I3lem-16-2016_Achref_Abel.pdf

البرامج التي تتصدى للفيروسات الداخلة إلى الجهاز⁽¹⁾، فهي البرامج التي يتم توظيفها من أجل الحظر والعثور على كل البرامج الخبيثة⁽²⁾.

تعمل برامج مكافحة الفيروسات على حظر دخول هذه البرامج الضارة إلى الأنظمة والعثور عليها قبل أن تحدث ضرراً بها، وتعمل على إزالتها، وتحتوى برامج مكافحة الفيروسات على خواص متعددة حيث تقوم بتحديث نفسها أوتوماتيكياً عند اتصالها بشبكة الإنترنت وهذا من أجل أن تعمل بكفاءة في التصدي للأنواع المستحدثة من الفيروسات⁽³⁾.

وتجدر الإشارة إلى أن التحديثات يمكن أن تكون من خلال آليتين؛ أولهما تلك التحديثات التي يكون بطريقة أوتوماتيكية حيث يعمل البرنامج الذي تم تثبيته على الجهاز بالاتصال بالشركة المنتجة للبحث عن وجود أي تحديثات وحال وجودها يقوم بتثبيته المستخدم بذلك ويتعين أن يكون الجهاز متصلاً بشبكة الإنترنت، أما ثانيهما فهي التحديثات اليدوية التي يقوم بها المستخدم حينما يقوم بتحميل التحديثات الموجودة على الشركة المنتجة وتثبيتها⁽⁴⁾.

كما تمتلك أيضاً تقنية التنقيب عن هذه الأخيرة من خلال مراجعة السلوك والتدقيق فيه ومراقبة أشكال الملفات التي يحتوى عليها الجهاز حيث تقوم بمتابعة التغيرات التي تطرأ عليه عبر تقنية اختيار لتكامل بناء يحوى بين طياته كل الملفات التي يتضمنها الحاسب الآلي بكل ما تحمله من بيانات الحجم والتاريخ ورصد أي نشاط غير مألوف فيها⁽⁵⁾، فمضادات الفيروسات الإلكترونية من مختلف البرامج يمكن أن ننظر إلى نشاطها على نحو هذا الترتيب الآتي ذكره:

- المسح والتحليل لأقراص جهاز الحاسب من للعثور على الملفات الملوثة

بالفيروسات: ويقوم بذلك من خلال العديد من الطرق والآليات ومن بينها مقارنة أجزاء من الملفات مع ملف التوقيع الذي يعتبر مختصر للفيروسات المعروفة، إنها بكل بساطة البصمة التي تسمح بالتعرف عليها داخل الملف، ولذلك يتعين المحافظة على التحديثات المتعلقة بهذه التوقيعات⁽⁶⁾، كما يوجد من بين الآليات أيضاً ما يعرف بالأسلوب الاستدلالي، ويعمل عن طريق الاستدلال في البرامج الضارة المحتملة التي لم يعرفها برنامج مكافحة الفيروسات بعد، وهو يعمل عن طريق

(1) هاجر بوعوة وأمال موترفي، المرجع السابق.

(2) أيمن محمد فارس الدنف، المرجع السابق، ص 92.

(3) أشرف عبد المحسن الشريف، المرجع السابق.

(4) أسماء فيلاي، عبد اللطيف شليل، المرجع السابق.

(5) أشرف عبد المحسن الشريف، المرجع نفسه.

(6) Patrick ANTOULY, surfer sans risque: (protéger votre ordinateur – virus, spywares, chevaux de Troie, spam), Éditions ENI, France, 2009, P.58.

تحليل السلوك المفترض للبرامج لتحديد إن كان ضارة أم لا، كما يوجد أيضا أسلوب السلوك المشبوه، والذي يعمل يقوم على تحليل سلوك البرامج التي تعمل على النظام، فيمكنه أن يقوم بحظر أي سلوك برنامجي يحتمل أن يكون ضارا، ومثل هذه التقنية يمكن أن تقوم باكتشاف برامج ضارة جديدة (1).

- " إزالة الفيروسات التي تم العثور عليها: تعمل برامج مكافحة الفيروسات عند عثرها على الملفات الملوثة بمحاولة إزالته أو إبطال مفعوله، أو تعمل على حجبها إذا لم تتمكن إزالتها وإبطال مفعولها؛

- منع النشاط الفيروسي: فبرامج مكافحة الفيروسات النشطة تعمل على التحليل تزامنا مع العمل على أحد الملفات داخل الجهاز، ويقوم برنامج مكافحة الفيروسات بمنع الوصول إلى الملف المعني ويحاول البرنامج إصلاحه في حال الكشف والعثور على فيروس؛

- تحليل البريد الإلكتروني: ومثل هذا النشاط يستهدف تلك الفيروسات التي تتهدد البريد الإلكتروني (2)، فمن الضروري للغاية، أن يقترن خادم البريد الإلكتروني مع برنامج مكافحة الفيروسات الذي يقوم بتحليل كل رسالة مع مرفقاتها بالاعتماد على قاعدة بيانات التوقعات المعروفة عن معظم الفيروسات، وتجدر الإشارة هنا أنه بالاستناد إلى ميزات وإعدادات برامج مكافحة الفيروسات لا يمكن أن يقوم بالضرورة بإجراء مسح كامل ومتكرر لجميع تنسيقات الملفات خصوصا تنسيقات الحاويات، فعلى سبيل المثال من النادر جدا أن يكون برنامج مكافحة الفيروسات وحده قادرا على اكتشاف الملف القابل للتنفيذ المصاب والمتضمن في المسند (3).

- مراقبة صفحات الويب: ويعمل على ذلك بنفس الآلية والطريقة التي يعمل عليها في معالجة ومراقبة الملفات داخل الحاسب الآلي والبريد الإلكتروني، حيث يعمل على تحليل الصفحات التي يتم تصفحها للمبحث عن أي نصوص ضارة (4).

يوجد على الساحة اليوم مجموعة كبيرة من البرامج المضادة للفيروسات، ولعل من أفضل هذه البرامج هي تلك التي أشار إليها الباحث هشام سياري (Hisyam Syarif) (5) والتي تتمثل في؛

(1) Lalonde Lévesque Fanny, prévention des attaques par logiciels malveillants: (perspectives de la santé publique), thèse présentée en vue de l'obtention du diplôme de philosophie doctor (génie informatique), école polytechnique de Montréal, université de Montréal, 2018, P.17.

(2) Patrick ANTOULY, Op.cit. P.58.

(3) Philippe LAGADEC, Filtrage de messagerie et analyse de contenu, 2004:

http://195.154.171.95/SSTIC04/Filtrage_messagerie/SSTIC04-article-Lagadec-Filtrage_messagerie.pdf

(4) Patrick ANTOULY, Ibid. P.58.

(5) (STIMIK) Stikom Bali-Indonesia.

- " برنامج (Bit defender Antivirus plus Anti-Virus) وهو برنامج يحتل الصادرة والمرتبة الأولى في العام، فهو برنامج له القدرة والبراعة الفائقة في التعامل مع الفيروسات التي من الصعب إزالتها؛

- برنامج (Anti-virus Kaspersky internet security) يعد هذا البرنامج من بين أعظم أنواع البرامج المقاومة للفيروسات التي يصعب التعامل معها وقد أثبت أن له أداء رائعاً في ذلك؛

- برنامج (AVIRA Protection) هو من بين البرامج التي تجعلنا نشر بالأمان حيال الانتشار الفيروسي" (1).

وفي الأخير، تجدر الإشارة إلى أن برامج مكافحة الفيروسات مهما كان معدل أمانها إلا أنها يمكن أن تتضمن عيوباً شتى (2)، "فعلى الرغم من الاعتقاد الشائع بأن برامج مكافحة الفيروسات تعمل على زيادة الأمان إلا أنها يتم إنتاجها بواسطة نفس عمليات البرمجة، مما قد يؤدي إلى برامج غير آمنة بشكل عام، فبرامج مكافحة الفيروسات تعمل على معالجة المدخلات التي قد تحمل ضرراً في مجموعة متنوعة من تنسيقات البيانات، ولما ثبت تاريخياً أن تحليل البروتوكولات والصيغ يعد عملاً معرضاً للخطأ فإن برامج مكافحة الفيروسات هي الأخرى معرضة لذات الخطأ، وتكبر الحساسية للخطأ في مثل هذه البرامج حين قيامها بالمحاكاة كأسلوب دفاع ضد أساليب إحباط الاكتشاف التي تستخدمها البرامج الضارة، وذلك نظراً لصعوبتها وتعقدها وتعاملها مع مدخلات يحتمل فيها الضرر" (3).

"يعتبر محرك الفحص أو المسح هو المسؤول عن تحديد الملفات الضارة بالاستناد إلى قواعد بيانات التوقع، وهي الأرضية المشتركة بين العديد من برامج مكافحة الفيروسات، وبسهل التجانس عملية تصميم البرامج الضارة، حيث أنه من الأسرع نسبياً اختبار البرامج الضارة قيد التطوير باستخدام جميع البرامج مكافحة الفيروسات الأكثر شيوعاً، وهذا ينعكس على معدلات الكشف المنخفضة عن البرامج الضارة الحالية، كما أن تجانس برامج مكافحة الفيروسات يعد بحد ذاته

(1) Hisyam SYARIF, English about Antivirus Software, International Research Journal of Management, IT & Social Sciences, Vol.2, No.1, January 2015, PP.17-21:

<https://www.semanticscholar.org/paper/English-about-antivirus-software-Syarif/6242947cf508e558524c92eafb795b94f363f624>

(2) أيمن محمد فارس الدنف، المرجع السابق، ص 93.

(3) Juhani ERONEN, Kati KARJALAINEN, Rauli RUUPERA Erno KUUSELA, Kimmo HALUNEN, Marko LAAKSO, Juha RONING, Software Vulnerability vs. Critical Infrastructure - a Case Study of Antivirus Software, International Journal On Advances in Security, vol 2, no 1, IARIA, year 2009, PP. 72-89.

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.233.491&rep=rep1&type=pdf#page=80>

عاملا لانتشار الفيروسات، كما أن برامج مكافحة الفيروسات تحتاج إلى حقوق وصول عالية من أجل مراقبة النظام وهذا من شأنه أن يجعلها نواقل جذابة لاختراق الأنظمة" (1).

يمكن أيضا لبرامج مكافحة الفيروسات أن تتضمن عيبا آخر، ويتمثل في إمكانية إضعافه لأداء الحاسوب إن كان تصميمه غير كفي، كما أن المستخدمين من استخدام هذه البرامج من غير الخبراء قد تصادفهم صعوبات في إدراك أوامر وقرارات برامج مكافحة الفيروسات، وقد ينجم عن أي قرار خاطئ مساس بالأمن، كما أن تطور الفيروسات واتخاذها لأشكال جديدة إذا اقترن ذلك مع غياب التحديثات للبرامج المتوفرة حاليا يضيع من قيمتها (2).

الفرع الثالث: نظام الحجب والمراقبة:

تنشط الجماعات الإرهابية على الفضاء الإلكتروني من خلال إنشاء مواقع تواصل أو إعلام ودعاية ومن أجل ذلك سعت الدول إلى خلق نظام يمكنها من حجب هذه المواقع بحيث لا يمكن للأفراد الوصول والاطلاع على ما تتضمنه من محتويات (أولا)، كما تعمل الدول أيضا في سبيل حماية هذا الفضاء من انتهاج نهج الرقابة الإلكترونية، ولكون هذا النظام من الأنظمة الماسة بحرية وسرية الاتصالات فقد عملت التشريعات على حفه بضمانات قانونية مختلفة (ثانيا).

أولا: الحجب والترشيح:

يمكن تعريف نظام الترشيح والحجب على أنه: (أسلوب لحجب صفحات معينة يمكن أن تكون مؤذية أو عدوانية أو إباحية بالنسبة لمستخدم الإنترنت فإذا حاول المستخدم الوصول إلى صفحة محجوبة ظهرت له رسالة تبلغه أن الوصول إلى هذه الصفحة غير مسموح به) (3).

يعتبر هذا النظام من النظم التي توظيفها الكثير من الدول، فالصين على سبيل المثال تتفق كل عام موارد ضخمة في بناء وصيانة أحد أكبر أنظمة الترشيح وأكثرها تطورا في العام وتوظف المملكة العربية السعودية أيضا نظام بروكسي الويب لحجب الوصول إلى المواقع المحظورة (4)، كما وضعت وحدة خدمات الإنترنت التي الخاضعة لمدينة الملك عبد العزيز والتي تخضع هي الأخرى للعلوم التقنية نظاما للترشيح والذي كلفت مهمة الإشراف عليه منذ سنة 2006 إلى هيئة

(1) Juhani ERONEN, Kati KARJALAINEN, Rauli RUUPERA Erno KUUSELA, Kimmo HALUNEN, Marko LAAKSO, Juha RONING, Op.cit.

(2) أيمن محمد فارس الدنف، المرجع السابق، ص 93.

(3) أنيس العذار، المرجع السابق.

(4) Nikolaos KOUMARTZIS, Andreas VEGGIS, Internet regulation: (The need for more transparent Internet filtering systems and improved measurement of public opinion on Internet filtering), First Monday (peer-reviewed journal on the internet), Volume 16, Number 10 - 3 October 2011: <https://firstmonday.org/ojs/index.php/fm/article/view/3266>

الاتصالات وتقنية المعلومات ⁽¹⁾، كما قدمت خدمات التحقيقات الجنائية الوطنية النرويجية (Telenor) و (KRIPOS) في 2004 نظاما لحظر المواد الإباحية للأطفال في النرويج والذي ارتكز عليه بعد ذلك النظام السويدي ⁽²⁾.

تعد عملية الحجب والترشيح تقنية من التقنيات التي يتم توظيفها في مواجهة ظاهرة الإرهاب الإلكتروني عبر حجب مواقعها، ودل على ذلك ما أفاد به المراسل السياسي أندرو تيليت بوضع نظام أجمع عليها عدد كبير من مزودي خدمة الإنترنت في أستراليا والذي يسمح بإصدار أوامر بحظر المواقع التي تستضيف مواد تصور الهجمات الإرهابية أو الجرائم العنيفة، كما أفاد أيضا نقلا عن مفوضة السلامة الإلكترونية جولي إيمان غرانت قولها: (قد علمتنا هجمات كرايستشيرش الإرهابية أنه لا يمكننا أن نتقاعس في مواجهة رغبة الإرهابيين في استغلال الإنترنت لإيذاء المجتمع والتحريض على المزيد من الأعمال الشنيعة) واستدركت: (في مجتمع حر مثل مجتمعنا ، يجب أن تكون عتبة حظر المواقع عالية للغاية. ومع ذلك ، فإن المجتمع له الحق في الحماية من المواد التي يمكن أن تنتشر فيروسية ، مما يتسبب في أضرار جسيمة ، لا سيما للأطفال أو أولئك الذين قد يكونون عرضة للتطرف) ⁽³⁾.

فعملية حجب المواقع إذا ليست أمرا مبتدعا، إنه نظام معتمد في الكثير من البلدان المتقدمة، ذلك أن الأمر ههنا متعلق بالأمن القومي للدول والذي يستلزم مواجهة تحسم الأمر فيما يتعلق بأبرز الوسائل التي يتم توظيفها من قبل الإرهابيين في الدعاية ونشر الأفكار عبر المواقع الإلكترونية التي تساهم في تهديد الاستقرار والأمن ⁽⁴⁾.

والأمثلة على توظيف الحجب من قبل الحكومات أكثر من أن تحصى، ومن بينها حجب دول كفرنسا وألمانيا والنمسا للفكر الذي يروج النازيون الجدد (Néonazisme)، كما تقوم بعض الدول الأخرى بحجب المواقع التي تتضمن تحريضا على العنف، وحجب الولايات المتحدة لموقع ويكيليكس سنة 2010، كما أنشأت الصين نظاما للحجم يطلق عليه اسم "الدرع الذهبي" ⁽⁵⁾.

(1) أنيس العذار، المرجع السابق.

(2) Nikolaos KOUMARTZIS, Andreas VEGLIS, Op.cit.

(3) Andrew TILLET, Deal with ISPs to block terror attack websites, Mar 25, 2020, Accessed on 13/08/2020, at 20:03h, in: <https://www.afr.com/politics/federal/deal-with-isps-to-block-terror-attack-websites-20200323-p54d0t>

(4) عبد النبي الشحات، حجب المواقع الإرهابية.. وقانون الجريمة الإلكترونية، صحيفة اليوم السابع، 30 مايو 2017، تم الاطلاع عليه بتاريخ

13 أوت 2020 على الساعة 20:17، مختصر الرابط: <https://n9.cl/yhe5>

(5) بروس شنابر، المرجع السابق، ص 150.

والدول حينما تقرر توظيف آلية ترشيح الإنترنت فإنها تقوم بادئ الأمر بإنشاء صرح من القوانين والتشريعات ومختلف التدابير التقنية التي من خلالها يمكن أن تحول بين مواطنيها وبين الوصول إلى نوع معين من المعلومات أو نشرها عبر الفضاء الإلكتروني، ويمكن لتلك القوانين أن تتخذ شكلين، فإنما أن تكون امتدادات للقوانين المنظمة لوسائل الإعلام أو الاتصالات السلكية واللاسلكية الموجودة مسبقاً، كما يمكن أن تكون قوانين خاصة تتعلق بالفضاء الإلكتروني على وجه محدد، ومن النادر جداً أن تحدد هذه القوانين نظام التصفية الفنية الذي سيتم اعتماده، ولكن الشائع أن تضع إطاراً لتقييد أنواع معينة من المحتوى عبر الإنترنت وحظر أنشطة معينة عبر الإنترنت⁽¹⁾.

ففي حالة الجزائر مثلاً، توجد العديد من النصوص القانونية التي تفيد معنى الترشيح والحجب، وهي متفرقة على عدة تشريعات مختلفة ومن أهمها المادة 118 التي تنص على أنه: (في حالة استعمال مخالف للأحكام المذكورة في المادة 117 أعلاه، يتم إغذار المتعامل من طرف سلطة ضبط البريد والاتصالات الإلكترونية، قصد التدخل الفوري لمنع النفاذ إلى الشبكات و/أو خدمات الاتصالات الإلكترونية)⁽²⁾، والحالات التي أشارت إليها المادة 117 هي: (النظام العام والدفاع الوطني والأمن العمومي؛ الكرامة وحفظ الحياة الخاصة للآخرين؛ حماية الأطفال، خصوصاً فيما يتعلق باستعمال خدمات الإنترنت).

كما أشارت المادة 12 من القانون رقم 04-09 إلى عملية الترشيح في معرض تحديد الالتزامات الواقعة على مقدمي الخدمات حينما نصت على أنه: (...يتعين على مقدمي خدمات الإنترنت ما يأتي: ب... وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوى معلومات مخالفة للنظام العام والآداب العامة وإخبار المشتركين لديهم بوجودها)⁽³⁾.

وأشار المشرع إليه أيضاً في المادة 24 من القانون 05-20 والتي تنص على أنه: (يمكن للجهات القضائية أن تأمر مقدم الخدمات، تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول بالتدخل الفوري لسحب أو تخزين المحتويات التي يتم الاطلاع عليها أو جعل

(1) Jonathan ZITTRAIN and John PALFREY, Internet Filtering: The Politics and Mechanisms of Control, publishing in Collective workbook themed: Access Denied: (The Practice and Policy of Global Internet Filtering) edited by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, usa, 2008, PP.29.56.

(2) المادة 118 من القانون رقم 04-18 المؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر عدد 27 لسنة 2018.

(3) المادة 12 من القانون رقم 04-09 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر عدد 47 لسنة 2009.

الدخول إليها غير ممكن عندما تشكل جريمة من الجرائم المنصوص عليها في هذا القانون، أو بوضع تقنيات تسمح بسحب أو تخزين هذه المحتويات أو لجعل الدخول إليها غير ممكن⁽¹⁾.

ومع ما لنظام الترشيح من كفاءة في حظر بعض المواقع الإلكترونية غير أن هذه الكفاءة لا تشمل جميع المواقع ولاسيما المواقع ذات الطبيعة السياسية والدينية، كما أن النفاذ إلى المواقع ليس أمراً عصياً على من يملك معارفاً فنية في تقنيات المعلومات، فهم قادرون على التخفي والنفاذ إلى المواقع التي فرض عليها الحجب عن طريق ما يسمى بالبروكسي، كما أن فعاليته تقتضي التناسب بين الرقابة المفروضة وبين سرعة تدفق الإنترنت، ذلك أنك إن أردت أن تحافظ على سرعة تدفق الإنترنت وفي الوقت عينه تفرض عليه رقابتك فيجب أن تخصص لكل شخص مراقباً يراقبه⁽²⁾.

كما أن أنظمة الترشيح الأكثر كفاءة من الممكن أن تجد صعوبات كبيرة في منع هؤلاء المستخدمين الذين يمتلكون قدراً عالياً من الإصرار والعزيمة في بلوغ المعلومات أو نشرها، فتلك الشريحة تكون على كامل الاستعداد لمكابدة العناء والمخاطر في سبيل تحقيق أهدافهم، وقد أقر المشرف على برنامج التصفية في المملكة العربية السعودية على ذلك حينما أكد بأنه ليس من الميسر تحقيق هذا الرشح والحجب بسلاسة أمام بعض المستخدمين الذين يتمتعون بنوع من البراعة الفنية في الوصول إلى المعلومات التي يتم حظرها، كما أن أنظمة الترشيح ليست أنظمة مثالية خالية من أي عيب، بل فيها عيوب أقلها عيبين⁽³⁾.

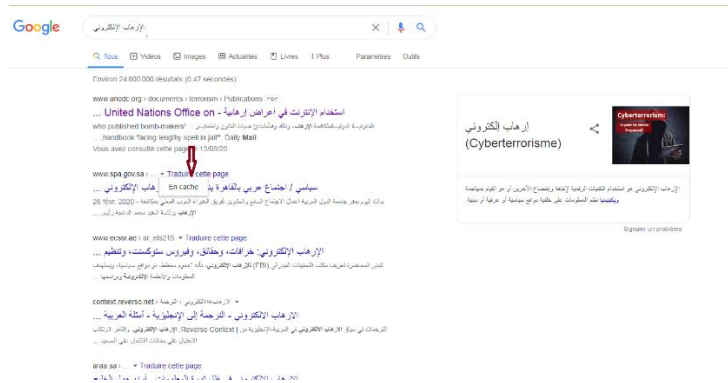
بالإضافة أيضاً إلى أنظمة البروكسي، فقد أفاد المحرر المختص بالشؤون التقنية فراس اللو على موقع الجزيرة أن هناك مواقع إلكترونية تمنح من الأدوات ما يمكن المستخدمين الراغبين من تجاوز الحظر، وما على المستخدم إلا أن يكتب رابط الموقع المحظر حتى يتم عرضه بالكامل، دون أن يقوم بتنشيط أي برنامج، كما يمكن القيام بذلك بإجراء بسيط على موقع جوجل فعند ظهور نتائج البحث قد يكون الموقع الأصلي للبحث محظوراً، وبكفي لفك الحظر بالضغط على السهم ليظهر له خيار تحت عنوان نسخة مخبأة (en cache) وبالضغط عليه يمكن الانتقال إلى نسخة تم حفظها في خوادم غوغل [كما هو موضح في الشكل 01]، ومن بين هذه المواقع موقع: (proxfree.com) و(hidemyass)، [كما أن هناك آلية أخرى والمتمثلة في إضافات المتصفحات (extension de navigateur)، والشكل 02 يوضح إضافة خدمة (VPN) التي تملك خاصية فك الحظر] وهناك ما

(1) المادة 24 القانون رقم 05-20، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.

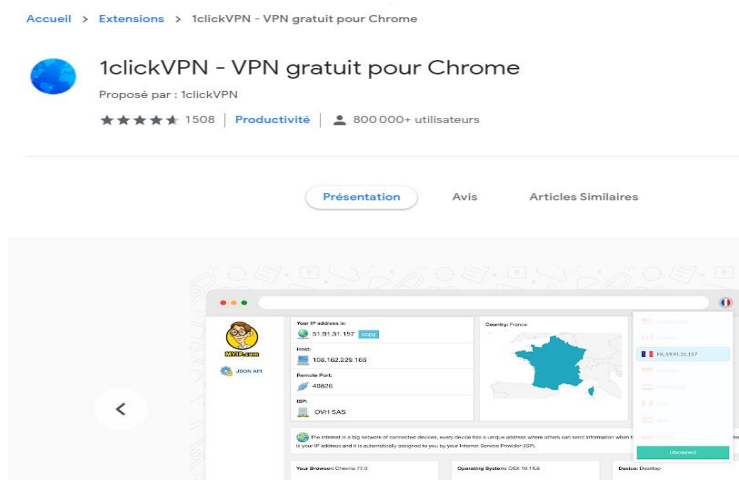
(2) أنيس العذار، المرجع السابق.

(3) Jonathan ZITTRAIN and John PALFREY, Op.cit.

يسمى أيضا بتغيير خادم النطاق، فتغييره يمكن من الدخول إلى المواقع المطلوبة، كما تتوفر الهواتف المحمولة الآن على تطبيقات قوية في هذا المجال (PureVPN) ⁽¹⁾.



الشكل 01.



الشكل 02.

يعد الحظر أيضا من الإشكاليات المطروحة في ساحة حوكمة الإنترنت، فالاتجاه الرفض لهذا التنظيم يبرز فكرة الحجب على أنها من بين المشاكل التي يصادفها الفضاء الإلكتروني، إذ يعتبر أنصار هذا الاتجاه أن الحريات على الإنترنت أصبحت على المحك مع توالي حالات الحجب والمساعي لتبديل طبيعة الإنترنت، والشاهد على ذلك ما تقوم به إيران مع موقعي تويتر واليوتيوب من حجب وما تفرضه على المواطنين من رقابة، وهذا الأمر ينطبق أيضا على روسيا التي وضعت قائمة سوداء لحجب المواقع تحت حجة ضبط الوصول إلى المواقع التي تشجع على

(1) فراس اللو، أفضل الأساليب التقنية لتخطي حجب المواقع، نشر على موقع الجزيرة بتاريخ 04 جوان 2017، تم الاطلاع عليه بتاريخ 18 جويلية 2020، على الساعة 18:22، مختصر الرابط: <https://n9.cl/c51e3>

الانتحار واستخدام الممنوع للمخدرات، غير أن القائمة تتضمن متخصصة في الشأن السياسي والاجتماعي، وهناك أمثلة أخرى عن ذلك في الكثير من الدول كتركيا التي عملت على غلق موقع تويتر، ومحكمة باريس حين وجهت طلبا إلى تويتر بتحديد الغريدات المعادية للسامية ووضع آلية لتحديد المحتوى غير المشروع، وبريطانيا التي عطلت خدمة البلاك بيرى خلال احتجاجات 2011، كما قامت البرازيل باعتقال المدير التنفيذي لشركة جوجل على خلفية رفضه حظر تسجيل مرئي يوجه انتقادات إلى مرشح في الانتخابات البلدية (1).

ثانيا: المراقبة الإلكترونية:

يعتبر نظام المراقبة الإلكترونية من بين النظم أو الأسس الفنية التي يمكن من خلالها القيام برصد متقدم لأشكال وصور الاعتداءات أو الانتهاكات التي يحتمل أن تكون مهددا للنظم، وهي في نفس الوقت آلية لضمان التدخل السريع من أجل تحديد مصدر هذه التهديدات والتوصل إلى معرفة مرتكبيها، فنظام الرقابة الإلكترونية يعتبر من بين أهم التقنيات أو الأساليب الوقائية ضد أشكال الجريمة الإلكترونية وفي الوقت عينه يمكن اعتبارها ضمن إجراءات التحقيق الجنائي حينما تسمح هذه الآلية بجمع الأدلة واستخلاصها، فنظام مراقبة الاتصالات الإلكترونية إذا هي: (العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني) (2).

ونظام المراقبة قد يتم اللجوء فيه إلى الهاكرز لتحقيقه، كما هو الحال في الولايات المتحدة الأمريكية التي يسخر فيها مكتب التحقيقات الفيدرالية الهاكرز لتقديم السند والعون لهم في الوصول إلى أجهزة الأفراد على الفضاء الشبكي بغرض التصدي لظاهرة الإجرام والإرهاب الإلكترونيين، ولهذا قام هذا المكتب بتوظيف المؤتمر الدولي "ديفكون" المتعلق بالقرصنة في مدينة لاس فيجاس من أجل اكتشاف الكفاءات في مجال التهكير (3).

غير أن الحق في الخصوصية وحرمة المساس بسرية الاتصالات يجعل من هذا الإجراء مرهون بالعديد من الشروط والإجراءات التي يجب الإتيان بها واستقائها، وهذا من أجل التوفيق بين الحق الشخصي للإنسان وبين حق المجتمع في قمع الجريمة (4).

(1) رضوى الخولي، المرجع السابق، ص ص: 9-10.

(2) عزيزة رابحي، المرجع السابق، ص 133.

(3) بشرى حسين الحمداني، المرجع السابق، ص ص: 47-48.

(4) نعيم سعيداني، المرجع السابق، ص 75.

وجدير بالذكر أن موضوع الحماية التشريعية للمعلومات الإلكترونية هو محط نظر بين الفقهاء، إذ يرى جانب منهم أن النصوص التجريبية التقليدية كفيلة بضمان الحماية الجنائية للمعلومات الإلكترونية ذات الطابع الشخصي، في حين يرى جانب آخر من الفقه أن النصوص التجريبية التقليدية غير صالحة لمثل هذا النوع من الاتصالات⁽¹⁾.

ومن الملاحظ بهذا الصدد أن المشرع الجزائري قد حسم الجدل في هذه المسألة حيث خصص نصوصا تجريبية خاصة من خلال القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لحماية الخصوصية في مجال الفضاء الإلكتروني.

نميز في عملية اعتراض البيانات -كصورة من صورة المراقبة الإلكترونية- بين نوعين من البيانات التي تم تجميعها أو تسجيلها، وأول هذه الأنواع هي "بيانات المحتوى" والمقصود بها محتوى الاتصال، بمعنى الرسائل أو المعلومات التي يحملها الاتصال، وأما النوع الثاني فيه بيانات الحركة والتي عرفتها اتفاقية بودابست على أنها: (بيانات كومبيوتر متعلقة باتصال عن طريق نظام الكومبيوتر والتي تنشأ عن طريق نظام كومبيوتر يشكل جزءاً في سلسلة الاتصالات توضح المنشأ والمواجهة، الزمن، والتاريخ، والحجم، والمدة أو نوع الخدمة)⁽²⁾.

وجدير بالملاحظة أن هذين النوعين من البيانات فيهما تقارب من حيث معناها غير أن هناك اختلاف بين وشاسع بينهما من حيث مقدرا المساس بالخصوصية، حيث تكون شديدة أو مهمة حينما يكون موضوع المراقبة هو محتوى البيانات، ولذلك لإن ضمانات حمايتها تكون أكبر، ومع هذا فإن هناك دول مثل فرنسا لا تضع مفهوما موحدا لهذين النوعين وبذلك فإن الضمانات الخاصة بحمايتها تكون موحدة⁽³⁾.

يشترط لسلامة إجراءات المراقبة الإلكترونية أن تتوافر على ثلاث شروط موضوعية هي؛

- الشرط الأول: يتعين أن تكون المراقبة الإلكترونية تحت إشراف القضاء وبإذن منه، كما هو واضح من خلال نص المادة 05 من القانون رقم 04-09، حيث ساقطت في مضمونها أنه لا

(1) محمود أحمد طه، التصنت والتلصص على سرية الاتصالات الشخصية بين التجريم والمشروعية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2014، ص ص: 35-36.

(2) توفيق مجاهد، طاهر عباس، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 03، كلية الحقوق والعلوم السياسية، جامعة الشهيد حقه لخضر، الوادي، الجزائر، ديسمبر 2018، ص

ص: 76-103: <https://www.asjp.cerist.dz/en/article/72222>

(3) عائشة بن قارة مصطفى، المرجع السابق، ص ص: 105-106.

يجوز إجراء عمليات المراقبة إلا بإذن من السلطة القضائية المختصة⁽¹⁾، فالسلطة القضائية إذا هي صاحبة الاختصاص بصفة عامة في منح الإذن الخاص بعملية المراقبة الإلكترونية وما ذلك إلا ضمان واجب لمشروعية اعتراض الاتصالات الإلكترونية، وهو الصورة التي يتجلى فيها ترسيخ الدولة الحق والقانون، بالإضافة إلى استدال صفة الشرعية على الإجراءات والتصرفات التي مكن أن يتم اتخاذها بهذا الصدد من قبل جهاز الضبطية القضائية⁽²⁾

- **الشرط الثاني:** يتعين أن يكون هناك ضرورة داعية إلى اتخاذ مثل هذا الإجراء، والضرورة تكون متحققة حينما يكون من العسير بلوغ نتيجة تخدم سير عملية البحث والتحري أو التحقيق دون الاعتماد على المراقبة الإلكترونية وهذا ما أسس له المشرع الجزائري من خلال الفقرة "ج" من نص المادة 04 من القانون رقم 04-09⁽³⁾، فشرط الوقاية من حدوث بعض الجرائم يعد المبرر القانوني الذي يبرر إجراء المراقبة الإلكتروني، ومن بينها؛ وجود معلومات ملائمة وتامة تنبأ باحتمالية وقوع شكل من أشكال الاعتداء على منظمة المعلومات بنسق وشكل يتهدد معه النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو في حالة ما إذا كان هناك من المعلومات التي تسري على الفضاء الإلكتروني ما يفيد وقوع اعتداء على أمن الدولة وتنبه إليه، ففي هذه الأحوال والظروف كلها يتم الترخيص بالمراقبة الإلكترونية⁽⁴⁾

- **الشرط الثالث:** مراعاة نطاق التوظيف المنصوص عليه قانونا: تبين المادة 04 من القانون الجزائري لمكافحة الجريمة الإلكترونية رقم 04-09 على الحالات والظروف التي يجوز ويسمح فيها باللجوء إلى إجراء عملية المراقبة الإلكترونية، والمشرع الجزائري قد ساق هذه الحالات والظروف على سبيل الحصر لا التمثيل، ومن بينها؛ احتمال اعتداء على منظومة معلوماتية تابعة لمؤسسات الدولة أو الدفاع الوطني أو النظام العام أو الاقتصاد، فضلا عن الوقاية من الجرائم الماسة بأمن الدولة⁽⁵⁾، وجرائم الموصوفة بالإرهاب والتخريب⁽⁶⁾

(1) نعيم سعيداني، المرجع السابق، ص 185.

(2) عبد الوهاب ملياني، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، السنة الجامعية، 2016-2017، ص 331.

(3) نعيم سعيداني، المرجع نفسه، ص 185.

(4) عبد الوهاب ملياني، المرجع السابق، ص 332.

(5) المرجع نفسه، ص 332.

(6) فتية رصاع، المرجع السابق، ص 113.

المطلب الثاني:

حماية الأصول المادية للفضاء الإلكتروني

تعتبر الطبقة المادية التكوينية للفضاء الإلكتروني من بين الأهداف الحيوية التي تستهدفها هجمات الإرهاب الإلكتروني، ونجاح تلك الهجمات من شأنه أن يحدث أثارا وخيمة على البنى التحتية الحرجة، ذلك أن شل هذه الطبقة يفضي إلى شل الكثير من جميع النشاطات التي يتم تسيرها وإدارتها بها، كما أنها قد تؤدي إلى ضياع ملفات ومعلومات جوهرية، وهذا ما يدعو إلى حمايتها من خلال تحوير المباني بجملة من إجراءات الحماية والأمان تقاديا للتسلل إليها ومنعا للإضرار بها (الفرع الأول)، كما يجب أن تشمل الأمان، حماية الموظفين من الأخطار التي تتهددهم وحماية المنظمة منهم أيضا ذلك لأنهم قد يشكلون خطرا على المنظمة من الداخل (الفرع الثاني)، ولا ريب بعد ذلك أن تشمل المعدات والأجهزة بالحماية نظرا لأهميتها القصوى في البناء التكويني الجوهري للفضاء الإلكتروني، وأي تهديد لها هو تهديد بكل الفضاء الإلكتروني (الفرع الثالث).

الفرع الأول: حماية المباني

تعتبر حدود المباني من بين أهم البنى التحتية التكوينية للفضاء الإلكتروني، فهي تتمتع بأهمية بالغة في بناء المنظمة الإلكترونية، إذ تمثل الحاضنة التي يجتمع فيها الموظفين والمعدات والتجهيزات الإلكترونية بالإضافة إلى عنصر المعلومات، ولذلك تعد من بين الأهداف الاستراتيجية التي يمكن أن تعمل جماعات الإرهاب الإلكتروني على استهدافها، وعليه يتعين إحاطتها بالحماية اللازمة (أولا)، وضبط عملية الدخول إليها والخروج منها درءاً للمخاطر والتهديدات الإرهابية (ثانيا).

أولا: ضبط حدود المباني ومكانها

يبرز تأمين محيط المباني باعتبارها عنصرا من العناصر التكوينية للمنظومة الإلكترونية على قائمة العناصر التي يجب على المشرفين أي كان مجال وطبيعة عملهم بالسهر على حمايتها والحفاظ عليها من أي تهديد أو هجوم يترصدها، وفيما يلي بعضا من أهم الأسس والمعايير والآليات التي من خلالها يتحقق هذا الغرض.

1- نظام الأسوار:

تعتبر أسوار الحماية حاجزا ماديا وفي الوقت ذاته حاجزا نفسيا لكل من يأمل أو يتطلع إلى التسرب والتغلغل إلى داخل المنشأة، وفي الوقت ذاته تعتبر الأسوار عاملا مساهما في التمكين المتقن لفرض الرقابة على عمليتي الدخول والخروج من المنشأة، والأسوار لها بطبيعة الحال أسس

تقوم عليها وقواعد تضبط فنياتها، حيث يأخذ بعين الاعتبار فيها تحقيق الهدف المرجو منها وتيسير عملية الرقابة بالأدنى التكاليف المستطاعة⁽¹⁾.

2- المراقبة السمعية البصرية:

تجلت في عصرنا هذا الكثير وبشكل واضح وبيّن، الكثير والعديد من المصالح والمنافع في استخدام كاميرات المراقبة، وتنامت الرغبة في الحصول عليها بشكل حاد، حتى ربت وأصبحت منتشرة في كل مكان، فهي متفشية في المساكن ومقرات العمل وغزيرة في السبل والطرق، الأمر الذي جعلها تكتسي أهمية خاصة للوقاية من العوارض، كما أنها تجلب ظروف الأمان للعوائل أو لأرباب العمل في مختلف القطاعات والمنظومات أيًا كانت طبيعتها⁽²⁾.

ولعل من أهم المجالات التي يمكن أن تستخدم فيها كاميرات المراقبة وغيرها من وسائل المراقبة المرئية والسمعية مجال الأمن الفيزيائي للبنية التحتية التكوينية للفضاء السيبراني، بما في ذلك البنايات التي تشتمل على الخوادم وتلك التي تتم فيها صناعة الأجهزة الإلكترونية أو تلك المؤسسات والقطاعات التي يتم تسييرها وإدارتها من خلال الحواسيب وأنظمة المعلومات كما هو الحال في المطارات وإدارات توزيع الطاقة وغيرها.

تعرف هذا الأجهزة في التشريع الإماراتي على أنها: (يقصد بها أي كاميرات أو معدات، أو أجهزة أخرى مماثلة، أو نظام إلكتروني يتضمن عددا من المعدات والأجهزة، تتم به، أو عبره، المراقبة الأمنية، المرئية و/أو الصوتية داخل أو خارج أي مبني خاضع لأحكام هذا المرسوم، أو يستخدم لرصد و/أو تسجيل حركة الأشخاص والمركبات، أيًا كان نوعها، بداخل المبني المعني أو خارجه، أو بداخل أي جزء معين فيه)⁽³⁾.

أما المشرع القطري فيعرف كاميرات وأجهزة المراقبة على أنها: (كل جهاز معد لنقل وتسجيل الصورة، بهدف مراقبة وملاحظة الحالة الأمنية)⁽⁴⁾.

وأوجب المشرع القطري على مالكي المنشآت تركيب مثل هذه الكاميرات من خلال نص المادة

(1) سر الختم عثمان نصر الشيخ، مفاهيم حماية المنشآت بين النظرية والتطبيق: (بالنظر إلى إدارات ومؤسسات حماية المنشآت)، بحث ماجستير في الدراسات الجنائية والأمنية، كلية الدراسات العليا والبحث العلمي، جامعة الرباط الوطني، 2016، ص 199.

(2) آمال عبد الجبار حسوني ونادية كعب جبر، كاميرات المراقبة بين دواعي الاستعمال وانتهاك الخصوصية، مجلة الحقوق، المجلد 01، العدد 29-30، كلية الحقوق، الجامعة المستنصرية، 2017، ص ص: 18-01 <https://www.iasj.net/iasj/article/142832>

(3) المادة 08/02 من المرسوم الأميري رقم 07 لسنة 2016، بشأن تنظيم تداول واستخدام أجهزة ومعدات الرقابة على المباني في عجمان.

(4) المادة 05/01، القانون رقم (9) لسنة 2011 المتعلق بتنظيم استخدام كاميرات وأجهزة المراقبة الأمنية، صدر بتاريخ 08 ماي 2011، في الجريدة الرسمية العدد 07، المنشورة بتاريخ 20 جوان 2011.

الثانية حين نص على أنه: (يجب على مالكي المنشآت والمسؤولين عن إدارتها، تركيب كاميرات وأجهزة المراقبة الأمنية وتشغيلها على مدار الساعة، على أن يكون لها غرفة تحكم)، وأحاطها المشرع بمجلة من الواجبات الأخرى بعد تركيبها وهذا ما يتضح لها من خلال نص المادة 03 إذ تنص على أنه: (على المنشآت صيانة كاميرات وأجهزة المراقبة وتحديثها، بصفة دورية ومستمرة، لضمان حسن أدائها، واستمرارية مطابقتها للمواصفات الفنية التي تحدد بقرار من الوزير. ويكون للجهة المختصة، الحق في دخول المنشآت، بغرض التفتيش على الكاميرات وأجهزة المراقبة، للتأكد من مدى مطابقتها للمواصفات الفنية ومدى فاعليتها في تحقيق الغرض منها)⁽¹⁾.

ونظرا خطورة هذا النوع من الآليات على الخصوصية وعلى الأمن والنظام العام في الدولة فقد أحيط بجملة من التشريعات والقوانين التي تتضمن جملة من الأحكام والشروط التي توفق بين الغرض الأمني الذي ترمي إليه مثل هذه الأجهزة وبين خطورتها على الأمن والنظام العام والخصوصية من جهة أخرى، فالمشرع الجزائري على سبيل المثال قد حدد شروط مثل هذه الأجهزة الحساسة من خلال المرسوم رقم 09-410 المؤرخ بتاريخ 10 ديسمبر 2009، يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة⁽²⁾، وتشمل الأجهزة الحساسة في مضمون هذا القانون عدة فئات حددها ملحق هذا المرسوم ومن بينهما تجهيزات المراقبة عن طريق الفيديو.

نظم المشرع الفرنسي بدوره المراقبة باستعمال هذه الوسائل في الأماكن ذات الطابع العمومي من خلال قانون 21 يناير 1995، ووفقا لنص المادة 10 منه، تم تحديد الهدف من استخدام المراقبة بهذه التقنية، ووضع عقوبة مدتها 03 سنوات وغرامة مالية 45 يورو على وضع أنظمة مراقبة متلفة دون الحصول على ترخيص أو القيام بعملية تسجيل من غير الحصول على إذن، وبالعقوبة ذاتها في حالة عدم إتلاف التسجيلات القديمة التي تجاوزت المدة القانونية للاحتفاظ بها⁽³⁾.

وهناك تشريعات والقرارات أخرى منظمة لهذا الشأن ومن بينها قرار 20 مايو 2020 المتعلق باللقب المهني لفني أنظمة الأمن، والأمر رقم 1427 لسنة 2019 المؤرخ في 23 ديسمبر 2019 والمتعلق بشروط اختبار استخدام الكاميرات الفردية من قبل موظفي مراقبة إدارة السجن في سياق مهامهم، وتكون أحكام استعمال هذه الوسائل خاضعة للقانون رقم 2004-801 المؤرخ في 06

(1) المادة 02 و03، القانون رقم (9) لسنة 2011.

(2) الجريدة الرسمية عدد 73 الصادرة بتاريخ 13 ديسمبر 2009.

(3) لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي وحجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي وعوامل حجية الصورة والصوت في الإثبات الجنائي: (دراسة مقارنة)، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2018، ص 199.

أغسطس 2004 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وتعديل للقانون رقم 78-17 المؤرخ في 06 يناير 1978 المتعلقة بمعالجة البيانات، الملفات والحريات.

وهناك بعض القوانين تمنع لفئة معينة اقتناء هذه المعدات والتجهيزات من بعض الدول، كما هو الشأن في الولايات المتحدة الأمريكية التي أصدرت قانونا يمنع على الوكالات الفيدرالية الأمريكية شراء المعدات والخدمات من بعض الشركات الصينية التي تراقب كاميراتها العديد من المباني⁽¹⁾.

ثانيا: ضبط الدخول والخروج:

يعد الخروج والولوج من وإلى المنشأة من بين أبرز التحديات الأمنية التي تواجه عناصر الفضاء الإلكتروني، فالدخول والخروج يمثل ثغرة أمنية على الجهات المختصة إحاطتها بالعناية اللازمة منعا لأي هجوم يستهد من خلاله الإضرار بأنظمة المعلومات وطبقاتها المادية المختلفة، وسنسوق لهذا الغرض بعضا من التقنيات والآليات التي من خلالها يمكن تأمين عملية الدخول والخروج:

أ- نظام البصمة الإلكترونية AFIS:

يندرج نظام البصمة الآلي ضمن الأنظمة الحوسبية، فمناطق عمل هذا النظام متعلق بسلسلة من الوظائف التي تتعلق بدراسة البصمة إذ تعمل على حفظ وفرز وتقيب ومعالجة البصمة وبعد ذلك الوصول إلى مخرجات تمثل الحاصل المبتغى، فهو بتعبير آخر؛ نظام يعمل على إجراء مقابلة بين السمات المختلفة التي تتسم بها كل بصمة، وهذا من أجل الوصول إلى تبين هوية الفرد، وأما عن التركيبة البنيوية لهذا النظام فهي إما مادية أو برمجية، إذ يتم استخدام الماسح الضوئي فيها وبرامج فاحصة، ومن خلال ذلك تتبلور السمات التي تتميز بها البصمات، وبعد ذلك تخزن على شكل بيانات يتم من خلالها التعرف على هوية المستخدم حال النفاذ إلى النظام⁽²⁾.

وقد بدأت بالفعل كثير من الوزارات والأجهزة الحكومية وعدد من المنشآت الخاصة في تبني هذا النظام والاعتماد عليه في نظام حضور وانصراف موظفيها، وذلك لإثبات حضورهم وانصرافهم عن العمل⁽³⁾، فضلا عن دوره في إثبات هوية الداخلين على المنشأة والمنصرفين عنها.

(1) Alexis ZEMA, Aux États-Unis, s'affranchir des caméras de surveillance chinoises vire au casse-tête, Publié le 8 août 2019, vu le 20 juillet 2012 à 22:43h, sur le lien: <https://www.lefigaro.fr/secteur/high-tech/aux-etats-unis-s-affranchir-des-cameras-de-surveillance-chinoises-vire-au-casse-tete-20190808>

(2) أميمه عثمان حسن عبد الرحيم، دور نظام البصمة الآلي (AFIS) في التعرف على مجهولي الهوية: (دراسة حالة: ولاية الخرطوم)، بحث لنيل درجة الماجستير في علوم الأدلة الجنائية، كلية الدراسات العليا والبحث العلمي، جامعة الرباط الوطني، يناير 2017، ص ص: 53-54.

(3) عبد الصبور عبد القوي علي المصري، التجارة الإلكترونية والقانون، الطبعة الأولى، دار العلوم للنشر والتوزيع، القاهرة، 2009، ص 64.

إلا إن هذا النظام قد وجهت إليه انتقادات خطيرة ذات صلة بصحة المستخدمين له، فقد حظّر أحد المتخصصين في الأمراض الجلدية من العواقب الوخيمة التي ستتجر عن استخدام نظام البصمة الإلكترونية، وذلك لكونها سببا من أسباب الإصابة بسرطان الدم، وسرطان الجلد، فضلا عن الأمراض الجلدية الأخرى كالجراثيم والفطريات التي تنتقل عبر الملامسة من الموظفين المصابين بها إلى الأصحاء منهم، كما أنها تعد سببا في تبدل تركيبة الحمض النووي "الطفرة الوراثية"⁽¹⁾.

ب- نظام التعرف من خلال قزحية العين:

تعود فكرة التعرف على الأشخاص من خلال قزحية العين إلى طبيب العيون الدكتور فرانك بورش (Frank Burch) عام 1936، ثم طور الطبيين آران سفير (Aran Safir) وليونارد فلوم (leonard flom) والأكاديمي جون دوجمان (John Daugman) العملية الأولى لتحديد الهوية على أساس القزحية، وحصلت على براءة اختراع سنة 1994 لصالح جون دوجمان، وتسمى طريقة دوجمان بـ شيفرة القزحية (Iriscode) وتعتبر هذه الشيفرة وراء غالبية الأنظمة التي تم تسويقها في مجال أثبات الهوية على أساس قزحية العين⁽²⁾.

و يتأسس هذا النظام على الاختلافات الواردة في الثقوب والشقوق المحيطة بحدقة العين والتي تختلف من شخص لآخر في عددها وحجمها ولونها والمسافة بينها، فيتم مسحها وأخذ صورة لها، ثم يتم تخزينها وتشكيل صورة مشفرة عنها⁽³⁾.

ج- نظام التعرف من خلال شبكية العين:

يعمل هذا النظام من خلال أخذ العلامة الفريدة التي تتميز بها الشبكية عبر توجيه الضوء إلى قاع العين، وبعدها يتم التقاط صورة لشبكة الأوعية الدموية التي تنتشر على غشاء الشبكية في قاعدة العين، والتي تشترك قناتها مع العصب البصري، وتتسم هذه الخريطة بمميزات خاصة، إذ أن طريقة توزع الأوردة والشرابين في قاع العين يختلف في الشخص ذاته، فطريقة توزيعها في العين اليمنى يتباين على ما هي عليه في العين اليسرى، وتجدر الإشارة أيضا إلى أن مثل هذا

(1) عبد الصبور عبد القوي علي المصري، المرجع السابق، ص 64.

(2) Houda BENALIOUCHE, Multimodalité Biométrique dans le cadre d'une Application d'Authentification, Doctorat en science, Option : Informatique, Faculté des Sciences, Université Ferhat Abbas Sétif 1, 2016, P.33.

(3) عزة حازم زكي، نمذجة نظام برمجي للتحقق من الهوية عن طريق بصمة العين، المجلة العراقية للعلوم الإحصائية، المجلد 12، العدد 22،

كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق، 2012، ص ص: 149-166: <https://iasj.net/iasj/article/67724>

الإجراء لا يترتب عنه أن شكل من أشكال الضرر لسلامة العين أو الدماغ، فهو لا يعدو أن يكون تصويراً لقاع العين⁽¹⁾.

د - البصمة الصوتية:

تعد البيانات التي يتم تحديدها بناءً على بصمة الصوت غير قابلة للمحاكاة، ذلك أن الذي يهيمن عليها هي نغمات الصوت وطبقاتها، إذ أن حقيقة هذه الطريقة تعتمد على أحبال الصوت والفرغات المتواجدة في كل من عضوي الأنف والفم، وهذه الاستراتيجية قد تم توظيفها لإحباط عمليات السرقة وهذا عن طريق وصل مداخل البيوت بالبصمة الصوتية التي تخص مالكيها، ولا يمكن بذلك لأحد فتح بابها إلا لمن تنطبق بصمته الصوتية مع تلك التي تم تسجيله فيه، وبمجرد أن يصدر الملك صوتاً أو يطلق عبارة فإن الباب يفتح آلياً ذلك، أن الآلة ستميز تلك النبرة وتقوم بإعدادها على شكل تردد يبلغ سرعة 1/1000/ثا، وتستعمل هذه الاستراتيجية في الدول التي اعتادت على استعمال بصمات اليد وهذا لإحباط عمليات السرقة والتسلل إلى البيوت⁽²⁾، وتستعمل أيضاً في حماية المباني الحيوية، كما تستعمل أيضاً في غلق الخزانات الحديدية أو بعض الغرف التي تحوى على أجهزة حساسة، ولذلك فإنه من الضروري حماية المنشآت والمباني التي تشتمل على معدات آلية حساسة أو تلك التي تنطوي على حواسيب الخدمة العامة أو خوادم الإنترنت بهذه التقنية.

هـ - البطاقة الذكية:

يعرف عبد الحسن البطاقة الذكية على أنها: (عبارة عن بطاقة بلاستيكية مزودة برقاقة ذات دائرة إلكترونية صغيرة لها القدرة على إدخال البيانات ومعالجتها كحاسوب إلكتروني صغير دون شاشة أو لوحة مفاتيح، بوصفها وحدة معالجة مركزية ذاكرة الوصول العشوائي وتخزين البيانات مثل شريحة الجوال)⁽³⁾.

وتنقسم البطاقات الذكية من حيث طريقة تواصلها من جهاز القارئ الآلي إلى ذلك بطاقات؛ البطاقة التلامسية، والتي يقترن عملها بإدراج البطاقة داخل هذا الجهاز لتبادل إرسال البيانات،

(1) عزة حازم زكي، المرجع السابق.

(2) عباس أحمد الباز، البصمة البصرية والصوتية ودورها في الإثبات الجنائي شرعاً وقانوناً، الندوة العلمية: (الجوانب الشرعية والقانونية لاستخدام الوسائل العلمية الحديثة في التحقيق الجنائي)، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، عمان، 23-25 أبريل 2007، ص 10.

(3) نقلاً عن: أحمد باحزر وعلي أحمد العمري، أمن المعلومات في البطاقات الذكية، المؤتمر العلمي الدولي العاشر: (التحديات الجيوفيزيائية والاجتماعية والانسانية والطبيعية في بيئة متغيرة)، المنعقد في 25-26 يوليو 2019، إسطنبول، تركيا، شبكة المؤتمرات العربية، ص ص: 653-668.

<http://proceedings.sriweb.org/akn/index.php/art/article/view/267>

البطاقة اللا تلامسية، ولا يشترط فيها الاقتران المادي بجهاز القارئ، وهناك بطاقة تحمل الخاصيتين معا⁽¹⁾.

كما تنقسم أيضا من حيث قدرتها التخزينية إلى؛ البطاقات ذات الدائرة المتكاملة، وهي على نوعين، بطاقات المعالج الأصغر، وبطاقات الذاكرة التي تستطيع تخزين ما يعادل 14 كيلوبايت، وهناك بطاقات الذاكرة الضوئية التي تمتلك قدرة على تخزين ما يجاوز 04 بيت من البيانات⁽²⁾.

الفرع الثاني: حماية الموظفين والحماية منهم:

تتطلب السياسية الأمنية الناجحة والفعالية إحاطة كاملة بكل العناصر الجوهرية للبيئة الإلكترونية، ولما أدركنا في بحثنا أن الموظفين والعمال يشكلون عنصرا جوهريا في بنية الفضاء الإلكتروني فإنه من الضروري العمل على حمايتهم من الأخطار التي تتهددهم (أولا)، كما يجب العمل أيضا على الحماية منهم، فالواقع قد أثبت أن غالبية الهجمات والتهديدات الأمنية السيبرانية كان سببها الرئيس هم الموظفين، سواء أكان ذلك مقصودا أم خطأ مهنيا حال أداءهم لأعمالهم (ثانيا).

أولا: حماية الموظفين:

لقد ذهب دراسات علم ضحايا الجريمة إلى إقرار وتوكيد أن طائفة من المهن والوظائف يكتنفها ويحيط بها خطر غير طبيعي، مما يترتب عنه تضاعف وقوع ممتهنيها فريسة سائغة لمجازفات وأخطار الجرائم، ففي بعض الأحيان يتعرض الفرد لمظاهر الإجرام دون أن يكون له يد فيها، ولا يربطه بمعالمها أي رابط سلبي كانت أم إيجابا، لكن احتلاله لموقع أو لمهنة يمتنها أحاطته بتهديدات جعلته ضحية من ضحايا الجريمة وهذا الأمر عائد إلى طبيعة الوظيفة التي تحتوى على عوامل تجر إليها المجرمين⁽³⁾.

وهذا التأكيد إنما جاء مما لاحظته علماء علم الضحايا حيث أنهم يحوزون على الكثير من المعطيات والحجج التي تثبت وتقر مذهبهم في ذلك، ومع أن العلماء لم يجمعوا على السمات التي تفرق وتضع الحدود في تصنيف الضحايا عمن سواهم غير أنهم لا يعلمون ولا يلمحون إلى طائفة

(1) ناصر إسماعيل وأمل حسن علوان وتغريد جليل، البطاقة الذكية وأثرها في التقليل من بعض المخاطر المصرفية: (دراسة استطلاعية لعينة من زبائن مصرف الرافدين-فرع الخضراء-)، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد 37، كلية بغداد للعلوم الاقتصادية الجامعة، 2013، ص ص: 77-96: <https://www.iasj.net/iasj/article/82829>

(2) المرجع نفسه.

(3) الطاهر سواكري، خصائص ضحايا الإجرام: (محاولة للتحليل السوسيولوجي)، مجلة الآداب والعلوم الاجتماعية، المجلد 07، العدد 11، جامعة البليدية 02، الجزائر، جوان 2014، ص ص: 01-09: <https://www.asjp.cerist.dz/en/Articles/354>

معينة على أنهم ضحايا بصورة عشوائية، بل يملكون من المادة العلمية المستندة إلى الكثير من العوامل والأسباب التي توضح وتبين أسباب وقوعهم ضحايا⁽¹⁾.

تشير الإحصائيات إلى أنه بالإضافة إلى العديد من الأطباء النفسيين وأطباء الأعصاب الذين وقعوا ضحايا لمرضاهم الذين كانوا يعالجون عندهم، فقد تعرض العديد من عمالة نقل الأموال والعاملين في القطاع المصرفي والسائقين الذين يعملون في وسائل النقل لجرائم السرقة وقد تصل في بعض الأحيان تلك الجرائم لحد إزهاق أرواحهم، وقد يكون القضاة ورجال الشرطة أيضا محلا لجرائم القتل والختف لهم أو لعائلاتهم من طرف عصابات المافيا والجماعات الإرهابية⁽²⁾.

وهناك عوامل أخرى تساهم أيضا في وقوع الشخص ضحية لجريمة وهي أسباب تنصب في إطار بحثنا هذا، ومن بين أهمها وأبرزها؛ التهور، فكثيرا ما يصدر عن الضحية فعل إيجابي مع كونه في جوهره فعل سلبي من شأنه أن يكون سببا في وقوعه ضحية، وقد يكون هذا السلوك في شكل التهور من الضحية، فالضحية المتهورة هي تلك التي لا تتخذ ما يلزم من احتياطات فيما تفعله، بل تتصرف بشكل متهور وبلا أدنى مبالاة، فشخصية مثل هذه الضحية تتسم بالمغامرة والتهور واقتحام المخاطر دون القلق عما ينجر كما نجد أيضا صفة الإهمال بعض الضحايا، فالشخص الذي يشوبه الإهمال والذي لا يتبع التعليمات المختلفة واللازمة والضرورية التي تفرضها وتُمليها الحياة اليومية، قد يقع ضحية للمعتدين الذين سيستغلون هذا الطيش والإهمال والنظر إلى مثل هذا الشخص باعتباره فريسة سائغة⁽³⁾، وهناك من الضحايا أيضا من هو جاهل، ومساهم، ومتسرع، ومتطوع، وراضي⁽⁴⁾.

وليس غريبا ولا بعيدا أن نعتقد بعد ذلك أن العمال والموظفين الذين يمتنون أعمالا متعلقة أو منصبة في مجال العمل السيبراني لمثل هذه الاعتداءات والجرائم، فمن وجهة نظرنا، أن المجال السيبراني وما يتعلق من مهن مرتبطة بالفضاء الإلكتروني بامتهان البرمجة الدقيقة أو عمال تقانة

(1) محمد الأمين البشري، علم ضحايا الجريمة وتطبيقاته في الدول العربية، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2005، ص 60.

(2) عقباوي محمد عبد القادر ومنصوري المبروك، تأثير الصفة الخاصة للضحية في وقوع الجريمة وأثرها على عقوبة الجاني في التشريع الجزائري: (دراسة مقارنة)، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 07، العدد 06، المركز الجامعي لمتنراست، 2018، ص ص:

<https://www.asjp.cerist.dz/en/article/63473:232-209>

(3) Nadia Nihel BOUAYAD-AGHA, Le role de la victime dans le passage à l'acte, Mémoire de magistère en sciences criminelles et criminologie, Faculté de droit, Université Aboubekr BELKAID, Tlemcen, Année universitaire : 2004-2005, P.25.

(4) جمال معنوق ونور الهدى قدوح، مساهمة الضحايا في السلوكيات الإجرامية والعنف الواقعة عليهم في المجتمع الجزائري، مجلة الآداب والعلوم الاجتماعية، المجلد 08، العدد 13، جامعة البليدة 02، الجزائر، جويلية 2015، ص ص: 11-28: <https://www.asjp.cerist.dz/en/Articles/354>

الحكومات الإلكترونية أو المتخصصون في أنظمة التسيير والإدارة الإلكترونية في المؤسسات المالية أو الاقتصادية بصفة عامة، وحتى عمال قطاعات البنية التحتية التي يتم إدارتها بالاعتماد على النهج الإلكترونية وتقنياتها هم من بين أهم الموظفين أو العمال الذين من المحتمل جدا أن يتعرضوا للجرائم ويكونوا ضحايا لها بمناسبة مهنهم.

كما أن الموظفين الذين يعملون في مثل هذه المجالات الحساسة كثيرا ما يتسمون بالتهاون والتهور والإهمال، فالموظف الذي يعمل على اللعب في البرامج الحوسبية تهورا منه يعرض نفسه لهجمة إلكترونية، والذي يقوم بإهمال التحديثات أو إهمال أجهزة المعلومات الخاصة به يعتبر ضحية إهمال قبل أن يكون ضحية إرهاب، وهذا الأمر ينطبق أيضا على الضحية الجاهل والمستفز والمتسرع وغيرهم.

ونحن إذ نتعرض إلى هذه المسألة في بحثنا هذا، لا نقصد منها ما يقع على الموظف في المنظومات المتعلقة بالمجال الإلكتروني بعينها من أفعال مادية، إذ أنها ليست من قبيل الجرائم الماسة بالفضاء الإلكتروني بشكل مباشر، وبذلك فهي مدرجة ضمن الجرائم التقليدية التي تخضع للقواعد العامة حتى وإن ارتبطت أغراضها بالإرهاب عموما، وإنما المقصود منها في بحثنا هو ما يترتب عن الجريمة الواقعة على هذا الموظف من تهديد للبيئة الإلكترونية.

فجريمة خطف الموظف هنا على سبيل المثال ليست مقصودة لذاتها، وإنما مقصودة لغيرها، وهي ارتكاب عمليات إرهابية على الساحة الإلكترونية من خلال هذا الموظف، كتعذيبه لإجباره على الكشف عن مفاتيح التشفير، أو تقديم معلومات ذات أهمية عن أساليب الدخول إلى الشبكات الداخلية الآمنة، أو خطف ذويه لإجباره على تنفيذ هجمة إلكترونية من داخل المنظومة، كما تشمل أيضا وقوع الموظف ضحية لجريمة الإرهاب الإلكتروني في حالة ما إذا تم استهدافه على الفضاء الإلكتروني بمناسبة وظيفته، كأن يتعرض حاسوبه لهجمات إرهابية أو أن يتم ابتزازه أو سرقة أرصده البنكية، أو من خلال تهديده من خلال الوسائل الإلكترونية.

هناك من اتجاهات الوقاية من الجريمة من يرى أنه يجب العمل في هذا المجال بإقرار إجراءات احترازية من أجل حفظ وحماية ضحايا الجريمة المحتملين، ويذهب أصحاب هذا الاتجاه إلى التصريح أنه يتعين إقرار هذه الإجراءات والتدابير بكل الأساليب المتاحة كالإعلام والتوعية والتعليم وهذا من أجل تعديل السلوكيات والتصرفات التي تتصف بهذا هذه الشريحة أو الأشخاص الذين يعتبرون من قبيل الضحايا المحتملة، كما تعمل أيضا على تشجيعهم وتحفيزهم على أخذ

التدابير والتعاليم الاحتراسية والوقائية اللازمة من أجل حماية أنفسهم وأموالهم من أي شكل من أشكال الاعتداء⁽¹⁾.

وعليه فإنه من أجل حماية العمال والموظفين الذين يعملون في سك تكنولوجيا المعلومات يجب العمل على وضع إجراءات وقائية من أجل الحفاظ والحماية عليهم من أي شكل من أشكال الاعتداء الذي قد يقع عليهم بمناسبة تأديتهم لمهامهم، ولاسيما حمايتهم من أي هجوم ذو غرض إرهابي، سواء أكان الهجوم تقليدياً أو سيبرانياً، ويكون ذلك بكل الوسائل المتاحة في يدي الإدارة.

يتعين بذلك ويفرض على الإدارة المسؤولة عن أمن المعلومات ألا تفي فقط بما يقع عليها من مسؤولية في تنفيذها للاستراتيجيات الأمنية فحسب، لكن يتعين عليها أيضاً أن تلعب دوراً تعليمياً يتماشى مع الدور الذي تلعبه في إرغام المستفيدين على العمل في تحقيق السياسة الأمنية، وليس العامل في هذا المجال إلا نقطة ضعف في البنية الأمنية، وعلى هذا يتعين أن تكون لسياسة التعليم والتوعية دوراً كبيراً إلى جانب تنفيذ الاستراتيجيات الأمنية، فذلك من شأنه أن يكون ذو دور في إتمام المهام الأمنية ومعالجتها التخطيطية مع ضمان سرعة إنزالها أرض الواقع، وبيان ما فيها من منافع تعود على المستفيدين، وهذا الأمر بدوره يساهم في بناء قاعدة ثقافية أمنية تكون السند والمعين للاستراتيجيات الأمنية داخل المنظومة⁽²⁾.

كما يجب على الموظفين من وجهة نظرنا من أجل حماية أنفسهم من جهة، والمنشآت التي تعملون بها من جهة ثانية، أن يلتزموا واجب التحفظ وكتمان السر المهني.

أما واجب التحفظ فمضمونه يلمح إلى الضوابط المقررة على حرية التعبير التي يملكها الموظف في الكشف عما له علاقة بالقضايا التي يمكن أن تعد من قبيل جوهر الوظيفة التي يشغلها، ويطلق عليه اسم واجب التحفظ الموضوعي، كما يلمح أيضاً من زاوية أخرى إلى ذلك الالتزام الذي يلتزم به الموظف في توقيير وظيفته والكف عن القيام بأي تصرف من شأنه أن يتعارض ويتصادم مع ما تتمتع به الوظيفة من جدية وهدف، سواء أكان ذلك حال قيامه بالمهام المسندة إليه أو خارجها، وهذا ما يطلق عليه اسم واجب التحفظ الشخصي⁽³⁾.

(1) صباح مصباح محمود الحمداني ونادية عبد الله الطيف أحمد، ماهية السياسة الوقائية الجزائرية، مجلة جامعة تكريت للعلوم القانونية والسياسية،

المجلد 2، العدد 1، الجزء 1، جامعة تكريت، العراق، 2017، ص ص: 35-80: <https://www.iasj.net/iasj/article/155755>

(2) أحمد بن علي عبد الله طارش، رؤية استراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية، رسالة ماجستير في

العلوم الاستراتيجية، كلية العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2015، ص ص: 56-57.

(3) فريد رناي، واجب تحفظ الأعوان العموميين في القانون الجزائري، مجلة القانون، المجتمع والسلطة، المجلد 04، العدد 02، جامعة محمد بن

أحمد، وهران 02، 2018، ص ص: 173-182: <https://www.asjp.cerist.dz/en/article/48045>

أما السر المهني فيمكن تعريفه على أنه: (كل شيء يعرفه صاحب المهنة أثناء أو بمناسبة ممارسة مهنته أو بسببها وكان في إفشائه ضرر لشخص أو لعائلة أو لشركة، إما لطبيعة الوقائع أو للظروف التي أحاطت بالموضوع)، ويعرف أيضا على أنها: (الواقعة تعد سرا إذا كانت هناك مصلحة يعترف بها القانون في حصر العلم بها في شخص أو أشخاص محددين) ⁽¹⁾.

وتجدر الإشارة بهذا الصدد إلى أن واجب التحفظ باعتباره التزاما يقع على الموظف في حريه التعبير يختلف عن كتمان السر المهني، ذلك أن السر المهني هو واجب تقني يفرض على أي عاملين سواء أكان تابعا للقطاع العام أو للقطاع الخاص ومضمون هذا الواجب هو إخفاء وكتمان وعدم اطلاع الغير عن المعلومات التي تعدها الإدارة المستخدمة من قبيل الأسرار المهنية ⁽²⁾، ويكون إفشاء هذه الأسرار إما بشكل كلي أو جزئي لها، أو بشكل صريح أو ضمني، سواء أكان بشكل تلقائي أو غير تلقائي، سواء أكان مباشرا أو غير مباشر ⁽³⁾.

فواجب التحفظ وكتمان السر المهني وعلى الرغم من أنهما يعتبران ضمانا لحماية المنظومة التي يعمل فيها الموظف إلا أنها في نفس الوقت تعتبر حماية للموظف نفسه، فاطلاع الغير على طبيعة عمله وعلى الأسرار التي يمكن أن يكون مرخصا له بالاطلاع عليها تجعله عرضة للاعتداء عليه بغية الحصول على أسرار أكثر حيوية، وهذا هدف أغلب الإرهابيين الناشطين على الفضاء الإلكتروني، وكتمه لذلك كله يعتبر حماية له من تعرضه لأي شكل من أشكال الهجمات الإرهابية سواء أكان ذلك على شخصه أو على ذويه أو على حساباته وحواسيبه الشخصية والوظيفية.

يقتضي الأمر أيضا أن يتم تدريب الموظفين على العادات الآمنة حال استعمالهم لأجهزة الحاسب الآلي، بما في ذلك الامتناع عن الضغط على الملفات التي يتم إرفاقها بالبريد الإلكتروني غير معروف المصدر، واستعمال البرامج المرخصة حصرا، وتخزين كلمة السر الخاصة وعدم كشفها لأي كان، والعمل على وضع الحاسب الآلي في موضع آمن وموثوق وبشكل خاص عند السفر ⁽⁴⁾.

(1) سلمان علي حمادي الحلوسي، المسؤولية المدنية الناشئة عن إفشاء السر المهني: (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص ص: 20-21.

(2) فريد رناي، المرجع نفسه.

(3) سلمان علي حمادي الحلوسي، المرجع نفسه، ص ص: 30-36.

(4) يوسف خليل يوسف عبد الجابر، مدى فعالية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية، رسالة ماجستير في المحاسبة، كلية الأعمال، جامعة الشرق الأوسط، كانون الثاني، 2013، ص ص: 23-24.

كما يتعين على الموظفين اتخاذ الحيطة والحذر من ضياع حواسيبهم المحمولة أو المساعد الرقمي الشخص الخاص بهم، فهذه الأجهزة في الغالب من الأغراض القابلة للضياع والسرقة، وضياعها أو سرقتها يفضي إلى ضياع للملفات والبيانات، وضياع معلومات الاتصال، كما يفضي أيضا إلى إمكانية استخدام هذه الأخيرة في اتصال الغير بالشبكة، فيجب إذا أن يحتاط لذلك، ويتخذ أسباب الوقاية بعدم تركها في أماكن تعرضها لمثل هذه التهديدات، وأن يعمل على جعل الوصول إلى الحاسب محويا بكلمة المرور، وأن يكون له دائما نسخة احتياطية من الملفات والمعلومات (1).

ثانيا: الحماية من الموظفين:

يمثل الأفراد الذين يستخدمون ويوظفون في مجال الأنظمة الآلية في المؤسسات واحدا من الأخطار والتهديدات والمخاوف الشديدة التي قد يكون لها بالغ الأثر على أمن المعلومات وسلامتها، فكثرا ما يمكن أن يقوم الموظف أو العامل في هذا المجال حال قيامه بعمله بارتكاب هفوة أو زلة سواء أكان ذلك حال استخدام الأنظمة أو حال إعداد البرامج أو خلال إعداد البرامج، وقد ينجر عن ذلك ضعف في كفاءتها وفعاليتها، دون أن ننسى أن الموظف أو العامل في هذا الميدان قد يكون شخصا مشكوك في أمره، وبهذا سيمثل أعظم التهديد على النظام بكامله (2).

فالمقصود الأول من أمن الأفراد العاملين هو: (مجموعة من الإجراءات والقواعد تتخذ لضمان ولاء الأفراد العاملين بالمنشأة الهامة في عدم تسريب المعلومات المتداولة من خلالها بحكم وظائفهم بالمنشأة للجهات المعادية، وكذلك ضمان ولاء هؤلاء الأفراد في الدفاع عن المنشأة ضد أي اعتداء محتمل وضد الكوارث الطبيعية والصناعية) (3).

إذ يطلع الموظف والعامل داخل منظومته على الكثير من المعارف والأسرار بما يتعلق بشأن الكثير من المواضيع التي تمثل نظم المعلومات أهمها وأبرزها، وهم يفهمون في الوقت ذاته ما يحوم حولهم من تطبيقات وتنفيذ لنظم الرقابة، وهم مطلعون أيضا على ما في النظام من مواطن القوة والضعف والقصور، وهم يملكون فوق ذلك كله، إمكانية التعامل مع المعلومات، ولهم الحق في بلوغها بما منح لهم من ترخيص للدخول إليها، وهذا كله يضع المنظومة في وضع حرج، إذ أن

(1) إيهاب أبو العزم، مفاهيم تكنولوجيا المعلومات، الرخصة الدولية لقيادة الحاسب الآلي، الإصدار الرابع، الطبعة الأولى، دار الحكمة للطباعة والنشر والتوزيع، ليبيا، 2012، ص 91.

(2) أشرف عبد المحسن الشريف، المرجع السابق.

(3) خالد محمد سليمان محمد، تقييم فاعلية الإدارة الأمنية في تأمين المنشآت الهامة: (دراسة حالة رئاسة قوات الشرطة)، بحث تكميلي لنيل درجة الماجستير في العلوم الأمنية والجنائية، كلية الدراسات العليا والبحث العلمي، جامعة الرباط الوطني، يونيو 2018، ص ص: 29-30.

بلوغ العمال عديمي الأمانة إلى البيانات قد يمنحهم فرصة العبث فيها بإتلافها أو تشويبها وتبديلها، وهذا كله إن كان يوحى على شيء فهو أن العامل داخل المنظومة يمثل أبرز مصدر للمخاطر التي تهدد نظم المعلومات الحوسبية (1).

وعلى هذا يجب العمل على التحري والتحقيق عن كل طلب يتم تقديمه إلى المنشأة من أجل الالتحاق بها، والنظر بعمق في ملفات الطالبين وتحليلها تحليلًا دقيقًا بما في ذلك النظر إلى أبعادهم السلوكية، والتأكد من انتفاء انتمائهم إلى تنظيمات راديكالية، وخاصة الموظفين الذين يتقدمون لمناصب أمنية، ويمكن للقائمين على المنشأة الاستعانة بما في حوزة الوكالات الرسمية المختصة للقيام بذلك، ويتعين أيضا على رجال الأمن داخل المنشأة الاستمرار في رصد الموظفين حال تواجدهم فيها وفرض الرقابة والتقصي على من يثيرون الريبة فيهم أو من هم على معرفة واسعة بأسرار المنشأة، تفاديا لعنصر المفاجأة، والتحقيق في أي نشاط مريب يهدف إلى هدم المنشأة من الداخل، والإحاطة الكاملة بالتوجهات التي يعتمدها الموظفون، والعمل على حل النزاعات التي تطرأ بين الموظفين أو بينهم وبين المسؤولين (2).

كما يمكن للغرض نفسه، العمل على حظر تجوال داخل المنظومة، ويكون ذلك من خلال تجزئتها إلى أقسام وفروع، ويحظر على أساسها لكل موظف قسم، الدخول إلى قسم غير مدرج في التصريح الممنوح له، ومن المستحسن أن يكون هناك ببطاقات مكتوبة أو أوسمة بألوان مختلفة يتم بها الاستدلال على موضع التشغيل وموقعه، ويكون مجديا لو تم اللجوء في ذلك إلى مسؤولي تلك الأقسام والفروع (3).

ويمكن أيضا الحد من هذا الظاهرة التي تشكل تهديدا صارخا بأمن وسلامة البيئة الإلكترونية من خلال اعتماد سياسة تشريعية صارمة، ونظام عقابي متناسب مع طبيعة التهديد والآثار المترتبة عنه، سواء أكان ذلك من خلال نصوص التجريم وأحكامها المتواجدة في التشريع المعمول به، كجريمة التواطؤ المنصوص عليها في القانون الجنائي الجزائري، أو أحكام تشديد العقوبات في بعض الجنايات والجناح التي يرتكبها الموظفون والقائمون بوظائف عمومية المنصوص عليها في القانون الجنائي الجزائري (4).

(1) لخضر دلال وإسماعيل بن ديلمى، المورد البشري خطر أم حصن للمنظمة: (مدخل أمن المعلومات في ظل الذكاء الاقتصادي، الأفاق للدراسات الاقتصادية، المجلد 05، العدد 01، كلية العلوم الاقتصادية والعلوم الاجتماعية وعلوم التسيير، جامعة العربي التبسي، تبسة، أبريل 2020، ص ص: 124-136: <https://www.asjp.cerist.dz/en/article/113712>

(2) فرج بن مزنان العتيبي، فاعلية خطط الحماية الخارجية للمنشآت الحيوية لصد الهجمات الإرهابية: (دراسة مسحية على الضباط المكلفين بأمن وحماية المنشآت الحيوية)، دراسة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2007، ص ص: 135-136.

(3) المرجع نفسه، ص 135.

(4) المادة 143 من الأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم.

أو من خلال استحداث نصوص تجريبية وعقابية خاصة بمثل هذه الجرائم، وقد نصت المادة 25 من مشروع قانون مكافحة الجريمة الإلكترونية على أنه: (إذا وقعت جريمة من الجرائم المنصوص عليها في هذا القانون بمعرفة أحد الموظفين العموميين وكان ذلك أثناء وبسبب تأديته لوظيفته فيجب عند الحكم بالإدانة أن تحكم بعزله من وظيفته)⁽¹⁾.

ويجب على الإدارة العمل على تنمية الولاء التنظيمي لدى موظفيها، فالولاء التنظيمي يعتبر داخل ضمن دائرة محددات تصرفات المواطنة التنظيمية، إذ أن العلاقة بين الولاء التنظيمي والمواطنة التنظيمية شديدة وقوية، فالأول يؤدي حتما إلى الثاني، وهذا الولاء الوجداني الشديد للموظف يصير منه شخصا أكثر رضا بأغراض المنظومة التي يعمل فيها، وتجعله أكثر شعورا بالانتماء إليها باعتباره جزء منها، فالولاء التنظيمي إذا؛ يمثل شعور وجدانيا كائنا حينما يكون الموظف مقتنعا وموقنا بأهداف منظومته، ويتجلى حينما يسعى إلى تحقيق هذه الأهداف وكأنها أهداف خاصة به⁽²⁾، وبهذا يكون الولاء الوظيفي سدا منيعا ضد الإغراءات الخارجية التي تبتغي الوصول إلى تفويض أمن المنظومة من خلال تحقيق هجمة داخلية من خلال الموظف.

كما يجب أيضا على الإدارة العمل على إدراج نظام الحوافز، فقد أكدت الأبحاث أن نظام الحوافز بما في ذلك نظام الترقية يتمتع بشأن عظيم وقدر كبير في التعاضد والتضافر مع المنظومة ومع زملاء العمل والوظيفة أيضا⁽³⁾، فهناك علاقة ورابطة قوية بين الأسباب الدافعة للعمل وبين الآليات أو الحوافز التي تقوم بها المنظومة من أجل ضمان المزيد من الحرص على العمل، فنظام الحوافز الذي يتمتع بفاعلية ونجاعة يعمل على جذب الكفاءات وزرع الوفاء والانتساب فيهم للمنظومة التي يعملون فيها⁽⁴⁾.

وهذا بطبيعة الحال سيكون له أثر كبير في حماية الفضاء الإلكتروني من ثلاث جوانب؛ أولهما اتقاء شر الموظف وسخطه الذي قد يكون له أثر خطير على سلامة بيئة الفضاء

(1) مشروع قانون مكافحة الجريمة الإلكترونية المقدم من النائب تامر الشهاوي، التنظيم القانوني والجرائم الإلكترونية: (ما بين أمن المعلومات وتقييد الحريات)، مركز هردو لدعم التعبير الرقمي، القاهرة، 2018، ص 09.

(2) منوبة مزوار، أثر الحوافز في الولاء التنظيمي مع دراسة حالة عينة من المؤسسات العمومية الجزائرية، المجلة العلمية المستقبل الاقتصادي، المجلة العلمية المستقبل الاقتصادي، المجلد 01، العدد 01، مخبر مستقبل الاقتصاد الجزائري خارج المحروقات، جامعة امحمد بوقرة، بومرداس، الجزائر، ديسمبر 2013، ص ص: 125-157: <https://www.asjp.cerist.dz/en/article/81420>

(3) نصر قاسمي ومنال عبد الليلة وأسماء بركان، نظم الحوافز والدافعية للإنجاز، مجلة التنمية وإدارة الموارد البشرية، المجلد 03، العدد 08، مخبر التنمية التنظيمية وإدارة الموارد البشرية، جامعة البليدة 02، لونيبي علي، الجزائر، فيفري 2017، ص ص: 126-135:

<https://www.asjp.cerist.dz/en/article/41210>

(4) نعيمة سعادي، نظام التحفيز لرفقي الفرد والمنظمة، مجلة دراسات اقتصادية، المجلد 02، العدد 22، جامعة زيان عاشور، الجلفة، أبريل 2014، ص ص: 237-246: <https://www.asjp.cerist.dz/en/article/86606>

الإلكتروني، ولاسيما المنظومة التي ينتمي إليها، وثانيهما هو تفادي الإغراء الخارجي له، وثالثهما، هو توطيد علاقة الموظف بوظيفته، وولائه لمنظومته.

الفرع الثالث: حماية الأجهزة والمعدات:

إن الحماية المادية المقررة لجملة العناصر المكونة للفضاء الإلكتروني ضد أي هجوم إرهابي لا بد أن يشمل بدوره الكوابل البحرية التي تعد أهم هذه العناصر، إذ تمثل الشريان الناقل للمعلومات والاتصالات عبر جميع أقطاب العالم، ولا يمكن للفضاء الإلكتروني أن يتسع مجاله لولاها وأي مساسا بها هو مساس بعنصر تكويني جوهري في بناء الفضاء الإلكتروني (أولا)، كما يجب أيضا حماية أجهزة الحاسوب وملحقاته وغيره من المعدات الإلكترونية الحساسة (ثانيا).

أولا: حماية الكوابل البحرية:

تشكل المنظمات الإرهابية والذئاب المنفردة خطرا كبيرا على الكوابل البحرية، فرغم أنها كوابل تقع في قاع البحار والمحيطات ورغم أنه ليس من اليسير أن تقوم منظمة إرهابية صغيرة أو أفراد ينشطون في مجال الأعمال الإرهابية والتخريبية بلوغها بسير وسهولة، ولكنه أمر غير مستبعد، ومع هذا فإن الأمر ليس بالعسير عن العدوان والإرهاب الذي يمكن أن تمارسه الدول، سواء أكان ذلك في وقت السلم أو في وقت الحرب.

إن الوسط البحري يعد وسطا غير مستقر، فهو كثيرا ما يشكل أكبر تهديد على الكوابل والخطوط الاتصالية التي تصل بين مختلف القارات والبلدان، ويكون ذلك أكثر تهديدا في فترة النزاعات الحربية، ففي عرض البحر الصومالي قطع أحد الكوابل البحرية سنة 2017 ونتج عنه انقطاع في الاتصال في المنطقة بأسرها للعديد من الأسابيع، وانجر عن ذلك خسائر وأضرار اقتصادية فادحة، تقدر بعشر مليون دولار في اليوم الواحد، وقد أحصى الفريق الحكومي الدولي المعني بهذا الشأن 300 تشويش مقصود أو غير مقصود على الكوابل البحرية، والذي يعطل في كل عام حركة الإنترنت عبر هذه الكوابل، ولا شك أن انقطاع مثل هذه الكوابل يحمل بين طياته آثارا حادا وشديدا على النشاط الاقتصادي للبلد، سواء أكان ذلك من خلال إبطاء سرعة تدفق الإنترنت، أو من خلال مكابدة خسائر مالية، ففي عام 2008 حدث وأن تعرضت الكوابل المارة في البحر المتوسط لعمليات قطع في مصر، فكان أن فقدت شبة الجزيرة العربية وحتى الهند ما بين 40 % إلى 50 % من قدرة شبكتها⁽¹⁾.

(1) Félix BLANC, Géopolitique des câbles: une vision sous-marine de l'internet, les carnets du CAPS, N026, technologies et puissance, France, juin 2018. PP.31-50:

<https://www.diplomatie.gouv.fr/fr/le-ministere-et-son-reseau/le-centre-d-analyse-de-prevision-et-de-strategie/publications-les-carnets-du-caps/les-carnets-du-caps-no26-technologies-et-puissance/>

إرغم أن خطورة الهجمات التي تستهدف البنية التحتية للشبكات السيبرانية والإلكترونية كثيرا ما تكون ذات أثر كبير وخطير على الدول المتقدمة التي تعتمد بشكل مفرط وكبير على تكنولوجيا الاتصال والفضاء السيبراني إلا أنه فيما يتعلق بالهجمات المادية على الكوابل البحرية لا يعد كذلك] وهذا لأن قلة أعداد هذه الألياف يمكن وبمفرده أن يشكل ظروفًا لهشاشة الدولة وضعفها، كما أنه يمكن أن يكون عاملا مسهلا لسيطرة وهيمنة الأنظمة السياسية الاستبدادية والديكتاتورية على مفاصل الدولة وشعبها، ففي فرنسا مثلا والتي تتمتع بتنوع نقاط الوصول والمشغلين وأصحاب الكابلات يجعل من غير المحتمل ولا من المرجح أن يصاب الإنترنت بالانقطاع، في حين أن هذا الحال لا ينطبق على سوريا مثلا، والتي شهدت قطعا لبضعة أيام في نوفمبر 2012 ومايو 2013، والتي أثرت أحيانا على جميع الاتصالات، ومثل هذا الهبوط الشديد يوحي بأن العمل متعمد لأن سوريا لها أربع كابلات وكان من المفترض أن يعمل أي من تلك الكوابل للحفاظ على بعض حركة الاتصال في حالة ما إذا كان هناك عطل فني، ولكن هذا لم يحدث، مما دل على هذا الضعف في بنية الكوابل إنما يخدم الأنظمة المستبدة والديكتاتورية (1).

وقد شهدت مصر أيضا مثل هذا الحادث خلال ثورتها، حيث توقف الإنترنت لمدة 5 أيام في جانفي 2011، ولم يتم تجاوز هذا الظرف إلا من خلال تدخل القراصنة الذين قاموا بتوظيف خطوط الهاتف وأجهزة المودم القديمة لإعادة الاتصال، ومع ذلك وكما هو ظاهر فإن الوصول المادي المقيد للإنترنت لم يكن العامل الوحيد في ذلك، فمصر كانت تملك في ذلك الوقت 04 مشغلين وجميعهم عانوا من قرارات النظام وأغلق الوصول فعليًا، وبذلك فإن تنوع المشغلين في بلد ما هو مصدر قوة وعائقا في وجه الأنظمة الاستبدادية، ومع هذا يبقى الأمر غير كافيا كما أشرنا، فمنطقة قناة السويس تظل منطقة حاسمة لأمن العديد من الكوابل البحرية بين أوروبا وجنوب شرق آسيا، أو في الأمانة الأخيرة أفريقيا، فمنذ القطع المشار إليه تم البحث عن طرق بزية أخرى من كخلال سوريا ثم إيران والعراق غير أن هذه الحلول بكاد تكون أكثر أمانا (2).

إن الوصف الذي ينسب إلى الكوابل البحرية والمتمثل في "البنية التحتية الحرجة" بسبب وظيفتها الاستراتيجية والحيوية يدعو إلى القول بأن التهديد السيبراني في الواقع يطال هذا النظام، فالدراسات المقارنة المجرات على نقاط ضعف شبكات الأرض التي تمتلك نفس الدور والوظيفة تسمح ببيان أو توضيح معالم بعض فرضيات التهديدات المادية أو السيبرانية التي يمكن تطبيقها

(1) Dominique BOULLIER, " Internet est maritime: les enjeux des câbles sous-marins", RIS, La Revue Internationale et Stratégique, n° 95, Automne 2014, pp. 149-158:

<https://www.cairn.info/revue-internationale-et-strategique-2014-3-page-149.html>

(2) Dominique BOULLIER, Op.cit

على الكوابل البحرية، فدراسة الانقطاعات على النظام الكوابل التي تم جردها حتى الآن كانت ذات فائدة، فالنظرة العامة على الحالات المعروفة تجعل من الممكن تقييم نقاط الضعف الحالية والاتجاهات المستقبلية⁽¹⁾، وعلى المتخصصين في مجال الإلكترونيات بالمشاركة مع الفزيائيين وعلماء البحار إيجاد حلول عملية تخصصية من أجل حماية هذه البنية التكوينية الحرجة للفضاء الإلكتروني، والعمل على صياغة استراتيجية أمنية قائمة على تقديرات العلماء كل في مجال تخصصه.

لم نهتدي في مسيرة بحثنا إلى آليات وتقنيات ميكانيكية أو تقنية يمكن من خلالها الوقاية من الهجمات التي تستهدف الكابلات البحرية، غير أن هناك آليات يمكن من خلالها الكشف عن الضرر واستدراكه، إذ يستخدم مالكو ومشغلو الكابلات مراكز عمليات الشبكة لمراقبة حركة البيانات "من خلال شبكاتهم على مدار الساعة طوال أيام الأسبوع، وهي تملك القدرة على تحديد أي انقطاع لحركة المرور الشبكي على الفور، كما تمتلك القدرة على الكشف عن تغيير في ظروف التشغيل العادية للقطاع البحري للشبكة، وسيحاولون بعدها استعادة حركة الشبكة في أقرب وقت باستخدام أنظمة الكابلات الأخرى، وقد يتعذر هذا الأمر إن كان العطب والضرر متزامنا مع عدة أعتاب أخرى، حيث يؤدي ذلك إلى التأخر في الاستعادة⁽²⁾.

وتبقي الحماية القانونية هي الضمان الأكبر لحماية الكوابل البحرية، إذ حفت الكوابل البحرية بجملة من الاتفاقيات الدولية التي تضمن سلامتها، وتتدارك ما قد يأتيها من تهديد وخطر، ووما يعثرها من فساد وعطب، ومن بين أهم المعاهدات والاتفاقيات الدولية نجد الاتفاقية الدولية المتعلقة بحماية الكابلات البحرية، التي تم التوقيع عليها في باريس في الرابع عشر من شهر مارس 1884، والمصادق عليها بتاريخ 23 أبريل 1888، ونجد أيضا اتفاقية سولاس المتضمنة سلامة الأرواح في البحار والتي دخلت حيز التنفيذ في 25 مايو 1980، والتي تضمنت المادتين 29 و34 التي تنظم القيود البحرية التي يجب أن تمتثل لها شركات السفن وتحديد المناطق⁽³⁾.

(1) Camille MOREL, menace sous les mers: les vulnérabilités du système câblé mondial, la découverte "Hérodote", N° 163, 2016, PP.33-43. <https://www.cairn.info/revue-herodote-2016-4-page-33.htm>

(2) Tara DAVENPORT, Submarine cables, cybersecurity and international law: (an international analysis), Journal of Law and Technology, volume 24, issue 01, Catholic University of America, USA, 2015, article 04: https://scholarship.law.edu/jlt/vol24/iss1/4/?utm_source=scholarship.law.edu%2Fjlt%2Fvol24%2Fiss1%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages

(3) Le cabinet JURISLITIS, CABLES SOUS MARINS – QUEL DROIT APPLICABLE , 24 octobre 2018, vu le 03 juillet 2020, à 06:13H, sur le site: <http://www.delpanqueparis.fr/fr/nos-publications/cables-marins-droit-applicable/>

كما وقد فرضت اتفاقية الأمم المتحدة للبحار على الدول وفاء منها بالتزاماتها الدولية العمل على احترام الكوابل البحرية وحمايتها وصيانتها، إذ تنص المادة 02/21: على أنه: (تحتزم الدولة الأرميلية الكابلات المغمورة الموجودة التي وضعتها دول أخرى والمارة خلال مياهها دون أن تمس اليابسة. وتسمح الدولة الأرميلية بصيانة هذه الكابلات واستبدالها عند تلقيها الإخطار الواجب بموقعها وبنية إصلاحها واستبدالها)، وتنص أيضا في المادة 114 على أنه: (تعتمد كل دولة ما يلزم من القوانين والأنظمة للنص على أنه إذا سبب أشخاص خاضعين لولايتها ممن يمتلكون أحد الكابلات أو خطوط الأنابيب المغمورة تحت أعالي البحار، عند وضع أو تصليح هذه الكابلات وخطوط الأنابيب، كشر أو إصابة أي من الكابلات أو خطوط الأنابيب الأخرى، تحملوا تكاليف التصليحات)⁽¹⁾.

وأوصت كذلك الجمعية العامة للأمم المتحدة الدول باتخاذ كل التدابير اللازمة لحماية كابلات الألياف الضوئية المغمورة في البحار والمحيطات وأن تتصدى للمسائل المتعلقة بها بشكل كامل، وفقا لقواعد القانون الدولي، ذلك أن تلك الألياف تعد ناقلة لغالبية البيانات والاتصالات على سطح الأرض، وإن ذلك كسبها أهمية اقتصادية بالغة على المستوى الدولي، والأمن الوطني للدول، ولذلك فإنه حري بالدول وضع تشريعات وأنظمة وطنية لضمان حماية الكابلات المغمورة من خلال تجريم أي فعل قصدي كان أو رعونة وإهمال يتسبب في إحداث ضرر بها⁽²⁾.

كما يمكن أيضا حماية الكوابل البحرية بقوانين الهجمات السيبرانية التي ترتقي إلى الهجمات الحربية، ومن ثم فإنه من حق الدول إقرارا لمبدأ الدفاع الفردي أو الجماعي عن النفس الدفاع عن نفسها في حالة وقوع أي هجوم متعمد على أنظمة الكابلات البحرية، ويمكن لمجلس الآن أن يثبت استخدام القوة ضد الدول التي تهاجم الكوابل البحرية بشكل متعمد إذا ارتقت إلى درجة هجوم مسلح، غير أن هذه القوانين لا يمكنها أن تعالج بشكل فعال حماية هذه البنية التحتية المادية للفضاء الإلكتروني لعدة أسباب، فيجب أن ترتقي هذه الهجمات إلى الوصف المذكور آنفا أو تكون مهددة للسلم والأمن العالميين، كما أنه من الصعب توقيع المسؤولية لعدم وضوح الجناة بالإضافة إلى أنها لا تتعرض إلى الجناة من غير الدول، ويجب أيضا أن يخضع الدفاع عن النفس هنا لقواعد التناسب وأن تكون الملاذ الأخير بعد فشل الآلية الدبلوماسية⁽³⁾.

يمكن أيضا أعمال الاتفاقيات الدولية لمكافحة الإرهاب وتطبيقها على الهجمات التي تنفذ ضد أنظمة الكوابل البحرية، كاستعمال متفجرات بشكل غير قانوني ومتعمد لتدمير منشآت البنية

(1) اتفاقية الأمم المتحدة لقانون البحار فتح التوقيع عليها بتاريخ 10 ديسمبر سنة 1982 جامايكا، ودخلت حيز النفاذ بتاريخ 14 نوفمبر 1994.

(2) قرار الجمعية العامة في 29 ديسمبر 2014، قرار رقم 69-245: المحيطات وقانون البحار.

(3) Tara DAVENPORT, Op.cit.

التحية، غير أن هذا لا ينطبق إلى على مواقع هبوط الكوابل البحرية وليس بالضرورة على الكوابل نفسها، كما أنها لا تغطي الهجمات مرافق كوابل من نوع "NMS" (1).

ثانياً: حماية الحواسيب والمعدات الحساسة الدقيقة:

تعتبر حماية المباني وحماية الموظفين التي سبق وأن تطرقنا إليها في بحثنا من أهم السبل والآليات الضامنة لحماية الحواسيب وملحقاته وغيرها من أجهزة المعالجة الآلية للبيانات، فلا شك أن حماية المباني وضمان ولاء الموظفين وحمايتهم مما يهددهم يشكل حماية أساسية لتلك الأجهزة، من الوصول إليها وتعطيل عملها، فيجب إذاً، من أجل حماية هذه الأجهزة والمعدات العمل على تطبيق سياسة أمنية مشددة وفق ما أشرنا إليه، من أجل حماية تلك المنشآت.

غير أن هناك تهديد يشكل خطراً جسيماً على تلك المعدات، إذ ليست الحماية المادية للمباني والموظفين ضماناً كاملاً لكل الهجمات، فقيام الإرهابيين بشن هجوم باستخدام القنابل الكهرومائية والحقول المغناطيسية لن ينفذ معه تأمين المبني، ذلك أن مثل هذا الهجوم لا يستوجب الوصول المادي إلى المبني أو المنشأة، فيكفي أن تكون القنبلة على مقربة من المبني ليتم تدمير كل ما في المبني من حواسيب.

تعتبر الآلية الأكثر فعالية للدفاع ضد القنابل الكهرومغناطيسية هو منع وصولها وذلك من خلال تدمير منصات إطلاقها أو عربات توصيلها، ومع هذا لا يعتبر الأمر ممكناً في كل الأحوال، وبذلك يجب أن يتم تقسيم الأنظمة التي يرجح أو يتوقع تعرضها لمثل هذه الهجمات، والآلية الأكثر فعالية لذلك هي جعل كل المعدات في حاوية يطلق عليها اسم قفص فاراداي، والذي يحول دون وصول المجال الكهرومغناطيسي إلى المعدات المحمية، لكن مع ذلك يبقى هناك مشكل تغذية هذه المعدات بالطاقة الكهربائية، وهذا ما يمثل نقطة ضعف دائمة، إذ يجب أن تدخل قناة موصلة للكهرباء إلى الحاوية، ولذلك يجب تركيب أجهزة إيقاف كهرومغناطيسية (2).

وقفص فاراداي هو: (عبارة عن هيكل فلزي مصنوع من مادة موصلة، تستخدم لعزل ما بداخله عن المؤثرات الكهرومغناطيسية والمؤثرات الكهربائية الخارجية. وقد سمي قفص فاراداي تيمناً بمكتشفه الكيميائي والفيزيائي الإنجليزي مايكل فاراداي والذي قام باختراعه عام 1836) (3)، فالعالم مايكل فاراداي

(1) Tara DAVENPORT, Op.cit.

(2) Carlo KOPP, The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction, Air & Space Power Journal – Chronicles Online Journal, US Air Force: <https://www.airuniversity.af.edu/ASPI/Archived-Editions/>

(3) الموسوعة الحرة، ويكيبيديا: قفص فاراداي:

https://ar.wikipedia.org/wiki/%D9%82%D9%81%D8%B5_%D9%81%D8%A7%D8%B1%D8%A7%D8%AF%D8%A7%D9%8A#cite_note-1

قد اكتشف أن وصل الكهرباء بصندوق أو قفص حديد يكون له دور حمائي للمعدات المتواجدة داخل ذلك الصندوق أو القفص ضد أي مجال كهربائي، بقطع النظر عن قوة أو كثافة الجهد الكهربائي⁽¹⁾.

يستعمل قفص فاراداي في ضمان الحماية ضد أي ضرر كهربائي أو كهروماني، إذ يعد النظام والوسيلة الأكثر تأثيراً في الحماية ضد الصواعق⁽²⁾، وهو ضمان حماية للطائرة ضد البرق⁽³⁾، كما يستعمل أيضاً في الكيمياء التحليلية من أجل توفير بيئة مناسبة للقسم بالتجارب، ويستخدم في غرف التصوير بالرنين المغناطيسي (IRM)، والمصاعد، والكابلات المحورية واليو إس بي (USB)، كما يستخدم أيضاً للحماية من الهجمات الكهرومغناطيسية⁽⁴⁾.

ققص فاراداي هو الوسيلة الوحيدة التي تمكنا من الوصول إليها في بحثنا للحماية ضد الهجمات الكهرومغناطيسية على البنية التحتية للفضاء الإلكتروني، بالإضافة إلى إجراء عملية تدمير منصات إطلاق مثل هذه القنابل أو تدميرها حال توصيلها، غير أن هناك من القنابل الكهرومائية ما يمكن حمله في اليد، لذلك فمن غير الممكن حينها إلا التعويل على قفص فاراداي لحماية عتاد وأجهزة الحواسيب والخوادم وغيرها من الأجهزة الإلكترونية الحساسة.

وفي الأخير تجدر الإشارة إلى أن كل هذه التقنيات والإرشادات المتعلقة بتأمين بيئة الفضاء الإلكتروني ولا سيما الآليات التقنية من تشفير وبرامج مكافحة الفيروسات والجدران النارية لا تمثل ضماناً كاملاً لحماية الفضاء الإلكتروني، وتبقى دائماً معها إمكانية نجاح الهجمات المصوبة نحوه، ومع ذلك، تبقى بالغة الأهمية وعظيمة النفع، وفي هذا الصدد يقول بروس شنابير: (ليس من السهل القول إنه لا جدوى من أمن الإنترنت، لأن الأمر بعيد عن ذلك. فعلى الرغم من سهولة الهجوم، فإن الدفاع ما زال ممكناً، إذ تتكفل الحماية الجيدة بجعل الهجمات أشد صعوبة، وأعلى تكلفة وأشد خطورة على منفذها، وإذا لم يكن المهاجم متمرساً، يستطيع الأمن المعلوماتي توفير حماية كاملة له)⁽⁵⁾.

ونحن بدورنا نؤيد أطروحة بروس شنابير، لأن المجرمين والإرهابيين الإلكترونيين يعولون كثيراً على الخواص والسمات التي يمتلكها الفضاء الإلكتروني من سهولة الاستعمال وعنصر الخفاء،

(1) ميق بايرن كرانجل، تغلب على الخوف من الطيران، ترجمة: (سيم هاشم)، الطبعة العربية الأولى، مكتبة العبيكان، الرياض، المملكة العربية السعودية، 2002، ص 76.

(2) عبد المطلب أبو سيف، الحماية ضد الصواعق، الموسوعة العربية، تم الإطلاع عليه بتاريخ 03 جويلية 2020، على الساعة 10:21 سا، على الموقع: <http://arab-ency.com.sy/detail/4924>

(3) ميق بايرن كرانجل، المرجع نفسه، ص 76.

(4) الموسوعة الحرة، ويكيبيديا، المرجع السابق.

(5) بروس شنابير، المرجع السابق، ص 218.

والثغرات التقنية والفنية وما إلى ذلك لنجاح عملياتهم، فإذا ما تم تصعيب المهمة عليهم، وتوفير الآليات التي من خلالها يتم الكشف عن تنفيذها، فذلك سيكون له دورا ردعيا كبيرا، أو على الأقل سيكون له دورا محوريا في التقليل من تلك الهجمات، أو التقليل من حجم الأضرار المترتبة عنها.

الفصل الثاني:

الجهود القانونية الدولية لمواجهة الإرهاب الإلكتروني

تتطلب كل استراتيجية موجهة لمكافحة أي شكل من أشكال الظاهرة الإجرامية العمل على بناء صرح قانوني يمكّن الدول من فرض سيطرتها وسلطتها بهدف حماية أمنها القومي من جهة، والمساهمة الفعالة والمثمرة في دعم منظمة التعاون الدولي التي ترمي إلى التصدي لمظاهر الإجرام الدولي واجتثاثها من أصولها، وردع منفذيه وتقديمهم أمام القضاء لتحقيق العدالة وحقوق المجتمع في العقاب، وظاهرة الإرهاب الإلكتروني تعد من بين أهم وأخطر الجرائم التي يتعين على الدول من أجل مكافحتها العمل على تكوين وصياغة نموذج قانوني يمكنها من سد الثغرات التشريعية في هذا المجال، والتصدي لها وفق ما تمليه المبادئ القانونية الأساسية، وعلى أساس الاعتبارات التي يملئها مبدأ الشرعية الجنائية القاضي بآلا جريمة ولا عقوبة إلا بنص صريح، ووفقاً لمبادئ العدالة، لذلك فإن الكثير من الدول قد أقدمت على سن تشريعات وقوانين جنائية تتناول الجرائم المتعلقة بتقنيات المعلومات والاتصال بما فيها جريمة الإرهاب الإلكتروني، وتعمل على تقنين جوانبها الموضوعية والإجرائية على حد سواء، فضلاً عن تعاونها عبر عقد الاتفاقيات المختلفة التي تركز وتعزز عمليات المواجهة والردع القانوني لهذه الظاهرة الإجرامية، وتحقيق الأمن والسلم على الفضاء الإلكتروني.

كما شهدت الدول التي تشعر بقلق كبير إزاء هذا التنامي الذي يميز الإرهاب الإلكتروني، وهذا التعدد في أشكال هجماته ونشاطاته، حركة قانونية شاملة عبر المنظمات الدولية المعهود إليها مهام الحفاظ على الأمن والسلم العالميين، وعبر المنتديات التي تربط بين أعضائها مصالح مشتركة في الحفاظ على أمن وسلامة الفضاء الإلكتروني، وذلك على خلفية إدراك الدول بحجم المخاطر التي تهددها في أمنها إذا ما استشرى توظيف الفضاء الإلكتروني لأغراض إرهابية (المبحث الأول)، ويمتد التعاون القانوني بين الدول ليشمل المساعدات القضائية الدولية، إذ لا جدوى من التشريعات الجنائية الوطنية والدولية إذا لم تكن غير قابلة للتنفيذ على أرض الواقع لأسباب تعود في مجملها إلى فكرة السيادة والولاية القضائية، لذلك فإن الضرورة دعت إلى بناء آليات قانونية توفق بين فكرة السيادة والتعاون الدولي في مجال مكافحة الجرائم، فكان أن استحدثت أساليب قضائية وفنية تساعد الدول على الوقوف أمام الأنشطة الإجرامية على الفضاء الإلكتروني (المبحث الثاني).

المبحث الأول:

الإطار القانوني الدولي في التصدي للإرهاب الإلكتروني

يعد مبدأ الشرعية الجنائية من بين أهم المبادئ القانونية المجمع عليها على الصعيد العالمي، وذلك لما تضمنه من حفاظ على حقوق الإنسان وحياته العامة، وعلى ضوئه تمارس السلطات القضائية وأجهزة إنفاذ القانون عملها، فهو المبدأ العاصم من الانزلاقات الخطيرة التي تتجر من التعسف في استعمال السلطة، فلا يمكن بمقتضى هذا المبدأ تجريم فعل من الأفعال أو توقيع عقوبة من العقوبات أو الإقدام على إجراء أمني إلا بموجب نص قانوني صادر عن هيئة مختصة.

ولما كان الإجرام ظاهرة تتسم بالتطور وتتأقلم مع مستجدات الحياة ، وتطور مع التطور الإنساني حيث دار، فإن ذلك يتطلب حركة تشريعية مستمرة لضمان مسايرتها وملائمتها لما يستجد من صور الإجرام، ومن أجل ذلك، وبعد ظهور الإرهاب الإلكتروني قامت الدول بإجراء تعديلات واستحداث تشريعات وطنية تمكنها من مكافحة وردع هذا الشكل من المستحدث للإجرام دون الإخلال بمبدأ الشرعية الجنائية، ودون أن تقع في تناقض مع التشريعات السابقة التي تعنى بمكافحة الإرهاب التقليدي، كما مدت أيضا من نطاق مكافحتها التشريعية لتتخذ بعدا إقليميا وثنائيا (المطلب الأول)، ومع هذا ونظرا للبعد الدولي للجرائم الإلكترونية بشكل عام، تطلب الأمر توسيع نطاق المكافحة القانونية وإطارها لتشمل هيئة الأمم المتحدة راعية الأمن والسلم العالميين، والمننديات والمنظمات ذات البعد الاقتصادي (المطلب الثاني).

المطلب الأول:

الجهود التشريعية الوطنية والإقليمية

تداركت الكثير من الدول الفراغات التشريعية التي تشوب قوانينها الجنائية في المسائل المتعلقة بالإجرام السيبراني وخاصة تلك المتعلقة بجريمة الإرهاب الإلكتروني في جانبه الموضوعي والإجرائي، وعملت على تسخير القوانين السابقة المعنية بمكافحة الإرهاب التقليدي لتتوافق مع المقاصد العليا التي يرمي الشارع إلى تحقيقها.

وسنسوق في بحثنا سياسية المشرع الجزائري في ذلك لما لها من سبق تاريخي في مواجهة الإرهاب، بالإضافة إلى النموذج الأمريكي لمقامها الدولي من جهة، ولكونها من أوائل الدول الأكثر تعرضا للهجمات السيبرانية (الفرع الأول)، ونظرا لكون جريمة الإرهاب الإلكتروني من الجرائم التي

تعد عابرة للحدود الإقليمية، فإن هناك تعاون قانوني إقليمي دؤوب لصياغة اتفاقيات أو معاهدات متعددة الأطراف لتشكل الإطار العام لمواجهة هذا الإجرام (الفرع الثاني)، ولم تغفل الدول أيضا إقامة اتفاقيات ثنائية بهذا الصدد لتكون سنداً قانونياً للتعاون في مكافحة هذا النوع من الإجرام (الفرع الثالث).

الفرع الأول: التشريعات الوطنية في مكافحة الإرهاب الإلكتروني:

تعد الجزائر من بين الدول التي عانت كثيرا من الظاهرة الإرهابية، فقد كانت محط تقدير العالم في دورها الكبير لمكافحة هذه الظاهرة، ومع ظهور الإرهاب الإلكتروني سعت الجزائر إلى سن قوانين جنائية تتعرض للإجرام السيبراني بشكل عام، قوانين يمكن بكل يسر التوفيق بينها وبين النصوص التقليدية لصياغة نهج كامل لمكافحة الإرهاب الإلكتروني (أولا)، وفي ذات السياق قامت الولايات المتحدة الأمريكية من أجل ردع هذه الظاهرة باعتماد جملة من القوانين والتشريعات التي تتعرض لهذا الظاهرة (ثانيا).

أولا: السياسة التشريعية الجزائرية في مواجهة الإرهاب الإلكتروني:

يعود الإقرار بالدور والمساعي الكبيرة التي تلعبها الجزائر في مكافحة الظاهرة الإرهابية إلى تقدير تجربتها القاسية في استئصالها وإنهائها، والواقع المعاش يرسخ هذا الدور في حسم المشاكل وإقرار السلام، فالدولة الجزائرية لها من التجربة الواسعة في مجال مكافحة الإرهاب، وهذا ما يصنع منها دولة ذات أهمية كبيرة على الصعيدين الإقليم والدولي، فتتمين الدور الكبير الذي لعبته الجزائر في ذلك وخبرتها المستفيضة في مجال فض النزاعات ترتب عنه توافق دولي على النهج الجزائري في هذا المجال⁽¹⁾.

إن الجزائر في عصر الحداثة والمعلوماتية وما تمخض عنها من سلبات وتحديات أمنية والتي يمثل الإرهاب الإلكتروني أكبرها وأكثرها خطورة على الأمن القومي الجزائري، يجعل منها تقف أمام تحدي جديد للحفاظ على أمنها القومي من المخاطر والتهديدات التي تفرزها النشاطات الإرهابية على الفضاء السيبراني، وقد انتهجت الجزائر سياسة تشريعية واسعة في حماية الفضاء الإلكتروني بكل الطبقات التكوينية له من خلال جملة من التشريعات والقوانين التي تضع إطارا شرعيا لهذه الجرائم وتوقع عقوبات صارمة على مرتكبيها.

(1) مخلوف ساحل، المقاربة الجزائرية في مجال مكافحة الإرهاب: (الأسس والآليات)، مجلة الدراسات القانونية والسياسية، المجلد 02، العدد 01،

جامعة عمار ثلجي، الأغواط، جانفي 2016، ص ص: 42-57:

<https://www.asjp.cerist.dz/en/article/37527>

1- قانون العقوبات:

اهتدينا في بحثنا هذا من خلال استقصاء وتحليل النصوص الجنائية المتعلقة بالجريمة المعلوماتية وتلك التي تتناول الجرائم الموصوفة بالأعمال الإرهابية والتخريبية إلى أن المشرع الجزائري حتى وإن لم يوظف مصطلح الإرهاب الإلكتروني أو الإرهاب السيبراني إلا أن هذه الأخيرة مجرمة فعلا في نصوص القانون الجنائي وقد وقعت عليها عقوبات شديدة وصارمة، وعدم توظيفه لمصطلح الإرهاب الإلكتروني لن يفسد للتجريم والعقاب قضية، ولا يتنافى من وجهة نظرنا مع مبدأ المشروعية، ولا يعتبر من قبيل القياس المحذور، إنما يمكن اعتباره تفسيرا وفق مبدأ الغائية، الذي هو منح: (أهمية قصوى للغاية من القانون أو الهدف منه. وهو يعتمد على الإرادة الصريحة "Déclarée" أو المفترضة "Présumée" للمشرع الجنائي)⁽¹⁾.

فالمشرع الجزائري في قانون العقوبات قد وضع قسما كاملا تحت عنوان: " المساس بأنظمة المعالجة الآلية للمعطيات لحماية الفضاء الإلكتروني من الجريمة المعلوماتية، وأقر فيها جملة من العقوبات التي تطال الشخص الطبيعي والشخص المعنوي على حد سواء⁽²⁾، كما طالت العقوبات المقررة في هذا القسم الشريك والمتفق بغرض الإعداد لجريمة أو أكثر من تلك المنصوص عليها في هذا القسم⁽³⁾، كما طالت أيضا عملية الشروع في هذه الجرائم المنصوص عليها في هذا القسم⁽⁴⁾، وتتمثل هذه الجرائم فيما يلي:

- الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو حاول القيام بذلك، كما تضاعف العقوبة المقررة إذا نتج عن عنه حذف أو تغيير للمعطيات، وتضاعف أيضا إذا نتج عن هذه النشاطات تخريب لنظم التشغيل⁽⁵⁾.
- الإدخال أو الإلتفاف أو التعديل عن طريق الغش في معطيات نظام المعالجة الآلية⁽⁶⁾.
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في المعطيات المزنة أو المعالجة أو المرسلّة عن طريق نظام معلوماتي يمكن أن يكون تكون وسيلة لارتكاب الجرائم التي تضمنها هذا القسم⁽⁷⁾.

(¹) أنظر في هذا التعريف: محمد الرازقي، محاضرات في القانون الجنائي: (القيم العام، - الأحكام العامة- الجريمة- المسؤولية الجنائية-)، الطبعة الثالثة، دار الكتاب الجديد المتحدة، لبنان، 2002، ص 43.

(²) المادة 394 مكرر 3، الأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، المعدل والمتمم.

(³) المادة 394 مكرر 5..

(⁴) المادة 394 مكرر 7.

(⁵) المادة 394 مكرر.

(⁶) المادة 394 مكرر 1.

(⁷) المادة 1/394 مكرر 2.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم التي تضمنها هذا القسم⁽¹⁾.

إن هذه الجنج قد ترتقي شدتها وحدثها لتكون أعمالا موصوفة بالأفعال الإرهابية أو التخريبية استنادا لنص المادة 394 مكرر 3 التي تنص على أنه: (تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد)⁽²⁾.

والعقوبات الأشد التي أشارت إليها هذه المادة هي العقوبات التي تضمنها القسم الرابع مكرر 1 المتعلق بالجرائم الموصوفة بأفعال إرهابية أو تخريبية، ولاسيما المادة 87 مكرر 2 والتي تنص على أنه: (تكون العقوبة ضعف العقوبة المنصوص عليها في قانون العقوبات أو في النصوص الخاصة غير المدرجة في هذا النص، بالنسبة لكل الأفعال غير التابعة للأصناف المشار إليها في المادة 87 مكرر أعلاه، عندما تكون نفس هذه الأفعال مرتبطة بالإرهاب أو التخريب)⁽³⁾.

فاستنادا إلى هذا النص قد تكتسب هذه الجنج وصف الأفعال الإرهابية وتعاقب بضعف العقوبات المقرر لها إذا ثبتت علاقتها بالإرهاب أو التخريب وفق تعريف الإرهاب الذي أشارت إليه المادة 87 مكرر.

وقد تكون أيضا أكثر شدة وحدة وصرامة إذا كانت هذه النشاطات تستهدف الأغراض التي أشارت إليها المادة 87 مكرر، فتكون العقوبة حينها وفق نص المادة 87 مكرر 1، وتفصيل ذلك، أنه لما ثبت يقينا أن الكثير من البنى التحتية الحرجة تتم إدارتها وتسييرها باستعمال تقنيات ونظم المعلومات وأن أي ضرر أو تلف أو تعديل فيها قد يشكل تهديدا خطيرا على الأمن القومي للدولة، فإن أي استهداف لتلك البنى من خلال العبث في أنظمتها تدرج في عداد المفهوم الموسع للإرهاب الإلكتروني، وسنسوق لشرح ذلك الأمثلة التالية من واقع نص المادة 87 مكرر:

أشارت المادة الآتفة إلى أن (الاعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في باطن الأرض أو إلقائها عليها أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة للإنسان أو الحيوان أو البيئة الطبيعية في خطر)، إن هذا النص القانوني قد بيّن بما لا يدع

⁽¹⁾ المادة 2/394 مكرر 2.

⁽²⁾ المادة 394 مكرر 3.

⁽³⁾ المادة 87 مكرر 2، الأمر رقم 66-156.

مجالا للشك أن التسميم على هذا النطاق إذا كان غرضه استهداف أمن الدولة وغيرها من الاعتبارات الجوهرية التي أشارت إليها الفقرة الأولى من هذه المادة فإنه يعد عملا إرهابيا تسرى عليه أحكام المادة 87 مكرر 1، ولما كانت منشآت المعالجة الكيميائية للمواد أو المفاعلات النووية تتم إدارتها عبر الفضاء الإلكتروني فإن أي هجوم على تلك الأنظمة من أجل فقدان السيطرة عليها وتسريب ما فيها من مواد بالغة الخطورة ينصب مباشرة في المقاصد التي يحميها هذا النص، وهي إرهاب إلكتروني بالمفهوم الفعلي له.

أورد المشرع الجزائري نصوصا قانونية قاطعة الدلالة وصريحة المعنى في تجريم توظيف الفضاء الإلكتروني لأهداف وأغراض إرهابية من خلال القانون رقم 16-02 المتمم لقانون العقوبات حيث نصت 87 مكرر 11 على معاقبة كل من يستخدم تكنولوجيات الإعلام والاتصال لتوفر أو الجمع العمدي للأموال بأي وسيلة من أجل استخدامها، أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص من دولة لأخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي التدريب عليها أو تسهيل لذلك السفر بالسجن المؤقت من 05 إلى 10 سنوات وبغرامة مالية من 100.000 دج إلى 500.000 دج.

وتعاقب المادة 87 مكرر 12 من نفس القانون (كل من يستخدم تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة) بالسجن المؤقت من 05 سنوات إلى 10 سنوات وبغرامة من 100.000 دج إلى 500.000 دج.

وسّع المشرع الجزائري من دائرة التجريم لتشمل أيضا حماية الطبقة المادية للفضاء الإلكتروني من أي نشاط إجرامي، وهذا الأمر واضح من خلال عدة نصوص قانونية، والتي تمثل المادة 177 أبرزها، حيث تنص على أنه: (يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة مالية من 500.000 دج إلى 1.000.000، كل شخص يرتكب عملا ماديا ضارا بخدمة الاتصالات أو يخرب أو يتلف، بأي شكل كان، الأجهزة أو المنشآت أو مصلات الاتصالات الإلكترونية)⁽¹⁾، كما نص المشرع أيضا في نفس القانون على عقوبة الحبس من 05 سنوات إلى 10 سنوات وبغرامة مالية تتراوح بين 5.000.000 دج إلى 10.000.000 دج على كل شخص يقوم عمدا بقطع كابلا بحريا أو يكون سببا في حدوث تلفا يرتب وقفا أو عطلا كلياً أو

(1) المادة 177 من القانون رقم 18-04.

جزئياً بالاتصالات الإلكترونية⁽¹⁾، وترتقي هذه النشاطات والأعمال إلى وصفها بالأفعال الإرهابية إذا كان الهدف منها استهداف الاعتبارات الجوهرية التي تضمنتها الفقرة الأولى المادة 87 مكرر من قانون العقوبات استناداً إلى ما نصت عليه الفقرة 11 من نفس المادة حين أقرت أن " تخريب أو إتلاف وسائل الاتصال " هو غرض من الأغراض التي تستهدف بها تلك الاعتبارات.

2- قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

يتضمن القانون رقم 04-09 المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على 06 فصول، أهمها وأبرزها:

- **الفصل الثاني:** والذي يتناول أحكاماً متعلقة بمراقبة الاتصالات الإلكترونية، وقد راعى في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية، إذ نص القانون على أربع حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو في حالة توفر المعلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو بمقتضيات التحريات والتحقيق، أو في إطار تنفيذ طلبات المساعدة الدولية المتبادلة⁽²⁾.

- **الفصلين الثالث والرابع:** يعد هذا الفصلين من بين أهم الفصول التي تضمنها هذا القانون إذ عملت على سد الفراغ التشريعي في عمليات البحث والتحري وجمع الأدلة المتعلقة بالجرائم التي تمس أنظمة الحواسيب أو تلك التي تقع بواسطتها، حيث تضمن الفصل الحجز المتعلقة بالمعطيات والالتزامات الملقة على عاتق مزودي الخدمة⁽³⁾.

- **الفصل الخامس:** تضمن هذا الفصل إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث حدد اختصاصاتها ومهامها التنسيقية في مجال الوقاية من الجرائم الإلكترونية⁽⁴⁾.

3- قانون مكافحة التمييز وخطاب الكراهية:

لقد رأينا في سابقا أن للتمييز وخطاب الكراهية القائم على المذهبية أو العرق أو الانتماء الثقافي والسياسي دوراً محورياً وأساسياً في نشوء الإرهاب عموماً والإلكتروني منه خصوصاً، كما تساهم مساهمة مباشرة في توسيع نطاقه وشيوع مظاهره وصوره، ولهذا أولى المشرع الجزائري

(1) المادة 179، من القانون رقم 04-18.

(2) المادة 04، القانون رقم 04-09.

(3) المواد من 05 إلى 12.

(4) المادتين 13 و14.

اهتماما خاصا بمكافحة هاتين الظاهرتين من خلال إصدار قانون الوقاية من التمييز وخطاب الكراهية ومكافحتهما.

وسّعت المادة 02 من القانون المشار إليه من دائرة أشكال التعبير عن التمييز وخطاب الكراهية لتشمل أي شكل من أشكاله والوسائل المستعملة لذلك، وقد رأينا أن الفضاء الإلكتروني يعتبر من أجل وأخطر الوسائل والآليات التي يتم الاعتماد عليها للتمييز ونشر خطاب الكراهية، وقد وضع المشرع الجزائري لمثل هذه الجرائم الخطيرة التي تهدد أمن واستقرار البلاد عقوبات رادعة حيث رفع المشرع الجزائري من عقوبة هاتين الجريمتين إذا كانت مرتكبة باستعمال تكنولوجيا الإعلام والاتصال ليتراوح الحبس فيها من سنتين إلى 05 سنوات وبغرامة مالية من 200.000 دج إلى 500.000 دج⁽¹⁾.

كما شدد العقوبة على الجريمتين السالفتين إن تضمنت دعوة إلى العنف لنتراوح عقوبة الحبس فيها من 03 سنوات إلى 07 سنوات وبغرامة من 300.000 دج إلى 700.000 دج⁽²⁾، وبعقوبة تتراوح بين 05 سنوات إلى 10 سنوات وبغرامة مالية بين 5.000.000 دج إلى 10.000.000 دج على كل من يعمل على إنشاء أو إدارة موقع أو صفحة إلكترونية لنشر معلومات ترويجية من شأنها أن تثير التمييز والكراهية داخل البنية الاجتماعية الجزائرية⁽³⁾.

من الناحية الإجرائية نصت المادة 22 على أنها: (يمكن للجهات القضائية المختصة، وبمناسبة التحقيق في إحدى الجرائم المنصوص عليها في هذا القانون، أن تأمر مقدمي الخدمات أو أي شخص آخر بتسليمها أي معلومات أو معطيات تكون مخزنة باستعمال وسائل تكنولوجيا الإعلام والاتصال تحت طائلة العقوبات المنصوص عليها قانونا) كما نصت المادة 23 على أنه: (يمكن للجهة القضائية المختصة عند الاقتضاء إصدار أمر إلى مقدمي الخدمات بالتحفظ الفوري على المعطيات المتعلقة بالمحتوى و/أو بحركة السير المرتبطة بالجرائم المنصوص عليها في هذا القانون...)، وألزم نص المادة 24 مقدم الخدمات عند تلقيه أمر من الجهة القضائية التدخل الفوري من أجل سحب أو تخزين المحتويات التي من الممكن الاطلاع عليها أو العمل على منع الدخول إليها إذا كانت تشكل جريمة من الجرائم المذكورة، أو العمل على وضع تقنيات تسمح بسحب أو تخزين هذه المحتويات أو جعل الدخول إليها غير ممكن⁽⁴⁾.

(1) المادة ، القانون رقم 05-20.

(2) أنظر : المادة 32، القانون رقم 05-20.

(3) أنظر : المادة 34.

(4) المواد 22 إلى 24.

كما منح نص المادة 25 لضباط الشرطة القضائية صلاحية وضع آليات تقنية للتبليغ عن هذه الجرائم عبر الشبكة الإلكترونية، كما استحدثت المشرع الجزائري إجراء التسرب الإلكتروني إلى منظمة المعلومات من أجل مراقبة الأشخاص المشتبه بهم⁽¹⁾.

وتضع الباحثة عائشة بن قارة مصطفى أشكالا عامة يمكن أن تتجسد فيها عملية التسرب بالإضافة إلى هاتين الجريمتين بقولها: (و يمكن تجسيد عملية التسرب في الجرائم الإلكترونية كاشتراك ضابط أو عون الشرطة القضائية في محادثات غرف الدردشة أو حلقات النقاش حول دعاية الأطفال أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل ممثلهم (مثلهم) ويحاول الاستفادة من معرفتهم حول كيفية اقتحام الهاكر لموقع ما...)⁽²⁾.

ثانيا: السياسية التشريعية الأمريكية لمكافحة الإرهاب الإلكتروني:

تعتبر الولايات المتحدة الأمريكية من بين أهم الدول التي تتعرض للهجمات السيبرانية، ويعود ذلك إلى العديد من الأسباب، فقد نقلت صفحة مكتب التحقيقات الفيدرالية مقولة للمحقق الكبير شون هنري والتي يقول فيها: (تتم أعمال الولايات المتحدة على الإنترنت) فالمعلومات التي تتدفق إلكترونياً على مدار الساعة وطوال أيام الأسبوع أصبحت هدفاً متزايداً ليس فقط للصيادين والهواة، ولكن لمجموعات الجريمة المنظمة والإرهابيين والحكومات الخارجية أيضاً⁽³⁾، ومن المؤكد أن اعتماد الولايات المتحدة الأمريكية في إدارة وتسيير بنيتها التحتية من خلال الفضاء الإلكتروني يجعل منها مطمعا للمهاجمين بتعدد أغراضهم كما أنه يضع أمنها القومي على المحك.

فمن بين أهم الهجمات الخطيرة والحديثة التي تعرضت إليها الولايات المتحدة الأمريكية والتي تهدد أمنها القومي بشكل مباشر نجد ما أفاد به المسؤولون الأمريكيون من أن الصين قد صعدت من هجمات القرصنة ضد مقدمي الرعاية الصحية ومصنعي الأدوية ووزارة الصحة والخدمات الإنسانية الأمريكية وسط جائحة كورونا، كما أعلنت كندا والولايات المتحدة الأمريكية أن قرصنة مرتبطين بالمخابرات الروسية حاولوا سرقة المعلومات المرتبطة بتطوير لقاح فيروس كورونا، كما

⁽¹⁾ المادة 25، القانون رقم 05-20.

⁽²⁾ عائشة بن قارة مصطفى، المرجع السابق، ص 74.

⁽³⁾ United States. Federal Bureau of Investigation, 17/10/2008, Homeland Security Digital Library: <https://www.hsdl.org/?abstract&did=234484>

وجهت وزارة العدل الأمريكية لائحة إتهام إلى مواطنين صينيين بتهمة غسل عملية مشفرة لمتسللين كوريين شماليين⁽¹⁾.

إن إدراك الولايات المتحدة لخطورة الوضع الراهن على بيئة الفضاء الإلكتروني كان وراء إصدارها للعديد من القوانين والتشريعات التي تضمن بها حماية أمنها الإلكتروني ضد أي شكل من أشكال العدوان والإرهاب الإلكتروني، ومن بين أهم وأبرز النصوص التشريعية التي وقعت بين أيدينا، ما تضمنه الكود الفدرالي الأمريكي المعدل والمتمم بالعديد من القوانين والتشريعات:

العنوان 18 المتضمن الجرائم والإجراءات الجنائية:

الفصل 47: المدرج تحت عنوان الاحتيال والبيانات الكاذبة (FRAUD AND FALSE STATEMENTS) ومن أبرز أقسامه:

القسم 1029 (18 U.S.C. § 1029): ويتعلق هذا القسم بالاحتيال والنشاط المرتبط بأجهزة الوصول (Fraud and related activity in connection with access devices)، ويجرم هذا القسم كل عملية أو نشاط متعمد يرمي إلى الاحتيال من خلال أجهزة الوصول المزيفة، وحدد البند الفرعي (أ) 10 حالات لمثل هذا الاستخدام، ومن بينها ما أشارت إليه الحالات الأولى وهو إنتاج أو استخدام أوز متاجرة في واحدة أو أكثر من أجهزة الوصول المزيفة عن علم وبقصد الاحتيال، وما أشارت إليه الحالة السابعة وهي تعديل أداة الاتصالات السلكية واللاسلكية أو تغييرها للحصول على استخدام غير مصرح به⁽²⁾.

القسم 1030 (18 U.S.C. § 1030): يتضمن هذا القسم سبعة أقسام فرعية، ويهتم بالاحتيال والنشاط المرتبط بأجهزة الكمبيوتر (Fraud and related activity in connection with computers)، وقد تعرض إلى العديد من الصور المتعلقة بالاحتيال والنشاط المرتبط بالكمبيوتر وفقا لحيوية المعلومات التي تم الدخول إليها دون إذن أو تجاوزا للتصريح الممنوح، ومن بين تلك الحالات ما تضمنه القسم الفرعي (أ) وهو إلى الوصول المتعمد دون إذن أو تجاوزا للتصريح من أجل الحصول على المعلومات التي حددتها الولايات المتحدة بموجب أمر تنفيذي أو قانون لطب الحماية من الكشف غير المصرح به لأسباب تتعلق بالدفاع الوطني أو العلاقات

⁽¹⁾ Significant Cyber Incidents, center dor stratefic & international studies(CSIS), Accessed on 18/08/2020, at 21:48H, in: <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>

⁽²⁾ A10, Section 1029, Chapter 47, Part I, title 18, U.S. Code, This title was enacted by act June 25, 1948, ch. 645, § 1, 62 Stat. 683, With the latest modifications.

الخارجية، أو أي بيانات مقيدة على النحو المحدد في الفقرة د. من القسم 11 من قانون الطاقة الذرية لسنة 1954، مع وجود سبب للاعتقاد بأن مثل هذه المعلومات التي تم الحصول عليها يمكن استخدامها لإلحاق الأذى بالولايات المتحدة، أو لصالح أي دولة أجنبية، وتعاقب نصوص القسم 1030 بعقوبة شديدة وصارمة تصل إلى 20 سنة سجن⁽¹⁾.

القسم 1037 (18 U.S. Code § 1037): ويتضمن هذا القسم الاحتيال والنشاط المرتبط بالبريد الإلكتروني (Fraud and related activity in connection with electronic mail)، يحدد البند (أ) من هذا القسم حالات الاحتيال والنشاط المرتبط بالبريد الإلكتروني وهي 5 حالات فيما يحدد البند (ب) العقوبات المقررة لهذه الجريمة في الحالات العادية وفي الحالات المشددة، وتضمن البند (ج) المصادرة والإجراءات والتعاريف التي يتضمنها هذا القسم⁽²⁾.

الفصل 65: المدرج تحت عنوان التصرفات الضارة: (MALICIOUS MISCHIEF) ويتضمن هذا الفصل:

القسم 1362 (18 U.S. Code § 1362): والذي يتضمن خطوط أو محطات أو أنظمة الاتصال (Communication lines, stations or systems)، حيث يجرم هذا القسم كل ما من شأنه أن يمس بالكوابل والمحطات والأنظمة الاتصالية إذ ينص على أنه: (كل من يتسبب عن قصد أو عن عمد في إصابة أو تدمير أي من الأعمال أو الممتلكات أو المواد الخاصة بأي راديو أو تلغراف أو هاتف أو كابل أو خط أو محطة أو نظام أو أي وسيلة اتصال أخرى، تديرها الولايات المتحدة أو تسيطر عليها، أو تستخدمها أو يُقصد استخدامها في وظائف الدفاع العسكري أو المدني للولايات المتحدة، سواء تم إنشاؤها أو في طور البناء، أو تتدخل عمداً أو عن عمد بأي شكل من الأشكال في عمل أو استخدام أي خط أو نظام من هذا القبيل، أو تتدخل عمداً أو عن عمد، يعيق أو يؤخر نقل أي اتصال عبر أي خط أو نظام، أو يحاول أو يتآمر على القيام بمثل هذا الفعل، يجب تغريمه بموجب هذا العنوان أو السجن لمدة لا تزيد عن عشر سنوات، أو كليهما...) ⁽³⁾.

⁽¹⁾ A1, , Section 1030, , Chapter 47, Part I, title 18, Op.cit.

⁽²⁾ Section 1037, , Chapter 47, Part I, title 18, Op.cit.

⁽³⁾ Section 1362/1, Chapter 65, Op.cit. "Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both"

العنوان 34: المتضمن مراقبة الجريمة وإنفاذ القانون:

القسم 30102: والذي يتعلق بتطوير ودعم قدرات الطب الشرعي للأمن السيبراني، حيث نص في البند (أ/ 1 و 2) على ما يلي: (بشكل عام، يجب على النائب العام إنشاء مختبرات جنائية حاسوبية إقليمية كما يراها المدعي العام مناسبة، وتقديم الدعم لمختبرات التحاليل الجنائية الحاسوبية الموجودة ، من أجل أن تتمتع جميع مختبرات التحاليل الجنائية الحاسوبية بالقدرة -1- لتوفير فحوصات الطب الشرعي فيما يتعلق بالأدلة الحاسوبية التي تم الاستيلاء عليها أو التي تم اعتراضها فيما يتعلق بالنشاط الإجرامي (بما في ذلك الإرهاب الإلكتروني)؛ 2- لتوفير التدريب والتعليم لموظفي إنفاذ القانون الفيدراليين والولائيين والمحليين والمدعين العامين فيما يتعلق بالتحقيقات والتحليلات الجنائية ومحاكمات الجرائم المتعلقة بالكمبيوتر (بما في ذلك الإرهاب الإلكتروني)؛...) (1).

قانون منع الإرهاب السيبراني لعام 2001:

هو مشروع قانون قدمه السيد أورين ج. هاتش (2) إلى الكونجرس الأمريكي لمجلس الشيوخ في 18 أكتوبر 2001، وتمت إحالته إلى لجنة القضاء، ويتضمن القسم الثاني من هذا القانون الردع ومنع الإرهاب السيبراني فيما يتعلق بأجهزة الكمبيوتر، ويحيل في نصوصه إلى الجرائم التي تضمنها القسم 1030 المشار إليه أعلاه ويقترح مجموعة من التعديلات، أما القسم الثالث فقد تناول الجانب الإجرائي وهو مجموعة من التعديلات على القسم 2707 من العنوان 18، أما القسم الأخير فيتناول موضوع تطوير ودعم أنشطة الطب الشرعي للأمن السيبراني (3).

(1) (A1/1 and 2, Section 30102, Chapter 301, Subtitle III, Title 34, Op.cit: "(a)In generalThe Attorney General shall establish such regional computer forensic laboratories as the Attorney General considers appropriate, and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability—(1)to provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity(including cyberterrorism);(2)to provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime(including cyberterrorism);...")

(2) أورين هاتش غرانت (Orrin Grant Hatch) سياسي أمريكي جمهوري والرئيس المؤقت لمجلس الشيوخ الأمريكي، ورئيس اللجنة المالية بالمجلس منذ 2015 وعضو المجلس عن ولاية يوتا منذ العام 1977. شغل هاتش رئاسة اللجنة القضائية ولجنة العمل والموارد البشرية بالمجلس سابقاً. (ويكيبيديا).

https://fr.wikipedia.org/wiki/Orrin_Hatch

(3) Orrin Grant HATCH, A BILL To prevent cyberterrorism, S. 1568, 107th CONGRESS, 1st Session, October 18, 2001.

قانون الاستعداد للإرهاب السيبراني لعام 2002:

هو مشروع قانون قدمه السيد جون إدواردز إلى الكونجرس الأمريكي في 8 يناير 2002، والذي يتضمن عدة أقسام، أهمها القسم الثاني والمتعلق بمنحة لبرامج حماية البنية التحتية للمعلومات ضد الاضطرابات، أما القسم الثالث فقد تعرض إلى أفضل الممارسات الملائمة في مجال الأمن السيبراني للحكومة الفيدرالية⁽¹⁾.

قانون تحديث أمن المعلومات الفيدرالي لعام 2014:

خصص هذا القانون لتعديل الفصل 35 من العنوان 44 من كود الولايات المتحدة الأمريكية، ومن بين أهم الأقسام التي تضمنها؛ القسم 3553 والمتضمن سلطة المدير وسكرتير الوكالات وصلاحياته، القسم 3554 والمتضمن مسؤوليات الوكالة الاتحادية، والقسم 3556 والمتضمن مركز حوادث أمن المعلومات الفيدرالي مبرزاً دوره ووظائفه، والقسم 3557 والمتعلقة بأنظمة الأمن القومي⁽²⁾.

إن النصوص القانونية المتعلقة بمكافحة وردع الإرهاب السيبراني في كلا العنيتين المذكورتين لا تزالان رغم الجهود المبذولة تعاني من قصور، فهي نصوص رغم أهميتها لا تعكس موقفاً صلباً في مواجهة هذا النوع من الجرائم، إذ أنها لا تغطي كافة الجرائم التي يمكن أن تمارس على الفضاء السيبراني أو به، كما أنها لا تزال قاصرة عن تحديد كافة العناصر الإجرائية المتعلقة بالتحقيق والمحاكمة في الجرائم السيبرانية، ثم إنه ورغم إمكانية العقاب على الإرهاب الإلكتروني بمقتضى النصوص التقليدية إلا أن ذلك قدر يثير العديد من الإشكالات القانونية، وعلى رأسها الشرعية الجنائية.

إذ أننا ورغم قناعتنا بأن جريمة الإرهاب الإلكتروني مجرمة قانوناً بمقتضى النصوص الجنائية المتعلقة بمكافحة الجرائم الإلكترونية، أو بمقتضى النصوص التقليدية في مكافحة الإرهاب، إلا أن ذلك لا يخلو من ثغرات يمكن أن ينفلت من خلالها مجرمي الإرهاب الإلكتروني، وعلى رأسها تحديد القصد الجنائي، الذي يعد صعباً أيما صعوبة في تحديده مع عدم كفاية الأدلة وأصالتها وموثوقيتها، فضلاً عن عدم النص صراحة على معايير قبول الأدلة أمام المحاكم الجنائية

⁽¹⁾ John EDWARDS, A BILL To protect against cyberterrorism and cybercrime, and for other purposes, S. 1900, 107th CONGRESS, 2d Session, January 28, 2002.

⁽²⁾ PUBLIC LAW 113-283, Federal Information Security Modernization Act of 2014, 113th Congress, DEC. 18, 2014.

في مجال الإرهاب الإلكتروني، والتي يمكن للمجرم أن يطعن في دقتها وأصالتها فضلا عن إمكانية الطعن فيها بالتزوير.

على أي حال، لقد خطت كلا من الجزائر والولايات المتحدة الأمريكية خطوات هامة نحو تنظيم الفضاء الإلكتروني وحماية أمنه ضد أشكال الإرهاب الإلكتروني، والمأمول أن يكون هناك تأطير أكثر تفصيلا وبيانا، دفعا للبس، وسدا للثغرات القانونية التي يمكن أن ينفلت منها الجناة في جرائم الفضاء الإلكتروني عموما، وجرائم الإرهاب الإلكتروني منها خصوصا.

الفرع الثاني: الجهود الإقليمية:

لعب الاتحاد الأوروبي من خلال مجلسه وبرلمانه دورا كبيرا في صياغة تشريعات وقوانين تنظم آليات ردع الإجرام السيبراني بعمومه، فتمخضت عنه اتفاقية بودابست لمكافحة الجريمة الإلكترونية التي تعد نموذجا تشريعا للكثير من التشريعات الوطنية، وآلية ذات صبغة دولية لمكافحة الإرهاب الإلكتروني (أولا)، وكذلك سعى الاتحاد الإفريقي إلى مسايرة هذا السبق التشريعي الأوربي، فكان أن وضعت اتفاقية بهذا الشأن إضافة إلى اتفاقياتها في مكافحة الإرهاب التقليدي (ثانيا).

أولا: جهود الاتحاد الأوربي:

1- دور اتفاقية بودابست:

تمثل اتفاقية بودابست الذروة التي تلخص مساعي ومبادرات الاتحاد الأوربي للوصول إلى بلورة نموذج قانوني لمواجهة الجريمة الإلكترونية، وقد كانت هذه الاتفاقية خلاصة التعاون بين المجلس الأوربي ودول أخرى خارج هذا الاتحاد وهي كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، وقد عملت هذه الاتفاقية على إظهار قناعة الدول التي صادقت عليها بخطورة ظاهرة الجريمة الإلكترونية، والحاجة الماسة إلى تآزر الجهود الدولية لمكافحةها⁽¹⁾.

تمت المصادقة على اتفاقية بودابست بتاريخ 23 نوفمبر 2001، ودخلت حيز التنفيذ في 01 يوليو 2004⁽²⁾، وقد وقعت عليها 30 دولة في العاصمة المجرية بودابست، وتتناول هذه الاتفاقية فحص مسألة الجريمة الإلكترونية وأبعادها التي تتخطى الحدود الجغرافية من خلال

(1) أنيس العذار، المرجع السابق.

(2) Hai Thanh LUONG, Huy Duc PHAN, *Cybercrime in Legislative Perspective: (A Comparative Analysis between the Budapest Convention and Vietnam Regulations)*, *International Journal of Advanced Research in Computer Science*, Volume 10, No. 3, May-June 2019: <https://search.proquest.com/openview/04d1ba118736e2474adb031b4bd0d20d/1?pq-origsite=gscholar&cbl=1606379>

التعرض لما يمكن الدول من مواجهتها وملاحقة المتورطين فيها، وإقامة الدليل عليهم، القبض عليهم، كما تتعرض هذه الاتفاقية إلى أحسن الأساليب والآليات التي يمكن توظيفها ضمن عملية التحقيق في محل هذه الجرائم، كما تعرضت أيضا إلى مسألة التجريم بمقتضي نصوص تتناول بالتفصيل هذه الجرائم من الناحية الموضوعية ببيان أصنافها⁽¹⁾.

وعلى الرغم مما عليه حال هذه الدول المؤسسة لهذه الاتفاقية من تباين في أنظمتها القانونية إلا أنها تجاوزت ذلك كله، وهذا يعود لما لهذه النوعية من الجرائم من تداعيات خطيرة إذا لم يكن هناك وجود لنطاق أو إطار قانوني للتعاون بين الدول في قمعها والتصدي لها، فتجاوز تلك الاختلافات وغض الطرف عن ذاك التباين الذي تشتمل عليه تلك الأنظمة يمكن تلك الدول من ترتيب العمل وتنسيقه⁽²⁾.

تعد معاهدة بودابست نتاج أربع سنوات من العمل والجد الذي بذله خبراء المجلس الأوروبي، والدول المتعاونة معها، وقد تم إتمامه وتكاملته بالبروتوكول الإضافي الذي يجعل أي نشر للدعاية العنصرية وأو خطاب الكراهية للأجانب عبر الفضاء الإلكتروني جريمة جنائية يعاقب عليها القانون⁽³⁾، ومنذ فبراير 2012، بدأت لجنة اتفاقية الجرائم الإلكترونية العمل المكثف من أجل إلى إيجاد حلول متعلقة بالوصول إلى البيانات التي تتجاوز النطاق المحلي التي توفرها آليات وخدمات الحوسبة السحابية، وهذا ما قد يفضي إلى بروتوكول إضافي آخر للاتفاقية أو قد يكون سببا في وضع مبادئ توجيهية تابعة لهذه الاتفاقية، كما أن هناك عمل دؤوب في الفترة الآخرة لإحاطة اتفاقية بودابست بمجموعة من آليات والنهج المرتبطة بهذه الاتفاقية مثل؛ التعاون بين أجهزة إنفاذ القانون ومقدمي الخدمات، والتدريب القضائي وأجهزة إنفاذ القانون، وغيرها⁽⁴⁾.

توفر اتفاقية بودابست للدول نموذجا أو إطار يمكن أن يتم الاستناد إليه في الحركة التشريعية الوطنية في مجال الجرائم الإلكترونية، ولذلك فإن الكثير من الدول قد اعتمدت عليها فعلا في

⁽¹⁾ ليندة شرايشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية: (الاتجاهات الدولية في مكافحة الجريمة الإلكترونية)، مجلة دراسات وأبحاث، المجلد 01، العدد 01، جامعة زياد عاشور، الجلفة، الجزائر، سبتمبر 2009، ص ص: 241-253.

<https://www.asjp.cerist.dz/en/article/4426>

⁽²⁾ أيمن عبد الله فكري، المرجع السابق، ص ص: 148-149.

⁽³⁾ Roberto **FLOR**, Cyber-criminality: (finding a balance between freedom and security), Selected papers and contributions from the International Conference on "Cybercrime: Global Phenomenon and its Challenges" Courmayeur Mont Blanc, Italy 2-4 December 2011 Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, Milan, Italy, 2012, PP. 13-20.

⁽⁴⁾ Alexander **SEGER**, The Budapest Convention on Cybercrime 10 years on: (Lessons learnt or the web is a web), Selected papers and contributions from the International Conference on "Cybercrime: Global Phenomenon and its Challenges" Courmayeur Mont Blanc, Italy 2-4 December 2011 Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, Milan, Italy, 2012, PP. 167-177.

صياغة قوانينها الداخلية المتعلقة بالجريمة الإلكترونية، وقد ذهب بعض الباحثين إلى اعتبارها إطاراً قانونياً يتم من خلالها تبادل المساعدات والتعاون بين أطرافها، وهذا ما يجعل منها معاهدة ذات طبيعة عدلية في نطاقها الجنائي، حيث أنها تؤسس اعتباراتها الجنائية على قاعدة سيادة القانون ومبادئ حقوق الإنسان، ولذلك فهي اتفاقية أبعد ما تكون عن تناول العلاقات الدولية من بعدها السياسي والعسكري، كما أنها لا تعتبر في الوقت نفسه معاهدة متعلقة بالأمن الإلكتروني⁽¹⁾.

ولا يزال الاتحاد الأوروبي في إطار مكافحة الجريمة والإرهاب السيبراني يشجع التصديق على اتفاقية بودابست بشأن الجرائم الإلكترونية وتنفيذها مع الشركاء المجاورين، كما هو واضح من الخطاب المشترك مع البرلمان الأوروبي والمجلس الأوروبي واللجنة الاقتصادية والاجتماعية الأوروبية ولجنة المناطق، الذي بين إلى جانب ما ذكرناه مكانة هذه الاتفاقية في اعتبارها نموذجاً لصياغة التشريعات الوطنية في مجال الجرائم الإلكترونية وأساساً للتعاون الدولي في هذا المجال⁽²⁾.

تنقسم الاتفاقية إلى أربعة أقسام، فأما القسم الأول فهو معني بأحكام التجريم والأحكام المترتبة بالجريمة الإلكترونية:

وتنقسم اتفاقية بودابست الجرائم الإلكترونية إلى أربعة أقسام وهي:

- الجرائم التي تمس الخصوصية وسلامة وتوافر بيانات ونظم المعلومات: ويتضمن هذا القسم جريمة النفاذ غير المشروع، الاعتراض غير المشروع، التدخل في البيانات، التدخل في النظام، إساءة استخدام الأجهزة.
 - الجرائم ذات الصلة بالكومبيوتر: وتتضمن التزوير المرتبط بالكومبيوتر، الاحتيال المرتبط بالكومبيوتر.
 - الجرائم ذات الصلة بالمحتوى: وتتضمن الجرائم ذات الصلة بمواد إباحية عن الأطفال.
 - الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة⁽³⁾.
- وتكتسي هذه الجرائم صفة الإرهاب الإلكتروني إذا اقترنت بالقصد الجنائي الخاص، فتكثيفها بأنها أعمال إرهابية وتخريبية يكون ضمن الاعتبارات التي تحددها المادة الأولى من القرار

⁽¹⁾ Alexander SEGER, Op.cit.

⁽²⁾ communication conjointe au parlement européen, au conseil, au comité économique et social européen, et au comité des régions, commission européenne, la haute représentante de l'union pour les affaires étrangères et la politique de sécurité, Bruxelles, le 18.11.2015, P.16.

⁽³⁾ أنظر : اتفاقية بودابست.

الإطارى للمجلس الأوروبى والذى يعرف الإرهاب ويحدد أغراضه، والتي تنص على أنه: (تتخذ كل دولة عضو التدابير اللازمة لضمان أن الأفعال المتعمدة المشار إليها في النقاط (أ) إلى (ط) ، على النحو المحدد في القانون الوطنى، والتي، بحكم طبيعتها أو سياقها، يمكن اعتبارها جرائم إرهابية عندما تلحق ضرراً جسيماً بدولة أو منظمة دولية عندما يرتكبها الجاني بهدف: تخويف السكان بشكل خطير أو - إجبار السلطات العامة أو منظمة دولية بشكل غير ملائم على القيام بأي عمل أو الامتناع عنه أو - زعزعة الاستقرار أو تدمير الهياكل الأساسية السياسية أو الدستورية أو الاقتصادية أو الاجتماعية لـ بلد أو منظمة دولية؛ ...) ⁽¹⁾.

فالجرائم الإلكترونية التي أشارت إليها اتفاقية بودابست يمكن أن تعد إرهاباً إلكترونياً فعلياً إذا كانت تهدف إلى الأغراض التي حددتها هذه المادة، أو إرهاباً إلكترونياً هجيناً استناداً إلى النصوص التشريعية المتعلقة بتجنيد الإرهابيين وتمويل الإرهاب والدعاية له، ويمكن أن نُسند رأينا هذا بما أجاب عنه السيد م. فيتورينو نيابة عن اللجنة حين قال: ("الإرهاب السيبراني" ، أي استخدام موارد الكمبيوتر بغرض التخويف أو الإكراه [الضغط]) ⁽²⁾، وما أشارت إليه حيثيات قرار البرلمان الأوروبي الصادر بتاريخ 12 مارس 2015 حين نص على أنه: (في حين يتم تسهيل نشر الدعاية الإرهابية عن طريق استخدام الإنترنت والشبكات الاجتماعية؛ أن الإرهاب السيبراني يسمح للجماعات الإرهابية بتشكيل والحفاظ على الروابط دون أن يعيقها العائق المادي للحدود، مما يقلل من حاجتها إلى قواعد أو ملاذات في بعض البلدان) ⁽³⁾.

فالرمي إلى تحقيق كل هذه الأهداف من خلال اتخاذ أشكال الجرائم المنصوص عليها في اتفاقية بودابست يكيفها بأنها أعمال إرهابية إلكترونية، سواء في شكلها الهجين الذي يمثل استعمال تقنيات المعلومات لدعم الإرهاب التقليدي أو إرهاباً إلكترونياً فعلياً إن كانت الهجمات واقعة على الفضاء الإلكتروني نفسه لأغراض إرهابية.

2- دور البرلمان الأوروبي:

يصدر البرلمان الأوروبي -كجهة تشريعية في الاتحاد الأوروبي- الكثير من القرارات المتعلقة بالأمن السيبراني ومكافحة الجرائم والإرهاب الإلكتروني، ومن بينها القرار الصادر بتاريخ 13 جوان

⁽¹⁾ Article 02, de la DÉCISION-CADRE DU CONSEIL du 13 juin 2002 relative à la lutte contre le terrorisme, (2002/475/JAI), J.O.U.E L 164 du 22. Juin 2002.

⁽²⁾ Réponse de M. Vitorino au nom de la Commission (8 mars 2001), J.O.U.E/C235E, P.151.

⁽³⁾ Résolution du Parlement européen du 12 mars 2015 sur les relations entre l'Union européenne et la Ligue des États arabes et sur la coopération dans la lutte contre le terrorisme (2015/2573(RSP)), J.O.U.E/ C316 du 30/08/2016, P.173.

2018، والذي يدعو إلى إقامة تعاون دولي ومبادرات متعددة الأطراف لإنشاء أطر صارمة للدفاع السيبراني والأمن السيبراني بهدف مكافحة الاستيلاء على الدولة من خلال الفساد والاحتيايل المالي وغسيل الأموال وتمويل الإرهاب ومعالجة القضايا المتعلقة بالإرهاب السيبراني والعملات المشفرة وطرق الدفع البديلة الأخرى⁽¹⁾، وقد تضمن القرار العديد من المحاور الأساسية لتطوير قدرات الدفاع الإلكتروني والردع السيبراني، وألقي على عاتق سياسة الأمن والدفاع المشتركة (CSDP) هذه المهمة، كما أشار القرار أيضا إلى مسألة التدريب والتعليم في مجال الدفاع السيبراني ووجوب شمولها للعسكريين في جميع الأعمار والرتب⁽²⁾، والتعاون بين الاتحاد الأوروبي وحلف شمال الأطلسي في مجال الدفاع السيبراني⁽³⁾، وترى اللجنة الاقتصادية والاجتماعية الأوروبية أن المسؤولية الاستجابة للهجمات الإلكترونية والإرهاب السيبراني يقع على عاتق الجيش، والنااتو هي الوكالة الرئيسية في هذا المجال بالإضافة إلى وكالة الاتحاد الأوروبي للأمن السيبراني⁽⁴⁾.

يدرك البرلمان الأوروبي أنه من الصائب والمستطيب العمل على إقامة تعاون معزز وأكثر تنظيما مع قوات الشرطة، لاسيما في بعض المجالات الحاسمة مثل مكافحة التهديدات كالجihad الإلكتروني، الإرهاب الإلكتروني والتطرف عبر الإنترنت وتمويل المنظمات المتطرفة والراديكالية وهذا ما أشار ودعا إليه البرلمان الأوروبي⁽⁵⁾.

ترى اللجنة الاقتصادية والاجتماعية الأوروبية أنه يجب على الاتحاد الأوروبي أن يسعى إلى تكثيف الحرب ضد التجسس الإلكتروني والإرهاب السيبراني وجميع أشكال الجرائم الإلكترونية الأخرى التي تستهدف المواطنين الأوروبيين والشركات الأوروبية⁽⁶⁾.

يقر البرلمان الأوروبي بأن الانتشار الواسع للجرائم الإلكترونية عبر الحدود الوطنية والإرهاب السيبراني يطرح تحديات كبيرة وشواغل خطيرة فيما يتعلق بحماية الحقوق الأساسية في بيئة

⁽¹⁾ Article 66, Résolution du Parlement européen du 13 juin 2018 sur la cybersécurité (2018/2004(INI)), Mercredi 13 juin 2018, Journal officiel de l'Union européenne, J.O.U.E/C28/6 du 27.1.2020

⁽²⁾ Article 23.

⁽³⁾ Article 23.

⁽⁴⁾ Avis du Comité économique et social européen sur la «Proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)», J.O.U.E/C107/12 du 06.04.2011, P.60.

⁽⁵⁾ Article 62, Résolution du Parlement européen du 13 juin 2018 sur la cybersécurité (2018/2004(INI)), Op.cit.

⁽⁶⁾ Article 7.1, Avis du Comité économique et social européen sur «L'avenir de l'UE: avantages pour les citoyens et respect des valeurs européennes» (avis exploratoire à la demande de la présidence roumaine du Conseil de l'Union européenne), 05 juillet 2019, J.O.U.E: C228/08/2019. P.65.

الإنترنت؛ ويعتبر أنه من الضروري أن يطور الاتحاد خبراته في مجال الأمن السيبراني من أجل تعزيز الامتثال للمادتين 7 و 8 من الميثاق في مجال الفضاء الإلكتروني⁽¹⁾.

وفي إطار مكافحة الإرهاب السيبراني والجرائم الإلكترونية يشير البرلمان الأوروبي في قراره الصادر بتاريخ 03 أكتوبر 2017، على أن (IOCTA) لسنة 2014 التابع لليوروبول قد أثار مسألة الحاجة إلى صكوك قانونية أكثر كفاءة وفعالية مع مراعاة النطاق الساري المفعول لعملية المساعدة القانونية المتبادلة، ويدعو أيضا إلى مزيد من تنسيق التشريعات عبر كل الاتحاد حسب الاقتضاء⁽²⁾.

كما شدد أيضا البرلمان الأوروبي على ضرورة الاستعانة بتقنية الاعتراض الإلكتروني التي يراها فعالة في مجال التصدي للقرصنة غير القانونية شريطة أن يكون ذلك في نطاق احترام القانون ولاسيما في حقوق الإنسان، ولذلك فإن البرلمان الأوروبي قد دعا إلى ضرورة الاستعانة بهذه التقنية لمراقبة المشتبه بهم كما دعا في الوقت نفسه إلى ضرورة إنشاء قواعد وأسس قانونية واضحة فيما يتعلق بالتراخيص القضائية المسبقة فيما يتعلق بهذا الإجراء، وخص منها ضوابط الاستخدام ومدته، لضمان الرقابة على الإجراء ولضمان حقوق الخاضعين له⁽³⁾.

كما دعا والتمس البرلمان الأوروبي من المجلس الأوروبي السعي إلى فحص الإجراءات والسياسات المتعلقة بالأسواق العامة فيما يتعلق بمنتجات الأمن الإلكتروني، وذلك من خلال تبسيط تلك الإجراءات والمزادات، فضلا عن دعوته أيضا إلى إعادة النظر في التنسيق بين الدول الأعضاء في الاتحاد الأوروبي لتحسينها بشكل يمنح لتلك الدولة القدرة على الاستجابة الفورية للتهديدات الرئيسية ذات الطابع الدولي والتي تتمثل في الإرهاب السيبراني والهجمات الإلكترونية⁽⁴⁾.

ثانيا: الاتحاد الإفريقي:

اعتمادا على الإحصائيات العالمية التي سجلت إلى غاية 1988 فإن عدد المنظمات الإرهابية في إفريقيا لوحدها دون الدول العربية قد قدرت بـ 229 منظمة إرهابية، أي ما يعادل 10.52 بالمئة⁽⁵⁾، وبلغ عدد قطع السلاح الموجودة في إفريقيا وفق التقديرات الدولية 100 مليون

⁽¹⁾ Article 27, Résolution du Parlement européen du 8 septembre 2015 sur la situation des droits fondamentaux dans l'Union européenne(2013-2014)(2014/2254(INI)), 8 septembre 2015, J.O.U.E C 316/2, 2017.

⁽²⁾ Article 14, Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité(2017/2068(INI)), 3 octobre 2017, J.O.U.E C 346 DU 2018.

⁽³⁾ Article 52.

⁽⁴⁾ Article 16, Résolution du Parlement européen du 21 mai 2015 sur l'incidence des évolutions des marchés européens de la défense sur les capacités de sécurité et de défense en Europe(2015/2037(INI)), 21 mai 2015, J.O.U.E C 353, 27.09.2016.

⁽⁵⁾ نسيم بهلول وآخرون، التطرف الديني: (رؤى دينية أمنية سياسية)، الطبعة الأولى، أمواج للنشر والتوزيع، عمان، الأردن، 2014، ص 71.

قطعة سلاح، وهو ما يعادل قطعة واحدة لكل 12 فردا إفريقيا⁽¹⁾، وهذه الإحصائيات إنما تبلور الحالة المزرية التي تعيشها القارة السمراء من انتهاك وإنهاك، بسبب الحروب الداخلية والصراعات المتفاوتة الحدة، والإرهاب الذي أصبحت إفريقيا ملاذا له بسبب ما تعيشه القارة من عدم الاستقرار والانفلات الأمني، والفتن الداخلية.

ويعد النموذج الليبي خير دليل على ما أسلفنا، إذ أصبحت تحتوى على أشكال من التهديدات التي تهدد الساحل الأفريقي كله، فانطلاق شرارة الصراعات بالمنطقة تفضي تبعا إلى اختلالات كبيرة بالاستقرار في هذه المنطقة، كما أنه تواجد المنظمة الإرهابية المعرفة بداعش فيها يزيد من عتمة الوضع، بالإضافة إلى أن هذا الجو السائد في المنطقة يضاعف من تدفع الجماعات المسلحة الدولية إليها كونها توفر لهم ظروفًا ملائمة للتدريبات العسكرية وتجنيد عناصر جديدة وممارسة الاغتيالات والعمليات الإرهابية ومعسكرات التدريب⁽²⁾.

وإذا ما اعتبرنا أن الإرهاب الإلكتروني هو صورة جديدة من صور الإرهاب الذي يستهدف أمن واستقرار المنطقة الإفريقية ومهددا كبيرة للبنية التحتية لدولها، وخطرا جسما على مواطنيها، فإنه بذلك يكتسي الخطورة ذاتها التي يشكلها الإرهاب التقليدي، خاصة إذا علما أن دول القارة الإفريقية تشهد في الآونة الأخيرة هجمات إلكترونية كثيفة، فوفقا لما نشر على موقع جريدة الإمارات اليوم فإن شركة (كاسبرسكي) كشفت تعرض إفريقيا إلى 49 مليون هجوم إلكتروني في الربع الأول من عام 2014، وكشفت شركة (سيمانتك) الأمنية أيضا، أن جنوب إفريقيا لوحده قد تعرض 70 بالمئة من مواطنيه لجرائم إلكترونية، وقدرت شركة (مكافي) للأمن الإلكتروني خسائر كبرى قدرها 500 مليون دولار سنة 2014⁽³⁾.

وأمام هذه الأوضاع الراهنة التي تعيشها القارة الإفريقية من انتشار للمنظمات الإرهابية وتساعد وتيرة الهجمات السيبرانية، اعتمد الاتحاد الأفريقي اتفاقية جديدة إلى جانب اتفاقية مكافحة الإرهاب من أجل التصدي لهذه الكوارث الأمنية التي تهدد دول الاتحاد، وكان محور هذه الاتفاقية هو تحقيق الأمن في الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

(1) نسيم بهلول وآخرون، المرجع السابق، ص 280.

(2) محمد عصام لعروسي، النزاعات المسلحة ودينامية التحولات الجيوسياسية في منطقة الشرق الأوسط وشمال إفريقيا، الطبعة الأولى، مجموعة النيل العربية، القاهرة، 2020، ص 122.

(3) إفريقيا تواجه مأزقا بين مكافحة الجريمة الإلكترونية وضمان حقوق الإنسان، الإمارات اليوم، دبي، نشر بتاريخ 28 أبريل 2015، تم الاطلاع عليه بتاريخ 17 أوت 2020، على الساعة 19:41 سا، في الموقع:

<https://www.emaratalyoum.com/technology/electronic-equipment/2015-04-28-1.779166>

تعرضت الاتفاقية إلى الجرائم الواقعة في الفضاء الإلكتروني حيث قسمتها أربعة أقسام نسوقها على النحو الآتي:⁽¹⁾.

- الهجمات على أنظمة الكمبيوتر: وتتضمن هذه الهجمات 06 أصناف من الجرائم وهي: الوصول أو محاولة الوصول غير المصرح به إلى جزء أو كل نظام الحاسوب أو تجاوز الوصول المسموح، الوصول أو محاولة الوصول غير المصرح به إلى جزء أو كل نظام الحاسوب بهدف القيام بارتكاب جريمة أخرى أو تسهيل ارتكابها، البقاء أو محاولة البقاء عن طريق الاختتيال في كل أو جزء نظام الحاسوب، أعاقا أو محاولة لإعاقا أو تشويه نظام الحاسوب، إدخال أو محاولة إدخال البيانات عن طريق الاختتيال في نظام الحاسوب، إتلاف أو حذف أو إفساد أو تغيير أو تعديل لبيانات الحاسب عن طريق الاختتيال أو محاولة القيام بذلك.

- الخروقات على البيانات المحوسبة: وتتضمن هذه الطائفة من الهجمات بدورها 06 أشكال من الجرائم وهي: اعتراض البيانات المحوسبة بشكل احتيالي واستعمال الآليات التقنية أو محاولة القيام بذلك، أو إتلاف سرية المعلومات، تزيف البيانات عمدا، استعمال البيانات التي تمت حيازتها عن طريق الاختتيال مع العلم بذلك، القيام بشراء عن طريق الاختتيال فائدة لأي شخص من خلال التدخل على أداء النظام الحاسوب، معالجة البيانات الشخصية أو السماح للقيام بذلك أيا كان السبب دون متابعة الإجراءات الأولية لذلك، الشراكة والاتفاق بغرض التحضير أو ارتكاب جريمة أو أكثر من هذه الجرائم.

- الجرائم المتعلقة بالمحتوى: وتتضمن هذه الفئة 08 أشكال من الجرائم حيث تضمنت الجرائم الأربع الأولى قضية المواد الإباحية الخاصة بالأطفال وجرمت أي شكل يمكن أن تتشكل فيه، وتضمنت أيضا أي شكل من أشكال استعمال الحاسب في إنتاج أو تحميل أو نشر أو إتاحة المواد ذات التوجه العنصري أو كراهية الأجانب، استعمال نظام الكمبيوتر للتهديد بقصد ارتكاب جريمة ضد أي شخص لدواعي عنصرية، استعمال الحاسب لإهانة مجموعة أشخاص بسبب انتماءاتهم، استعمال الحاسب لإنكار أو الموافقة أو التبرير لأعمال الإبادة الجماعية والجرائم ضد الإنسانية.

- الجرائم بضمان تأمين الرسائل الإلكترونية.

وبالنظر إلى هذه الجرائم التي تضمنتها الاتفاقية يمكن أن نلاحظ بشكل جلي أن مظاهر الإرهاب الإلكتروني الهجين قد تم تجريمها بشكل واضح، فالاتفاقية تجرم بشكل صريح الإرهاب الإلكتروني الهجين من خلال تجريم كل وصول أو محاولة وصول لارتكاب جريمة أخرى والتي

(1) المادة 29، اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

يمكن أن تكون نشاطا إرهابيا، كما تجرم أشكال استعمال الحاسب الآلي لإطلاق النعرات الطائفية والعنصرية وكراهية الأجانب التي تمثل سببا منشأ للإرهاب ومعزز له ولاانتشاره، كما جرمت أيضا كل أشكال الدعم المعنوي باستعمال الحاسب للأفعال الموصوفة بالإبادة الجماعية والجرائم ضد الإنسانية والتي يمثل الإرهاب واحدة منها.

كما أشارت الاتفاقية أيضا إلى إلزامية قيام الدول بالتدابير التشريعية و/أو التنظيمية لاعتبار كل استخدام للتقنيات المعلوماتية والاتصالية لأغراض إرهابية ظروفًا مشددا للعقوبة إذ تنص على أنه: (تلتزم الدول الأطراف باتخاذ ما يلزم من تدابير تشريعية و/أو تنظيمية لاعتبارها ظروفًا مشددة للعقوبة، عندما يتم استخدام تكنولوجيا المعلومات والاتصالات من أجل ارتكاب جرائم مثل السرقة والاحتيال وحيازة بضائع مسوقة، وإساءة استخدام الثقة وابتزاز الأموال والإرهاب، وغسل الأموال)⁽¹⁾.

غير أن الاتفاقية لم يظهر لنا في مضمونها ما يفيد تجريمها الصريح للإرهاب الإلكتروني الفعلي الذي يقع على أنظمة الحاسوب نفسها أو على البنية التحتية المرتبطة بها، وهذا لا يعني أن الاتحاد الإفريقي ليس له آلية تشريعية تتصدى بها للإرهاب الإلكتروني الفعلي، فبالرجوع إلى اتفاقية منظمة الاتحاد الإفريقي للوقاية من الإرهاب ومكافحته، ولاسيما المادة الأولى منه، نجد أن الاتحاد يجرم (...أ- أي عمل يعتبر انتهاكاً للقانون الجنائي للدولة الطرف، والذي يمكن أن يعرض حياة الأفراد للخطر أو يشكل خطراً على التكامل الفيزيائي، وحرية الشخص أو جماعة أشخاص، الذي يسبب أو يمكن أن يسبب خسائر للممتلكات الخاصة أو العامة، للمواد الطبيعية، للبيئة أو للتراث الثقافي والمرتكب بغرض: 1- ترويع، وخلق حالة رعب، وإكراه، أو إجبار أو إغراء أية حكومة، أو هيئة أو مؤسسة، أو أي قطاع للقيام أو الامتناع عن القيام أي عمل، أو تبني أي موقف أو التخلي عنه، أو العمل وفق مبادئ معينة، 2- الإخلال بالوظيفة العادية للخدمات العامة، تقديم أي خدمات أساسية للجمهور، أو خلق حالة طوارئ عامة، 3- خلق حالة عصيان عامة في الدولة العضو...)⁽²⁾.

(¹) المادة 30، اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

(²) Article 2/3, convention de l'OUA sur la prévention et la lutte contre le terrorisme, adopté en 01 juillet 1999, entrée en vigueur le 06 décembre 2002: ((a) tout acte ou menace d'acte en violation des lois pénales de l'État Partie susceptible de mettre en danger la vie, l'intégrité physique, les libertés d'une personne ou d'un groupe de personnes, qui occasionne ou peut occasionner des dommages aux biens privés ou publics, aux ressources naturelles, à l'environnement ou au patrimoine culturel, et commis dans l'intention : (i) d'intimider, provoquer une situation de terreur, forcer, exercer des pressions ou amener tout gouvernement, organisme, institution, population ou groupe de celle-ci, d'engager toute initiative ou de s'en abstenir, d'adopter, de renoncer à une position particulière ou d'agir selon certains principes ; ou (ii) de perturber le fonctionnement normal des services publics, la prestation de services essentiels aux populations ou de créer une situation de crise au sein des populations ; (iii) de créer une insurrection générale dans un État Partie.)

واستنادا إلى هذا النص، يمكن اعتبار أي اختراق حاسوبي، أو أي تنفيذ لهجمة باستخدام البرامج الضارة، من أجل التحكم في أنظمة المعالجة الآلية، أو من أجل تدمير بيانات أنظمة التشغيل بغرض التأثير على الأوامر والتعليمات التي تصدرها في تسيير البنى التحتية الحرجة بغية تدميرها أو شل حركتها من قبيل الإرهاب الإلكتروني الفعلي.

الفرع الثالث: الاتفاقيات الثنائية لتحقيق الأمن السيبراني:

تشكل الاتفاقيات الثنائية بين الدول أو المنظمات الدولية والإقليمية إحدى الضمانات القانونية لمكافحة الإرهاب الإجرام السيبراني، لذلك عملت الصين على إبرام العديد من الاتفاقيات الثنائية بين مختلف الدول لمواجهة هذه الظاهرة (أولا)، وكذلك فعلت الولايات المتحدة الأمريكية (ثانيا)، وروسيا الاتحادية مع الكثير من الدول (ثانيا)، أما على الصعيد العربي، فتحل قطر مرتبة مرموقة بين الدول العربية في إبرام اتفاقيات متعددة مع دول ومنظمات دولية بغرض تحقيق الأمن السيبراني ومكافحة أشكال الإجرام فيه (رابعا).

أولا: الصين:

تعتبر الصين من بين الدول الكبرى التي تولي الأمن السيبراني اهتماما خاصا، ولاسيما مع تصاعد اعتمادها على الفضاء الإلكتروني مع نهضتها الاقتصادية المعاصرة، فالفضاء الإلكتروني في الصين يكتسي من وجهة نظرنا أهميتين أساسيتين، أولهما أن الكثير من البنى التحتية في الصين على غرار سائر الدول المتطورة تعتمد كثيرا في إدارتها وتسييرها على الفضاء الإلكتروني⁽¹⁾، وثانيهما؛ أنا الصين تعتبر من بين الدول المنتجة والمصنعة لبعض البنى التحتية التكوينية للفضاء السيبراني، فالصين تنتج من الأصول المرتبطة بالفضاء الإلكتروني الشيء الكثير، وهي من بين القوى السيبرانية الصاعدة⁽²⁾، وهذا كله يجعلها تهتم بشكل كبير بالأمن السيبراني، خاصة مع تصاعد الهجمات السيبرانية التي أثرت على العديد من مجالاتها الحيوية ولاسيما القطاع الاقتصادي، حيث أنها -كما أكد أحمد يوسف كيطان- قد خسرت في سنة 2011 ما يزيد عن 830 مليون دولار⁽³⁾.

(1) أحمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني للين: (قراءة في قانون الأمن السيبراني الصيني)، 27 نوفمبر 2019، تم الاطلاع عليه بتاريخ 05 مارس 2021، على الساعة 22:15 سا، مختص الرابط: <https://cutt.us/hKL4A>

(2) فرح عصام، استراتيجية "تشي" الثورية.. كيف تغير الصين مستقبل الإنترنت في العالم؟، موقع الجزيرة، 02 جويلية 2020، تم الاطلاع عليه بتاريخ 05 مارس 2021، على الساعة 22:17 سا، مختص الرابط: <https://cutt.us/E6TqF>

(3) أحمد يوسف كيطان، المرجع السابق.

ولما كانت الاتفاقيات الثنائية تكتسي أهمية خاصة في مواجهة الإرهاب السيبراني وسائر الهجمات الإلكترونية، فإن الصين قد أبرمت 15 اتفاقية ثنائية مع 12 دولة، حيث أبرمت أربعة اتفاقيات منها كانت مع إندونيسيا والتي تتضمن بشكل خاص معالجة الجريمة الإلكترونية وبناء القدرات السيبرانية، كما أن هناك بوادر لاتجاه العلاقات الصينية الإندونيسية إلى التعاون الحربي والعسكري في المجال العسكري، فعلى الرغم من عدم وجود أي اتفاق من هذا النوع بين الدولتين إلا أن تصريحات أحد كبار المسؤولين في مجال الفضاء الإلكتروني في إندونيسيا كما نقلتها بعض التقارير الإخبارية تؤكد أن هناك تفعيل للاتفاقيات المتعلقة بالتعاون الثنائي في مجال الفضاء الإلكتروني سيشتمل على تنفيذ مختلف العمليات التي تحاكي فيها الحروب الإلكترونية فضلا عن مختلف التدريبات المتعلقة بإدارة الأزمات⁽¹⁾.

كما وأبرمت الصين اتفاقيتين ثنائيتين بينها وبين روسيا والتي تتضمن بين طياتها مسألة فرض السيطرة على الفضاء الإلكتروني، كما وتتضمن أيضا قضايا الأمن السيبراني ولاسيما منها موضوع الجرائم المعلوماتية، وتبادل التقنيات والتكنولوجيا المتعلقة بالرقابة على محتوى الإنترنت وبسط الحماية على الشبكات الداخلية، كما وتضمنت أيضا "مسألة التعاون في مجال أمن المعلومات الدولي"⁽²⁾.

ثانيا: الولايات المتحدة:

تعتبر الولايات المتحدة الأمريكية كقوة سيبرانية عظمي، فهي تمتلك من البنية التحتية التكوينية للفضاء الإلكتروني ما يؤهلها لتصدر في مجال القوى السيبرانية، فبيتها التحتية الحرجة تدار بشكل أساسي بتقنيات المعلومات المختلفة، وهذا ما يجعلها مهددة في أمنها القوي، ولعل من بين الدول الأكثر تهديدا لها ولأمنها السيبراني نجد الصين والتي تملك بدورها قوة لا يستهان بها في هذا المجال، وكعادتها فإن الولايات المتحدة الأمريكية سعت من خلال إبرام معاهدات ثنائية مع الدول التي توازيها في القوة لضمان أمنها السيبراني.

غير أن إبرام معاهدات أو اتفاقيات ثنائية بين الولايات المتحدة الأمريكية وبين الصين ليس بالأمر الهين، وذلك نظرا للتوترات القائمة بين البلدين، فالولايات المتحدة الأمريكية حاولت أن تظهر نوعا من الحدة والشدة في تعاملها مع الهجمات الصينية حينما أكدت من خلال توجيه لائحة تهم لخمسة من أعضاء جيش التحرير الشعبي الصيني بأنه لن تسمح لمرور الهجمات التي

⁽¹⁾Theresa **HITCHENS**, Nilsu **GOREN**, *International Cybersecurity Information Sharing Agreements, phase I Study Report*, Center for International & Security Studies, U. Maryland, 2017, P.11

⁽²⁾ Ibid. PP.12-13.

تستهدف شركاتها دون عقاب رادع، كما وحذرت الولايات المتحدة الأمريكية الصين على خلفية الهجمات التي استهدفت مكتبها لإدارة شؤون الموظفين بأنها تفكر في ممارسة حقها في الرد من خلال توقيع عقوبات على الصين، لكن الولايات المتحدة الأمريكية بعد ذلك فقدت مصداقيتها بعد قضية إدوارد سنودن، لكن الغالب أن افتضاح الممارسة السببرانية لكلا الدولتين قد فتح أفقا لتخفيف التوتر والذي وجد منفذا لنشوء اتفاق ثنائي للشروع في تدابير بناء الثقة في الفضاء السببراني. في اتفاقية 2015⁽¹⁾ إذ حقق كل من الرئيسين أوباما وشي جينغ بينغ خطوة هامة عندما تعهد كلا البلدين بعدم ممارسة أو رعاية أي شكل من أشكال الجوسسة التي تهدف إلى المساس بالقطاع، فهذه الاتفاقية بهذا الشكل إنما هي اتفاقية تتضمن بشكل خاص حظر الجوسسة الاقتصادية السببرانية بين البلدين، وبشكل خاص تلك المتعلقة بحقوق الملكية الفكرية والأسرار التجارية،⁽²⁾.

لاحظ المتخصصون والخبراء في مجال الأمن السببراني التابعين للولايات المتحدة الأمريكية أن الهجمات التي تمارس من الصين ضد أهدافها الاقتصادية قد تقلص بشكل كبير عقد تلك الإتفاقية الثنائية، لكن الخبراء لاحظوا أيضا زيادة في عدد الهجمات التي تستهدف الولايات المتحدة الأمريكية من دول أخرى، وذهب الخبراء إلى تحديد بعض الفرضيات التي يمكن أن تفسر تزايد هذه الهجمات من دول أخرى وانخفاضها في الصين، فاقترحوا إما أن يكون المهاجمون الصينيون قد وكلوا غيرهم بتنفيذ هذه الهجمات، وإنما أن الاتفاقية قد أجبرت الصين بأن تكون أكثر حذرا من خلال تطوير وتصعيب آليات الهجوم بطريقة تكون أكثر صعوبة في الكشف عنها، وإنما أن يكون المنفذون للهجمات تحت وقع الاتفاقية قد وجهوا هجماتهم إلى أهداف أكثر سهولة خارج الولايات المتحدة الأمريكية، وإما أن حملة الصين التي شنتها لمكافحة الفساد في الحكومة وجيش التحرير الشعبي بعد توقيع الاتفاقية قد ثنت من عزيمة الموظفين الذي كانوا قبل ذلك يشنون هجمات إلكترونية بغرض زيادة رواتبهم⁽³⁾.

على أي حال، الظاهر أن هذه الاتفاقية لا تعد كافية لتأمين الفضاء الإلكتروني بين الدولتين، ولاسيما الأمن السببراني للولايات المتحدة الأمريكية، لذلك دعا بعض الباحثين إلى

(¹) Marie **BAEZNER**, Cybersecurity in Sino-American Relations, center for security studies(SCC), analyse in Security Policy, ETH Zurich, N^o 224, April 2018, PP.01-04: <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse224-EN.pdf>

(²)Celia **LOUIE**, U.S.-China Cybersecurity Cooperation, SEPTEMBER 8, 2017, Accessed on 20/08/2020 at 01:01 in: <https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/>

(³) Marie **BAEZNER**, Op.cit.

ضرورة بذل الصين المزيد من المجهودات التي ترمي إلى كبح هذه الهجمات السيبرانية، فضلا عن واجب الولايات المتحدة الأمريكية في زيادة الجهود الرامية إلى تأمين البنية التحتية الحيوية من أمثال هذه الهجمات، كما يجب أيضا إجراء دراسة دقيقة في الوضع الذي آلت إليه هذه الهجمات وفي هذا التحول، من خلال بيان دقيق يؤكد مدى توقف تلك الهجمات، أم أن الهجمات الصينية في حقيقتها لم تتوقف بل يتم الاستعانة فيها بجهات خارجية أو بآليات وأساليب أكثر تعقيدا⁽¹⁾.

ثالثا: روسيا:

تعتبر الأمن السيبراني من بين أولويات السياسة الأمنية لروسيا، ويعود هذا الأمر إلى الأهمية التي يكتسبها الفضاء الإلكتروني في تحقيق سياساتها الخارجية، إذ أنها تعد قوة ناعمة يتم توظيفها لفرض السيادة، فضلا عن دورها الدعائي لكسب الدعم وفرض المكانة على طاولة صناع القرار، ناهيك عن توظيفه في توطيد علاقاتها مع غيرها من الدول الصديقة والمتحالفة معها، ووصون مصالحها القومية⁽²⁾.

ولكن مع هذا لا نجد اهتمام روسيا بإقامة علاقات ثنائية أو بالأحرى اتفاقيات ثنائية مع غيرها من الدول في مجال الأمن السيبراني، فروسيا لا تمتلك سوى 03 اتفاقيات في هذا الباب، وهي تلك التي تربطها بالهند وإيران ومنظمة شنغهاي، وهذا إنما يبلور عدم رضا روسيا بمساعدة الدول أو منظمة الإنتربول لها في تعقب المجرمين في الفضاء الإلكتروني، وأما عن علاقتها بالولايات المتحدة فكل الجهود الرامية إلى التعاون في هذا المجال معلقة، وذلك أن الخلاف بين الدولتين فيما يتعلق بالإشكاليات التي يثيرها هذا الفضاء عميقة، فروسيا تميل إلى أمن المعلومات الدولي، في حين تميل الولايات المتحدة الأمريكية إلى الأمن السيبراني معتقدة أن الجرائم الإلكترونية والتجسس الإلكتروني والإرهاب الإلكتروني هي التهديدات الأساسية والرئيسية في بيئة الفضاء الإلكتروني، ومن المشجع أن البلدان قد توصلا إلى اتفاق في يونيو 2013 بشأن الحاجة إلى التعاون بشأن التهديدات التي تواجه تكنولوجيا المعلومات والاتصالات، أو في استخدامها في سيقا الأمن الدولي⁽³⁾.

⁽¹⁾ Celia LOUIE, Op.cit.

⁽²⁾ زينب مصطفى رويحه، تحديات الدور: الأمن السيبراني في توجهات روسيا الإفريقية، 13 نوفمبر 2019 تم الاطلاع عليه بتاريخ 12 فيفري 2021، على الساعة 11:23 سا، مختصر رابط الموقع: <https://cutt.us/jME02>

⁽³⁾ Thomas REMINGTON, Chris SPIRITO, Elena CHERNENKO, Oleg DEMIDOV, Vitaly KABERNIK, Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity, Working Group Paper 7, WORKING GROUP ON THE FUTURE OF U.S.- RUSSIA RELATIONS, Kathryn W. and Shelby Cullom Davis Center for Russian and Eurasian Studies Harvard University, MAY 2016, P.01.

"لقد كان هناك تعاون بين الولايات المتحدة الأمريكية وروسيا بشأن الجرائم الإلكترونية في الماضي، ولقد تم الترحيب بحملة القمع الأخيرة التي حظيت بتغطية إعلامية كبيرة على الجريمة الإلكترونية في روسيا، والتي سبقت بتعاون وثيق وكبير بين مكتب التحقيقات الفيدرالية الأمريكي (FBI) وجهاز الأمن الفيدرالي الروسي (FSB)، ويعد هذا تعاونا جديدا بين البلدين، التعاون الذي لا يزال قائما وخاضعا للاختبار، وما يثير الإشكال على حد تصريح أحج المختصين الروس هو التعاون في ظل منظمة الإنترنت التي تعتبر منظمة مثيرة للجدل في روسيا والتعاون معها يعد أمرا عصيا وصعبا، لذلك يتعين وجود قنوات تعاونية أخرى"⁽¹⁾.

يوجد ما لا يقل عن أربعة مجالات أو ركائز للتعاون بين الولايات المتحدة الأمريكية وروسيا في مجال الفضاء الإلكتروني، وهذا التعاون من شأنه أن يعود بالمنافع المشتركة بين البلدين على البلدين، بل إن لهذا التعاون أهمية كبيرة لضمان الأمن القومي للبلدين واستقرار العلاقات الدولية، وتعتبر معالجة هذه القضايا الأربع في المستقبل القريب عاملا مساعدا بشكل كبير في التغلب ولو جزئيا على الأزمة الحالية في العلاقات الثنائية بين البلدين، وهذه الركائز أو المجالات هي؛ مكافحة الجريمة السيبرانية، المسار في تبادل المعلومات، إلزامية عمل البلدين على وفق الحرب الإلكترونية، معالجة مسألة حوكمة أو إدارة الإنترنت⁽²⁾.

رابعاً: قطر:

1- اتفاقية قطر ومكتب الأمم المتحدة المعني بالمخدرات والجريمة:

أبرمت حكومة دولة قطر اتفاقاً بينها وبين مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن إنشاء وتمويل مركز الأمم المتحدة الإقليمي لمكافحة الجريمة السيبرانية في الدوحة⁽³⁾، حيث يهدف هذا الاتفاق بناء على نص المادة 02 منه إلى: (إقامة مركز إقليمي في دولة قطر للتدريب وبناء القدرات يعنى بالجريمة السيبرانية، ويعتبر هذا المركز جزء من البرنامج العالمي المعني

⁽¹⁾ Franz-Stefan GADY, Greg AUSTIN, Russia, The United States, And Cyber Diplomacy:(Opening the Doors), The EastWest Institute, New York, USA, 2010, P.12.

⁽²⁾ Bruce W. MCCONNELL, Pavel SHARIKOV, Maria SMEKALOVA, Suggestions on Russia-U.S. Cooperation in Cybersecurity, POLICY BRIEF, No. 11, Russian International Affairs Council (RIAC), Moscow, May 2017, P.07.

⁽³⁾ المادة الأولى، من المرسوم رقم 07 لسنة 2020، المتعلق بالتصديق على اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر ومكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن إنشاء وتمويل مركز الأمم المتحدة الإقليمي لمكافحة الجريمة السيبرانية في الدوحة، 02 مارس 2020، ج.ر. عدد 07، 22 أبريل 2020.

بالجريمة السيبرانية الذي يديره مكتب الأمم المتحدة المعني بالمخدرات والجريمة⁽¹⁾، وأشارت المادة 03 من الاتفاقية أن نشاط المركز يغطي كل منطقة الشرق الأوسط وشمال إفريقيا.

وقد أتفق الطرفان على جملة من مجالات التعاون وهي محددة بمقتضى نص المادة 05 من الاتفاقية هي؛

- دعم برامج التدريب وبناء القدرات في مجال مكافحة الجريمة السيبرانية؛
- تبادل الخبرات والمعلومات بشأن الجريمة السيبرانية ومتغيراتها على المستويات الوطنية والدولية من أجل تعزيز فعالية برامج التدريب وبناء القدرات؛
- تطوير الأدوات الفنية بصورة مستمرة⁽²⁾.

2- الاتفاقية القطرية الجزائرية:

صادقت حكومة دولة قطر وحكمة الجمهورية الجزائرية في العاصمة القطرية الدوحة بتاريخ 31 من شهر أكتوبر 2016 على اتفاقية تعاون بين البلدين في مجال مكافحة الجريمة المنظمة⁽³⁾، وتتضمن الاتفاقية التعاون التقني وتبادل المعلومات والخبرات في العديد من الميادين المتعلقة بالجريمة المنظمة، ومن بين تلك الميادين التي أشارت إليها المادة الأولى من الاتفاقية؛ (مكافحة الجرائم الإلكترونية، الشرطة العلمية والتقنية، الأمن الجنائي والأدلة الجنائية)⁽⁴⁾.

أبرزت المادة الثانية من نص الاتفاقية 09 محاور أو عناصر أساسية للتعاون بين البلدين والتي تتمثل في:

- تبادل المعلومات بكافة أشكال الجرائم المنصوص عليها في هذه الاتفاقية، بما في ذلك عناصر الجماعات والشبكات الإجرامية، وكيفية سيرها من خلال إبراز تنظيمها وآليات نشاطها؛
- التكوين والتدريب؛
- تبادل المعلومات والتقنيات والخبرات والتجارب المهنية؛
- تبادل ما ينتج من عمليات الأبحاث والمعاينات والوسائل المستعملة في التحقيقات وعلم الإجرام والبيانات المرتبطة بآليات التحقيق ومجابهة الجريمة؛
- تبادل النصوص التشريعية والتنظيمية؛

⁽¹⁾ المادة 02 من المرسوم رقم 07 لسنة 2020.

⁽²⁾ المادة 05.

⁽³⁾ المادة الأولى، من المرسوم رقم 84 لسنة 2017، المتعلق بالتصديق على اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر وحكومة الجمهورية الجزائرية الديمقراطية الشعبية، 06 نوفمبر 2017، ج.ر. عدد 15، 27 ديسمبر 2017.

⁽⁴⁾ المادة الأولى، اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر وحكومة الجمهورية الجزائرية الديمقراطية الشعبية.

- تبادل الزيارات بين المسؤولين والخبراء؛
- تبادل المساعدة في البحث عن المتهمين بالأفعال التي يشملها وصف الإجرام المنظم؛
- تبادل المعلومات بخصوص المشتبه فيهم في نشاطات غسل الأموال أو تمويل عمليات إجرامية سواء أكانوا طبيعيين أو معنويين، وبخصوص النشاطات المتعلقة بالنهج التي يتم توظيفها في هذه العمليات؛
- التعاون في مجال التعليم والتدريب للأجهزة الأمنية على الأسس والمعايير الدولية الحديثة⁽¹⁾.

3- الاتفاقية القطرية العمانية:

صادقت حكومة دولة قطر وحكومة سلطنة عمان في العاصمة القطرية الدوحة بتاريخ 26 أبريل 2016 على اتفاقية تعاون في المجال الأمني⁽²⁾، والتي تضمنت مجال الجرائم الإلكترونية وجرائم الحاسب الآلي⁽³⁾، وتتضمن الاتفاقيات محاور عدة في التعاون بين البلدين والتي يتصدر تبادل المعلومات فيما يرتبط بهذه الجرائم قائمتها⁽⁴⁾.

بالإضافة إلى منح التسهيلات فيما يتعلق بالتعليم والتدريب وتبادل الزيارات بين المعاهد والكلليات والمؤسسات التابعة لوزارة الداخلية والأجهزة الأمنية⁽⁵⁾، وإعلام كل طرف للآخر بما يعقد من مؤتمرات وحلقات وندوات فيما يرتبط بنطاق الاتفاقية⁽⁶⁾، كما تتضمن الاتفاقية أيضا تبادل بيانات ذوى السوابق الإجرامية الخطيرة الذين أدرجت أسمائهم ضمن الأشخاص ممنوعين من الدخول إلى البلد أو الخروج منها⁽⁷⁾.

وفي الأخير تجدر الإشارة إلى أن الاتفاقيات الثنائية في مجال مكافحة الإرهاب الإلكتروني تلعب دورا مهما ومحوريا في التصدي لها وتحقيق الأمن السيبراني بشكل فعال بين الدولتين المتعاقبتين، وذلك لما تتميز به هذه النوعية من الاتفاقيات من ميزات وخصائص مهمة وجوهرية،

⁽¹⁾ المادة 02، اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر وحكومة الجمهورية الجزائرية الديمقراطية الشعبية.

⁽²⁾ المادة الأولى، من المرسوم رقم 55 لسنة 2016، المتعلق بالتصديق على اتفاقية تعاون بين حكومة دولة قطر وحكومة سلطنة عمان في المجال الأمني، 14 ديسمبر 2016، ج.ر. عدد 01، 12 فبراير 2017.

⁽³⁾ المادة الأولى، اتفاقية تعاون بين حكومة دولة قطر وحكومة سلطنة عمان في المجال الأمني.

⁽⁴⁾ المادة 02.

⁽⁵⁾ المادة 04.

⁽⁶⁾ المادة 05.

⁽⁷⁾ المادة 07.

تعمل على دعم التعاون وتتجنب مواطن الزلل والجوانب السلبية التي تتميز بها المعاهدات والاتفاقية الجماعية.

فالمعاهدات أو الاتفاقيات الثنائية يتم تحرير مضمونها بلغتي طرفيها، أو اللغة التي يتم الإجماع عليها بين الدولتين، فضلا عن كونها اتفاقيات ومعاهدات يكفي لتعديلها تفاهم الدولتين المتعاقدين فيما بينهما دون الحاجة إلى إجراءات معقدة، ناهيك عن اقتصار آثارها على الدولتين المتعاقدين⁽¹⁾.

وهذه الخواص تلعب دورا مهما سواء أكانت الاتفاقية تتضمن جانبا عقديا أو شارعا، فبالنسبة للغة تحريرها، سيكون لها إسهام كبير في تحديد الوصف الإجرامي لظاهرة الإرهاب الإلكتروني، كما وتلعب اللغة دورا مهما في تفسيرها وتطبيقها في المستقبل، وأما عن إجراءات التعديل البسيطة فهي تمنح للطرفين إمكانية مسايرة ما يستجد في مجال الإجرام والإرهاب السيبرانيين، ومسايرة طبيعته المتقلبة والمتحولة، وأما عن الآثار واقتصارها على طرفي الاتفاقية فإنها ذات دور كبير في حصر عناصر الخلاف.

ومع ما لهذه الاتفاقيات من أهمية كبيرة، إلا أن الاتفاقيات الثنائية التي وقت بين أيدينا في إطار بحثنا هذا لا تتضمن نوعا من التفصيل في مجال التعاون بين طرفيها في مجال مكافحة الإرهاب الإلكتروني، وتفتقر بشكل واضح إلى معالجة هذه الجريمة موضوعيا وإجرائيا، فغالبية الاتفاقيات التي عاينها ليست اتفاقيات شارة، إذ لا يتضمن فحواها أي شكل من أشكال القواعد الجنائية، فهي في عمومها تعاقدية أكثر منها شارة.

كما أن غالبية الاتفاقيات الثنائية التي وقعت عليها أيدينا لا تتناول موضوع الإرهاب الإلكتروني كجريمة مستقلة عن الأشكال الأخرى للجرائم السيبرانية، وهذا ما سيكون له أثر كبير في تنفيذها وتفسيرها، إذ حتى وإن اتفقت الدول على تجريم بعض الأفعال والتصرفات والنشاطات على الفضاء الإلكتروني، إلا أنه يمكن أن يرد خلاف في مسألة الإرهاب الإلكتروني، وهذا سيشكل عقبة أمام التعاون الثنائي الفعال.

(1) ماهر ملندي وماجد الحموي، القانون الدولي العام، منشورات الجامعة الافتراضية السورية، سوريا، 2018، ص ص: 43-49.

المطلب الثاني:

جهود الهيئات الدولية

يأتي الإرهاب السيبراني في مقدمة الجرائم التي تهدد النظام الدولي بأمنه وسلامته، فهو كما تقدم بنا البحث من الجرائم الدولية التي لا تعترف بالحدود، ولا تعبأ بالنطاق الجغرافي، وإن الغياب التام لقرارات صادرة عن مجلس الأمن الذي يعتبر الهيئة ذات القرارات الملزمة في هيئة الأمم المتحدة بشأن الإرهاب، لم يكن عائقاً أمام هيئة الأمم لممارسة دورها الدولي في الحفاظ على الأمن والسلم العالميين على الفضاء السيبراني، فالهيئة تعمل بشكل جدي، وتبذل جهداً محموداً في سبيل الوصول إلى إجماع دولي على إدراك المخاطر التي تنتج عن توظيف هذا الفضاء لأغراض إرهابية وتدعو إلى المزيد من التعاون في هذا الميدان (الفرع الأول)، ولم يغيب هذا الموضوع عن القمم التي تعقدها مجموعة الثمانية، فهي ورغم كونها منتدى اقتصادي إلا أنها بذلت هي الأخرى جهداً (الفرع الثاني) بجانب الجهد الذي تبذله منظمة التعاون الاقتصادي والتنمية في تأمين الفضاء الإلكتروني (الفرع الثالث).

الفرع الأول: جهود منظمة هيئة الأمم المتحدة:

تعد قضايا الأمن السيبراني على المستوى الدولي من القضايا الشائكة والمعقدة التي كثيراً ما تتباين فيها آراء الدول، فالحوار الدولي في مسألة حماية الفضاء السيبراني تعرف توترات وتباين في وجهات النظر، ومع هذا فإن هيئة الأمم تعمل بجهد لتقريب هذه الآراء وصبها في مصلحة التعاون الدولي (أولاً)، وقد عملت الهيئة على تشكيل البوادر الأولى لثقافة الأمن السيبراني من خلال قراراتها في هذا الباب، كما تنشط الهيئات واللجان التابعة لها بالتنسيق مع بعضها لتحقيق هذا الهدف (ثانياً).

أولاً: إطار الحوار الدولي في مواجهة الإرهاب الإلكتروني:

1- واقع الأمم المتحدة في شأن قضايا الأمن السيبراني:

يعتبر القصور الواضح وعدم كفاءة الإجراءات الأحادية الجانب في ضمان الأمن على الفضاء الإلكتروني السبب الذي يضع مسؤولية حقيقية وفعلية على عاتق المجتمع الدولي من أجل بناء وتشكيل أنظمة متكاملة موحدة لمواجهة التهديدات في الفضاء الإلكتروني، وهيئة الأمم المتحدة هي المنظمة الأنسب في مجال تسهيل إنشاء سياسة ومنهج متفق عليه للمشاكل الملحة في

عصرنا الحاضر⁽¹⁾ كما أنها تعتبر الجهة الرائدة التي تشارك في التنسيق والتعاون فيما يتعلق بظاهرة الإرهاب الدولي⁽²⁾.

ويعتبر الأمن السيبراني من بين المسائل الرئيسية والمحورية في المناقشات التقليدية السائدة في هيئة الأمم المتحدة فيما يتعلق بالسياسة الأمنية، ويتجلى لنا ذلك من خلال المناقشات التي تتناول موضوع التهديد الإرهابي، كما يتجلى أيضا من خلال قرارات مجلس الأمن التابع للأمم المتحدة، ومسألة الأمن السيبراني هي من المسائل التي تمت مناقشتها وإدراجها ضمن برنامج عمل لجنة مكافحة الإرهاب التي أنشأها مجلس الأمن، كما عُنيت بها أيضا استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، حيث لم يقتصر الهدف ضمن هذه الاستراتيجية على مكافحة الإرهاب بجميع أشكاله ومظاهره على الإنترنت، ولكن أيضا الاعتماد على نهج فعال ومتكامل لاستخدام الإنترنت كآلية لمكافحة انتشار الإرهاب⁽³⁾.

يُرجع الدكتور عادل عبد الصادق هذا الاهتمام الذي تحظى به قضية الأمن السيبراني إلى تشعب القضية وتعلقها بالكثير من مناحي الحياة بالإضافة إلى كثرة أبعادها، ويحصر الدكتور أهم الأبعاد المؤثرة في ذلك والتي يمثل البعد السياسي أولها وهو علاقة الأمن الإلكتروني بالأمن القومي وبقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي، وما تفرضه تكنولوجيا المعلومات من تهديدات على كل المستويات، أما ثانيهما فهو البعد القانوني ودورها في تأمين الفضاء الإلكتروني على الصعيدين المحلي والدولي، وثالثهما هو البعد التنظيمي ومفاده وجود أجهزة تنظيمية تعنى بقضايا الأمن السيبراني في كل مسائله المتفرعة، أما البعد الرابع فهو البعد التكنولوجي، وهذا البعد يتجلى في فهم الإمكانيات والقدرات التقنية المتعلقة بتكنولوجيا الاتصال والمعلومات من خلال فهم طبيعة الخطر وتداعياته، وكيفية توظيفه للتصدي لها، أما البعد الخامس والأخير فهو البعد الاجتماعي ودوره في تعزيز الأمن السيبراني من خلال بناء قاعدة معرفة متعلقة

(¹) Darya MAZURTSOVA, *Un legal sources in the field of regulation of online space at the present stage*, THE YOUTH OF THE 21ST CENTURY: EDUCATION, SCIENCE, INNOVATIONS Proceedings of VI International Conference for Students, Postgraduates and Young Scientists, Publisher: Vitebsk State University named after Masa Masheroova(Vitebsk), 2019, PP. 319-321: <https://www.elibrary.ru/item.asp?id=42293436>

(²) Nazura Abdul Manap, Pardis Moslemzadeh Tehrani, *Cyber Terrorism: Issues in Its Interpretation and Enforcement*, International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012, PP.409-413: <http://www.ijiee.org/papers/126-I149.pdf>

(³) Mitko BOGDANOSKI, Drage PETRESKI, cyber terrorism –global Security theart, international scientific defence, security and peace journal, MINISTRY OF DEFENCE OF THE REPUBLIC OF MACEDONIA, 2013, PP.59-72: <https://core.ac.uk/display/35330211>

بجميع مجالات الأمن السيبراني بالإضافة إلى دور المورد البشري الذي يتشكل بفعل التعليم والتدريب بمواجهة الأخطار ورفع مستوى الوعي⁽¹⁾.

تصنف عملية ظهور المعايير المتعلقة بالأمن السيبراني في الأمم المتحدة إلى المسارات الثلاث للمفاوضات في هذا المجال، أولهما هي تلك المفاوضات المتعلقة بالقضايا السياسية-العسكرية، وثانيهما هي المفاوضات المتعلقة بالجوانب الاقتصادية، ويعبر عن كلا الاتجاهين أو المسارين الأساسيين بمصطلح الحرب السيبرانية والجريمة السيبرانية، أما المسار الثالث فهو مسار ثانوي مرتبط بظهور منتدى حوكمة الإنترنت وهو متعلق بمفاوضات إدارة الإنترنت⁽²⁾.

يوجد على الساحة خمس مجموعات من الخبراء الحكوميين في المسائل والقضايا المرتبطة بمجال الفضاء الإلكتروني، غير تحقيقها لنتائج في مجال الأمن السيبراني يبقى مربكا نظرا لعدم توحيد أعمال ونشاطات هيئة الأمم المتحدة في مجال تحقيق الأمن الإلكتروني، ويعود ذلك إلى أن المفاوضات التي تجريها تلك المجموعات ضمن هيئة الأمم المتحدة كثيرا ما تكون كساحة أو مجال يستغل كمنصات تنظيمية لأجندتها التنافسية⁽³⁾.

يمكن للعديد من الكيانات في الأمم المتحدة أن تصدر قرارات، وهذه القرارات غالبا ما تتجلى وتصدر من خلال الجمعية العامة أو مجلس الأمن، والفرق بين القرارات التي تصدرها الجمعية العامة ومجلس الأمن يتجلى في أبعاد إلزاميتها للدول الأعضاء⁽⁴⁾، فالجمعية العامة تصدر توصيات غير ملزمة في حين أن مجلس الأمن يصدر قرارات ملزمة، وليس هناك إلى حد الآن أي

(1) عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية: نمد جديد وتحديات مختلفة)، المرجع السابق، ص ص: 382-383.

(2) Tim MAURER, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security, Science, Technology, and Public Policy Program, Explorations in Cyber International Relations Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, September 2011, PP.15-16.*

(3) Ibid. P.18.

(4) يشير تيم مورير في الصفحة 13 من المرجع السابق إلى أن مجلس الأمن هو السلطة الشرعية الوحيدة لخلق قانون دولي ملزم استنادا إلى نص المادة 25 من ميثاق الأمم المتحدة التي تنص على أنه: (يتعهد أعضاء "الأمم المتحدة" بقبول قرارات مجلس الأمن وتنفيذها وفق هذا الميثاق)، فما يقتصر دور الجمعية العامة على تقديم التوصيات استنادا إلى المادة 10 من ذات الميثاق والتي تنص على أنه: (للجمعية العامة أن تناقش أية مسألة أو أمر يدخل في نطاق هذا الميثاق أو يتصل بسلطات فرع من الفروع المنصوص عليها فيه أو وظائفه. كما أن لها في ما عدا ما نصّ عليه في المادة 12 أن توصي أعضاء الهيئة أو مجلس الأمن أو كليهما بما تراه في تلك المسائل والأمور) والمادة 12 منه والتي تنص على: (1- عندما يباشر مجلس الأمن، بصدد نزاع أو موقف ما، الوظائف التي رسمت في الميثاق، فليس للجمعية العامة أن تقدم أية توصية في شأن هذا النزاع أو الموقف إلا إذا طلب ذلك منها مجلس الأمن. 2- يخطر الأمين العام - بموافقة مجلس الأمن - الجمعية العامة في كل دور من أدوار انعقادها بكل المسائل المتصلة بحفظ السلم والأمن الدولي التي تكون محل نظر مجلس الأمن، كذلك يخطرها أو يخطر أعضاء "الأمم المتحدة" إذا لم تكن الجمعية العامة في دور انعقادها، بفراغ مجلس الأمن من نظر تلك المسائل وذلك بمجرد انتهائه منها)

قرار صادر عن مجلس الأمن يتضمن مسألة من مسائل الأمن السيبراني⁽¹⁾، وهذا ما لا يضيف الإلزامية على القرارات التي تتناول موضوع الأمن السيبراني على الساحة الدولية.

يقسم الاتحاد الدولي للاتصالات عمل منظمات الأمم المتحدة بشأن الأمن السيبراني على النحو التالي:

■ "مكافحة الجريمة السيبرانية: الاتحاد الدولي للاتصالات ومكتب الأمم المتحدة المعني بالمخدرات والجريمة؛

■ بناء القدرات: الاتحاد الدولي للاتصالات، ومعهد الأمم المتحدة لبحوث نزع السلاح، ومعهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة؛

■ حماية الأطفال على الإنترنت: الاتحاد الدولي للاتصالات، واليونيسيف، ومعهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة"⁽²⁾.

2- نحو صك دولي جديد لتحقيق الأمن السيبراني:

إن المحور الأساسي الأكثر أهمية في عملية تأمين الفضاء الإلكتروني؛ هو إنشاء صك أو اتفاقية دولية جديدة ملزمة، يكون الغرض منها هو تحقيق الأمن السيبراني والتصدي للهجمات السيبرانية التي تهدد السلم والأمن الدوليين بما في ذلك جريمة الإرهاب الإلكتروني، وقد أشارت الباحثة داريا مازورتسوف إلى أن مشروع اتفاقية بشأن أمن المعلومات الدولي هو الخطوة التالية لتحقيق الأمن السيبراني، كما أشارت إلى مضمون مسودة وثيقة المشروع التي تنص على التزام الدول بالتعاون مع بعضها البعض أثناء تشكيل نظام دولي لأمن المعلومات، مسترشدة بمبادئ عدم قابلية الأمن للتجزئة والمسؤولية عن مساحة المعلومات الخاصة بها⁽³⁾، والظاهر من حاشية بحثها أنها تشير إلى المسودة المقدمة من قبل الحكومة الروسية إلى هيئة الأمم المتحدة، والتي قوبلت بالكثير من الجدل.

إذ أن روسيا وعلى خلفية تزايد المخاوف لديتها من سيطرة وهيمنة الدول الغربية على هذا الفضاء ولاسيما التطور العسكري الذي تتمتع به الولايات المتحدة الأمريكية والذي ظهر جليا في حرب الخليج سنة 1991 فضلا عن تنامي توجه الدول الغربية إلى استعمال الفضاء الإلكتروني كساحة حرب، على خلفية ذلك كله، اقترحت سنة 2000 مجموعة من "مبادئ أمن المعلومات

⁽¹⁾ CCDCOE: <https://ccdcoe.org/organisations/un/>

⁽²⁾ Tim MAURER, Op.cit.P.18.

⁽³⁾ Darya MAZURTSOVA, Op.cit.

الدولي" التي يمكن اعتبارها قاعدة يتأسس عليها صك قانوني دولي جديد، أو يمكن أيضا أن يمثل مدونة تتضمن سلوكيات بموجبها يتم تنظيم لجوء الدول إلى توظيف الفضاء الإلكتروني، وكان الغرض منه -حسب رأيها- هو ضمان فضاء إلكتروني آمن، فضلا عن حظر أشكال الأسلحة التي يتم توظيفها في هذا الفضاء الإلكتروني⁽¹⁾.

وقد اعتبارات وزارة الخارجية الروسية وفق جريدة «كومرسانت» الروسية هذا المقترح بأنه مسعى وتجربة جديدة مبتكرة وعالمية لإحلاله محل اتفاقية بودابست، التي لم توافق عليها روسيا ولم تصادق عليها رغم مصادقة الملائات المتحدة عليها مع خمس وخمسين دولة وذلك نظرا لأن روسيا تعتبر الاتفاقية ماسة لسيادتها -كما أعربت الجريدة-، كما ونشرت المجلة جزء من هذا الاقتراح أيضا⁽²⁾.

وأعربت روسيا أيضا عن إدراكها للتهديدات العالمية التي تنتج عن توظيف تكنولوجيا المعلومات لأغراض إجرامية، وسلطت الضوء على عدم وحدة النهج في هذه القضية، كما أن الوضع على الصعيد الدولي يعتبر وضع متفاقم بسبب عدم وجود إطار قانوني دولي شامل للتعاون، كما سلطت الضوء أيضا على إشكالية الاصطلاح، حيث أكدت أنه لا يوجد أي أساس مصطلحي مشترك، أما على المستوى الإقليمي فقد تم استحداث بعض من المنظمات وتم اعتماد بعض الصكوك، غير أنها صكوك لا تملك القدرة في معالجة هذه الجرائم بفاعلية، ووجهت روسيا وابلا من الانتقادات إلى اتفاقية بودابست حين اعتبرتها غير كافية لمواجهة التهديدات الحالية بسبب قدمها وعدم مسايرتها للأساليب الإجرامية الحديثة، كما أنها تمنح الفرصة لانتهاك سيادة الدولة، ومبدأ عدم التدخل في الشؤون الداخلية⁽³⁾.

غير أن هذه المسودة أو هذا المشروع قد قوبل بعدم الثقة من قبل الدول الغربية، وهذا يرجع في جزء كبير منه إلى تركيز مشروع القرار على المعلومات في حد ذاتها، والآثار المحتملة لمثل هذا التركيز على حقوق الإنسان، والدور المركزي الذي منحه النظام المقترح للحكومات والمنظمات متعددة الأطراف في إدارة حالات انعدام الأمن والمخاطر المتعلقة بتكنولوجيا المعلومات

⁽¹⁾ Camino KAVANAGH, *The United Nations, Cyberspace and International Peace and Security: (Responding to Complexity in the 21st Century)* UNIDIR RESOURCES), United Nations Institute for Disarmament Research (UNIDIR), 2017, P.15

⁽²⁾ ديفيد اغناتيوس، روسيا تحاول السيطرة على الفضاء السيبراني، جريدة الشرق الأوسط: (جريدة العرب الدولية)، العدد 14216، 30 أكتوبر 2017، تم الاطلاع عليه بتاريخ 22 أوت 2020 على الساعة 05:42، مختصر الرابط: <https://n9.cl/14va>

⁽³⁾ تقرير الأمن العام، مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، الدروة 74 للجمعية العامة، مؤرخ بتاريخ 30 جويلية 2019، ص 78.

والاتصالات، مع عدم ذكر الدور الذي تلعبه الجهات الفاعلة غير الحكومية مثل الشركات الخاصة والمنظمات الفنية في إدارتها وحلها⁽¹⁾.

وقد أشارت النمسا على سبيل المثال في رفضها للدعوات التي تتادي إلى صك دولي جديد بشأن الجريمة السيبرانية إلى اتفاقية بودابست، التي تعتبرها نموذجا للتشريعات الوطنية وإطار نموذجيا للتعاون الدولي، كما وصفها بأنها توفر صكا مرنا ومفضلا حتى بالنسبة للدول غير الأطراف في مجلس أوروبا⁽²⁾، كما اعتبرت كوستاريكا صكا دوليا⁽³⁾، فبدلا من صياغة صك دولي جديد والذي يمكن أن تنتج عنه آثار عكسية بسبب المدة التي تأخذها عملية اعتماد اتفاقيات الأمم المتحدة والتصديق عليها يجب توجيه الاهتمام إلى التنفيذ الفعال للصكوك القانونية القائمة على حد رأي دولة تشيكيا⁽⁴⁾.

كما أن ألمانيا لا تدعم هذه الدعوات أيضا، محتجة بأن التكيف مع آخر التطورات يجب أن يكون على أساس اتفاقية مجلس أوروبا، كما هو الشأن بالبروتوكول الإضافي الثاني في مجال تأمين الأدلة الإلكترونية، والتي ستعمل على تحسين التعاون في ملاحقة الجرائم والاستدلال عليها⁽⁵⁾، فيما ترى سلوفاكيا ضرورة لإعداد صك دولي جديد، وترى أنه من الضروري تشجيع البلدان التي لم تنظم إلى اتفاقية مجلس أوروبا بالانضمام إليها⁽⁶⁾.

قد نلاحظ مما تقدم من فقرات تقرير الأمين العام أن الكثير من الدول تعارض فكرة صياغة قانون دولي جديد فيما يتعلق بالجريمة السيبرانية، غير أن التقرير يشير أيضا إلى الكثير من الدول التي تدعم هذه الفكرة ومن بينها جنوب إفريقيا التي تصرح على أنها: (و يشكل غياب صك معترف به عالميا على مستوى الأمم المتحدة يتناول التعاون الدولي في مسائل الجريمة السيبرانية عاملا هاما يسهم في عدم فعالية التعاون الدولي في هذا المجال)⁽⁷⁾، كما أشار المغرب أيضا إلى دعمه لصياغة صك دولي جديد بحجة التحدي الذي يمثله الاتصال بمزودي الخدمات الاتصالية التابعين لولايات قضائية أخرى⁽⁸⁾.

(¹) Camino KAVANAGH, Op.cit. P.15

(²) تقرير الأمن العام، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، المرجع السابق، ص 13.

(³) المرجع نفسه، ص 28.

(⁴) المرجع نفسه، ص 28.

(⁵) المرجع نفسه، ص 35.

(⁶) المرجع نفسه، ص 86.

(⁷) المرجع نفسه، ص 89.

(⁸) المرجع نفسه، ص 60.

فمن خلال هذا العرض يمكن نتوصل إلى أن الاتجاه نحو صك دولي جديد فيما يخص الجريمة الإلكترونية وأمن الفضاء السيبراني ليسا على وشك الوقوع، فهذه التوترات والتباين بين الرؤى الدولية حول مسألة تأمين هذه البنية الحيوية يشكل أكبر عائق نحو ذلك.

وستضاعف مسألة حوكمة الإنترنت من هدة هذه الخلاقات والتوترات بين الدول لارتباط هذه الأخيرة بالسياسات الخارجية التي تتبناها الدول، والتي يطغى عليها طابع الاختلاف والتصادم، ولاسيما تلك السياسات الخارجية التي تتعامل بها الولايات المتحدة الأمريكية وروسيا فيما بينها، إذ ليس من اليسير أن تتقارب وجهات النظر بين الدولتين، وكل المؤشرات تؤكد أن المفاوضات بينهما في هذا المجال ستكون عسيرة، وبشكل خاص في هذه البيئة التي تتصادم فيها رؤى الدولتين حول مسألة الفضاء الإلكتروني والأمن السيبراني، ولذلك فإن عدم التوافق بينهما سيظل قائماً إذا ما استمرت الولايات المتحدة الأمريكية في محاولة فرض هيمنتها على هذا الفضاء والمسائل المتعلقة به، وإصرار روسيا على رفض هذه الهيمنة⁽¹⁾.

من الواضح جداً أن هناك انقسام وعدم توافق دولي بشأن المشروع الروسي للأمن المعلومات، وتدعم الباحثة الرأي الرافض لهذا المشروع لما طرح من أسباب، بالإضافة إلى اعتقاد الباحثة أن روسيا كدولة تميل إلى الشمولية والقمع السيبراني ستأثر بشكل شديد على المسار الديمقراطي والعمل السياسي الحر على الفضاء الإلكتروني، والتقليص بل والقضاء على النشاط السياسي المعارض، وقد أثارت الباحثة زينب مصطفى رويحه⁽²⁾ العديد من النقاط التي كونت عقيدتنا بأن روسيا لا تهدف إلى تأمين الفضاء السيبراني بقدر ما تريد تحية العالم الغربي من السيطرة عليه وفرض هي سيطرتها عليه، ومن بين أهم النقاط التي أشارت إليها الباحثة في سياق منفصل عن بحثنا؛ حرص الحملات الإلكترونية الروسية على بقاء عمر البشير كرئيس للسودان وشن حملات تشويه ضد المتظاهرين عليه، وكان ذلك لدواعي اقتصادية، حيث تعتبر السودان الدولة الثانية في أفريقيا بعد الجزائر في اقتناء السلاح الروسي، كما أن ما تملكه السودان من بنية تحتية يسهم في نقل النفط إلى العالم وهذا ما جعلها تيرم العديد من الاتفاقية معها لهذا الهدف، وكان الرئيس المخلوع عمر البشير على توافق تام مع الروس⁽³⁾.

(1) أحمد عبد العليم، اعتبارات الأمن القومي: (لماذا تقاوم روسيا "أمركة" الإنترنت؟)، المستقبل للأبحاث والدراسات المتقدمة، 10 مارس 2015، تم الاطلاع عليه بتاريخ 22 أوت 2020، على الساعة 21:01 سا، في الموقع:

<https://n9.cl/z849>

(2) باحثة ماجستير في كلية الدراسات الإفريقية العليا - جامعة القاهرة

(3) زينب مصطفى رويحه، تحديات الدور: (الأمن السيبراني في توجهات روسيا الإفريقية)، قراءات إفريقية، 13 نوفمبر 2019، تم الاطلاع عليه بتاريخ 22 أوت 2020 على الساعة 21:28 سا، مختصر الرابط: <https://n9.cl/vlhao>

3- نحو إنشاء قوة لحفظ السلام السيبراني:

لقد تطرقنا في بحثنا إلى أن الإرهاب الإلكتروني هو مظهر وآلية من آليات الحرب الإلكترونية التي تستهدف أمن الدول وحرية الأفراد على حد سواء، وإذا كانت الأحداث مثل انهيار الدولة والمعاناة الإنسانية وانتهاكات حقوق الإنسان تشكل تهديدات للسلم والأمن الدوليين، فهذا مؤشر على أن حفظ السلام الإلكتروني سيكون ضرورياً، فالهجمات السيبرانية لها كامل القدرة في إنشاء أو تزيد أو تمديد تلك الأحداث، إذ يمكن للهجمات السيبرانية أن تساهم على الأقل في انهيار الدولة إذا أحدثت فشلاً في البنية التحتية الوطنية الحيوية أو أطالت في مدة عجزها وهذا لارتباط معظم تلك البنى بالفضاء السيبراني، وهذا الأمر أيضاً ينطبق على انتهاكات حقوق الإنسان، فحفظ السلام العالمي عبر الإنترنت سيصبح ضرورة لحفظ المستخدمين المتزايدين والحيلولة دون تصعيد النزاعات وتوفير سبل للتحكيم بين الدول، والمساهمة في بناء الثقة والحفظ عليها في هذا الوسط الافتراضي⁽¹⁾.

ترجع الأبحاث المبكرة حول موضوع حفظ السلام الإلكتروني إلى يوليو 2002 على أقل تقدير، ففي ذلك الحين قام توماس ب. كاهيل وكونستانتين روزينوف وكريستوفر مولي بتحديد حفظ السلام عبر الإنترنت كمجال من المجالات البحثية في المستقبل، وهذا من خلال فحص مبادئ حفظ السلام الحالية للأمم المتحدة، اقترح هؤلاء العلماء كيفية تطبيق مبادئ حفظ السلام في المجال السيبراني⁽²⁾.

وقد اعتمدت هيئة الأمم المتحدة اصطلاحاً جديداً يشير إلى أن الأمم المتحدة تعتبر أنها لها دوراً ستلعبه في المستقبل في مجال حفظ السلام على الفضاء الإلكتروني، ألا وهو مصطلح "الخوذ الزرقاء الرقمية" الذي يقابله في العالم المادي مصطلح يماثله وهو الخوذ الزرقاء الذين هم قوات لحفظ السلام التابعة لها، ورغم أن هذه المبادرة لا تزال في بداياتها لكونها تقتصر فقط على حماية الفضاء الإلكتروني للمنظمة نفسها، إلا أن ذلك يمكن أن يتطور في المستقبل، وذلك عندما تتوفر الهياكل والخبرات الضامنة لحماية الفضاء الإلكتروني، وكذلك إذا طالب الدول الأعضاء بها⁽³⁾.

⁽¹⁾ Michael ROBINSON, Kevin JONES, Helge JABICKE, Leandros MAGLARAS, *An Introduction to Cyber Peacekeeping*, [Submitted on 26 Oct 2017([v1](#)), last revised 24 Apr 2018(this version, v2)]:

[arXiv:1710.09616v2](https://arxiv.org/abs/1710.09616v2) [cs.CY]

⁽²⁾ Fahad Nabeel, *Establishment of UN Cyber Peacekeeping Force: Prospects and Challenges*, *NUST Journal of International Peace & Stability*, Volume II, Number 2, Edited at the Centre for International Peace and Stability(CIPS), National University of Sciences and Technology(NUST), July 2019, PP.17-31:

<https://njips.nust.edu.pk/index.php/njips/issue/view/4>

⁽³⁾ Walter DORN, *Cyberpeacekeeping: (A New Role for the United Nations?)*, *GEORGETOWN JOURNAL OF INTERNATIONAL AFFAIRS*, Volume 18, No. 3, Fall 2017, PP.138-146:

<https://walterdorn.net/home/257-cyberpeacekeeping-new-role-for-the-united-nations>

ثانيا: الأمم المتحدة وثقافة الأمن السيبراني:

1- المواثيق والقرارات الدولية:

أ- ميثاق الأمم المتحدة:

يشير الدكتور عادل عبد الصادق في مقال له، إلى أن جوهر ميثاق الأمم المتحدة يتفق مع تجريم استعمال حرب المعلومات كأداة إرهابية، وهذا لكونه يمثل تهديدا وانتهاك صارخا لما عبر عنه الميثاق فيما يتعلق بالتهديد أو استعمال أشكال القوة ضد سلامة إقليم الدولة أو استقلالها السياسي، كما يرى الدكتور أيضا أن اعتبار الإرهاب الإلكتروني وتوظيف حرب المعلومات يندرجان ضمن العدوان الذي يرمي إلى إجبار الدول على القيام بعمل ما فإن ميثاق الأمم المتحدة بما ورد فيه من غرض مواجهة النزاعات المسلحة فإنه تنطبق هنا قوة القانون، وهذا يجعل من الإرهاب الإلكتروني ضمن المقاصد السنية للأمم المتحدة وميثاقها⁽¹⁾.

ب- القرارات والمؤتمرات:

تطالب هيئة الأمم المتحدة من خلال مختلف قراراتها من الدول الأعضاء العمل على تعزيز النظرة الشاملة والتمكين للاعتبارات المتنوعة إزاء كافة التهديدات سواء أكانت قائمة بالفعل أو كانت محتملة، وذلك في مجال أمن الفضاء الإلكتروني، بالإضافة أيضا إلى الاعتبارات الخاصة والمتعلقة بالتدابير والإجراءات التي يمكن من خلالها التصدي لهذه التهديدات، وترمي هذه القرارات إلى تحسين وتعزيز الوعي بالأمن على الفضاء الإلكتروني سواء أعلق الأمر بالأمن الداخلي للدول، أو الأمن العالمي بجملته⁽²⁾.

اعتمدت الجمعية العامة للأمم المتحدة قرارا يقضي بإنشاء ثقافة عالمية للأمن السيبراني، وهو قرار من بين القرارات الأولى التي لفتت الانتباه العالمي إلى مفهوم "الأمن السيبراني" كما وتضمن هذا القرار إلى جانب النظرة المفاهيمية آليات وعناصر ضرورية وأساسية لتحقيق هذا النوع من الأمن⁽³⁾ كما وأصدرت العديد من القرارات الأخرى في هذا المجال، وفيما يلي بعض من تلك القرارات الصادر عن هيئة الأمم المتحدة:

(¹) عادل عبد الصادق، الأمم المتحدة ودعم الاستخدام السلمي للفضاء الإلكتروني، المركز العربي لأبحاث الفضاء الإلكتروني، 06 أغسطس 2015، تم الاطلاع عليه بتاريخ 27 أوت 2020، على الساعة 07:38، في الموقع:

http://accronline.com/article_detail.aspx?id=22762

(²) Nazura Abdul Manap, Pardis Moslemzadeh Tehrani, Op.cit.

(³) Darya MAZURTSOVA, Op.cit.

في أعقاب مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين في هافانا، وفي القرار 45_121 بشأن جرائم الكمبيوتر الصادر في 14 ديسمبر / كانون الأول 1990 عن هذا المؤتمر، أعربت اللجنة عن أملها في أن تضاعف وتعزز الدول الأعضاء من مساعيها الرامية إلى التصدي لأشكال إساءة استخدام الكمبيوتر وذلك بشكل أكثر نجاعة وكفاءة، وهذا يتطلب اعتماد إجراءات جنائية على المستوى الداخلي بما في ذلك عند ؛ تجديد اللوائح والإجراءات الجنائية، وبشكل خاص تلك المتعلقة بالترتيبات الهادفة إلى كفالة تطبيق إجراءات مناسبة من قبل سلطات التحقيق والتصديق على الأدلة بشكل يتناسب مع طبيعتها، وتوفير النصوص المرتبطة بالأدلة والعقوبات والإجراءات للتعامل مع هذه الأنشطة الإجرامية الجديدة والمعقدة، كما حث الاجتماع الدول الأعضاء على مضاعفة أنشطتها على المستوى الدولي لمواجهة الجرائم المتعلقة بالإرهاب الإلكتروني ومنها الانضمام إلى معاهدة الأطراف وتبادل المساعدة الخاصة المتعلقة بتسليم المجرمين وجرائم الحاسوب وتعزيز التعاون الدولي في هذا المجال، لا سيما في إنشاء أو تطوير الجوانب التالية⁽¹⁾:

- مقاييس وضوابط دولية لأمن المعالجة الآلية للبيانات؛
- ترتيبات مناسبة لتجاوز إشكالية الولايات القضائية واختصاصها الإقليمي التي تتمخض عن الطبيعة التي يتسم بها هذا الفضاء الإلكتروني؛
- اتفاقيات دولية تحمل بين طياتها نصوصا من شأنها أن ترتب وتضبط الغجرات المتعلقة بإجراء التفتيش وإجراءات الضبط العابر للحدود في الفضاء الإلكتروني، فضلا عن غيرها من أساليب التعاون⁽²⁾.

بالإضافة إلى مؤتمرها الذي انعقد بالعاصمة المصرية القاهرة سنة 1995 بشأن منع الجريمة ومعاملة المجرمين، حيث أوصى المؤتمر بحماية حياة الناس الخاصة وحقوق الملكية الفكرية من زيادة وارتفاع مخاطر التكنولوجيا، كما دعي المؤتمر إلى ضرورة التعاون بين أعضاء المجتمع الدولي من أجل تنفيذ أفضل الممارسات، وكذلك مؤتمر الأمم المتحدة الخامس عشر للجمعية الدولية لقانون العقوبات الذي تم إبرامه في العاصمة البرازيلية ريو دي جانيرو سنة 1994 والذي تضمن الكثير من التوصيات والتي يبرز من بينها؛ من الضروري تحديد الجهة التي تقوم بإجراء التفتيش والضبط والزامية صياغة القواعد الخاصة بالإثبات الإلكترونية وموثوقية الأدلة⁽³⁾.

(¹) نجيب بن عمر عوينات، الإرهاب الإلكتروني: (المفهوم والجهود الدولية والإقليمية لمكافحته، المرجع السابق).

(²) المرجع نفسه.

(³) صباح كزيز وأمال كزيز، الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي، مجلة التراث، المجلد 07، العدد 05، جامعة زيان عشور، الجلفة، الجزائر، جوان 2018، ص ص: 312-328: <https://www.asjp.cerist.dz/en/article/60114>

كما نجد أيضا المؤتمر السابع الذي تم عقده بالمدينة الإيطالية في ميلانو سنة 1985، والذي بموجبه تم تكليف لجنة الخبراء العشرين بالبحث ومعالجة مسألة حماية نظم المعالجة الآلية وإساءة استخدام الكمبيوتر، وكلف بإنهاء مهمتها بتقرير تعدد وتعرضه على المؤتمر الثامن الذي عقد بهافانا سنة 1990، ومن بين أهم التوصيات التي تمخضت عنه نجد؛ تعزيز مكافحة الجريمة الإلكترونية باللجوء إلى توظيف تكنولوجيا المعلومات والاتصال في ذلك، تعرضت أيضا إلى قضية الخصوصية على ساحة الفضاء الإلكتروني، وأبرز أيضا ضرورة العمل على إعادة صياغة القوانين بشيء من الحداثة بحيث تتعرض إلى مثل هذه الجرائم وتضع من التدابير الأمنية ما يقي منها، والعمل على تكوين القضاة وكل جهات أنفاذ القانون وتدريبهم، وتعزيز التعاون بين كل الجهات ذات الصلة⁽¹⁾.

عقدت الأمم المتحدة أيضا بتاريخ 2010 مؤتمرها الثاني عشر بالبرازيل، وقد نادت من خلال هذا المؤتمر لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع يضم خبراء حكوميين على المستوى الدولي من أجل البحث وتقضي مسألة الجريمة الإلكترونية واتخاذ ما يرويه مناسبا من الإجراءات للوقوف أصاها ومكافحتها، كما صدر عن مؤتمر الأمم المتحدة الثالث عشر المنعقد بدولة قطر سنة 2015 القرار 184/67 والذي يتضمن إنشاء حلقات لتعزيز تدابير الجرائم الإلكترونية⁽²⁾.

2- دور اللجان والمنظمات التابعة للأمم المتحدة:

أ- لجنة الأمم المتحدة الاقتصادية والاجتماعية لغربي آسيا:

قدمت لجنة الأمم المتحدة الاقتصادية والاجتماعية لغربي آسيا في عام 2015 نصائحا وتوصيات مرتبطة وخاصة بالنهج والسياسات المرتبطة بالأمن السيبراني والتصدي لمظاهر الإجرام على الفضاء الإلكتروني في نطاق الدول العربية، كما وأبرزت وحللت في الآن ذاته البيئة الحالية للإجرام على الفضاء الإلكتروني وكذلك الأمن على هذه البيئة على الصعيد الإقليمي والدولي، كما وأبرزت أيضا الترتيبات والتدابير التي تعمل على تكريس وضمان تنسيق الجهود الرامية للتصدي لهذه الجرائم، فضلا عن على الإطار التشريعي الذي يضمن بيئة إلكترونية سليمة سودها الأمن والثقة، بالإضافة إلى ضرورة تكريس وتعزيز الهياكل والإجراءات التي تهدف إلى هذا الغرض وتعزيز الدور التوعوي لذوى المصلحة⁽³⁾.

(1) نعيم سعيداني، المرجع السابق، ص ص: 83-84.

(2) سهيلة هادي، آليات تعزيز حق الإنسان في الأمن المعلوماتي، المجلة الجزائرية للعلوم القانونية، السياسية والاقتصادية، المجلد 54، العدد 05 (خاص)،

كلية الحقوق، جامعة الجزائر 01، بن يوسف بن خدة، مارس 2017، ص ص: 223-251: <https://www.asjp.cerist.dz/en/article/83207>

(3) Darya MAZURTSOVA, Op.cit.

ب- الاتحاد الدولي للاتصالات:

الاتحاد الدولي للاتصالات هو منظمة أو لجنة تابعة للأمم المتحدة التي تقع على عاتقها غالبية المسؤولية في المسائل والقضايا العملية للأمن السيبراني، وهي المنظمة المعاهدة الوحيدة التابعة للأمم المتحدة التي أنيطت بها الأعمال المرتبطة بمسائل الفضاء الإلكتروني، ويلعب الاتحاد الدولي للاتصالات دوراً مهماً وحاسماً في صياغة المعايير الفنية ضمن دائرة الجهود والمساعي الذي يبذلها لتعزيز ودعم الفضاء السيبراني، ولأسما تحقيق الأمن فيه والذي يظهر جلياً من خلال اعتبار الجريمة الإلكترونية ضمن أولويات الاتحاد الثلاث⁽¹⁾.

وتظهر ريادته في مجال أمن الفضاء الإلكتروني من كل ما يتهدهده، من خلال نشاطاته المختلفة والتي يمثل بناء الثقة والأمن في الفضاء السيبراني أحدها، حيث تولى الاتحاد هذه المهمة ودعي تحت غطاءها إلى التعاون بين القطاع العام والخاص بغرض تنسيق الجهود وتبني سياسة عالمية للأمن الإلكتروني وإقامة بوابة إلكترونية للأمن الإلكتروني، كما ويتعاون الاتحاد مع الكثير من الهيئات الإقليمية والعالمية في وضع إطار عالمي للأمن السيبراني كما هو واضح من تعاونه مع المجلس الأوروبي ومكتب الأمم المتحدة لمكافحة الجريمة والمخدرات وجهات إنفاذ القانون كالإنتربول واليوروبول⁽²⁾.

ج- معهد الأمم المتحدة الإقليمي لأبحاث الجريمة والعدالة:

تم إنشاء هذا المعهد سنة 1968 بناء على قرار المجلس الاقتصادي والاجتماعي رقم 1086 "ب"، وكان الغرض الذي يرمي إليه من إنشائه هو القيام بعدد من الأنشطة المختلفة والتي تتبني على البحوث التطبيقية، التدريبات، التعاون التقني، وبشكل خاص في الميادين التي تهتم الدول النامية أو التي تسير على خط التحول الاقتصادي⁽³⁾.

من بين الوظائف والأدوار الرئيسية التي تلعبها هذه المؤسسة في مجال أمان الشبكات أو أمن الفضاء الإلكتروني ومكافحة الحروب الرقمية؛ التزامها المذهل بمشروع برنامج الأبحاث الأوروبي بشأن الجريمة والإرهاب الإلكترونيين، وهي تقوم حالياً ببرامج استكشاف وبحث حول استغلال الإجرام السيبراني من قبل جماعات الإجرام المنظم، كما تقوم المنظمة أيضاً بإبراز

⁽¹⁾ Charletta ANDERSON, *Cyber Security and the Need for International Governance*, April 24, 2016, P. 06:

[#https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769579.](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769579)

⁽²⁾ عادل عبد الصادق، الأمم المتحدة ودعم الاستخدام السلمي للفضاء الإلكتروني، المرجع السابق.

⁽³⁾ شبكة الأمم المتحدة للعدالة الجنائية ومنع الجريمة، جامعة نايف العربية للعلوم الأمنية:

<https://nauss.edu.sa/ar-sa/departments/InternationalCooperation/international-acts/Pages/CrimePrevention.aspx>

القضايا المتعلقة برفع الوعي بشأن الخصائص النمطية للقراصنة على الفضاء السيبراني، والجريمة المنظمة أيضاً، وذلك من خلال ورش العمل والاجتماعات على المستوى العالمي، كما أنها تقود أيضاً إعداد فصول دراسية مع شركائها المختلفين، ويحاول المعهد أو المؤسسة أيضاً تقديم المعلومات لذوي التخصص والاهتمام بشأن قضايا توظيف الإرهابيين لفضاء الإنترنت⁽¹⁾.

وختاماً يمكن القول أن جهود هيئة الأمم المتحدة إلى حد الآن ورغم أهميتها في رفع الوعي لدى أصحاب المصلحة ولاسيما الدول منها بضرورة تفعيل الآليات القانونية والتقنية والتنظيمية والهيكلية لمكافحة الإرهاب الإلكتروني وتأمين البيئة السيبرانية، إلا أنها لا تخرج في جملتها عن مجرد توصيات، يمكن الأخذ بها أو نبذها، وهذا بطبيعة الحال سيكون له أثر كبير في فاعلية الخطط والسياسات العالمية لمكافحة الإرهاب الإلكتروني.

فالدور الذي يجب أن تلعبه هيئة الأمم المتحدة إلى جانب ما تقوم به من توصيات وقرارات وما إلى ذلك، يجب أن يكون مرفقاً بتفعيل دور مجلس الأمن في مكافحة الإرهاب الإلكتروني، خاصة ذلك الذي تمارسه الدول أو ترعاه، خاصة وأن بعض الباحثين أمثال محمود أديب فتاح أغا الكاكه وبعد استقصائه لمختلف النصوص القانونية يرى أن الاختصاص في مجال مكافحة الإرهاب الإلكتروني معقود لمجلس الأمن⁽²⁾، فلا بد إذاً أن يكون ذات فعالية ودور كبير في مجابهة هذه الظاهرة بموجب قرارات ملزمة للدول الأعضاء.

الفرع الثاني: جهود مجموعة الثمانية:

تتكون مجموعة الثمانية من الدول الأكثر قوة في جميع الميادين، وعلى رأسها الميدان الاقتصادي والحربي، وتتعاون فيما بينها لتجاوز العقبات والخلافات التي قد تطرأ على أو بين أعضائها، وبين تلك العقبات والتحديات التي تواجه ظاهرة الإرهاب الإلكتروني وقضية الأمن السيبراني، خاصة وأن الفضاء الإلكتروني بالنسبة لهذه الدول يعد مجالاً حيويًا من مجالات أمنها القومي (أولاً)، لذلك فإن الكثير من قممها قد تعرضت لهذه المسألة بالنقاش واقتراح الحلول (ثانياً).

(¹) أنظر: عمل معهد الأمم المتحدة الأقاليمي لأبحاث الجريمة والعدالة، تقرير المجلس الاقتصادي والاجتماعي، الأمم المتحدة، 9 مارس 2015، الوثيقة (E/CN.15/2015/12)، ص 05.

(²) أنظر في ذلك؛ محمود أديب فتاح أغا الكاكه، اختصاصات مجلس الأمن في التصدي للإرهاب الدولي الإلكتروني، مجلة دراسات علوم الشريعة والقانون، المجلد 47، العدد 01، عمادة البحث العلمي وضمان الجودة، الجامعة الأردنية، الأردن، 2020، ص ص: 644-659.

<https://journals.ju.edu.jo/DirasatLaw/issue/view/710>

أولاً: سياق الأمن السيبراني في مجموعة الثمانية:

مجموعة الدول الثماني أو ما يعرف أيضا بمجموعة الدول الصناعية الثمانية، هي مجموعة مكونة من ثمان دول وهي؛ الولايات المتحدة الأمريكية، اليابان، ألمانيا، روسيا، إيطاليا، المملكة المتحدة، فرنسا، كندا، وحصة هذه الدول من الاقتصاد العالمي قد وصلت إلى 65 بالمئة، وتجمع عددا من الدول الأكثر قوة وإنفاقا على التسليح، تقوم هذه المجموعة بأدوارها من خلال نشاطات مختلفة، أهمها القيام بعقد المؤتمرات السنوية، وإنشاء مراكز البحثية⁽¹⁾.

وتعد مجموعة الثمانية منتدى غير رسمي - أي أنها ليست منظمة دولة بالمفهوم القانوني - ولذا فهي تفتقر إلى هيكل إداري مقارنة بالمنظمة الدولية، وأما عن تشكيلها فتعود في الأصل لسنة 1975 وتتكون من ستة أعضاء وكانت تعرف باسم وكانت تعرف بمجموعة الست، انضمت كندا بعد ذلك في عام 1975 وأصبحت روسيا عضواً رسمياً في عام 1998، يجتمع القادة من تلك الدول في كل عام لمناقشة أهم القضايا المستجدة ومن بين هذه القضايا مسألة الجريمة والإرهاب والمسائل والطريق السريع للمعلومات⁽²⁾ (information highway)⁽³⁾.

وفي سياق مكافحة الجريمة الإلكترونية، عقد وزراء العدل والداخلية للدول الأعضاء في مجموعة الثمانية اجتماعات عديدة لتحديد أساليب وسياسات ونهج مكافحة الجرائم المرتبطة بالفضاء الإلكتروني والتعامل معها، وتقوم جميعها إلى المبادئ والقواعد التالية؛ صد المجرمين المتورطين في جرائم تكنولوجيا المعلومات وعدم توفير البيئة التي يؤوون إليها، توثيق الصلة والتعاون بين الدول من أجل العمل على ملاحقة المجرمين وضمان تقديمهم للقضاء دون عقد الاختصاص بقضاء مكان وقوع الجريمة، تكوين وتدريب الموظفين والعاملين المتخصصين في إنفاذ القانون، وتوفير كل المعدات اللازمة للتفاعل مع هذا النوع من الجرائم، وتدعو الدول الأعضاء أيضا في مجموعة الثمانية بالعمل الحثيث من أجل التوصل إلى حلول موفقة في هذا المجال على المستوى الدولي، باعتماد اتفاقيات ذات طابع دولي في مكافحة الجريمة الإلكترونية،

(1) عصام عبد الفتاح، القيصر: (التحدي.. الإرادة.. صناعة عالم جديد)، الطبعة الأولى، كنوز للنشر والتوزيع، القاهرة، 2015، ص 48 (الحاشية).

(2) "كان طريق المعلومات السريع أو infobahn مصطلحاً شائعاً تم استخدامه خلال التسعينيات للإشارة إلى أنظمة الاتصالات الرقمية وشبكة اتصالات الإنترنت. وهو مرتبط بالسيناتور الأمريكي ونائب الرئيس لاحقاً آل جور". (ويكيبيديا):

- https://ar.wikipedia.org/wiki/%D8%B7%D8%B1%D9%8A%D9%82_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA_%D9%81%D8%A7%D8%A6%D9%82_%D8%A7%D9%84%D8%B3%D8%B1%D8%B9%D8%A9

(3) Nazura Abdul Manap, Pardis Moslemzadeh Tehrani, Op.cit.

كما تدعو إلى الاستفادة مما قامت به المجموعة من دراسات وخطط وبين تلك الخطط والتوصيات التي قامت بها سنة 1997 وسنة 1999 وعام 2002⁽¹⁾.

وفيما يتعلق بتوصياتها لتعقب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية فقد نص بيان قمة مجموعة الثمانية لسنة 2002 على ما يلي: (استخدم الإرهابيون الإنترنت للتواصل والتخطيط للهجمات. كما كان تعطيل شبكات الاتصال الخاصة بهم جزءاً مهماً من جهود مجموعة الثماني. وضعت مجموعة الثماني توصيات لتتبع الاتصالات الشبكية التي ستساعد الشرطة ووكالات الأمن القومي في تحديد مواقع المجرمين والإرهابيين الذين يستخدمون شبكات الاتصال الدولية لأغراض غير قانونية والتعرف عليهم بسرعة. طورت مجموعة الثماني مجموعة من المبادئ التي ستساعد الحكومات في تطوير سياسات لتعزيز توافر بيانات الاتصال ، مع الموازنة بين اهتمامات الخصوصية للجمهور ومصالح صناعات الاتصالات. أنشأت مجموعة الثماني شبكة من الاتصالات ذات الخبرة والمتوفرة على مدار الساعة للتعاون في التحقيقات الجنائية والإرهابية ذات التقنية العالية. وقد وسعت الشبكة من 16 إلى 28 دولة مشاركة منذ 11 سبتمبر⁽²⁾).

بالإضافة إلى ذلك، ووفقاً للتوصيات التي اعتمدها رؤساء الدول في مدينة ليون في عام 1996، أنشأت مجموعة الثمانية تشكيلة رفيعة المستوى من الخبراء في مجال الجريمة العابرة للحدود ويطلق على هذه التشكيلة أسم "مجموعة ليون"، ويدخل ضمن إطار اختصاص هذا الفريق من الخبراء وضع المعايير والمبادئ والممارسات العظيمة والفضلى في مجال جرائم الكمبيوتر، كنوع محدد من أنواع الجريمة المنسقة والمنظمة العابرة للحدود الوطنية⁽³⁾.

ولقد تم توسيع وظيفة هذه الوحدة الفرعية فيما بعد، وتوسعها يمكن النظر إليه من زاويتين، أولهما هي الزاوية الموضوعية، حيث أصبحت المجموعة توسع من مهمتها لتشمل توظيف الإنترنت من قبل الإرهابيين وحماية البنية التحتية للمعلومات الحيوية، وثانيهما هو التوسع في

(¹) جورج لبكي، المعاهدات الدولية للإنترنت: حقائق وتحديات، العدد 83، الموقع الرسمي للجيش اللبناني، كانون الثاني 2013، تم الإطلاع عليه بتاريخ 02 جويلية 2020 على الساعة 12:44 سا، مختصر الرابط: <https://n9.cl/w84mw>

(²) Fact Sheet, G8 Counter-Terrorism Cooperation Since September 11, G-7/8 Kananaskis Summit, Kananaskis, Canada, June 26, 2002:

<https://2001-2009.state.gov/e/eeb/rls/fs/11477.htm>

(³) 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 agendas institutionnels*, *Revue québécoise de droit international*, Société québécoise de droit international, volume 2-1, Hors-série novembre 2018, PP.25-39:

https://www.persee.fr/doc/rqdi_0828-9999_2018_hos_2_1_2371

نطاقها لتتجاوز نطاق اختصاص مجموعة الثمانية، وذلك من خلال بناء وتكوين مجموعة من التوصيات والإرشادات التي يمكن أن تستعين بها دول أخرى خارج مجموعة الثمانية، فضلا عن ذلك قائمة المجموعة بتكوين وإنشاء شبكة اتصال على مدار الساعة طوال أيام الأسبوع لجرائم التكنولوجيا العالية، كما أنشأت دليلا دوليا لحماية البنية التحتية للمعلومات الحرجة، ونشرت أيضا وثائقها الخاصة التي تشتمل على مبادئ وممارسات توجيهية لتقييم التهديدات التي تواجه أمن الفضاء الإلكتروني، كما ونظمت أيضا العديد من المؤتمرات تدريبية الدولية للأجهزة المعنية بالجريمة الإلكترونية⁽¹⁾.

وفي سياق مكافحة الجريمة الإلكترونية فإن وزراء العدل والداخلية في مجموعة الثمانية قد وافقوا في إطار الاجتماع المنعقد في ولاية واشنطن الأمريكية في الفترة بين 09 و 10 من شهر ديسمبر 1997 على مبادئ تأسيسية لشبكة نقاط الاتصال والتي أنيط بها اختصاص مكافحة الجريمة المتصلة بالتكنولوجيا المتقدمة⁽²⁾، وهي نقطة مراقبة دائمة للإنترنت تعمل على مدار 24 ساعة تقوم بإعطاء إنذار عندما يتسلل أحد المعتدين إلى شبكة الفضاء الإلكتروني وعندما يتم إطلاق صفارة الإنذار بوجود هذا النوع من التسلل أو الانتهاك تتطلق فرقة من كبار المتخصصين في مجال الفضاء الإلكتروني المعدة لهذا الغرض من أجل القيام تحديد الموقع الذي تم تنفيذ الهجوم منه لتحديد مرتكبيها، ويكون ذلك من خلال تتبع الأثر الإلكتروني الذي يخلفه المهاجم⁽³⁾.

ومن أجل انضمام الدول إلى هذه الشبكة يجب عليها أن تسوفي مجموعة من الشروط والتي من أهمها وأبرزها؛

- "تعيين جهة اتصال يمكن الوصول إليها على مدار الأربع وعشرون ساعة وفي كل أيام الأسبوع، ويمكن أن تكون جهة الاتصال شخص واحد يتوفر فيه فهم للتكنولوجيا والقانون المحلي المعمول به في بلده، وما هي جائر قانونا من التصرفات والنشاطات التي يجيزها له القانون لمساعدة الدول الأخرى، أو على الأقل أن يكون قادرا على الوصول الآني إلى الأشخاص أو الجهات صاحبة الأهلية في تقديم المساعدة؛

- يجب أن تكون الاتصالات بين الجهات المعنية من قبل الدول بطريق مباشر دون إشراك أي مكتب آخر في دولها، فكل جهة من تلك الجهات تقوم بالاتصال بالجهة الأخرى لبلد آخر نيابة

⁽¹⁾ Mitko **BOGDANOSKI**, Drage **PETRESKI**, Op.cit.

⁽²⁾ Pierre **BERTHELET**, Ibid.

⁽³⁾ نجيب بن عمر عوينات، المرجع السابق.

عن طالب الاتصال في بلدها، وهذا الشرط يكون ظرفياً، إذ أنه في حالة قيام التعاون بين البلدين، يمكن أن تتسحب جهة الاتصال من التحقيقات لتتابعها جهات التحقيق الأخرى بالاتصال بصفة مباشرة مع البلد المتعاون معه؛

- يجب على هذه الجهات ألا تحل محل مساهمات التعاون والمساعدة القانونية المقررة بين البلدين، فدورها هو ضمان السرعة والاهتمام بالطلب المقدم من البلد الآخر كمبدأ أولي، إذ يمكن للدولة الطالبة أن تلجأ إلى توظيف الأساليب أو الآليات الأخرى للتعاون المتبادل بين البلدين؛

- يجب على أي دولة ترغب في الانضمام إلى هذه الشبكة أن تجري اتصالاً برئيس الفريق الفرعي المتخصص في جرائم التكنولوجيا العالية في مجموعة الثمانية، ويكون ذلك بمجرد تقديم استمارة بسيطة دون اتفاقيات أو مذكرات تفاهم أو معاهدات، ومن الجدير بالذكر أن الانضمام إلى هذه الشبكة لا يعتبر قاصراً على الدول الصناعية الثمانية، بل هناك ما يزيد عن 50 دولة منضمة إليها، ويقع على الوحدة المنضمة مسؤولية إعلام جهات إنفاذ القانون في بلدها بوجودها والاستعداد لتقديم الدعم لها فيما يتعلق بأي إجراء خارج حدود الدولة⁽¹⁾

يمكن لمكتب المدعى العام بهذا الصدد الحصول على المساعدة من خلال الإنترنت بمساعدة نظام استجابة دولي الذي يضم أكثر من 100 دولة، والذي أقرته ووافقت عليه فرقة مكافحة الجريمة عالية التقنية في مجموعة الثمانية، وهذا النوع من المساعدة يعتبر ذو أهمية كبيرة وخاصة للمدعين العامين الذين يجرون تحقيقات بناء على معلومات حول الجرائم الإلكترونية الأكثر خطورة، والتي تحدث على الصعيد العالمي ضمن اختصاص المحكمة، والتي ترتكب من قبل أحد المواطنين المنتمين إلى الدولة الطرف، أو على أراضيها وفي حدود إقليمها⁽²⁾.

تشجع مجموعة الثماني أعضائها على تعزيز قوانينهم الخاصة في مجالات معينة تهم مجموعة الثماني مثل الجريمة المنظمة وجرائم التكنولوجيا العالية والاتصالات والمنظمات الإرهابية⁽³⁾، والتي تعتبرها مجموعة الثمانية ضمن إطار الجرائم العابرة للحدود⁽⁴⁾، وتشجع أيضاً

(¹) الاتحاد الدولي للاتصالات، المسألة 22/1 تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني (التقرير النهائي)، قطاع تنمية الاتصالات، لجنة الدراسات 01، فترة الدراسة الرابعة 2006-2010، ص ص: 18-19.

(²) Judge Stein **SCHIOLBERG**, *An International Criminal Tribunal for Cyberspace (ICTC) Prosecution for the Tribunal Police investigation for the Tribunal, Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes, A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group, March 2012, P.27.*

(³) Ali Obaid Sultan Alkaabi, *Combating Computer Crime: An International Perspective*, Thesis submitted in accordance with the regulations for the Degree of Doctor of Philosophy, Information Security Institute Faculty of Science and Technology, Queensland University of Technology, October 2010, PP.26-27.

(⁴) Fatima **TALAT**, *Transnational Crimes: (Investigatory Challenges)*, international Conference : Criminal Justice Under Stress, ILI Golden Jubile, Law Institute, New Delhi, Indian, 2007, PP. 302-311:
<http://14.139.60.114:8080/jspui/handle/123456789/989?mode=full>

المجموعة ضمن توصياتها على وضع خريطة لتصنيف هذا النوع من الجرائم من أجل جعلها أكثر قابلية للتخاطب بها بين البلدان، إذ أنه من الضروري محاولة تطوير تصنيف أكثر تفصيلاً للجرائم الإلكترونية مع الاتفاق على تعريف لها لتمكين المحققين والوكالات من التحقيق والتواصل والتعاون فيما بينهم وفق تفسير أو نهج أو ممارسات متسقة⁽¹⁾.

لقد أعربت مجموعة الثمانية أيضاً عن قلقها من المخاوف المختلفة المترتبة عن الوتيرة السريعة التي تتقدم بها تكنولوجيا المعلومات في البند 11 من بيان قمة أوكيناوا⁽²⁾، وأشارت في البند 44 إلى أنه: (يجب أن نتخذ نهجاً متضافراً تجاه جرائم التكنولوجيا المتقدمة، مثل الجريمة الإلكترونية، التي يمكن أن تهدد بشكل خطير الأمن والثقة في مجتمع المعلومات العالمي. تم تحديد نهجنا في ميثاق أوكيناوا لمجتمع المعلومات العالمي. للمضي قدماً في هذا الأمر، سنعمل على تعزيز الحوار مع الصناعة، بما في ذلك في اجتماع برلين المشترك في أكتوبر. نرحب بالنتائج والزمخ الذي أوجده الحوار بين الحكومة/ الصناعة حول السلامة والثقة في الفضاء الإلكتروني في باريس، ونتطلع إلى الاجتماع الثاني رفيع المستوى بشأن الجريمة ذات التقنية العالية مع الصناعة الذي سيعقد في اليابان)، ومن بين التوصيات والنهج التي تضمنها البيان؛

- تعزيز التعاون القاضي من خلال تعزيز التحقيق في الجريمة ومحاكمة مرتكبيها، وقم تم توجيه الخبراء من أجل إيجاد السبل لذلك⁽³⁾.
- دعم الجهود الرامية إلى بناء القدرات في الولايات القضائية الأكثر ضعفاً لتعزيز نظام العدالة الجنائية⁽⁴⁾.
- حماية الفئات الضعيفة وأشراك جميع السلطات المختصة في اتخاذ التدابير بالتعاون مع المجتمع المدني⁽⁵⁾.

⁽¹⁾ Ali Obaid Sultan Alkaabi, Ibid. P.81

⁽²⁾ G8 Communiqué Okinawa 2000, Okinawa, Japan, July 23, 2000:

<http://www.g8.utoronto.ca/summit/2000okinawa/finalcom.htm>

⁽³⁾ clause 48, Communiqué Okinawa 2000, Op.cit. "Enhanced investigation and prosecution of crime requires enhanced judicial co-operation. We direct our experts to find ways to do so"

⁽⁴⁾ clause 49, ibid. " We must assist capacity-building efforts in the more vulnerable jurisdictions to strengthen their criminal justice systems, in order to prevent criminal groups from threatening their social, economic and political structures and exploiting them as loopholes in the global framework to fight crime."

⁽⁵⁾ clause 50, ibid. " We must also protect vulnerable groups and the young in the fight against crime, and provide particular care for the victims of crime. We reaffirm the need for effective co-operation among competent authorities and for measures to be taken in co-operation with civil society "

ثانياً: أهم القمم التي تناولت موضع مكافحة الإرهاب الإلكتروني:

يبرز ضمن القمم والاجتماعات التي تجريها سنوياً مجموعة الثمانية اجتماعين مهمين لوزراء العدل والداخلية التابعة لمجموعة الثمانية، فكان الأول سنة 2004، حيث أقرت فيها 41 دولة على ضرورة عمل الدول على تحسين وتحديث تشريعاتها الجنائية واعتماد اتفاقية بودابست كنموذج أو كأساس يرجع إليه في ذلك من أجل السعي الفاعل والكفء في محاربة ومواجهة الإرهاب والإجرام على الفضاء السيبراني، كما وشجعت الدول على تبني المعايير والترتيبات وأسس التي تتضمنها اتفاقية بودابست، كما وشجعت أيضاً فتح آفاق جديدة للتعاون الفعال في مجال إنفاذ القانون⁽¹⁾.

أما الاجتماع الثاني فهو اجتماع موسكو سنة 2006، والذي ناقش فيه الوزراء المذكورين ضرورة العمل وبذل الجهود الرامية إلى مواجهة الظاهرة الإرهابية وسائر الجرائم على الفضاء السيبراني، والاهتمام بالمسائل المتعلقة بالفضاء الإلكتروني وضرورة العمل من أجل تحسين وتعزيز الإجراءات التي من خلالها تواجه هذه الظواهر بشكل أكثر كفاءة وفاعلية، وأكد إعلان القمة على التزام الدول بتنفيذ وتعزيز وتطوير الإطار القانوني الدولي الذي يرمي إلى مواجهة الظاهرة الإرهابية بعمومها، كما حوى البيان أيضاً بين طياته المواجهة الفعالة التي ترمي إلى قمع توظيف الفضاء السيبراني لأغراض وأهداف إرهابية، بما في ذلك استعماله في التحريض أو في استخدامه كآلة دعائية للأعمال الإرهابية أو كآلية للتخطيط لها، فضلاً عن استعماله لتجنيد وتدريب الإرهابيين⁽²⁾، ومن بين أهم النقاط التي أشار إليها الإعلان نجد؛

- "تنفيذ وتحسين الإطار القانوني الدولي لمكافحة الإرهاب؛
- ضمان تكييف التشريعات الوطنية، حسب الاقتضاء، لمواجهة التحديات الإرهابية الجديدة؛
- الانخراط في حوار نشط مع المجتمع المدني للمساعدة في منع الإرهاب؛
- وضع وتنفيذ استراتيجية فعالة لمكافحة الدعاية والتجنيد الإرهابيين، بما في ذلك ما يتعلق باستخدام المفجرين الانتحاريين؛
- التصدي الفعال لمحاولات إساءة استخدام الفضاء الإلكتروني لأغراض إرهابية ، بما في ذلك التحريض على ارتكاب أعمال إرهابية ، والإبلاغ عن الأعمال الإرهابية والتخطيط لها ، فضلاً عن تجنيد الإرهابيين وتدريبهم"⁽³⁾.

⁽¹⁾ Stein **SCHJOLBERG**, *Terrorism in Cyberspace-Myth or reality?*, Terrorism, , vol 01, 2006:

https://www.cybercrimelaw.net/documents/Terrorism_in_cyberspace.pdf

⁽²⁾ Stein **SCHJOLBERG**, Op.cit.

⁽³⁾ clause 04, G8 Summit Declaration on Counter-Terrorism, St. Petersburg, July 16, 2006:

<http://www.g8.utoronto.ca/summit/2006stpetersburg/counterterrorism.html>

أشار إعلان مجموعة الثمانية لمكافحة الإرهاب في القمة المتعددة بلاكويا بتاريخ 09 يوليو 2009 إلى قضية بالغة الأهمية والمتمثلة في التطرف الذي يفضي إلى العنف، وأعرب البيان عن قلقه من زيادة ذلك، وأوصى بتوجيه الاهتمام الخاص للانتهاكات التي ترتكبها المنظمات الإرهابية من خلال وسائل الاتصال بهدف الدعاية والتجنيد، واستغلال الإنترنت لنشر رسائل التطرف والتخطيط لأعمال العنف وتسييرها ومن بين توصيات الإعلان؛

- زيادة فهم الطرق والأساليب التي من خلالها تقوم الجهات الإرهابية باستغلال تقنيات الاتصال؛

- تعزيز الديمقراطية وحقوق الإنسان وتفعيل مبدأ سيادة القانون، وتحقيق العدالة الاجتماعية؛

- تعزيز ثقافة الحوار والاحترام لمواجهة التحريض وخطاب الكراهية؛

- تعزيز التعاون لتحسين اندماج المهاجرين (الأجانب) في مجتمعات مجموعة الثمانية⁽¹⁾.

أوضح بيان قادة مجموعة الثمانية حول مكافحة الإرهاب لسنة 2010 أن الإرهاب لن يتم قهره واستئصاله بالقوة فحسب، بل يجب العمل على تجفيف منابعه ومعالجة الظروف المؤدية إليه، وعلى رأس الأساليب التي تتيح ذلك تعزيز سيادة القانون وحماية حقوق الإنسان والحريات الأساسية، والقيم الديمقراطية والحكم الرشيد والتسامح والشمول من أجل وضع بديل يغني النفوس المعرضة للتجنيد من السقوط في هذه البؤرة، وتكرر مجموعة الثمانية التزامها بتقديم الدعم التتبعي وتلبية تطلعات شعوبها بغرض تجفيف منابع التطرف والإرهاب⁽²⁾.

ومن المثير للاهتمام، أن مجموعة الثمانية قد أوردت لأول مرة قضايا الإنترنت على جدول أعمال قمتها لسنة 2011، وعنيت النقاشات والمحادثات فيها حول تأثير الإنترنت على النمو الاقتصادي وحقوق الإنسان والحريات في سياق "الربيع العربي"، وأكد إعلان القمة على أهمية انفتاح وشفافية الإنترنت ومجانيته، لكن ومع ذلك فإنه من الضروري أيضاً العمل على صياغة قواعد لتنظيم الفضاء الإلكتروني وتجنب الانتهاكات التي تهدد الخصوصية وحقوق الملكية الفكرية، واعتبر الإعلان أن اليقظة والتعاون الدولي يعتبران أمرين مهمين وضروريين للغاية للتصدي للجرائم الإلكترونية⁽³⁾، التي يعتبر الإرهاب الإلكتروني أهمها وأخطرها.

⁽¹⁾ G8 Declaration on Counter Terrorism, L'Aquila Summit, July 9, 2009:

<http://www.g8.utoronto.ca/summit/2009laquila/2009-counterterrorism.html>

⁽²⁾ G8 Leaders Statement on Countering Terrorism, Muskoka, June 26, 2010:

<http://www.g8.utoronto.ca/summit/2010muskoka/counterterrorism.html>

⁽³⁾ Romain BOOS, La Lutte contre la cybercriminalité au regard de l'action des États, doctorat de droit privé et sciences criminelles, faculté de droit, sciences économiques et gestion, unevirsite de Lorraine, 2016, PP. 258-259.

ضمنت مجموعة الثمانية إعلانها بشأن الالتزام بالحرية والديمقراطية جملة من التوصيات والقضايا الهامة المتعلقة بالإنترنت حيث خصصت لها البنود من 04 إلى 22، وفي نطاق بحثنا أبرز البند 17 من هذا الإعلان ضرورة تعزيز التنسيق والتعاون بين الحكومات والمنظمات الإقليمية والدولية والقطاع الخاص والمجتمع المدني وعمل مجموعة الثمانية لمنع وردع ومعاينة أي استخدام لتكنولوجيا المعلومات والاتصالات لأغراض إرهابية وإجرامية، بجميع أشكال الهجمات التي يمكن أن تتخذها سواء أكانت على البنى التحتية أو الشبكات أو الخدمات، بما في ذلك هجمات البرامج الضارة، وعليه يتعين على الجهات الفاعلة التعاون على نطاق دولي لحماية الموارد الحوية وتكنولوجيا المعلومات والاتصالات والبنية التحتية الأخرى⁽¹⁾.

الفرع الثالث: دور منظمة التعاون الاقتصادي والتنمية:

تصدر قضايا الأمن السيبراني في الآونة الأخيرة قائمة جدول أعمال منظمة التعاون الاقتصادي والتنمية، نظرا لتزايد الهجمات على الفضاء الإلكتروني والبنى التحتية التابعة له، وتسارع انتشار ظاهرة الإرهاب الإلكتروني بكل أشكاله، فعملت هذه المنظمة الدولية على خلق جو للتعاون بين أعضائها (أولا)، وأصدرت توصيات عديدة أهمها المبادئ الأساسية التي تشكل النموذج العام الذي يتعين على الدول اعتماده لمواجهة التحديات التي تواجه أمن الفضاء الإلكتروني (ثانيا).

أولا: نشاطات منظمة التعاون الاقتصادي لتحقيق الأمن السيبراني:

تعتبر منظمة التعاون الاقتصادي والتنمية منتدى اقتصادي استثنائي، ففي إطاره تجتمع حكومات 30 دولية للعمل معا في مواجهة ما يعترض طريقها من تحديات أفرزتها العولمة سواء أكانت اقتصادية أو اجتماعية أو بيئية⁽²⁾، وهي عبارة عن جهة تتعامل من خلالها حكومات الدول المختلفة بشكل مشترك مع مختلف الصعوبات والتحديات التي تتمخض عن العولمة، وو المتعلقة بالدول الأعضاء وغير الأعضاء على حد سواء⁽³⁾.

⁽¹⁾ G8 Declaration: Renewed Commitment for Freedom and Democracy, Deauville, 26-27 mai 2011(publiée le 27 mai 2011): <http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-fr.html>

⁽²⁾ Nazura Abdul Manap, Pardis Moslemzadeh Tehrani, Op.cit.

⁽³⁾ Oluwafemi Osho, Agada D. Onoja, *National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis*, *International Journal of Cyber Criminology(IJCC)*, Vol. 9(1), June 2015, PP. 120–143: <https://zenodo.org/record/22390#.X3iwYsJKiM8>

تتعامل منظمة التعاون الاقتصادي والتنمية منذ ربح من الزمن مع عدد من القضايا السياسية المتعلقة بمجتمع المعلومات، وهي تتراوح بين البنية التحتية والخدمات وحماية المستهلك والخصوصية والأمن إلى القضايا الأوسع لتكنولوجيا المعلومات والاتصالات والنمو الاقتصادي⁽¹⁾.

فقد بدأت المنظمة بفحص شامل وواسع في قضايا ومسائل قانون الإصلاحات المتعلقة بانتهاكات الكمبيوتر الشخصي على الصعيد العالمي، وأتمت المنظمة في الفترة ما بين 1983 و1985 تحقيقاً حول احتمالية التنسيق العالمي للقوانين الجنائية لمعالجة السلوكيات والنشاطات غير المشروعة المرتبطة بجهاز الحاسب الآلي، وفي سنة 1986 تم الإعلان عن الفحص المتعلق بمراجعة القوانين الحالية واقتراح التعديلات والتغييرات⁽²⁾، وكان ذلك أعقاب قرار منظمة التعاون الاقتصادي والتنمية في سنة 1982 في باريس تعيين لجنة خبراء لمناقشة الجرائم المتعلقة بالحاسوب وكذلك لمناقشة الحاجة أو الضرورة إلى إحداث تغييرات وتبديلات في القوانين الجنائية، وأوصت سنة 1986 بما يلي: (و فيما يتعلق بالجوانب عبر الوطنية للنشاط الإجرامي المتصل بالحاسوب، لوحظ وجود مسائل هامة تشير إلى استصواب التعاون الدولي في قمع هذا النشاط ومكافحته، وأن تنظر جميع الدول الأعضاء في مدى شمولية القوانين الجنائية الوطنية للأعمال التي ترتكب عن علم في هذا المجال، ويمكن التعبير عن هذه الأفعال بقدر الإمكان في شروط الوظائف بدلا من التكنولوجيا)⁽³⁾.

اعتمدت منظمة التعاون الاقتصادي والتنمية أيضا المبادئ التوجيهية بشأن أمن نظم المعلومات والشبكات في يوليو 2002، ودعت حكومات الدول الأعضاء إلى وضع التخطيط والإدارة الأمنية ضمن أولوياتها الكبرى، فضلا عن تعزيز الثقافة الأمنية في وسط جميع الجهات الفاعلة كوسيلة لحماية هذا الفضاء، وترمي هذه التوجيهات في جملتها إلى تعزيز وتطوير ثقافة أمن عالمية وذلك من خلال تقديم المشورة بشأن السياسات والتدابير لمعالجة التهديدات الداخلية والخارجية مثل الإرهاب الإلكتروني أو فيروسات الكمبيوتر أو القرصنة في مجتمع مترابط عالمياً، مع الحفاظ على القيم المجتمعية المهمة مثل الخصوصية والحرية الفردية⁽⁴⁾، وسنتطرق إلى التوصيات والإرشادات التسعة التي تضمنتها في ما سيأتي من دراستنا.

⁽¹⁾ Nazura Abdul Manap, Pardis Moslemzadeh Tehrani, Ibid.

⁽²⁾ M.B. **RAQIB**, Combating Cybercrime in Bangladesh: (A Critical Analysis in the context of Legal ramification of Law), Research paper presented to Department of Law, Daffodil International University, 11 December, 2018, P. 20.

⁽³⁾ Laura **ANI**, Cyber crime and national security: the role of the penal and procedural law, " Law and Security in Nigeria, 2011, PP. 200-202: <http://nials-nigeria.org/pub/lauraani.pdf>

⁽⁴⁾ Nazura Abdul Manap, Pardis Moslemzadeh Tehrani, Op.cit

أصدرت منظمة التعاون الاقتصادي والتنمية في 2003 خطة تنفيذ المبادئ التوجيهية لأمن نظم المعلومات والشبكات، وقد تضمن المنشور عدة محاور أولهما هو الترويج لثقافة أمن عالمية، أما المحور الثاني فقد تطرق إلى الأدوار التي تلعبها الحكومة وما يقع عليها من مسؤوليات في هذا الميدان، سواء مسؤوليتها عن السياسة العامة في الأمن السيبراني ومسؤوليتها باعتبارها مالك ومشغل لأنظمة وشبكات المعلومات، وكذلك مسؤوليتها باعتبارها مستخدماً لأنظمة وشبكات المعلومات، وأما المحور الثالث فقد تعرض إلى الأدوار التي يلعبها قطاع الأعمال والمجتمع المدني⁽¹⁾.

نشرت منظمة التعاون الاقتصادي والتنمية عام 2005 تقرير تحت عنوان " تعزيز ثقافة الأمن لأنظمة المعلومات والشبكات في دول منظمة التعاون الاقتصادي والتنمية" ويتضمن هذا التقرير حصراً مفصلاً للمبادرات الوطنية الفعالة لتنفيذ المبادئ التوجيهية لأمن نظم وشبكات المعلومات الصادر عن المنظمة في عام 2002، وقد تم إعداده على أساس الردود التي ردت عليها 18 دولة في المنظمة على استبيان استقصائي تم تعميمه في شهر نوفمبر 2004⁽²⁾.

أصدرت منظمة التعاون والتنمية في الميدان الاقتصادي سنة 2008 تقرير مشروع بعنوان "ورقة تحديد النطاق بشأن سرقة الهوية عبر الإنترنت"، وتوصي الورقة بوضع ترتيبات وإجراءات ملائمة لإنفاذ القانون للوقوف أمام هذه الجريمة بمنعها واكتشافها وردعها، تضمن التقرير أو الورقة أيضاً تحليلاً للنهج القانونية المختلفة التي اعتمدتها الدول الأعضاء في منظمة التعاون الاقتصادي والتنمية للتصدي لسرقة الهوية على الفضاء السيبراني، ويبحث أيضاً في الآثار المترتبة على إنشاء جريمة جنائية منفصلة لسرقة الهوية وفي سنة 2009 قامت المنظمة بنشر كتاباً عن "فيروسات الكمبيوتر والبرامج الضارة الأخرى: تهديد لاقتصاد الإنترنت." الذي يوصي بمجموعة واسعة من التحسينات من بينها تحسين الأطر القانونية وتعزيز تطبيق القانون⁽³⁾.

تقوم منظمة التعاون الاقتصادي والتنمية بعقد العديد من الملنقيات وورشات العمل بشكل سنوي فيما يتعلق بمجال مكافحة الجريمة الإلكترونية وتحقيق الأمن السيبراني من أجل الوصول

(¹) seed: Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, Implementation Plan for the OECD Guidelines for the Security of Information Systems and Network : (Towards a Culture of Security), 02 jul 2003, (DSTI/ICCP/REG(2003)5/REV1): <http://www.oecd.org/internet/ieconomy/31670189.pdf>

(²) seed: Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, the Promotion of a culture of security for information systems and networks in OECD countries, 16 dec 2005, (DSTI/ICCP/REG(2005)1/FINAL): <http://www.oecd.org/internet/ieconomy/35884541.pdf>

(³) cybercrime law: <https://www.cybercrimelaw.net/OECD.html>

إلى معايير أمنية وقانونية التي تتمكن من خلالها مسيطرة الطفرات التي تحدث في جرائم الإنترنت⁽¹⁾، ومن بينها ما قامت به المنظمة بالتعاون مع البنك الدولي حيث تم تنظيم ورشة عمل حول اتساق السياسات في تطبيق تكنولوجيا المعلومات والاتصالات من أجل التنمية، وناقشوا فيه أيضا الاعتبارات الأمنية وتحدياتها⁽²⁾.

ثانيا: توصيات منظمة التعاون الاقتصادي والتنمية:

تتضمن التوصيات المتعلقة بالأمن على الفضاء الإلكتروني 09 مبادئ هي: الوعي، المسؤولية، الاستجابة، الأخلاق، الديمقراطية، تقييم المخاطر، تصميم وتنفيذ الأمن، إدارة الأمن، إعادة التقييم⁽³⁾.

1- الوعي:

تعتبر عملية تطوير نهج وطني لرفع الوعي بالقضايا المتعلقة بالأمن السيبراني كمنطلق أولي للأمن السيبراني⁽⁴⁾، إذ يتعين العمل على تكوين دراية تامة لأصحاب المصلحة بضرورة العمل إلى ضمان أمن أنظمة وشبكات المعلومات، فضلا عن توعيتهم بالتحركات والترتيبات التي تمكنهم حال اتخاذها من تعزيز هذا الأمن، والإجراءات التي يمكنهم اتخاذها لتعزيز الأمن؛ يتمثل خط الحماية والدفاع الرئيسي لتحقيق الأمن على الفضاء الإلكتروني في إدراك ومعرفة أشكال المخاطر التي تتهدد هذا الفضاء، والإحاطة بالسبل المتاحة للتصدي لها، فأصحاب المصلحة في أمس الحاجة إلى فهم أن الإخفاقات الأمنية لن تؤدي فقط إلى إلحاق أضرار جسيمة بالأنظمة والشبكات التي تقع تحت سيطرتهم، ولكن أيضا تلحق الضرر بالأنظمة والشبكات الأخرى، فعليهم إذا بناء نظام متكامل لتحسين الأمن في الفضاء الإلكتروني⁽⁵⁾.

وعلى المستوى الداخلي ينبغي لمجلس الإدارة أن يوافق على صياغة بيان السياسة من قبل الإدارة والتي تنص بشكل واضح على أن أمن أنظمة الحواسيب في الشركة هو مسؤولية تقع على جميع الموظفين⁽⁶⁾. وبإسقاط هذه التوصية النفيسة على موضوع دراستنا يمكن أن نقول أن هناك حاجة ماسة إلى

(1) رزيقة حيزير، واقع مكافحة الجريمة الإلكترونية، مجلة الحكمة للدراسات الإعلامية والاتصالية، المجلد 05، العدد 10، مؤسسة كنوز الحكمة للنشر والتوزيع، الجزائر، جوان 2017، ص ص: 80-95: <https://www.asjp.cerist.dz/en/article/63716>

(2) cybercrime law, Op.cit.

(3) Mitko **BOGDANOSKI**, Drage **PETRESKI**, Op.cit.

(4) علي زياد العلي، المراكز النظرية في السياسة الدولية، الطبعة الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2017، ص 226.

(5) Organization for Economic Co-operation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD PUBLICATIONS, France, 2002, P.8 and 20: <http://www.oecd.org/sti/economy/15582260.pdf>

(6) Walter O. **BAGGETT**, reating a culture of security: The OECD standards for systems security provide internal auditors with a tool for operationalizing tone at the top, " Internal Auditor, vol. 60, no. 3, June 2003, p. 37. Gale Academic OneFile, Accessed 1 Sept. 2020, at 09:45h, in: <https://link.gale.com/apps/doc/A103194416/AONE?u=maine&sid=AONE&xid=4280cb74>.

رفع الوعي في المسائل المتعلقة بأمن الفضاء الإلكتروني والمخاطر التي تتهدده جراء توظيفه كمحل للهجمات الإرهابية أو كوسيلة لخدمة الأغراض الإرهابية والتخريبية، وقد أوصى الدكتور عادل عبد الصادق فيما يتعلق بتوظيف أسلحة الفضاء الإلكتروني على أهمية إدراج كافة ذوى المصلحة في استراتيجية رفع الوعي بمخاطر استخدامها على الأمن الدولي⁽¹⁾.

2- المسؤولية:

يجب على ذوى المصلحة أن يكونوا على قدر كبير من الوعي والإدراك بما يقع عليهم من مسؤولية في الجوانب المتصلة بأمن وسلامة الفضاء السيبراني، وأن يتحملوها بشكل فردي وفقاً للدور الذي يلعبونه في منظومة الأمن السيبراني، ويدخل في نطاق مسؤوليتهم أيضاً بتقييم ومراجعة كل ما يتعلق بالأمن السيبراني من سياسات وتدابير وما إلى ذلك من المسائل المتعلقة بالأمن السيبراني، ويتعين أن يكون ذلك بشكل مستمر ودوري أجل ضمان ملائمتها، كما يتعين على أولئك الذين يطورون ويصممون ويقدمون المنتجات والخدمات أن يأخذوا بعين الاعتبار الأمن السيبراني ونشر من المعلومات أنسبها وأكثرها ملائمة، حتى يتمكن المستخدمون من فهم خصائص ومميزات الأمان بشكل أفضل⁽²⁾.

ويندرج أيضاً في نطاق المسؤولية أن تحدد الاستراتيجية المعنية بالأمن السيبراني وكالة أو كياناً مسؤولاً عن زيادة الوعي العام بالمخاطر الإلكترونية والحاجة إلى توفير بيئة آمنة على الفضاء السيبراني، وتوفير الموارد التعليمية التي تعمل على المساعدة ودعم عملية تعزيز الحالة العامة للأمن السيبراني، ويجب أن يشمل ذلك أيضاً تحسين العنصر البشري في الأمن السيبراني⁽³⁾، ويجب على الاستراتيجية الوطنية المرتبطة بالأمن السيبراني وقضايا الفضاء الإلكتروني أن تحدد كياناً لإنفاذ القانون تقع على عاتقه المسؤولية بشكل أساسي في قضايا والمسائل الأمن السيبراني⁽⁴⁾.

3- الاستجابة:

يمكن تعريف الاستجابة لحوادث الأمن الإلكتروني على أنها: (عملية مستمرة تقوم فيها فرق معينة بتحديد حوادث الأمن الإلكتروني المحتملة والتحقيق فيها والاستجابة لها والتعلم منها في الوقت المناسب وبطريقة فعالة من حيث التكلفة)⁽⁵⁾.

(¹) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المرجع السابق، ص 155.

(²) Organization for Economic Co-operation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD PUBLICATIONS, France, P.20, Ibid.

(³) Cristin Flynn GOODWIN, J. Paul NICHOLAS, Developing a National Strategy for Cybersecurity: (foundations for Security), growth and innovation, Microsoft Corporation, 2013, P.19

(⁴) Ibid. P.21.

(⁵) Humza NASEER, A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility, Submitted in fulfilment of the requirements of the degree of Doctor of Philosophy, School of Computing and Information System, University of Melbourne, octobre 2018, P.01

فيجب على أصحاب المصلحة العمل على الاستجابة بالسرعة الملائمة والتعاون الجدي والفعال للحوادث الأمنية التي تحدث بالفضاء السيبراني، كما يجب عليهم أيضا العمل على تبادل معلوماتهم حول أشكال التهديدات ونقاط الضعف في الفضاء الإلكتروني بطريقة مناسبة ووضع إجراءات للتعاون السريع والفعال من أجل الحيلولة دون وقوع الحوادث واكتشافها والاستجابة لها، ويمكن أن يكون ذلك على نطاق واسع يتجاوز الحدود الوطنية⁽¹⁾.

4- الأخلاق:

يحتاج أصحاب المصلحة في الفضاء الإلكتروني إلى أن يكونوا على دراية تامة بالضرر الذي يمكن أن يتسببوا فيه للآخرين من خلال بعض السلوكيات والتصرفات على الفضاء الإلكتروني، أو حتى الإحجام عن بعض التصرفات، ولذلك فإن السلوك الأخلاقي على الفضاء الإلكتروني يعتبر ضروري ومهم، ويجب على أصحاب المصلحة السعي لتطوير وتبني أفضل الممارسات وتعزيز أحسن السلوكيات التي تأخذ في الاعتبار الضرورات الأمنية وتحترم المصالح المشروعة لأصحاب المصلحة من غيرهم⁽²⁾.

وكذلك تطوير الأخلاقيات الأمنية وفهمها فهما دقيقا واحتراما من قبل جميع الفاعلين على الفضاء السيبراني للوصول إلى جعل هذا الفضاء إرثا مفتوحا يمكن للجميع الاستفادة به دون أن يتعرضوا لأي شكل من أشكال التهديد أو لأي خطر من الأخطار الأمنية⁽³⁾.

وبهذا الصدد ينص دليل الأمن السيبراني للبلدان النامية الصادر عن الاتحاد الدولي للاتصالات على أن: (نهج الأمن السيبراني هو مشروع اجتماعي بالقدر الذي يهتم الجميع بتحقيقه، سيتم تعزيز صلاحيتها إذا تم تطوير أخلاقيات الاستخدام والسلوك السيبراني فيما يتعلق بتكنولوجيا المعلومات)⁽⁴⁾.

ومن بين أهم الممارسات الأخلاقية التي يجب مراعاتها على الفضاء السيبراني، صيانة الفضاء الإلكتروني من أشكال الدنس التي تتضمنها بعض النصوص والملاحظات، احترام الأطراف الأخرى التي تتعامل على ساحة الفضاء الإلكتروني، والتقييد بعدم التسبب في أي ضرر للآخرين،

⁽¹⁾ Organization for Economic Co-operation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD PUBLICATIONS, France, P20, Op.cit.

⁽²⁾ Ibid.

⁽³⁾ Union internationale des télécommunications, Guide de la cybersécurité pour les pays en développement, Bureau de développement des télécommunications, Union internationale des télécommunication, Genève, Suisse, 2007, P.17.

⁽⁴⁾ Ibid. P.08.

الحرص على تقديم الأفضل على هذا الفضاء والتزام التشريعات والقوانين المعمول بها، احترام الخصوصية ما إلى ذلك من الأخلاقيات والسلوكيات الشخصية والاجتماعية على الفضاء الإلكتروني⁽¹⁾.

وفي العموم يمكن تقسم أخلاقيات الفضاء الإلكتروني إلى ثلاث أقسام رئيسية، أولها هي أخلاقيات التي ترتبط بتوظيف الفضاء الإلكتروني بين المستخدم وضميره، وثانيهما هي تلك الآداب التي يتعامل من خلالها المتعامل على الفضاء الإلكتروني بينه وبين بقية الجهات أو الأشخاص الآخرين، وأما ثالثهما فهي التي الآداب المرتبطة بكيفية تعامل المستخدم مع الأجهزة نفسها⁽²⁾.

5- الديمقراطية:

يحدث في الكثير من الأحيان الدس على حقوق الإنسان وحررياتهم الأساسية بدعوى مكافحة أشكال الإرهاب، وقد وجه العديد من المختصين تحذيرات بشأن التداعيات التي تنعكس على الديمقراطية وحرية التعبير تحت عباءة مكافحة الإرهاب، وبينوا أن الإنترنت ينسجم انسجاماً تاماً مع مبادئ الديمقراطية وحرية التعبير والرأي وقيم الشفافية والعدالة الاجتماعية والمساواة⁽³⁾ وقد رصد مركز الخليج لحقوق الإنسان انتهاكات خطيرة بشأن حرية الرأي والتعبير على الإنترنت في قانون مكافحة الجريمة الإلكترونية، والتي تمثل قضية المجلة الإلكترونية "طلعنا عالحرية" أبرزها⁽⁴⁾.

ومشكلة التوفيق بين الديمقراطية ومكافحة الإرهاب عموماً ليس مشكلة حديثة، بل تعود جذورها إلى الموجة الأولى من عمليات مكافحة الإرهاب الدولي كما سبق وأن أشرنا إليه في معرض حديثنا عن انتهاكات سجنى جوانتانامو وأبو غريب، فالخروقات القانونية في سياق مكافحة الإرهاب كثيرة، وقد أشار مارتين شاينين إلى سبب ذلك حين أكد أن (انعدام المراقبة والمساءلة السياسية والقانونية قد يسرا مزاوله وكالات الاستخبارات أنشطة غير قانونية. ويحتمل أن يكون

(1) صباح محمد عبد الكريم كلو، أخلاقيات مجتمع المعلومات في عصر الإنترنت، مجلة الملك فهد الوطنية، المجلد 13، العدد 01، مكتبة الملك فهد الوطنية، الرياض، يناير-يوليو 2007، ص ص: 286-305.

https://www.researchgate.net/publication/259589506_akhlayat_mjtm_almlwmat_fy_sr_alantrnt

(2) حسين حسيني جامع وأميرة رضا مسعد السعيد ومثال عبد العال مبارز، تطوير تدريس منهج الكمبيوتر وتكنولوجيا المعلومات لطلاب المرحلة الإعدادية في ضوء متطلبات الوعي بأخلاقيات للتكنولوجيا المعاصرة، مجلة العلوم التربوية، المجلد 24، العدد 04، الجزء 03، معهد الدراسات

التربوية، جامعة القاهرة، مصر، أكتوبر 2016، ص ص: 377-402: <http://search.shamaa.org/FullRecord?ID=119838>

(3) محمد قيراط، الإرهاب الإلكتروني... التحديات وآليات المواجهة، 20 يونيو 2015، تم الإطلاع عليه بتاريخ 02 سبتمبر 2020 على الساعة 10:36، في الموقع: <https://elaph.com/Web/NewsPapers/2015/6/1017643.html>

(4) سوريا: قانون مكافحة الجرائم الإلكترونية يهدد حرية الرأي والتعبير على الإنترنت، مركز الخليج لحقوق الإنسان، 16 ماي 2018، تم الاطلاع عليه بتاريخ 02 سبتمبر 2020، على الساعة 10:55، في الموقع: <https://www.gc4hr.org/news/view/1862>

مسؤولون حكوميون قد غضوا الطرف عن ذلك السلوك المخالف للقانون إن لم يكونوا قد أوعزوا فيه (سرا) ونفى مارتين إمكانية التبرير بقواعد الحصانة التي تتمتع بها أسرار الدولة أو المصلحة العامة لتقوم الدول بغض الطرف عن التزامها الإيجابي بقوانين حقوق الإنسان⁽¹⁾.

ولهذا تؤكد منظمة التعاون الاقتصادي والتنمية يتعين في إطار توفير بيئة آمنة على الفضاء الإلكتروني العمل في الوقت نفسه على احترام تلك القيم المتعارف عليها في الأوساط أو المجتمعات الديمقراطية، وبشكل خاص تلك المتعلقة بحرية تبادل الأفكار والآراء، والتدفق الحر للمعلومات، ومبدأ سرية المعلومات والاتصالات، وضمان حماية كافية للمعلومات التي تعتبر ضمن الإطار الشخصي، والانفتاح والشفافية⁽²⁾.

6- تقييم المخاطر:

تتدرج عملية تقييم مخاطر تكنولوجيا المعلومات ضمن دائرة إدارة مخاطر هذه الأخيرة⁽³⁾، وتساعد هذه العملية في تحديد التهديدات ونقاط الضعف، وتشترط منظمة التعاون الاقتصادي والتنمية أن يكون التقييم واسعاً بما يكفي لتغطية جميع العوامل الداخلية والخارجية الرئيسية، ويعمل تقييم المخاطر على تحديد المستوى المقبول للمخاطر، كما ويسهل اختيار الضوابط المناسبة لإدارة مخاطر الضرر المحتمل على أنظمة وشبكات المعلومات، مع مراعاة طبيعة وأهمية المعلومات التي يتعين حمايتها، و يجب أن يأخذ تقييم المخاطر في الاعتبار الضرر الذي يلحق بمصالح الآخرين أو يتسبب فيه الآخرون نتيجة الترابط المتزايد لأنظمة المعلومات⁽⁴⁾.

7- التخطيط الأمني وتنفيذه:

يشكل التخطيط [أو التصميم] النطاق الجامع والشامل الذي في سياقه يتم التعامل مع أشكال الأزمات، وهذا ما يشير إلى صياغة تصميمية نموذجية مسبقة لما يجب القيام به والطريقة التي يجب أن يتم به، ومن هو الذي سيناط به أمر القيام به، وعلى هذا فإن التخطيط يعد في الغالب

⁽¹⁾ نقلا عن: فرج محمد لامة، المرجع السابق، ص 114.

⁽²⁾ Organization for Economic Co-operation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD PUBLICATIONS, France, Op.cit. P.21.

⁽³⁾ ملحم خوري نيكولا، تقييم مخاطر تكنولوجيا المعلومات، رحلة التميز في مجال التدقيق الداخلي: (رؤى حول الحوكمة وإدارة المخاطر والرقابة الداخلية)، المدقق الداخلي - الشرق الأوسط -، معهد المدققين الداخليين الدولي، يونيو 2017، ص ص: 10-11:

<http://www.internalauditor.me/jomiz-ia/wp-content/uploads/2017/07/Arabic-final-1.pdf>

⁽⁴⁾ Organization for Economic Co-operation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD PUBLICATIONS, France, Ibid. P.22.

ذو صلة وثيقة بجوهر الأزمات وبتصور مآلتها في المستقبل، والنهج التوقعي للأحداث والترتيب لما قد يستجد من طارئ، وتصميم افتراضي لتعاقب الأنشطة وما يكون كفيلاً من أعمال لمعالجة ما يطرأ من أزمات ، وفي مجال مكافحة الإرهاب وردعه يعرفه على أنه: (التنبؤ بالأحداث الإرهابية المحتملة في المستقبل والتي يمكن من خلالها تحديد الأهداف ووضع السياسات والاستراتيجيات للتقليل من الأحداث والحد منها)⁽¹⁾.

فيتعين في توصية منظمة التعاون الاقتصادي والتنمية -من أجل العمل على تحسين الأمن السيبراني-؛ "القيام بتصميم الأنظمة والشبكات والسياسات وتنفيذها وتنسيقها، مع التركيز بشكل رئيسي على تصميم واعتماد تدابير وحلول وقائية مناسبة من أجل منع أو الحد من الضرر المحتمل المرتبط بنقاط الضعف والتهديدات المحددة، ويجب أن تكون الإجراءات الوقائية والحلول تقنية وغير تقنية وأن تكون متناسبة مع قيمة المعلومات في أنظمة وشبكات معلومات المنظمة، يجب أن يكون الأمن جزءاً أساسياً من جميع المنتجات والخدمات والأنظمة والشبكات وجزءاً لا يتجزأ من تصميم وبنية الأنظمة، وبالنسبة للمستخدمين النهائيين، يتضمن تصميم وتنفيذ الأمن بشكل أساسي اختيار المنتجات والخدمات وتكوينها لأنظمتهم"⁽²⁾.

8- إدارة الأمن:

نظم إدارة أمن المعلومات بشكل عام هي: (جزء من النظام العام للإدارة، تقدم نموذجاً مبني على منهج مخاطر أنشطة أعمال، لإنشاء وتنفيذ وتشغيل ومراقبة ومراجعة وصياغة وتحسين أمن المعلومات لتحقيق أهداف المنظمة)، أو هي: عبارة عن عملية مستمرة من تطوير وتنفيذ وتشغيل ومراجعة وتحسين نظام أمن المعلومات موثق في المنظمة، ومعرفة وتقييم المخاطر المتوقعة وتقديم الحلول المناسبة سواء كانت حلولاً تقنية أو إدارية أو تشغيلية وإجرائية)⁽³⁾.

ولذلك توصي منظمة التعاون الاقتصادي والتنمية يجب أن تستند إدارة السلامة إلى تقييم المخاطر وأن تكون ديناميكية وشاملة لتغطية جميع مستويات نشاط أصحاب المصلحة وجميع

(¹) صالح خلف زيد المطيري، دور القيادة الأمنية في مواجهة الحدث الإرهابي: (دراسة تطبيقية على قوات الطوارئ الخاصة وقوات الأمن الخاصة بمنطقة الرياض)، رسالة ماجستير في قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005، ص 49.

(²) Organization for Economic Co-operation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD PUBLICATIONS, France, Op.cit. P.22.

(³) رؤى يونس، دراسة واقع إدارة أمن نظم المعلومات في المؤسسات السورية، مجلة جامعة البعث للعلوم الهندسية، المجلد 39 العدد 31، جامعة البعث، حمص، سوريا، 2017، ص ص: 61-90.

<http://magazine.albaath-univ.edu.sy/modules.php?name=News&file=article&sid=16#.X3kFXsJKiM8>

جوانب عملياتهم، يجب أن تتضمن أيضاً وبشكل مسبق الاستجابات للتهديدات الناشئة وأن تتضمن أيضاً ما يحول دون وقوع هذه الحوادث واكتشافها قبل حدوثها ومعالجتها حال وقوعها⁽¹⁾.

9- إعادة التقييم:

تدعو الطبيعة التي يتسم بها الإجرام على الفضاء السيبراني وحتى طبيعة هذا الفضاء إلى إعادة التقييم في كل مرة، فالتغيرات الأمنية والتهديدات السيبرانية تعرف حركة تطور وتجدد، وهذا يدعو إلى إلزامية ووجوب مراجعة وإعادة تقييم وتعديل جميع جوانب الأمن باستمرار لمواجهة هذه المخاطر المتطورة والمستجدة⁽²⁾، ويتعين أيضاً القيام من حين لآخر بإعادة تقييم لكل من الخطة وعلى تنفيذها أيضاً وذلك من أجل قياس أبعاد ما تم تحقيقه من أهداف وغايات، وبيان للجوانب التي تتطلب إجراء تحسينات في التصميم أو في طريقة تنفيذها⁽³⁾.

وفي ختام هذا المبحث، يمكن القول بأن الاستجابة القانونية لظاهرة الإرهاب الإلكتروني يمكن أن تتخذ عدة نهج، أولهما توظيف تشريعات الجرائم الإلكترونية الحالية لتجريم استخدام الإرهابيين للإنترنت، غير أن تحديات موضوعية وإجرائية تصادف هذا النهج، وثانيهما هو استخدام تشريعات مكافحة الإرهاب الحالية لتجريم ومقاضاة الإرهابيين السيبرانيين، كجريمة التحريض العلني على ارتكاب أعمال إرهابية أو تجنيد الإرهابيين، غير أن هذه التشريعات لا تتضمن -على سبيل المثال- أحكاماً متعلقة بتلك الجرائم الإرهابية الموجهة ضد أنظمة الكمبيوتر، وثالثهما هو نهج صياغة تشريعات حديثة تتناول بشكل خاص توظيف الإرهابيين للإنترنت، كما هو الحال بالقيم F66 من قانون تكنولوجيا المعلومات الهندي لعام 2000، المعدل في عام 2008⁽⁴⁾.

⁽¹⁾ Organization for Economic Co-operation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD PUBLICATIONS, France, Op.cit. P.23.

⁽²⁾ Ibid. P.23

⁽³⁾ الاتحاد الدولي للاتصالات، المسألة 22/1: تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني (التقرير النهائي)، المرجع السابق، ص 23.

⁽⁴⁾ Marco GERCKE, Understanding cybercrime: (Phenomena, challenges and legal response), the ITU publication, telecommunication Development Sector, Geneva, Switzerland, September 2012, PP.220-221

المبحث الثاني:

التعاون القضائي الدولي في التصدي للإرهاب الإلكتروني

تشكل السيادة الوطنية للدول على حدودها إقليمها، عمالا مثبطا في سير عمليات التحقيق وجمع الأدلة والوثائق والمعلومات المتعلقة بكافة صور الإجرام العابرة للحدود، وبصورة خاصة في النشاطات الإرهابية التي توظف مجال الفضاء الإلكتروني أو تحدده كهدف لها، في حين نجد أن هذه الجرائم ونخص منها جرائم الإرهاب الإلكتروني موضوع الدراسة قد تحلت من هذه القيود، فلا عبرة للسيادة في هذا النوع من الإجرام الذي يمكن أن يقع بضغطة زر من بعد أميال عن الموضع المستهدف، ونظرا لخطورة هذه الجرائم وإدراكا من الدول بأن مواجهتها لا يمكن بحال أن تكون شأنا داخليا محضا تستغني فيه عن مساعدات غيرها من الدول أو المنظمات، فإنها قد عملت على خلق آليات قانونية تمكنها من التوفيق بين مقتضيات السيادة وحفظها، وبين تنشيط وتكثيف الجهود القضائية الرامية إلى مواجهة هذه الجرائم وتقديم المتورطين فيها أمام العدالة لنيل الجزاء العادل عما اقترفته أيديهم، وهذا من خلال تبادل المساعدات القضائية المختلفة عبر القنوات الدولية أو الإقليمية المخصصة لذلك أو من خلال الأجهزة الوطنية التي خصها التشريع بمباشرة صور وأشكال متعددة من المساعدات القضائية (المطلب الأول)، كما وضعت أيضا نظام تسليم المجرمين والجناء في جرائم الإرهاب السيبراني لتسليمهم إلى طالبهم إثر ما أسند إليهم من تهم، وهذا على خلفية المبدأ القاضي بالمحاكمة أو التسليم (المطلب الثاني).

المطلب الأول:

المساعدة القضائية الدولية

تحيط بظاهرة الإرهاب الإلكتروني الكثير من الصعوبات والتحديات في التعاون الدولي لمكافحته ومواجهة قضائيا، ورفعاً لهذه التحديات فإن غالبية الدول قد ساهمت في بناء منافذ للتعاون فيما بينها عبر توافيقها على إنشاء دوائر أو منظمات دولية وإقليمية لتشكل قنوات تعمل أو تحاول أن تعزز من التعاون القضائي بين الدول في مكافحة أشكال الإجرام التي يمثل الإرهاب الإلكتروني واحدة منها (الفرع الأول)، كما تقوم الدول أيضا لهذا الغرض بدعم التعاون الإجرائي من خلال تجديد الأساليب التقليدية وتحديثها لتكون أكثر مواءمة مع هذه الجريمة، كما تعمل على إيجاد صيغ قانونية ملائمة لتطبيق الأحكام الجنائية الأجنبية (الفرع الثاني)، ويمتد إطار التعاون والمساعدة القضائية الدولية ليشمل تبادل البيانات والمعلومات والوثائق الاستدلالية وتعزيز تكوين

وتدريب أجهزة إنفاذ القانون لمواكبة ما يستجد في ميدان الإرهاب الإلكتروني والتحديات التي تطرأ في أساليب مواجهته (الفرع الثالث).

الفرع الأول: قنوات المساعدة القضائية:

تتطلب مقتضيات التعاون والمساعدة القضائية الدولية في مجال مكافحة الإرهاب الإلكتروني منافذ خاصة يمكن أن تنفذ من خلالها متجاوزة العقبات السياسية والقانونية التي يثيرها مبدأ سيادة الدولة على إقليمها، خاصة في مجال التعاون الشرطي بين الدول، فكان أن ظهرت المنظمة الدولية للشرطة الجنائية التي تكتسي طابعا عالميا (أولا)، بالإضافة إلى منظمات أخرى تمارس مهامها ضمن إطار جغرافي محدد تم في إطار الاتحادين الأوروبي والأفريقي (ثانيا).

أولا: على الصعيد الدولي:

الإنتربول:

الإنتربول أو (المنظمة الدولية للشرطة أو المنظمة الدولية للشرطة الجنائية) هي وكالة أمنية دولية مسؤولة ومشرفة على إنفاذ القوانين وتنفيذ الإجراءات والآليات القانونية التي تم الاتفاق والإجماع عليها بين الدول للتفاعل والتصرف مع الجرائم والمتورطين فيها، وتلتزم بتسيخ التضافر بين الأجهزة الأمنية وأجهزة الشرطة في مختلف البلدان من أجل العمل على التصدي للنشاطات الإجرامية وعلى رأسها النشاطات الإرهابية التي زاد الاهتمام بها من قبل منظمة الشرطة الجنائية الدولية وزاد اهتمامها في مطاردة المتورطين فيها في الفترة التي أعقبت الهجمات الإرهابية في الحادي عشر من أيلول⁽¹⁾.

وتعد هذه المنظمة من بين المنظمات الدولية الحكومية التي تمتلك كيانا دائما وشخصية قانونية دولية، كما تعد أيضا أضخم منظمة شرطية على المستوى العالمي، وقد تم إنشاؤها سنة 1923 حيث اجتمع فيها أجهزة الشرطة لـ 194 دولة، واتخذت من مدينة ليون الفرنسية مقرا رئيسيا لها، وتتكون من خمس أجهزة أساسية هي؛ الجمعية العامة، اللجنة التنفيذية، الأمانة العامة، المكاتب المركزية الوطنية، لجنة الرقابة على المحفوظات⁽²⁾.

لعبت المنظمة الدولية للشرطة الجنائية دورا حقيقيا في النضال والمكافحة ضد الجرائم، ذلك لكونها منظمة دولية مكرسة لتطوير التعاون الشرطي بين الدول وإزالة العوائق التي تقف كحجر

(1) جهاد عودة، هيكل العلاقات العربية الأمريكية في مجال مكافحة الإرهاب، المكتبة الأكاديمية، القاهرة، مصر، 2010، ص 61.

(2) جيلالي مانيو، دور قواعد بيانات منظمة الشرطة الجنائية الدولية (الإنتربول) في التحقيقات الجنائية والكشف عن الجرائم، معالم للدراسات القانونية والسياسية، المجلد 03، العدد 02، المركز الجامعي، تندوف، الجزائر، ديسمبر 2019، ص ص: 73-92 <https://www.asjp.cerist.dz/en/article/103080>

عثرة في مواجهة هذه الجرائم التي أصبحت تمثل خطراً كبيراً وتشكل أضراراً جسيمة على حياة الإنسان وسلامته. في جميع أصقاع العالم، لا سيما عند ارتكاب أصناف الجرائم العابرة للحدود⁽¹⁾ التي تعتبر جرائم الإرهاب الإلكتروني واحدة منها.

كما تلعب أيضا دورا مهما وحيويا في مواجهة ومقارعة الجرائم الإلكترونية بجميع أصنافها وأشكالها بما في ذلك جريمة الإرهاب السيبراني الذي يعد بما يكتنف هذا الفضاء من مميزات وخصائص ميدانا من الميادين الإجرامية الأكثر تزايدا ونموا، وفي هذا النطاق من الجرائم وما يتطلبه من مواجهة فقد سارت المنظمة على خط مسير متعدد المراحل، وفي هذا السياق بين الأمين العام لهذه المنظمة أن المبادرات الدولية التي ترمي إلى مواجهة الجريمة الإلكترونية وترسيخ الأمن السيبراني لا بد أن يكون مشتملا على إنفاذ القوانين والعمل بشكل مباشر مع القطاعات الخاصة المتخصصة في أمن الإنترنت، مع وجوب تنسيق القوانين والأحكام فيما يتعلق بهذا النطاق بين كافة دول العالم⁽²⁾.

ومن الجدير بالإشارة إليه، أن منظمة الشرطة الجنائية الدولية لا تمتلك نفس الوظيفة ولا تقوم بنفس العمل الذي تقوم به أجهزة الشرطة على المستوى الوطني، فهي منظمة لا تمتلك محققين ذوي صبغة دولية، فالأعمال التي تقوم بها في ظل التعاون والتعاقد الشرطي إنما تقوم به من خلال أعضاء الشرطة الوطنية الذين ينطون تحت سلطة الدول الأعضاء في المنظمة داخل حدود اختصاصهم الإقليمي، وضمن الأحكام التشريعية الوطنية لهذه الدول، فالمرمى من إقامة هذه المنظمة الدولية هو التعاون في العمل على التصدي لأشكال الجريمة العالمية وملاحقة المتورطين فيها والعمل على كبح شيوعتها وانتشارها⁽³⁾، وتقوم المنظمة من أجل تحقيق هذا الهدف ولاسيما فيما يتعلق بالإجرام السيبراني بالاعتماد على وسيلتين:

أولهما: العمل على جمع البيانات والمعلومات المرتبطة بالجريمة والنشاط الإجرامي عن من خلال المكاتب المركزية الوطنية التي تتوزع على مستوى الحدود الإقليمية للدول الأعضاء⁽⁴⁾، ولقواعد البيانات هذه دورا بالغ الأهمية على محليا ودوليا، فهي قواعد تحمل بين ثناياها أعداد

⁽¹⁾ مؤيد عبيد حسن العزي، حق المتهم في محاكمة عادلة: (دراسة مقارنة وتطبيقية)، الطبعة الأولى، المركزي العربي للدراسات والبحوث العلمية للنشر والتوزيع، مصر، 2020، ص 263.

⁽²⁾ صباح كزيز وأمال كزيز، المرجع السابق.

⁽³⁾ معمر بن علي وعبد الملك الدح، الوسائل المتاحة لمنظمة الإنترنت لمواجهة الجريمة المنظمة، مجلة البحوث القانونية والاقتصادية، المجلد

02، العدد 02، المركز الجامعي لأفلو، الجزائر، ماي 2020، ص: 130-143: <https://www.asjp.cerist.dz/en/article/114321>

⁽⁴⁾ نعيم سعيداني، المرجع السابق، ص 108.

مهولة من القيود المثبتة والتي من شأنها أن تتيح معلومات بالغة الأهمية عن الأشخاص، فمثل هذه القواعد التي تتضمن الآليات والتقنيات وما إلى ذلك من القدرات والإمكانات الشرطية يمنح إمكانية الاطلاع بصورة لحظية على البيانات الهامة والجوهرية التي من شأنها أن تعمل على تحديد هوية المتورطين في الجرائم الخطيرة، ولهذه القواعد أيضا دور كبير في عملية مكافحة المقاتلين الإرهابيين الأجانب وحدث هوة في هذا المجال، بمفضل ما تتيحه من آليات لتبادل المعلومات المرتبطة بتطبيق القانون على المستوى الدولي⁽¹⁾.

ثانيهما: دعم آليات التعاون من أجل مطاردة المتورطين في النشاطات الإجرامية ووضع اليد عليهم وتقديمهم -بموجب إجراءات التسليم- إلى الدول التي تطالب بتسليمهم إليها⁽²⁾.

طور الإنتربول أيضا نظام تعاون خاص، وهو النظام الوطني للنقطة المرجعية المركزي (NCRP)، كما تتوفر كل دولة من الدول المنظمة إلى منظمة الشرطة الدولية على مكتب مركزي على المستوى الوطني حيث يلعب فيها دور مقر أو موضع الاتصال بين مختلف الإدارات الأجنبية التي تقوم بتنفيذ عمليات التحقيق خارج إطار حدودها، وتشكل هذه المراكز ثلة من المحققين الذين يناط بهم اختصاص الجرائم حيث تعمل على تسهيل الاتصالات على أرض الواقع بين مختلف الدول الأعضاء في منظمة الإنتربول، كما يناط بها أيضا مهمة العمل على تطوير السياسات والأساليب والمعلومات فيما يتعلق بأخر التطورات المرتبطة في نهج وسبل الإجرام في ميدان تكنولوجيا المعلومات، كما تتوفر أيضا على المستوى الإقليمي فرق متخصصة في هذا الشأن أيضا، وقد قامت أيضا بإنشاء برنامج محدد متخصص في مجال مواجهة ظاهرة الجريمة المعلوماتية الذي يهدف إلى إتاحة أشكال من التدريب للعمل على صياغة المعايير والالتزام بمقتضياتها، وتيسير قنوات وسبل تبادل المعلومات بين الدول الأعضاء في المنظمة، وكذلك العمل على التوفيق بين مختلف العمليات على الصعيد الدولي، كما تقوم أيضا بوضع لوائح تضم أسماء الضباط المناط بهم عملية الاتصال بحث يتم وضعها بين يدي المحققين في الجرائم السيبرانية، كما تقوم أيضا بمد يد العون في التحقيقات السيبرانية، وبناء شراكات بينها وبين مختلف المنظمات الدولية ومؤسسات القطاع الخاص، كما تقوم أيضا بضبط أشكال التهديدات وتبادل مختلف البيانات وإنشاء نوافذ على الساحة الإلكترونية تسمح بنشر المعلومات والوثائق⁽³⁾.

(1) جيلالي مانيو، المرجع السابق.

(2) نعيم سعيداني، المرجع السابق، ص 108.

(3) مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، المجلد 12، العدد 02، جامعة غرداية، الجزائر،

ديسمبر 2019، ص ص: 703-726: <https://www.asjp.cerist.dz/en/article/108893>

كما وضع الإنتربول أيضا ما يعرف بمجموعة جريمة التكنولوجيا المتقدمة المعرفة اختصارا بـ (FHT) وهذا عقب إنشاء وتشكيل سكرتارية الإنتربول العامة ومجلس المالية المصغرة بداية من تاريخ 17 سبتمبر 2001، والهدف من إنشاء مثل هذه المجموعة هو القيام بالتصدي لظاهرة الإجرام المنظم التي ترتبط بالجرائم المتعلقة بالتكنولوجيا المتطورة مثل العملات المزورة وانتهاك المعلومات والمعالجة الآلية للمعلومات⁽¹⁾.

أنشاء الإنتربول أيضا في إطار مجابهة ومحاربة ظاهرة الجريمة السيبرانية مركزا متعدد الاختصاصات والذي يتكون من تشكيلة من المتخصصين في مسائل الإنترنت يتم تعيينهم من بين أجهزة تطبيق القانون والقطاع الخاص من اجل العمل على حشد كل المعلومات المتوفرة عما له علاقة بنشاط الإجرامي الذي يتم تنفيذه على ساحة الفضاء الإلكتروني وتحليلها، والهدف من هذا كله هو تمكين الدول الأعضاء من الاطلاع ووضع اليد على المعلومات ذات الطابع الاستخباراتي التي مكن صياغتها في نموذج عملي، كما يعمل المركز أيضا على إصدار تقارير من اجل إنذار وتحذير الدول الأعضاء ولفت نظرهم إلى مختلف المخاطر السيبرانية المستجدة، والملاحظ من خلال التقارير التي صدر إلى الآن من المركز اشتغالها على مخاطر محددة، بما في ذلك البرمجيات الخبيثة، وأنواع الرسائل التي يتم استغلالها في التصيد الاحتيالي، والمواقع الحكومية التي تم اختراقها، وصور الاحتيال التي يتم التوظيف فيها الهندسة الاجتماعية وما على ذلك من الآليات والأساليب⁽²⁾.

ومن بين أهم النشاطات التي قامت بها منظمة الشرطة الجنائية الدولية في إطار ما سبق ذكره ما يلي:

- "قام الإنتربول بالدخول في شراكة مع Fortinet لتحديد وإحباط عمليات الجريمة السيبرانية ذات المستويات المنخفضة والمتوسطة، كما قامت أيضا بجلب خبراء في الأمن السيبراني من إندونيسيا وماليزيا وميانمار والفلبين وسنغافورة وتايلاند، كما ساعد الإنتربول ومكتب التحقيقات الفيدرالي حكومة ماليزيا في إحباط مجموعة Anonymous Malaysia، والتي تعتبر مجموعة قراصنة تعمل على الصعيد الدولي؛

(1) مراد قريبيز وفاطمة الزهراء تيشوش، الإنتربول في مواجهة تحديات الجريمة المنظمة، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد

02، المركز الجامعي لأفلو، الجزائر، ماي 2020، ص ص: 119-129: <https://www.asjp.cerist.dz/en/article/114320>

(2) التصدي لتهديدات الجريمة السيبرية، موقع الإنتربول: تم الإطلاع عليه بتاريخ 03 سبتمبر 2020 على الساعة 09:56 سا: في الموقع: <https://www.interpol.int/ar/4/6/1>

- يخطط خبراء الأمن السيبراني في الإنتربول لحضور قمة غرب إفريقيا للأمن السيبراني لتبادل أفضل الممارسات مع وحدات مكافحة الجرائم الإلكترونية التابعة للحكومات الإقليمية، كما أنشأ الإنتربول مجموعة العمل الأفريقية المعنية بالجرائم الإلكترونية من أجل العمل على تبادل المعرفة والأدوات وأفضل الممارسات، وكذلك تسهيل التعاون الوثيق بين وحدات مكافحة الجرائم الإلكترونية الوطنية، ورفع الوعي بالجوانب العملية للتعاون الدولي؛

- قامت منظمة الإنتربول في يونيو 2017، برصد الهجمات الإلكترونية في أوكرانيا، وتواصلت مع الجهات المستجيبة والمتضررة من جراء هذه الهجمات والتي كانت تستهدف بشكل خاص البنية التحتية للبنوك والحكومة الأوكرانية، كما قام الإنتربول بالتبليغ عن مواطن روسي كان مطلوباً على خلفية اشتباهه في تنفيذ عملية الاختراق الإلكتروني للجنة الوطنية الديمقراطية خلال الانتخابات الرئاسية لعام 2016⁽¹⁾.

- نظم الإنتربول دورة تدريبية لأفراد أجهزة إنفاذ القانون الليبيين أمام التزايد المستمر لاستخدام الإنترنت لأغراض إرهابية والتي تتناول منافذ الانتفاع بشكل أكثر فعالية من الإنترنت ومن مواقع معينة للتواصل الاجتماعي في إطار التحقيقات المتعلقة بمحاربة الإرهاب، حيث تم تنظيم الدورة المشار إليها في تونس، وشارك فيها 20 من موظفي أجهزة تنفيذ القانون الذين يندرجون في كل من جهاز المباحث الجنائية وجهاز المباحث العامة في طرابلس (ليبيا)، وطرحت أمامهم توصيات بشأن الأساليب التي تكفل الاستخدام الأمثل للتقنيات الاستخبارات من أجل جني الفوائد العظيمة من موارد التي يتيحها عالم الإنترنت مع الالتزام بالأحكام التي تمليها قواعد حقوق الإنسان، والسبل الليبية لحماية البيانات، والمعايير الدولية لحماية الخصوصية والبيانات، وتعتبر هذه الدورة نموذجاً للتعاون الساري المفعول بين جهاز الإنتربول والدولة الليبية في هذا الباب⁽²⁾.

- تقوم منظمة الإنتربول بجانب عملها المؤسسي، بالإشراف على عمليات أمنية ذات الصلة بالبحث والتحري في الجرائم المنظمة والتي تنفذها المؤسسات الأمنية للدول الأعضاء فيها، والعمل على تعزيز عمليات التنسيق فيما بينها من أجل ضمان الكفاءة والفعالية في محاربة هذا النوع من الجرائم، وقد لعب الإنتربول دوراً مهماً في عملية "نماسك" سنة 2012 على إثر مجموعة من الهجمات التي وجهت من أقاليم بعض الدول ضد مواقع إلكترونية تابعة للحكومة

(1) BACKGROUND GUIDE, INTERPOL, Specialized Committee, tmun 2018, p.14:

https://static1.squarespace.com/static/533e6b7de4b0d84a3bd7c4be/t/5a387def71c10b6d1365dabc/1513651697948/Interpol_Background_Guide.pdf

(2) تدريب ضباط ليبيين على التصدي لأنشطة الإرهابيين على الإنترنت، الإنتربول، 24 يناير 2020، تم الاطلاع عليه بتاريخ 03 سبتمبر 2020، على الساعة 10:07 سا، في الموقع: <https://www.interpol.int/ar/1/1/2020/4>

الكولومبية، والتي كان موضوعها استهداف جريمة القرصنة الحاسوبية، وقد ترتب عن هذه العلمية إلقاء القبض على عدد من المتورطين فيها قدر بـ 25 فردا في أمريكا اللاتينية وأوربا بجانب الأرجنتين وإسبانيا وشيلي وكولومبيا، بالإضافة إلى 250 جهاز معلوماتي وهواتف خلوية وبطاقات دفع مالية ومبالغ مالية⁽¹⁾.

ومن خلال ما تم عرضه، نلاحظ أن دور الإنترنت في الفترة الأخيرة قد حدث فيه طفرة كبيرة في مواجهة كافة صور ومظاهر الإجرام السيبراني ولاسيما ذاك الذي يكتسي طابعا دوليا، فنشاطات الإنترنت في هذا المجال إنما هي قبل كل شيء انعكاس للوعي الدولي حول خطورة وتداعيات الجرائم السيبرانية ولاسيما الإرهاب الإلكتروني منها على السلم والأمن الوطنيين والدوليين، وليس الأمن المراد هنا مجرد الأمن المادي المعروف، إنما الأمن الذي نتحدث عنه، هو الأمن بمفهومه الواسع الذي يشمل كافة عناصر الحياة الإنسانية، ثم إن نشاطات الإنترنت في مجال مكافحة الإرهاب الإلكتروني لا تعكس فقط أهمية الدور الذي تلعبه المنظمة في حماية الفضاء الإلكتروني، بل تعكس في الوقت عينه أبعاد فاعلية التعاون القانوني الدولي في مواجهة هذه الظاهرة، حيث تؤكد نشاطات الإنترنت ضرورة فتح المزيد من المنافذ دوليا وإقليميا للمزيد من التعاون لتعزيز فرص قمع هذه الجريمة النكراء.

ثانيا: على الصعيد الإقليمي:

1- الاتحاد الأوروبي: يضمن الاتحاد الأوروبي منظمات أساسيين من منافذ المساعدة

القضائية وهما:

أ- اليوروبول:

اليوروبول هو اختصار لتسمية المنظمة التي أطلق عليها اسم (المكتب الأوروبي للشرطة)⁽²⁾، وهي مؤسسة على مستوى الاتحاد الأوروبي تأسست في لوكسمبورغ في عام 1992، ومقرها لاهاي، وتعتبر بمثابة آلية تصل وتربط بين إدارات الشرطة الوطنية في الدول الأعضاء في مجالات جرائم الإرهاب والمخدرات والجريمة المنظمة وجرائم المعلومات. تهدف الوكالة إلى تيسير وتعزيز تبادل المعلومات بين إدارات الشرطة في الدول الأعضاء فيها، فضلا عن قيامها بتجميع

⁽¹⁾ نسيم تمرنتات، مكافحة الجريمة المنظمة العابرة للأوطان في ظل جهود "الإنترنت": (نظرة تقييمية)، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد

02، المركز الجامعي لأفلو، الجزائر، ماي 2020، ص ص: 211-229: <https://www.asjp.cerist.dz/en/article/114327>

⁽²⁾ مكافحة الإرهاب.. مهام وصلاحيات اليوروبول، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، 04 يوليو 2019، تم الاطلاع عليه

بتاريخ 20 سبتمبر 2020، على الساعة 20:34 سا، في موقع المركز: <https://wp.me/p8HDP0-c7Z>

وتحليل المعلومات لمد يد العون والمساعدة في التحقيق في إحدى الجرائم السالفة الذكر، بما في ذلك جرائم المعلومات، في أي دولة من الدول الأعضاء، ولقد دعمت أيضا الشرطة القضائية الفرنسية وأطلقا دعما لبناء جهاز خاص داخل منظمة اليوروبول تم تسميته بـ (Internet Crime Reporting online System ICROS)⁽¹⁾.

وقد قام اليوروبول في إطار مكافحة الجرائم السيبرانية بتكوين واستحداث المركز الأوروبي للجرائم الإلكترونية (EC3) سنة 2013، ويهدف هذا المركز إلى تكوين أرضية لثلية ودعم تجاوب تنفيذ القانون فيما يتعلق بالجرائم ذات الطابع الإلكتروني داخل الاتحاد الأوروبي، وهذا ما يفضي بالتبعية إلى توطيد نمط المساعدة في حفظ أمن أصحاب المصالح من مواطنين وشركات وحكومات من صور الإجرام التي تتهددهم على الفضاء السيبراني⁽²⁾.

كما يعد هذا المركز كقاعدة معلومات على الصعيد الأوروبي فيما يتعلق بهذا النوع من الجرائم، ويسعى أيضا إلى بناء وتطوير قدرات وإمكانيات الطب الشرعي الرقمي من أجل تعزيز عمليات التحقيق في الإجرام السيبراني، بالإضافة إلى الإسهام في التكوين وتنمية الوعي العام ورفع مستوى تقنيات وأساليب إجراء التحقيقات في على مستوى الاتحاد الأوروبي⁽³⁾.

وتحوى أيضا شركاء خارج هذا الاتحاد وتساهم في تعزيز التعاون بين مختلف القطاعات، وتساعد في تبادل الخبرات والكفاءات⁽⁴⁾، فكان لهذا المركز الدول الكبير من تاريخ ظهوره في الانخراط والإسهام في مجال مجابهة الإجرام الإلكتروني وذلك من خلال إسهامها في العديد من العمليات المهمة وعمليات نشر الدعم التشغيلي الفوري الأمر الذي تمخض عنه ضبط للعديد من المتورطين في مثل هذه الجرائم، كما عملت أيضا على تحليل كددا كبيرا من الملفات الضارة⁽⁵⁾.

ومن بين أهم الأدوار التي لعبها اليوروبول في مكافحة الإرهاب السيبراني:

(¹) نعيم سعيداني المرجع السابق، ص 108.

(²) Europol website, european cybercrime center- EC3,:(Combating crime in a digital age):

<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

(³) Europol website, new european cybercrime centre- EC3, 21 January 2013, Accessed on 05/09/2020, At 15/50H, in:

<https://www.europol.europa.eu/newsroom/news/new-european-cybercrime-centre-ec3-opens-europol>

(⁴) MINISTÈRE DE L'INTÉRIEUR, la réponse du ministère de l'intérieure de la menace liée au numérique en 2019, Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, Rapport n° 3, France, Mai 2019 P.34.

(⁵) Europol website, european cybercrime center- EC3, Ibid.

- ناقش حسب ما ذكر اليوروبول في بيانه الصادر في يناير 2018 أنه بالإضافة إلى مسؤولي الشرطة البريطانية والفرنسية والبلجيكية، شارك ممثلو Instagram أيضاً في المناقشة بهدف تحديد المحتوى الإرهابي والمتطرف العنيف الذي يتم تنزيله والتأكد من حذفه بسرعة من الموقع، وفي يناير 2018، شارك Facebook في حوار رئيسي مع وكالة الشرطة الأوروبية لمناقشة كيفية إيقاف واستئصال منشورات الإنترنت المتطرفة المتعلقة بالإرهاب والعنف، بالإضافة إلى محاولة إيجاد منافذ لإجراء التحقيقات، وأساليب مواجهة أشكال النزاعات المستحدثة وآليات الدفاع عن النفس في مواجهة هذا الشكل من الاعتداءات⁽¹⁾.

- "و في أبريل 2018 ، صرحت الشرطة الأوروبية عن إطلاق عملية إلكترونية منسقة، أدت إلى قطع متزامن لوكالة دعاية لتنظيم الدولية الإسلامية في العراق والشام المعروف اختصاراً بداعش على الإنترنت، وأفادت منظمة يوروبول أيضاً أن العملية الإلكترونية كانت بتعاون بين شرطة أوروبية وأمريكية حيث تسببت في عجز مواقع التنظيم الإلكترونية لأجل غير مسمى"⁽²⁾.

- عقدت منظمة اليوروبول العديد من الشركات الجماعية والثنائية فيما يتعلق بالإرهاب والإجرام السيبراني، ومن أبرزها الشراكة بينها وبين معهد الأمم المتحدة الأقاليمي لأبحاث الجريمة والعدالة في إطار مشروع جدول الأعمال الأوربي لبحوث الجريمة السيبرانية والإرهاب السيبراني المعروف بـ(COURAGE)⁽³⁾، كما تعتبر المنظمة عضواً في التحالف الذي أعلنت عنه بريطانيا لمكافحة الجرائم الإلكترونية على الصعيد العالمي⁽⁴⁾،

- "قام المركز الأوروبي للجرائم الإلكترونية التابع لليوروبول على إنشاء فرقة العمل المشتركة لمكافحة الجرائم الإلكترونية(J-CAT) في 2014، وهذه الفرقة هي أول فرقة عمل لمكافحة الجرائم الإلكترونية فعلية ومشتركة، وتتألف من ضباط أو مسؤولي الاتصال السيبراني من الدول الأعضاء الملتزمة والمشاركين بشكل وثيق داخل وخارج أوروبا، وتتضمن عمليات فرقة J-CAT تحقيقات منسقة حول أقوى التهديدات السيبرانية وأكثرها انتشاراً، بما في ذلك الهجمات على الأطفال والفيروسات التي تسرق معلومات تسجيل الدخول المصرفي والمجرمين البارزين، مثل أولئك المنخرطين في أدوات القرصنة والتداول في المنتديات السرية. المجرمون الذين يبيعون

(1) مكافحة الإرهاب .. مهام وصلاحيات اليوروبول، المركز الاوربي لدراسات مكافحة الإرهاب والاستخبارات، المرجع السابق.

(2) المرجع نفسه.

(3) مذكرة من الأمين العام حول عمل معهد الأمم المتحدة الأقاليمي لأبحاث الجريمة والعدالة، المجلس الاقتصادي والاجتماعي للأمم المتحدة، 05 افريل 2016، المرجع السابق، ص 18.

(4) إنشاء تحالف دولي جديد لمكافحة الجرائم الإلكترونية حول العالم، موقع قناة بي بي سي(BBC)، 05 يوليو 2011، تم الاطلاع عليه بتاريخ 12 سبتمبر 2020 على الساعة 11:36سا، في الموقع:

https://www.bbc.com/arabic/scienceandtech/2011/07/110705_intrenational_body_cyber_crimes

البيانات الشخصية. تجمع J-CAT بيانات حول موضوعات جريمة محددة من الوكالات الوطنية والحكومات ذات الصلة والشركاء من القطاع الخاص ، وتحويل هذه البيانات الأولية إلى معلومات استخباراتية قابلة للتنفيذ ، وتقتصر أهدافاً وشبكات تحقيق⁽¹⁾.

- "تتبنى منظمة اليوروبول مؤخرًا منهجية تحليل استراتيجي جيد في إطار تقييمها الأولي لتهديدات الجريمة الخطيرة والمنظمة المعروفة بـ(SOCTA)، وتم إنشاؤها بشكل عام لتحليل التهديد الذي تشكله الجماعات المنظمة والتي يمكن توظيفها أيضا بعد إجراء ما يلزم لفحص خصوصيات تهديدات الجرائم الإلكترونية وتهدف هذه المنهجية إلى تحليل خصائص التعدد لمجموعات الجريمة المنظمة والسمات المهددة لمناطق الجريمة المنظمة والخطرة، وأبعادها الجغرافية"⁽²⁾.

ب- اليوروجيست:

تعتبر منظمة اليوروجيست مؤسسة أو جهاز يعمل على محاربة مختلف الجرائم داخل أوروبا، وقد تم تأسيسها في عام 2002، فعندما يؤثر الفعل الإجرامي على دولتين عضوين في الاتحاد الأوروبي أو دولة عضو أخرى من غير الاتحاد الأوروبي فإن ذلك الفعل الإجرامي يخضع لولايتها القضائية، ويعتبر هذا الجهاز بمثابة رابطة تدعم التعاون قضائي، وتتمثل مهمتها الرئيسية في التنظيم والتنسيق بين الأجهزة القضائية المسؤولة عن التحقيقات، ولديها سلطة جعلها مؤهلة لإجراء التحقيقات وبدء الإجراءات الجنائية⁽³⁾.

فالجهاز يؤدي دورا داعما فيما يتعلق بالتحقيقات والملاحقات التي تطلقها الأجهزة القضائية على الصعيد الوطني وبشكل خاص فيما يرتبط منها بالجريمة الإلكترونية⁽⁴⁾، وقد تم إنشاء اليوروجيست Eurojust بموجب القرار 187/2002 / JHA1 كهيئة تابعة للاتحاد الأوروبي تتمتع بالشخصية القانونية لتحفيز وتحسين التنسيق والتعاون بين السلطات القضائية المختصة في الدول الأعضاء⁽⁵⁾.

⁽¹⁾ traduire du: Tuesday **REITANO**, Troels **OERTING**, Marcena **HUNTER**, *Innovations in International Cooperation to Counter Cybercrime:(The Joint Cybercrime Action Taskforce(J-CAT))*. **The joint cybercrime action taskforce The European Review of Organised Crime**, vol. 2, no 2, 2015 PP. 142-154: https://www.academia.edu/download/39045137/08_ReitanoEtAl_pp142-154.pdf

⁽²⁾ traduire du: Laviero **BUONO**, *Fighting cybercrime through prevention, outreach and awareness raising*, " **ERA Forum**. Vol. 15. No. 1. Springer Berlin Heidelberg, 2014: <https://link.springer.com/content/pdf/10.1007/s12027-014-0333-4.pdf>

⁽³⁾ نعيم سعيداني المرجع السابق، ص ص: 108-109.

⁽⁴⁾ فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01-بن يوسف بن خدة-، السنة الجامعية 2017-2018، ص 90.

⁽⁵⁾ DÉCISION 2009/426/JAI DU CONSEIL du 16 décembre 2008, sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, J.O.U.E L138 du 04/06/2009.

تتمثل إحدى المهام الرئيسية لليوروجيست في تسهيل وتعزيز التعاون بشكل أفضل بين الدول الأعضاء، وبشكل أخص من خلال تبادل المعلومات أثناء اجتماعات التنسيق، مع مراعاة السرعة المحتملة التي يمكن بها ارتكاب الجرائم الإلكترونية، ففي رسالة من اللجنة إلى البرلمان الأوروبي، ومجلس ولجنة المناطق: " نحو سياسة عامة بشأن مكافحة الجريمة الإلكترونية"، يوصف اليوروجيست بأنه أداة قوية في مكافحة الجرائم الإلكترونية، ويقدم نهجاً منسقاً⁽¹⁾.

تهدف منظمة اليوروجيست حسب ما نصت عليه المادة 03 من قرار المجلس بشأن تعزيز يوروجيست وتعديل القرار JHA / 187/2002 إلى ما يلي:

- "ترمي منظمة اليوروجيست في نطاق العمل التحقيقي والملاحقات القضائية التي تشمل دولتين أو أكثر من الدول الأعضاء والمتعلقة بالسلوك الإجرامي المشار إليه في المادة 4 في مجال الجرائم الخطيرة، خاصة عندما تكون على نسق منظم إلى تعزيز التنسيق بين السلطات المختصة في الدول، مع مراعاة أي طلب من سلطة مختصة في دولة عضو وأي معلومات مقدمة من قبل هيئة مختصة بموجب الأحكام المعتمدة في إطار المعاهدات، وترمي أيضا إلى " تحسين التعاون بين السلطات المختصة في الدول الأعضاء، ولا سيما من خلال تسهيل تنفيذ طلبات التعاون القضائي والقرارات في هذا المجال، وخاصة فيما يتعلق بالأدوات التي تُنفذ مبدأ الاعتراف المتبادل"، كما تهدف أيضا إلى دعم الجهات المختصة في تلك الدول لتطوير وتعزيز فعالية التحقيقات والملاحقات القضائية؛

- ترمي اليوروجيست أيضا إلى تقديم المساعدة والدعم في مجال إجراء التحقيقات والملاحقات القضائية المتعلقة بتلك الدولة العضو المنفردة، ودولة ثالثة، شريطة أن يكون هناك اتفاق من أجل إقامة علاقة تعاون ت إبرامه مع تلك الدولة، أو إذا كانت هناك، في حالة معينة، مصلحة أساسية في تقديم هذا الدعم والمساندة؛

- يمكن لليوروجيست أيضا تقديم المساعدة القضائية في مجال التحقيقات والملاحقات القضائية المتعلقة بتلك الدولة العضو وحدها أو المفوضية بناء على طلب أي من السلطة المختصة لدولة عضو أو من المفوضية⁽²⁾.

⁽¹⁾ UROJUST, Cybercrime, UROJUST News, European Union Agency for Criminal Justice Cooperation, Issue No. 7 - October 2012, P.06:

[http://www.eurojust.europa.eu/doclibrary/corporate/newsletter/Eurojust%20News%20Issue%207%20\(Nov%202012\)%20on%20the%20fight%20against%20cybercrime/EurojustNews_Issue7_2012-11-EN.pdf](http://www.eurojust.europa.eu/doclibrary/corporate/newsletter/Eurojust%20News%20Issue%207%20(Nov%202012)%20on%20the%20fight%20against%20cybercrime/EurojustNews_Issue7_2012-11-EN.pdf)

⁽²⁾ Article 03, Décision du Conseil sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI du Conseil instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, conseil de l'union européenne, bruxelles, 15 juillet 2009.

- عقدت يوروجست اجتماعًا استراتيجيًا حول "ظاهرة الفرد المنفرد المتورط في الإرهاب" ("الذئب المنفرد") و"الشبكات الاجتماعية في سياق الإرهاب"، حضره المسؤولون والسلطات القضائية من 24 عضوًا.⁽¹⁾

- إنشاء فريق يوروجست للجرائم المالية والاقتصادية (FECT) والذي يعتبر "مصدر للخبرة في مجال الجرائم الإلكترونية ويدعم التطورات التي تؤدي إلى استنتاجات المجلس الأوروبي بشأن خطة عمل لتنفيذ استراتيجية منسقة لمكافحة الجريمة الإلكترونية، هذا الفريق هو المسؤول عن تخصيص موارد وخبرات اليوروجيست فيما يتعلق بمشاركتها في المركز الأوروبي للجرائم الإلكترونية"⁽²⁾.

- "في عام 2014 نسق اليوروجيست عمليتين رئيسيتين تتضمن الجرائم الإلكترونية، ففي مايو تم استهداف منشئو برامج BlackShades الضارة وبائعوها ومستخدموها من قبل السلطات القضائية وسلطات إنفاذ القانون في 16 دولة، أما في شهر نوفمبر، تم إغلاق أسواق الشبكة المظلمة المستضافة على شبكة Tor، بما في ذلك Silk Road 2.0 و Hydra و Cannabis Road.⁽³⁾

- "قامت منظمة اليوروجيست عقب نجاح الاجتماعات السابقة حول الجرائم الإلكترونية باستضافة اجتماع خصص من أجل إنشاء شبكة قضائية لمكافحة الجرائم الإلكترونية بدعم من يوروجست، حضر الاجتماع جملة من خبراء في مجال الجرائم الإلكترونية من 28 دولة عضو في الاتحاد الأوروبي، وكذلك من النرويج وسويسرا والولايات المتحدة الأمريكية والمركز الأوروبي للجرائم الإلكترونية ومجلس أوروبا، واتفق المشاركون على ضرورة إنشاء شبكة قضائية للجرائم الإلكترونية بدعم من اليوروجست، كما ناقشوا عملية المساعدة القانونية المتبادلة بين الولايات المتحدة والدول الأعضاء في الاتحاد الأوروبي، وتم تعريفهم بالمشاريع التي بدأها ودعمها مجلس أوروبا فيما يتعلق بالجرائم الإلكترونية، بالإضافة إلى ذلك، قدم ممثلو وزارة الأمن والعدل في هولندا لمحة عامة عن أولويات رئاستهم القادمة للاتحاد الأوروبي والتي تشمل مكافحة الجرائم الإلكترونية"⁽⁴⁾.

⁽¹⁾ UROJUST, Cybercrime, Op.cit. P.06

⁽²⁾ Ibid. P.07.

⁽³⁾ Cyber security in the spotlight, Official Website of Eurojust, 04/17/2015, Been watched on 05/09/2020 At 15:21H, in: http://www.eurojust.europa.eu/press/News/News/Pages/2015/2015-04-16_Cyber-security-in-the-spotlight.aspx

⁽⁴⁾ Eurojust Meeting on Cybercrime-Towards a Judicial Cybercrime Network, Official Website of Eurojust, 11/26/2015, Been watched on 05/09/2020 At 15:23H, in: http://www.eurojust.europa.eu/press/News/News/Pages/2015/2015-11-26_Eurojust-Meeting-on-Cybercrime-Towards-a-Judicial-Cybercrime-Network.aspx

2- الاتحاد الإفريقي:

أنشأ الاتحاد الإفريقي "أفريبول" كآلية للتعاون الشرطي وبوادرها تعود لعام 2013 في إطار المؤتمر الإقليمي الإفريقي الثاني والعشرون المنعقد بالجزائر في الفترة ما بين 10 إلى 12 سبتمبر 2013 حيث شارك فيها كل قادة أجهزة الشرطة الأفارقة، ثم إنه في المؤتمر الإفريقي للمدراء والمفتشين العاملين للشرطة حول الأفريبول الذي دعت إليه الجزائر تم تبني إعلان الجزائر في خلق وتكوين الاتحاد الإفريقي للتعاون الشرطي، والذي تم اعتماده نهائيا في الدورة العادية الخامسة والعشرين للمجلس التنفيذي للاتحاد الإفريقي في الفترة الممتدة من 20 إلى 24 يونيو 2014 بغينيا الاستوائية⁽¹⁾.

وبالنظر إلى ديباجة النظام الأساسي لهذه الآلية تتبين لنا الأهداف التي من أجلها تم إنشائها، فالدول الإفريقية قد تحسست قلقا من تعاظم الظاهرة الإجرامية في الكثير من الدول الإفريقية، بما في ذلك الإرهاب الدولي والتطرف، والجرائم السيبرانية وما إلى ذلك من صور الإجرام المنظم والعابر للحدود الوطنية⁽²⁾.

وعبر عن ذلك في الديباجة بـ(وإذا نشعر بالقلق إزاء تنامي حجم الجريمة في العديد من الأقاليم الفرعية في أفريقيا، خاصة تلك المتعلقة بتكنولوجيا المعلومات والاتصالات والتحويلات غير المشروعة لرؤوس الأموال والإتجار غير المشروع بالموارد الطبيعية وممارسات التعريب؛) فالدول شعرت أن هناك ضرورة تحتم عليها العمل على ترسيخ ودعم التنسيق في المجال الشرطي الإفريقي من خلال تقييم هذه التهديدات المحدقة وتحليل كل ما يرد من معلومات استخباراتية جنائية، والعمل على وضع خطط إجرائية وتنفيذها، وتبادل المعلومات، والتصدي بشكل فعال للجريمة على النطاق الإفريقي، والذي يتطلب تنسيق وانسجام في الطرق والنهج الشرطية وتبادل أحسن الممارسات، كما يجب أن تتسع آفاقها لتشمل التدريب والوقاية وآليات التحري وإجراء التحقيقات والقيام بالخبرات، ومساندة ودعم الكفاءات الشرطية الإفريقية⁽³⁾.

(1) خديجة خالدي، آلية الاتحاد الإفريقي للتعاون الشرطي - أفريبول -، مجلة العلوم الاجتماعية والإنسانية، المجلد 11، العدد 01، جامعة العربي التنيسي، تبسة، الجزائر، جوان 2018، ص ص: 65-79.

<https://www.asjp.cerist.dz/en/article/59399>

(2) أمين ودرار، الشرطة الجنائية الإفريقية "الأفريبول"، حوليات جامعة الجزائر 1، المجلد 34، العدد 01، جامعة بن يوسف بن خدة، الجزائر، مارس 2020، ص ص: 135-149: <https://www.asjp.cerist.dz/en/article/114177>

(3) ديباجة النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول"، اعتمدته الدورة العادية الثامنة والعشرون للمؤتمر المنعقد بأديس أبابا، إثيوبيا، بتاريخ 30 يناير 2017.

الفرع الثاني: المساعدة الإجرائية:

تساهم المساعدة الإجرائية بين الدول بشكل كبير في مكافحة جريمة الإرهاب الإلكتروني، فقيام دولة من الدول بتفويض دولة أخرى وإبانتها للقيام بالإجراءات القضائية اللازمة التي لا يمكنها لاعتبارات قانونية وسياسية القيام بها، فتقرير الإنابة القضائية في الجرائم السيبرانية لا سيما الإرهاب الإلكتروني من شأنه أن يحد من ظاهرة الإفلات من العقاب (أولاً)، كما يمكن أيضاً للمساعدة القضائية أن تمتد إلى تنفيذ الأحكام الجنائية الأجنبية التي تتناول أحكاماً متعلقة بالإرهاب السيبراني أمام الولاية القضائية الوطنية (ثانياً).

أولاً: الإنابة القضائية:

1- تعريف الإنابة القضائية:

تقضي القاعدة العامة أن السلطة القضائية التي عقد لها الاختصاص بالنظر في الدعوى المطروحة أمامها هي التي تقوم دون غيرها بدراستها ومتابعة التحقيقات فيها، غير أن لهذه القاعدة العامة استثناء تقتضيه العوائق التي تواجه الدعوى كغياب المتهم أو الشاهد أو محل المعاينة عن دائرة الاختصاص الوطني للجهة القضائية الفاحصة خاصة في المواد الجنائية خاصة مع بروز ظاهرة الجريمة المنظمة والعابرة للحدود الوطنية⁽¹⁾، ولذلك تقوم الجهات القضائية الوطنية المعقود لها الاختصاص بإنابة جهة قضائية أجنبية للقيام بمتابعة هذه الإجراءات نيابة عنها، وهذا ما يعرف في القانون بالإنابة القضائية.

تعرف الإنابة القضائية بأنها: (طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم بها الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة، ويتعذر عليها القيام به بنفسها)، فمحل الإنابة القضائية إذاً، يحمل بين طياته طلباً موجهاً من أجل القيام بإجراء من الإجراءات القضائية في المواد الجنائية الذي تقدمه دولة طالبة في سلوك أو فعل من الأفعال المجرمة في القوانين الجنائية للدولة الطالبة، والذي أتاها فرد من أفراد رعايا الدولة المطلوبة أو مقيم داخل حدودها الإقليمية بصفة مؤقتة⁽²⁾.

(1) نبيل بن عودة وعائشة بن قارة مصطفى، التعاون القضائي بين الدول ودوره في مكافحة الجرائم المتعلقة بالتميز وخطاب الكراهية في التشريع الجزائري، مجلة الفكر للدراسات القانونية والسياسية، المجلد 03، العدد 02، جامعة خميس مليانة، جوان 2020 ص ص: 367-357.

<https://www.asjp.cerist.dz/en/article/122622>

(2) هشام بشير وإبراهيم عبد ربه إبراهيم، غسل الأموال بين النظرية والتطبيق، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص 100.

وأما عن الموضوع الذي تحمله الإنابة القضائية في المواد الجنائية فهو غير ثابت، إذ يتنوع بتنوع الأهداف أو الأغراض التي تروم الدولة الطالبة اقتناؤها من أجل متابعة سير التحقيق في دعوى جنائية والوصول إلى إصدار حكم فيها، فالإنابة القضائية يمكن أن يكون موضوعها هو أخذ شهادة الشهود، استلام تقارير الخبرة ومناقشتها، القيام بإجراء معاينات، وما إلى ذلك من الإجراءات الأخرى⁽¹⁾.

تعد الإنابة القضائية آلية من آليات المساعدة القضائية. غير أنها تعتبر إجراء مرهق للتعامل به، كما أن الاستجابة له يأخذ وقتاً طويلاً، فهو إجراء إذا ما قورن بسرعة تنفيذ الجرائم الإلكترونية وسرعة تقلب الأدلة الرقمية عد إجراءً بطيئاً ومحدوداً، وتظهر محدوديته من خلال خضوعها لوجود اتفاقات بين الدول، سواء أكانت ثنائية أو متعددة، وفي غيابها لا يكون مقدم الطلب متأكداً من الاستجابة للطلب، كما أن طلب الإنابة خاضع لتقدير السلطة المختصة في الدولة المطلوب منها، كما تقابل الإنابة القضائية صعوبات منها أنها تكون خاضعة للقواعد الإجرائية للدولة المطلوب منها، كما يمكن للاتفاقيات أن تقدم على سبيل الحصر موضوع الإنابة، وقد تخضع إجراءات أخرى لشروط خاصة⁽²⁾؛

ومن بين المعاهدات التي نصت صراحة على خضوع الإنابة القضائية للإجراءات الداخلية للدولة المطلوب منها نجد معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي، والتي تنص في مادتها 11 التي تنص على أنه: (ينفذ طلب الإنابة وفقاً لأحكام القانون الداخلي للدولة المطلوب منها التنفيذ وعلى وجه السرعة...)، كما أن هذه الاتفاقية أجازت للدول الأطراف رفض طلب تنفيذ الإنابة القضائية في حالتين نصت عليهما المادة 10 وهي: (1- إذا كانت الجريمة موضوع الطلب محل اتهام أو تحقيق أو محاكمة لدى الدولة المطلوب منها تنفيذ الإنابة. 2- إذا كان تنفيذ الطلب من شأنه المساس بسيادة أو أمن الدولة المكلفة بتنفيذه أو بالنظام العام فيها)⁽³⁾.

(1) نعيمة بن يحيى، الإنابة القضائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم، مجلة الدراسات الحقوقية، المجلد 04، العدد 01، جامعة طاهر مولاي، سعيدة، جوان 2017، ص ص: 10-32: <https://www.asjp.cerist.dz/en/article/28113>

(2) Sophie JOISSAINS et Jacques BIG, RAPPORT D'INFORMATION FAIT au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale et de la commission des affaires européennes sur la lutte contre la cybercriminalité, Enregistré à la Présidence du Sénat le 9 juillet 2020, N° 613, PP. 49-50: <http://www.senat.fr/rap/r19-613/r19-6131.pdf>

(3) المادة 11 و 10 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي، الصادرة بتاريخ 28 جويلية 1999، ج.ر عدد 07 لدولة قطر، 27 جويلية 2006.

تقوم الإنابة القضائية في المواد الجنائية على أسس قانونية مختلفة، إذ يمكن أن تتبنى وتقوم على أساس التشريع الجنائي الوطني، كما يمكن أيضا أن يبنى أساسها القانوني على الاتفاقيات التي تكون فيها الدولة طرفا فيها [سواء كطرف أصيل أو منظم]، كما يمكن أيضا أن يكون أساسها القانوني هو إعمال للقاعدة المعرفة باسم "مبدأ المعاملة بالمثل"، أو على أساس المجاملات الدولية المتبادلة بين الدول⁽¹⁾.

ومن بين الاتفاقيات التي تضمنت إجراء الإنابة القضائية نجد اتفاقية الرياض العربية للتعاون القضائي، حيث تنص المادة 14 منها على أنها: (لكل طرف متعاقد أن يطلب إلى أي طرف متعاقد آخر أن يقوم في إقليمه نيابة عنه بأي إجراء قضائي متعلق بدعوى قائمة وبصفة خاصة سماع شهادة الشهود وتلقي تقارير الخبراء ومناقشتهم، وإجراء المعاينة وطلب تحليف اليمين). ثم تلي هذه المادة مجموعة من المواد التي تنظم هذه المسألة فيما ما بين الدول الأعضاء، حيث أشارت المادة 16 إلى تحديد وطلب الإنابة القضائية وبياناته، وحددت المادة 17 حالات الرفض أو التعذر التي تحول دون تنفيذ الإنابة القضائية، فيما حددت المادة 18 آليات تنفيذ الإنابة القضائية، فيما حددت المادة 20 الأثر القانوني الناتج عن الإنابة القضائية، وبيّنت المادة 21 الأحكام المتعلقة بالرسوم والمصاريف المتعلقة بتنفيذ هذه الإنابة⁽²⁾.

كما نصت المادة 25 من اتفاقية مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب على أنه: (تتعهد الدول المتعاقدة بأن تقدم أقصى تعاون ممكن في تنفيذ طلبات الإنابة القضائية المتعلقة بدعوى جنائية ناشئة عن جريمة إرهابية، وذلك وفقا لاتفاقية تنفيذ الأحكام والإنابات والإعلانات القضائية بدول مجلس التعاون لدول الخليج العربية)⁽³⁾.

و قد نصت المادة 13 من اتفاقية المذكورة في النص السالف والتي هي اتفاقية تنفيذ الأحكام والإنابات والإعلانات القضائية بدول مجلس التعاون لدول الخليج العربية على أنه: (لكل دولة عضو أن تطلب من أي من الدول الأعضاء، أن تقوم في إقليمها، نيابة عنها، بأي إجراء قضائي متعلق بدعوى قائمة؛ وبصفة خاصة سماع شهادة الشهود، وتلقي تقارير الخبراء

(1) نبيل بن عودة وعائشة بن قارة مصطفى، المرجع السابق.

(2) اتفاقية الرياض العربية للتعاون القضائي، وقعت في الرياض بتاريخ 06 أبريل 1983، ودخلت حيز التنفيذ بداية من 30 أكتوبر 1985.

(3) المادة 25 من اتفاقية مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب، الصادرة بتاريخ 04 ماي 2004، ج.ر. عدد 07 لدولة قطر، 24 جويلية 2008.

ومناقشتهم، وإجراء المعاينة، وطلب تحليف اليمين؛ وذلك في سائر القضايا المدنية والتجارية والإدارية والجزائية، وقضايا الأحوال الشخصية.⁽¹⁾

تعد معظم الاتفاقية المبرمة والصادرة في مجال التعاون القضائي الدولي سابقة لبروز أو شيوع استخدام الفضاء السيبراني، ولما كان التصدي ومجابهة الجرائم المتعلقة بهذا الفضاء تستوجب السرعة في اتخاذ الإجراءات، فإن هناك حاجة ماسة للعمل على تعديل مضمون هذه الاتفاقيات التقليدية، إذ يعد هذا الأمر من بين أهم الضروريات خاصة أما هذه الطفرة المعاصرة في مجال تكنولوجيا المعلومات والاتصال، ولهذه الأسباب ومن أجلها تم عقد اتفاقيات محدثة والتي كان لها دور في تقصير المدة الزمنية وإيجاز الإجراءات من خلال تبني أسلوب الاتصال المباشر بين جهات التحقيق المعنية بالاتفاقية الأمريكية الكندية التي حوت صلاحية تبادل المعلومات عن طريق شفوي حال الاستعجال⁽²⁾.

كما تضمنت أيضا معاهدة بودابست وهي معاهدة ذات صبغة دولية نماذج من التعامل الإجرائي مع الجريمة السيبرانية بما يتوافق مع طبيعتها التي لا يصمد الدليل فيها وقتا طويلا، كما هو الحال في الجرائم العادية، ومن بين النصوص التي تعرضت إلى هذه الجزئية المهمة نجد المادة 3/25 والتي تنص على أنه: (يجوز لكل دولة طرف، في الظروف العاجلة، المطالبة بالمساعدة المتبادلة أو بوثائق عن طريق وسائل الاتصال العاجلة بما في ذلك الفاكس أو البريد الإلكتروني، بقدر ما توفره تلك الوسائل من مستويات ملائمة للأمن والتحقق من صحة البيانات) بما في ذلك استخدام التشفير عند الضرورة) مع التأكيد الرسمي بتطبيق تلك الوسائل عندما تطالب الدولة الطرف المطلوب منه تقديم المساعدة، وتقبل الدولة المطلوب منها المساعدة وتستجيب للطلب بأي من وسائل الاتصال العاجلة⁽³⁾.

أما الاتفاقية العربية لجرائم تقنية المعلومات فإن فيها العديد من النصوص التي تضع التزامات على عاتق الدول الأطراف بإسداء المساعدة القضائية بما في ذلك الإنابة في أقصى سرعة ممكنة، وهذا ما يمكن أن نستخلصه من نص المادة 1/43 الوارد نصها كالاتي: (تكفل كل دولة طرف، وفقا للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرع على مدار

⁽¹⁾ المادة 13 من تنفيذ الأحكام والإنابات والإعلانات القضائية بدول مجلس التعاون لدول الخليج العربية، التي صودق عليها بدول مجلس التعاون لدول الخليج العربية في دورته السادسة عشر، المنعقدة بسلطنة عمان في ديسمبر 1995، أنظر: المرسوم رقم 16 لسنة 1996 المتضمن تصديق دولة قطر على هذه الاتفاقية الصادر بتاريخ 24 أبريل 1996، ج.ر. عدد 04، المنشورة بتاريخ 20 ماي 1996.

⁽²⁾ إسراء طارق جواد كاظم الجابري، المرجع السابق، ص: 118-119.

⁽³⁾ المادة 3/25 من اتفاقية بودابست.

الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة في جريمة معينة...) كما نصت المادة 39 على أنه: (1- يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها... 3- تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضة للفقْدان أو التعديل)⁽¹⁾.

كما نصت الاتفاقية أيضا على حالة طلب المساعدة القضائية المتبادلة في حالة عدم وجود اتفاقيات دولية واجبة التطبيق، حيث نصت المادة 9/27 أ على أنه: (في الحالات الطارئة، يجوز للسلطات القضائية بالدولة الطرف مقدمة الطلب أن ترسل مباشرة الطلبات الخاصة بالمساعدة المتبادلة أو المراسلات المتعلقة بذلك إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة، وفي هذه الحالات، يتم إرسال نسخة في الوقت نفسه إلى السلطة المركزية في الدول الطرف المطلوب منها المساعدة عن طريق نظيرتها في الدولة الطرف مقدمة الطلب)⁽²⁾.

2- تنفيذ الإنابة القضائية الدولية:

أ- التنفيذ الدبلوماسي للإنابة القضائية:

يعد الطريق الدبلوماسي لتنفيذ الإنابة القضائية الجنائية هو الطريق الأصيل في ذلك، فبعد أن تقوم الجهات القضائية في الدولة المنيبة بإصدار طلب الإنابة القضائية فإنها تقوم بتوجيهه إلى وزارة الخارجية، ثم تقوم بعدها بتوجيهه إلى الجهات الدبلوماسية في إقليمها ثم تقوم بإرساله إلى وزارة الخارجية للدولة المناوبة التي ستقوم بتوجيهه إلى الجهات القضائية المعقود لها الاختصاص، ويتم إعادة إرساله بنفس الطريقة المذكورة إلى الدولة المنيبة⁽³⁾.

والظاهر أن المشرع الجزائري اعتمد هذا النهج في توجيه طلبات الإنابة القضائية في المواد الجنائية، وهذا ما صرحت به المادة 721 من قانون الإجراءات الجزائية التي تنص على أنه: (في حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الإنابات القضائية الصادرة من السلطة الأجنبية بالطريق الدبلوماسي وترسل إلى وزارة العدل بالأوضاع المنصوص عليها في

(¹) المادة 1/43 و 39/1 و 3 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقع عليها بالقاهرة بتاريخ 21 ديسمبر 2010، والداخله حيز التنفيذ بتاريخ 06 فيفري 2004.

(²) المادة 9/27 أ من اتفاقية بودابست.

(³) صالح عبد الله محمد راشد الوارد، الإنابة القضائية في قانون الإجراءات الجزائية القطري: (دراسة تحليلية مقارنة)، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة قطر، يونيو 2017، ص 60.

المادة 703 وتنفذ الإنابات القضائية إذا كان لها محل للقانون الجزائري وكل ذلك بشرط المعاملة بالمثل⁽¹⁾.

نصت أيضا المادة 13 من اتفاقية التعاون القضائية والإعانات والإنابات القضائية وتنفيذ الأحكام وتسليم المجرمين التي وقعت بينها وبين الإمارات العربية المتحدة على أنه: (ترسل طلبات الإنابة القضائية مباشرة من وزير العدل في الدولة طالبة الإنابة إلى وزير العدل في الدولة المطلوب إليها اتخاذ الإجراء القضائي)⁽²⁾.

ب- التنفيذ عبر سلطة مركزية:

يكون التنفيذ من خلال سلطة مركزية بأن تقوم كل دولة طرف في اتفاقية بتعيين سلطة مركزية تعنى بتبادل المساعدة القضائية بما في ذلك الإنابة القضائية، ومن خلالها يتم توجيه وتلقي وإعادة الطلبات بينها وبين الجهة الأجنبية المركزية التي عينتها الدولة الأخرى بدورها، وبعد تأكدها من مطابقتها للشروط المقررة قانونا يتم توجيهها إلى السلطة القضائية المختصة لتنفيذها، وهو طريق أكثر سرعة مقارنة بالطريق الدبلوماسي⁽³⁾.

ج- التنفيذ القضائي للإنابة القضائية:

يعتمد الأسلوب القضائي في توجيه طلب الإنابة القضائية على السلطات القضائية في كلا جهات الإنابة (المنبية والمنابة)، ولعل هذا الطريق في توجيه الإنابة القضائية في المواد الجنائية بين الدولتين من شأنه أن يبسط ويسرع الإجراءات في الظرف الطارئة والمستعجلة لتنفيذها، وهذا بطبيعة الحال لا يتوفر في التوجيه من خلال المنفذين السابقين، ولا سيما في جريمة الإرهاب الإلكتروني التي يجب أن تكون الإجراءات فيها متسمة بالسرعة والفورية⁽⁴⁾.

د- التنفيذ الإلكتروني للإنابة القضائية:

تعلب التقنيات الحديثة المرتبطة بالتطور العلمي والتكنولوجي بما في ذلك الآليات الإلكترونية دورا مؤثر بما توفره من سرعة وسهولة في تنفيذ وإجراء المساعدات القضائية الدولية، ومن بين ما يعكس ويجلي التوظيف الإيجابي والبناء لهذه التقنيات والآليات في إطار هذه المساعدة، تجربة

(1) المادة 721 من الأمر رقم 66-155 المؤرخ في 08 يونيو 1966 الذي يتضمن قانون الإجراءات الجزائية، المعدل والمتمم.

(2) المادة 13 من المرسوم الرئاسي رقم 07-323 المؤرخ في 23 أكتوبر 2007، يتضمن التصديق على اتفاقية التعاون القضائي والإعانات والإنابات القضائية وتنفيذ الأحكام وتسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ودولة الإمارات العربية المتحدة، الموقعة بالجزائر بتاريخ 12 أكتوبر 1983، ج.ر. عدد 67، 24 أكتوبر 2007.

(3) صالح عبد الله محمد راشد الوارد، السابق، ص 62.

(4) المرجع نفسه، ص 65.

التنفيذ الإلكتروني للإنابة القضائية⁽¹⁾، وهذا الأسلوب في التنفيذ قد صرحت به اتفاقية بودابست دون أن تحصره في الإنابة، وهذا من خلال نص المادة 3/25 المذكور آنفاً.

3- آثار تنفيذ الإنابة القضائية:

أ- الالتزامات الناشئة على الدولة المطلوب منها [المنابة]:

تقع على الدولة المنابة مجموعة من الالتزامات ومن بين أبرزها عند انتهاء تنفيذ الإنابة إرسال جميع ما تم جمعه وكل النتائج والمحجوزات المرتبطة بموضوع الإنابة إلى الدولة المنبئة، التي يمكن أن تسترجعها بعدة مدة من الزمن، أما في حالة ما إذا كان موضوع الإنابة يتضمن نقل إجراءات المحاكمة، فيجب حينها تقرير العقوبة بما لا يكون أشد من العقوبة التي قررها القانون الجنائي في الدولة المنبئة، ويقع على الدولة المنابة أيضاً عدم الخروج عن إطار موضوع الإنابة فلا يجوز لها القيام بأي إجراء لم تطلبه الدولة المنبئة، كما يتعين عليها أيضاً كتم سرية الطلب ومضمونه وما ألحق به من مستندات داعمة⁽²⁾.

ب- الالتزامات الواقعة على عاتق الدولة الطالبة [المنبئة]:

تقع على الدولة المنبئة أيضاً بعد انقضاء تنفيذ الإنابة وتسليم كل ما تم الحصول عليه من معلومات ومخرجات مجموعة من الالتزامات، إذ يتعين عليها أن تعمل على المحافظة على ما تضمنته عملية التنفيذ من أسرار، بما في ذلك المعلومات والنتائج والأدلة المتحصل عليها في الدولة المنابة إلا بناء على موافقتها⁽³⁾.

ختاماً، يمكن القول أن الإنابة القضائية في الجرائم الإلكترونية عموماً، والإرهاب الإلكتروني منه خصوصاً، يعد وفق التشريعات المعمول بها حتى الآن إجراءً معيماً، فهو يتضمن العديد من العيوب والثغرات، ولا يتناسب مع حجم السرعة التي ترتكب بها هذه الصور من الجرائم ولا مع السرعة التي يتلاشي فيها الدليل الإلكتروني.

فعلى الرغم من أن الاتفاقيات والمعاهدات المتعلقة بالجرائم الإلكترونية وأمن المعلومات قد تضمنت نصوصاً تفيد رعايتها لخصائص الإجرام السيبراني، إلا أنها غير كافية من جهة،

⁽¹⁾ زينة حازم خلف الجبوري، طرق تنفيذ الإنابة القضائية الدولية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 06، العدد 22، الجزء الأول، كلية الحقوق، جامعة كركوك، العراق، 2017، ص ص: 36-93: <https://iasj.net/iasj/article/130724>

⁽²⁾ مروان العشاب، الإنابة القضائية كأحد تجليات التعاون القضائي الدولي، مجلة مغرب القانون، 15 ديسمبر 2015، تم الاطلاع عليه بتاريخ 03 سبتمبر 2020، على الساعة 12:31 سا، مختصر الرابط: <https://n9.cl/9hf2>

⁽³⁾ المرجع نفسه.

وتصادفها العديد من العقبات والعراقيل من جهة ثانية، ولا سيما حين تنفيذها وفق الطريق القضائي أو الدبلوماسي الذي لا يمكن بحال أن يكون طريقا مناسباً لتحقيق التعاون القضائي الدولي، والأكثر خطورة من ذلك كله، هو عدم وجود منظور دولي موحد إزاء ظاهرة الإرهاب الإلكتروني، وهذا يعد من أكبر العوائق التي تصادف الإنابة القضائية والتعاون القضائي بشكل عام.

وتبرز إشكالية أخرى أيضا في آثار تنفيذ الإنابة القضائية، وهي تلك المتعلقة بالتزام الدولة المثابة بإرسال المحجوزات وكافة العناصر التي تم جمعها حال التحقيق، ذلك أن بعض العناصر المتعلقة بتكنولوجيا المعلومات سواء في طبقتها المادية أو المنطقية تشكل نقطة حساسة لا يمكن أن تخاطر بها الدولة، وإرسال البرامج التي تمت بها الهجمة الإرهابية سواء أكانت برامج اختراق أو تجسس هو منح لسلح فتاك لدولة أخرى يمكن أن توظفها هذه الأخيرة في تنفيذ أشكال الهجمات عليها لاحقا، خاصة إذا كان بين الدولتين صراع على القوة السيبرانية، فليس من المعقول مثلا أن ترسل الصين مضبوطات من برامج اختراق وتجسس للولايات المتحدة الأمريكية على خلفية هجمة إرهابية وهي تعلم أن هذا السلاح سيكون في يد أكبر منافس لها.

ثانيا: تنفيذ الأحكام الأجنبية:

يفضي التطبيق المطلق لمبدأ إقليمية القانون الجنائي بشكل حتمي إلى أحكام جنائية نافذة وفق مبدأ إقليمي، لذلك، لا يطبق القضاة الجنائيون إلا قوانين بلادهم، والأحكام الجنائية الأجنبية الصادرة عن الأجهزة القضائية في بلدان معينة معترف بها فقط في الولايات القضائية الإقليمية الخاصة بها، فهي أحكام غير حائزة للحجية في الأمور المقضي بها، ولذلك لا يحق تنفيذها في أراضي دولة أجنبية، لكن أمام هذا الشيع في مظاهر وصور الجريمة التي تتخطى الحدود الإقليمية للدولة وعظم ما ينتج عنها من عظيم الخطر، فإن الضرورة حينها تدعو إلى الاعتراف بحجية الحكم الجنائي الأجنبي الذي قضي به في محاكم دولة أجنبية، ومع هذا، وعلى ما لتنفيذ الأحكام الجنائية الأجنبية من فائدة عميمة في التصدي لظواهر الإجرام بما فيها الإجرام المنظم، إلا أن الحكم الأجنبي لن يعادل الحكم الصادر عن الجهات القضائية الوطنية، فلا يقتضي أن يعامل معاملتها، بل يجب أن يكون تنفيذه مشروطا، كما يجب إبراز الحالات التي لا يجوز فيها تنفيذه⁽¹⁾.

(1) عمر زغودي، الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، المركز الجامعي لأفلو، الجزائر، ماي 2020، ص ص: 101-118: <https://www.asjp.cerist.dz/en/article/114319>

تظهر مكانة ووزن الاعتراف بتنفيذ الأحكام الجنائية الأجنبية فيما يتحقق في إثرها من مقتضيات الردع العام، التي لا تتال إلا من خلال التوقيع الفعلي للعقوبة المقضي بها، كما أن هذا الاعتراف من شأنه أيضا أن يكون دافعا في إيجاد أرضية لتتلاقى التشريعات الجنائية الوطنية بعضها ببعض، خاصة فيما يتعلق بالأفعال والنشاطات التي يتم تجريمها باعتبارها أعمالا إرهابية، والعقوبات المقررة على المتورطين فيها، إذ أن وحدة التفسير بين الجهات القضائية على الصعيدين الوطني والدولي من شأنه أن يدفع بسير قابلة التعاون الدولي في المواد الجنائية على الأحسن، كما أن هذا الاعتراف بالأحكام الجنائية الأجنبية يمكن أن تعد من بين السبل التي تحول دون الوقوع في الجريمة، والفرار من التبعات الجنائية المترتبة عن ارتكاب الجريمة أو الحكم عليه فيها⁽¹⁾.

وبعد هذا الاعتراف أيضا صورة متجلية للتطور الحضاري للبلدان، حيث يكتسي التشريع الجنائي الوطني طابعا واسعا ليشمل العالم كله، وهذا سيفضي تبعا لتنشيط افضل للقضاء الجنائي الدولي، كما أن الاعتراف بتنفيذ الأحكام الجنائية الأجنبية يعتبر تلبية لمقتضيات العدالة، فهو يعمل على تعزيز واحدا من الأصول التي تتطلبها أسس العدالة، والذي يتمثل في الأصل الأصل الذي يقضي بعدم جواز المحاكمة على ذات الجرم مرتين، كما أن هذا الاعتراف بتنفيذ هذه الأحكام يشارك في التقريد التنفيذي للعقوبة⁽²⁾.

ومع ذلك ورغم أهمية تطبيق الأحكام الجنائية الأجنبية في التصدي لظاهرة الإرهاب الإلكتروني، إلا أن هذا الأمر ليس بهذه السهولة، نظرا للإشكاليات القانونية التي تثيرها الجرائم الإلكترونية من جانب، والصراعات الدولية على القوة السيبرانية من جهة ثانية، أما عن الإشكاليات القانونية فإن الشرعية الجنائية تشكل عائقا كبيرا في تنفيذ الأحكام الجنائية الأجنبية المتعلقة بجريمة الإرهاب الإلكتروني، ذلك أن تنفيذها يكون من خلال المحاكم الوطنية التي تراعي العديد من العناصر لتنفيذها وعلى رأسها الجانب الإجرائي، ولما كان الإرهاب الإلكتروني محل أخذ وعطاء في التشريعات الجنائية الوطنية فإن تنفيذ حكم أجنبي حيالها يعد أمرا معقدا إن لم يكن مستحيلا.

أما من ناحية الصراع على القوة السيبرانية أو ما يعرف في أوساط الأكاديميين بالسباق نحو التسلح السيبراني فإن ذلك سيكون حائلا كبيرا دون تنفيذ الأحكام الأجنبية، ذلك أن الحكم الأجنبي قد يتضمن مصادرة لعناصر الجريمة، وعناصر الجريمة قد تتضمن أسلحة برمجية فتاكة لا يمكن بحال تسليمها إلى دولة أخرى صديقة كانت أم عدوة.

(1) نسيب نجيب، المرجع السابق، ص 140.

(2) المرجع نفسه، 141.

ولذلك نرى أنه من الضروري بـمكان أن يتم بناء وتشكيل منظومة قانونية أو صرح قانوني جديد يحمل كافة الجزئيات التي أشرنا إليها، ولاسيما قضية مصادرة العائدات الإجرامية وتسليمها إلى الدولة التي صدر الحكم الجنائي عن محاكمها، هناك ضرورة ملحة تدعو أيضا إلى توحيد الجانب الموضوعي والإجرائي للدول فيما يتعلق بالإرهاب الإلكتروني خدمة لهذا الشكل من أشكال التعاون القضائي.

الفرع الثالث: المساعدة الفنية:

يتطلب العمل القضائي وجود معلومات أصيلة وموثوقة يتم على أساسها الاستدلال على الجرائم الإرهابية التي تقع على أو في الفضاء الإلكتروني، ونظرا لكون هذا الفضاء مجالا مترامي الأطراف متعدد الفواعل فإنه من الضروري بـمكان التعاون من أجل ضمان تدفق المعلومات الاستدلالية إلى أجهزة إنفاذ القانون المختصة (أولا)، كما تملي أيضا حادثة هذه الظاهرة الإرهابية والتعقيدات الفنية والتقنية التي تتسم بها وجوب التعاون في مجال تدريب أجهزة إنفاذ القانون وإعدادها (ثانيا).

أولا: تبادل المعلومات:

يكرس المجتمع الدولي للمساعدة القضائية التي يكون موضوعها تبادل المعلومات شأنًا كبيرا ومكانة مهمة وعالية ذلك لكونها آلية ووسيلة لمواجهة الجريمة بصفة عامة والجريمة المعلوماتية بشكل خاص، ذلك لكون المعلومات التي تتمتع بالصحة والموثوقية ذات دور كبير في عدم أجهزة إنفاذ القانون⁽¹⁾، وتحقيق المساعدة القضائية لقمع ظاهرة الإرهاب الإلكتروني من خلال العمل على تسليم ومنح المعلومات والبيانات والوثائق الاستدلالية التي تقوم السلطة القضائية الأجنبية بطلبها إذا ما تم مباشرة النظر في دعوة مرفوعة ضد رعية من رعاياها أو رعية لدولة أخرى⁽²⁾

تشمل عملية تبادل المعلومات عمليات كتبادل السوابق القضائية للأشخاص الذين يتم متابعتهم أمام القضاء لمثل هذه الجرائم، ولهذه الصور سريان في العديد من المعاهدات والاتفاقيات الدولية، كما هو الحال فيا تضمنته الفقرتين 6 و 7 من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية، والفقرات 3 و 4 من المادة الثامنة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة، كما نصت عليه أيضا المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة

(1) نعيم سعيداني، المرجع السابق، ص 89.

(2) إسماء طارق جواد كاظم الجابري، المرجع السابق، ص 116.

القضائية⁽¹⁾ حيث تنص على أنه: (تبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كما تتبادل المعلومات المتعلقة بالتنظيم القضائي، وتعمل على اتخاذ الإجراءات الرامية إلى التوفيق بين النصوص التشريعية والتنسيق بين الأنظمة القضائية لدى الأطراف المتعاقدة حسبما تقتضيه الظروف الخاصة بكل منها).

كما تشجع الاتفاقية أيضا في نص الفقرة الثانية من المادة 02 على (زيارة الوفود القضائية وتبادل رجال القضاء والعدل بقصد متابعة التطور التشريعي والقضائي في كل منها، وتبادل الرأي حول المشاكل التي تعترضها في هذا المجال وتشجيع أيضا تنظيم زيارات تدريبية للعاملين في كل منها) كما نصت المادة 05 من الاتفاقية على تبادل صحف الحالة الجنائية بين الدول الأعضاء

وتنص المادة 1/26 من اتفاقية بودابست على جواز لدولة طرف (في حدود قانونها الوطني ودون طلب مسبق، أن ترسل إلى طرف آخر معلومات يتم الحصول عليها في إطار التحقيقات التي تنجر في حال إذا ما ارتأت أن الإفصاح عن هذه المعلومات قد يساعد الطرف المتلقي لهذه المعلومات في الشروع أو القيام بتحقيقات أو متابعات بشأن جرائم جنائية مقررة طبقا لهذه الاتفاقية أو أن ذلك يؤدي إلى تقديم طلب تعاون مكن جانب تلك الدولة الطرف بموجب هذا الباب)

غير أن تبادل المعلومات في إطار التعاون والمساعدة القضائية في الجرائم السيبرانية تواجهه العديد من التحديات، وقد أشارت البرازيل إلى أنه في حالة وجود طرف أجنبي ضمن التحقيقات والولاية فإن ذلك يؤثر سلبا على السير الحسن للإجراءات إذ يعمل على تبطيئها في غالبية الأحيان لما في مفهوم حماية الخصوصية من تباين فيه بين الدول، وهذا الأمر يشكل حجر عثرة أمام المتطلبات الداخلية فيما يتعلق بالكشف عن البيانات، كما أشارت أيضا إلى أن البيانات نظرا لحجمها الكبير فإن الشركات لا تحتفظ بها مدة تسمح بتوظيفها⁽²⁾.

كما أفادت أستراليا في هذا السياق أيضا أن من بين التحديات التي تواجهه أجهزة إنفاذ القانون في حصولها على المعلومات أو البيانات التي تكفل المتابعة والملاحقة القضائية في هذا النوع من الجرائم تشتت البيانات وتوزعها على العديد من الخدمات ومزودي الخدمات والأماكن

(1) فيصل بدري، المرجع السابق، ص: 68-69.

(2) تقرير الأمن العام، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، المرجع السابق، ص 19.

والولايات القضائية، ويمكن لهذا الأمر أن يكون حائلاً دون تحديد نطاقها المكاني إلا وفق تعاون قضائي يشوبه التعقيد والبطيء⁽¹⁾.

ومع كل هذه التحديات التي تواجه تبادل المعلومات والبيانات الاستدلالية في إطار مكافحة الجريمة السيبرانية ولاسيما جريمة الإرهاب الإلكتروني إلا أن الاتفاقيات المتعلقة بجرائم تقنيات المعلومات أو الجرائم الإلكترونية قد وضعت حلولاً عملية لتخطيها، قد تختلف أو تتفق على مدى فعاليتها في تحقيق ذلك، وأبعاد تجسيدها على الواقع، إلا أنها تعد خطوة محدودة نحو المزيد من التعاون المستقبلي في مكافحة هذه الجرائم، ومن بين أهم من تم رصده في هذه الدراسة من نصوص قانونية تركز مبدأ التعاون والمساعدة القضائية من خلال تبادل المعلومات والبيانات مع مراعاة الطبيعة التكوينية للفضاء الإلكتروني والتركيب الإجرامي الذي تتسم به الجرائم الواقعة فيه، ومن بين أهم هذه النصوص نجد:

- المادة 1/41 من الاتفاقية العربية لجرائم تقنيات المعلومات والتي أشرنا إليها فيما سبق من دراستنا، بالإضافة أيضاً إلى نص المادة 1/32 والتي تنص على أنه: (على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم)، كما أنشأت الاتفاقية أيضاً جهازاً متخصصاً يكفل تسهيل وتيسير عملية المساعدة القضائية، خاصة فيما يتعلق بتبادل المعلومات، وهذا بناء على نص المادة 43 من الاتفاقية.

- المادة 3/25 من اتفاقية بودابست المشار إليها سابقاً والتي تضمنت بين طياتها تسهيلاً لتبادل المعلومات أو الوثائق عبر الوسائل الحديثة من فاكس وبريد إلكتروني لتوخي عسر الإجراءات ولتحقيق المرونة في المساعدات القضائية بشكل عام، كما أنشأت الاتفاقية أيضاً لذات الغرض شبكة على مدار الساعة 7 أيام في الأسبوع بموجب نص المادة 35 والتي تنص الفقرة الأولى منها على أنه: (تعين على كل دولة طرف نقطة اتصال متاحة على مدار الساعة وسبعة أيام في الأسبوع بغية ضمان توفير المساعدة الفورية لأغراض التحقيقات أو الإجراءات الخاصة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكمبيوتر أو من أجل جمع الأدلة الخاصة بجريمة جنائية في شكل إلكتروني...).

(1) تقرير الأمن العام، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، المرجع السابق، ص 10.

ثانيا: التدريب والتكوين:

يعد نظام العدالة الجنائية النطاق القانوني الذي تعمل به الدولة على صون المجتمع مما يتمخض عن الجرائم من مخاطر، وتحفظه من أضرارها ومفاسدها، ولعل القاضي الجنائي باعتباره الآلية المحورية في النظام الجنائي هو الذي يقوم بمباشرة هذه الوظيفة الحمائية بشكل علمي من خلال إنفاذ القانون وفق ما تفرضه الاعتبارات القانونية، ومن خلال توقيع العقاب والعناية بالجانب الإجرائي، فهو الذي يقوم بضمان العدالة وتحقيق الأمن والاستقرار، ولأجل ذلك فإن هناك ضرورة أو أهمية كبيرة في تدريبه وإعداده من أجل جعله أكثر مواءمة وأكثر حصيلة وكفاءة في قيامه بما أسند إليه من اختصاصات وأدوار جلية⁽¹⁾، بالإضافة أيضا إلى تدريب وتكوين وإعداد الآليات الأخرى المكونة لنظام العدالة الجنائية بما في ذلك ضباط الشرطة القضائية، والمحققين والمدعين العامين.

ومع التطور التكنولوجي المعاصر فإن التدريب على إثره يكون أدعى وأكثر ضرورة، ويجب أن يكون التدريب مستجدا حديثا لا وفق الأنماط التقليدية فحسب، إذ أنه لا يغني في مجال الجريمة السيبرانية - والإرهاب الإلكتروني بشكل خاص وأساسي - مجرد اكتساب المعرفة القانونية وأسس العمل الشرطي، بل يتعين أن تكون هناك قاعدة من الخبرة الفنية المستفيضة في مجال هذا النوع من الجرائم، ولا يمكن أن تتحقق هذه الخبرة إلا من خلال تدريب متخصص يأخذ بعين الاعتبار الجوانب الشخصية من حيازته المدرب على إمكانيات ذهنية ونفسية للخضوع لمثل هذا الشكل من أشكال التدريب⁽²⁾.

ونظرا لكون الجريمة الإلكترونية عموما و- الإرهاب الإلكتروني منه خصوصا- غير قابل لتطبيق الإجراءات التقليدية المعتادة، فإنه من الضروري العمل على تدريب رجال القضاء الذين يناط بهم اختصاص الجرائم المتصلة بتقنيات المعلومات على النسق والنهج التي يتم توظيفها في ارتكاب مثل هذه الجرائم، والأساليب التي يتم الاعتماد عليها لكشفها، وتكوين الأدلة من أجل إثباتها، والطرق التي تؤهل لمعاينتها وحفظها وفحصها⁽³⁾.

(¹) أحمد السراج الأندلسي، نظام العدالة الجنائية ودور القاضي ورجل القانون في مكافحة الجريمة والوقاية منها، جامعة نايف العربية للعلوم الأمنية، الرياض، 2013، متوفر على الموقع:

<https://9anonak.blogspot.com/2016/04/Le-systeme-de-justice-penale-et-le-role-du-juge-et-d-un-homme-de-loi-dans-la-lutte-contre-la-criminalite-et-la-prevention-CDC.html>

(²) فيصل بدري، المرجع السابق، ص 84.

(³) أيسر محمد عطية، ورقة علمية بعنوان: دور الآليات الحديثة للحد من الجرائم المستحدثة: (الإرهاب الإلكتروني وطرق مواجهته)، الملتي العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية، كلية العلوم الاستراتيجية، خلال الفترة من 2-4 سبتمبر 2014، عمان، المملكة الأردنية الهاشمية، 2014، ص 23.

قطعت الدول المتقدمة شوطاً كبيراً في مجال تدريب رجال العدالة الجنائية من قضاة ومحققين⁽¹⁾، ففي إسبانيا مثلاً أسند إلى المعهد الإسباني للقضاء التابع للمجلس العام للقضاء مهمة تدريب القضاة على الجرائم المتصلة بتقنيات المعلومات والأدلة الرقمية، ويتولى مركز الدراسات القانونية التابع لوزارة العدل تقديم مثل هذا التدريب لرجال النيابة، وهذا كله بالتعاون مع شركة متخصصة في هذا المجال تدعى "سابيكس"، أما في البرتغال فالتدريب أُنشئ الخدمة يكون من اختصاص مركز الدراسات القضائية الذي ينظم قرابة 30 فعالية سنوياً⁽²⁾، أما الدول النامية فلا تزال تعاني كثيراً في هذا المجال من نقص في الكفاءة لرجال العدالة والقضاء والتقنيات⁽³⁾، لذلك فإنه من الضروري العمل على التعاون الدولي سواء بطريقة جماعية أو ثنائية لتكوين كادر هيئات إنفاذ القانون والعدالة الجنائية للتصدي لظاهر الجريمة السيبرانية على وجه عام والإرهاب السيبراني على وجه خاص.

وقد أقدمت الكثير من الدول على تقديم المساعدة اللازمة في مجال التكوين والتدريب الفني والتقني، فاستراليا مثلاً تقدم دعماً في بناء القدرات والمساعدة الفنية للدول لتتمكن هذه الأخيرة من بناء قدراتها التقنية⁽⁴⁾، كما أن للهيئة الأمم دورات تدريبية يقيمها مكتب الأمم المتحدة المعنى بالمخدرات والجريمة والشركاء الإقليميين الآخرين، بهدف تعزيز قوات الشرطة وبناء القدرات الكشف عن الجرائم الإلكترونية⁽⁵⁾، والتي أوصت لجنة منع الجريمة والعدالة الجنائية في دورتها السابعة والعشرون على ضرورة دعم جهودها من خلال (...إعداد مشروع أو برنامج تعليمي يركز على التوعية بالجريمة السيبرانية والإجراءات المناسبة للتصدي لها في أوساط السلطات القضائية، وسلطات النيابة العامة وخبراء الطب الشرعي في الدول الأعضاء...) ⁽⁶⁾، أما إقليمياً وعلى مستوى المجلس الأوروبي تم اعتماد مشاريع تهدف إلى بناء القدرات مثل برنامج العمل العالمي الممدد بشأن الجريمة السيبرانية⁽⁷⁾.

(1) الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: (توصيات سياسية)، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، المرجع السابق، ص ص: 19-20.

(2) مشروع حول الجريمة المعلوماتية وشبكة لشبونة، التدريب على الجريمة المعلوماتية للقضاة وأعضاء النيابة العامة: (المفهوم)، المديرية العامة لحقوق الإنسان والشؤون العامة، قسم مجتمع المعلومات والعمل على مكافحة الجريمة، المجلس الأوروبي، فرنسا، 08 أكتوبر 2009، ص 20.

(3) الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: (توصيات سياسية)، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، المرجع نفسه، ص ص: 19-20.

(4) تقرير الأمن العام، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، المرجع السابق، ص 12.

(5) UNODC, Rapport sur la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 27 au 29 mars 2019, P.03

(6) التوصية ألف/1/ك، لجنة منع الجريمة والعدالة الجنائية، الدورة 27، تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عقد في فيينا في الفترة من 03 إلى 05 أبريل 2018، المجلس الاقتصادي والاجتماعي 13 أبريل 2018، ص 05.

(7) المرجع نفسه، ص 10.

المطلب الثاني:

تسليم مجرمي الإرهاب الإلكتروني

أسفرت الحدود السيادية التي تفصل الدول عن بعضها البعض على صعوبات قضائية في تقديم المجرمين الهاربين من وجه العدالة أمام القضاء لمواجهتهم بما أقدموا عليه من صور الإجرام، ومعاقبتهم عليها، فتصاعدت بذلك وتيرة الإجرام، وحجب القضاء عن الوفاء بحق المجتمع في العقاب، فاستجارت الدول من أجل وضع حد لهذا المعضلة بنظام تسليم المجرمين الذي برز كآلية تحول دون تمتع المجرمين بملاذات آمنة (الفرع الأول)، وتفاديا للتصادم الذي قد يحصل بين هذا النظام وبين اعتبارات السيادة الوطنية، وتلك التي قد تقع بينه وبين متطلبات حماية حقوق الإنسان، والتناقضات التي تق تترتب عنه مع النصوص القانونية الأخرى ولاسيما تشريعات حماية اللاجئين، فإن معظم القوانين الداخلية والاتفاقيات الدولية قد أحاطت هذا النظام بجملة من الشروط التي يتعين استفاؤها (الفرع الثاني)، وبذلك ينتج أثره ويبلغ مقصده، رغم ما قد يعتبره من عقبات وتحديات (الفرع الثالث).

الفرع الأول: مفهوم تسليم المجرمين:

أظهر التعامل بنظام تسليم المجرمين توافقاً قضائياً وفقهياً على أهميته وضرورته رغم بعض الخلافات في صياغة تعريفه، إلا أن الجميع قد أجمعوا على أنه نظام فريد يتميز عن غيره من المفاهيم، ويتأسس قانوناً على مجموعة من الأسس السامية (أولاً)، إلا أن آراء الفقهاء في طبيعته وقوة إلزاميته ولاسيما في باب جرائم الإرهاب الإلكتروني لا تعد محط إجماع، فقد ذهب فيه الفقهاء مذاهباً لا تتوافق مع بعضها البعض، وهي تعكس في حقيقتها جانباً من جوانب الصعوبات التي تصادف هذا النظام (ثانياً).

أولاً: تعريف التسليم:

يعتبر تسليم المجرمين أحد أقدم أشكال التعاون بين الدول، وتعود أصوله إلى الحضارات الغابرة، كالحضارة المصرية والصينية والكلدانية والآشورية البابلية، وأقدم وثيقة سياسية، هي معاهدة السلام بين رمسيس الثاني، فرعون مصر، والملك الحثي هاتوسيلي الثالث والتي تتضمن وتحتوي على شرط تسليم المجرمين، والتي نحتت بالهيروغليفية على معبد عمون بالكرنك، وهي محفوظة على ألواح طينية في أكودرين في أرشيفات الحثيين في بوزازكي، ومع قدم هذه الممارسة إلا أن الاتفاقيات القديمة لا تشير إلى وجود جهد دولي واسع في التعاون لقمع الجرائم العادية، فذلك لم يبدأ

إلا في القرن 18 تقريبا، فقبل هذه الفترة، كان نظام التسليم يتم توظيفه في الغالب للحصول على مرتكبي الجرائم السياسية، والزنادقة، واللاجئين، والمهاجرين⁽¹⁾.

يجلي نظام تسليم المجرمين قانونا قيام (دولة ما بالتخلي عن شخص مقيم على أراضيها وتقوم بتسليمه إلى دولة أخرى لتتولى بمقتضى قوانينها محاكمته عن جريمة منسوبة إليه، أو لتنفيذ حكم صادر عليه من محاكمها) والقرار القاضي بالتسليم لا يمكن اعتباره قرار صادرا من السلطات القضائية في البلد، بل هو قرار سيادي يتخذ في غالبية الأحيان الطريق الدبلوماسي لتنفيذه بعد أن يحال إلى الجهات القضائية المختصة للنظر والفصل في مدى صحة طلب موضوع التسليم⁽²⁾، كما يمكن تعريفه أيضا بأنه: (نظام في العلاقات الدولية من مقتضاه أن تتخلى الدولة عن شخص موجود على إقليمها ولا يحمل جنسيتها لدولة أخرى بناء على طلبها لتتولى محاكمته عن جريمة منسوب إليه ارتكباها لتنفيذ فيه حكما صادرا من محاكمها وذلك باعتبار أن هذه الدولة الأخيرة هي صاحبة الاختصاص الطبيعي أو الأفضل في تلك المحاكمة أو ذلك التنفيذ)⁽³⁾.

وأمام إجماع غالبية الجهات القضائية على تقديم تعريف لمسألة تسليم المجرمين، قامت بعض الجهات القضائية الأخرى بالتصدي له بالتعريف، ومن بين تلك الجهات التي تطرقت إلى تعريفه نجد المحكمة الأمريكية العليا التي عرفت به بأنه (إجراء بمقتضاه تسلم الدولة متهم أو محكوم عليه لدولة أخرى لجريمة ارتكبت خارج نطاق حدودها الإقليمية أو داخل الولاية القضائية لدولة أخرى حيث يكون لها الاختصاص لمحاكمته أو معاقبته)، وقامت المحكمة العليا الإنجليزية هي الأخرى بتقديم تعريف له حين قضت بأنه: (إجراء قانوني شكلي يدعم حق الدولة الطالبة للتسليم في الملاحقة القضائية للمطالبة باستعادة أحد الأشخاص محل الملاحقة والمتواجد على إقليم الدولة المطلوب منها التسليم لمحاكمته عن اتهامات جنائية تم ارتكابها في الدولة الطالبة للتسليم أو لهروبه من الحبس القانوني المحكوم به عليه في الدولة الطالبة للتسليم)⁽⁴⁾.

(1) Robert Louis PARRILLO, *Extradition: A Test of International Cooperation in the Enforcement of Domestic Criminal Law*, A Dissertation submitted to the Department of Political Science in partial fulfillment of the requirements for the degree of Doctor of Philosophy, COLLEGE OF SOCIAL SCIENCES, FLORIDA STATE UNIVERSITY, 2009, P.08.

(2) وسيم حسام الدين الأحمد، مكافحة الجريمة المنظمة عبر الوطنية في ضوء أحكام الشريعة الإسلامية والأنظمة السعودية، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2016، ص 133.

(3) أردلان نور الدين محمود، المسؤولية الجزائية لرئيس الدولة في التشريعات الداخلية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2014، ص 167.

(4) آلاء محمد صاحب وتبارك ناصر عزوز الزاملي، ماهية التجريم المزدوج في نظام تسليم المجرمين: (دراسة مقارنة)، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 01، العدد 1/44، كلية الحقوق، جامعة الكوفة، العراق، ص ص: 347-376 <https://www.iasj.net/iasj/article/180425>

يختلف التسليم عن عدة مفاهيم أخرى مشابهة له، فالتسليم يختلف في مفهومه عن الطرد الذين يتعلق في غالبية الأحيان بالجانب الإداري الداخلي للدولة الطاردة، وعملية الطرد تكون بأمر فرد معين بأن يغادر حدود الإقليم الذي يقيم فيه دون ترخيص، ويختلف التسليم أيضا عن الإعادة إلى البلد الأصلي حيث تقوم بتأمين عودة فرد من الأفراد إلى بلده الأصلي أو إلى أي بلد آخر انطلق منه، ويكون ذلك في نطاق غير جنائي، كما يختلف أيضا عن النقل الذي تمخض عن النظام الأساسي للمحكمة الدولية التي أنيط بها اختصاص محكمة من تفترض مسؤوليته في ارتكاب انتهاكات جسيمة للقانون الدولي الإنساني ارتكبت في إقليم يوغوسلافيا⁽¹⁾، وتسمى الإجراءات الصادرة بحقهم بأوامر النقل⁽²⁾، كالنقل الذي قامت به حكومة صربيا والجبل الأسود لعدة متهمين من بينهم "فيزيلين سليفانكانين" الذي يعد آخر ما يطلق عليه اسم "ثلاثي فوكوفار" في تهمة ارتكاب الأحداث الواقعة في فوكا بالبوسنة والهرسك⁽³⁾، كما يختلف التسليم أيضا عن ذلك التسليم الذي تم تطويره في الاتحاد الأوروبي بناء على مذكرة توقيف أوروبية والتي ترمي إلى إلغاء إجراءات التسليم الرسمية عبر اعتماد مبدأ الاعتراف المتبادل بالقرارات الجنائية⁽⁴⁾.

يتميز نظام تسليم المجرمين تسليم المجرمين بجملة من الخصائص والمميزات، فهو نظام مؤسسي دولي يتخذ فيما بين الدول، وبين دولة وجهة قضائية دولية، هو يندرج ضمن دائرة القانون الدولي العام، كما أنه نظام ذو صبغة إجرائية وتعاونية، فهو يحمل خاصية إجرائية أيا كانت الجهة التي اتخذته، وذو خاصية تعاونية من وجه نظر الفقه الدولي كون التسليم آلية لمد يد العون للدول من أجل إنفاذ قوانينها الداخلية، ويحمل التسليم بجانب الخاصيتين السابقتين طابعه القمعي والردعي، حيث أنه كلما كان التسليم واجبا كلما كان ذلك مانعا من الإفلات من العقاب أكثر، فالتسليم يشكل آلية ردعية وأسولب من أساليب قمع الجريمة، وفي الأخير، يمكن أيضا أن نقول

(1) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب، الأمم المتحدة، نيويورك، 2009، ص 202.

(2) القاموس العملي للقانون الإنساني، المحكمة الجنائية الدولية ليوغوسلافيا السابقة والمحكمة الجنائية الدولية لرواندا، موقع أطباء بلا حدود، (د.ت.ن)، تم الاطلاع عليه بتاريخ 25 سبتمبر 2020، على الساعة 01:30 مساء، في الموقع:

<https://ar.guide-humanitarian-law.org/content/article/5/lmhkm-ljnyy-lwly-lywgslyfy-lsbq-wlmhkm-ljnyy-lwly-lrwnd/>

(3) محضر مجلس الأمن، الجلسة 4838 المنعقدة بتاريخ 09 أكتوبر 2003، والتي تضمن جدول أعمالها: المحكمة الدولية لمحكمة الأشخاص المسؤولين عن الانتهاكات الجسيمة للقانون الدولي التي ارتكبت في أقاليم يوغوسلافيا السابقة منذ عام 1991، المحكمة الجنائية الدولية لمحكمة الأشخاص المسؤولين عن أعمال الإبادة الجماعية وغير ذلك من الانتهاكات الجسيمة للقانون الدولي الإنساني المرتكبة في إقليم رواندا والمواكطين الروانديين المسؤولين عن أعمال الإبادة الجماعية وغيرها من الانتهاكات المماثلة المرتكبة في أراضي الدول المجاورة بين 1 يناير و 31 ديسمبر 1994، (نسخة مؤقتة)، ص 37.

(4) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب، المرجع نفسه، ص 202.

بأن التسليم يتميز بكونه عقدا ثنائيا بين السلطات العليا المختصة بين دولتين، ويرتب أثرها بالنسبة لهما حتى وإن كان محل العقد شخصا طبيعيا، فهو بذلك مختلف عن سائر العقود المعروفة⁽¹⁾.

يهدف نظام تسليم المجرمين للحيلولة دون إفلات الجناة من العدالة في حالة ما إذا قاموا بالهروب واللجوء إلى دولة من الدول غير تلك التي قام بها بارتكاب جريمته فيها، وبالتالي ليس من الممكن محاكمته أمام جهاتها القضائية، فكثيرا ما يفر الجناة من الدولة التي ارتكبوا فيها جرما إلى دولة أخرى فرارا من العقاب، وتظهر أيضا أهمية تسليم المجرمين في كونه يخلي بين الجاني وبين قاضيه الطبيعي الذي تم ارتكاب الجريمة في إقليم بلاده، ذلك لكون هذا القاضي أكثر قدرة على أن يفصل في موضوع الجريمة بناءً على القانون الوطني التي ارتكبت فيها الجريمة، أين تكون الأدلة متاحة ومن اليسير جمعها⁽²⁾.

تؤسس الدولة قيامها بتنفيذ تسليم المجرمين على ما تحتويه اتفاقياتها مع الدول الأخرى بشكل جماعي أو ثنائي من نصوص تقرر التسليم، ويمكن أيضا أن تؤسسه على مبدأ المعاملة بالمثل والذي مفاده أن تقبل الدولة تسليم المجرمين إذا ما تعهدت الدولة طالبة التسليم بقبول طلبات التسليم التي تأتيها من هذه الدولة⁽³⁾، ومع هذا لم يرد إجماع بين الدول في شأن الأخذ بقاعدة تسليم المجرمين، حيث نجد أن الدول الأوروبية وبعض الدول الأخرى تسمح بالتسليم المجرمين بناءً على المعاملة بالمثل، وذلك لأن شرط المعاملة بالمثل هو من القضايا السياسية التي يخضع لتقدير الحكومة لا لمقتضيات العدالة، وقد أقر جانب من الفقه إلى اعتبار المعاملة بالمثل كقاعدة موجهة ومرشدة لمعاهدات تسليم المجرمين⁽⁴⁾.

ومن بين كل أصناف المعاهدات والاتفاقيات تعد الثنائية منها الشكل الأكثر انتشارا لتسليم المجرمين لما في ذلك من مصالح موحدة بينها في التصدي لأشكال الجريمة، بالإضافة أيضا إلى ما يكتنف هذا النوع من الاتفاقيات من يسر وبساطة في التفاوض مقارنة بتلك التي تتعدد فيها الأطراف التي قد تجردها من الفاعلية حال تحفظها على بعض ما يرد فيها من بنود محتجة في ذلك بتصادمه وعدم مطابقته لما هو متعارف لديها على المستويات المختلفة التي يمثل المجال القضائي أحد منها، والجدير بالذكر أيضا أن مثل هذه المعاهدات ليست على نمط واحد في

(1) فافة لحمر، إجراءات تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية، مذكرة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة وهران، الجزائر، السنة الجامعية 2013-2014، ص ص: 10-12

(2) أردلان نور الدين محمود، المرجع السابق، ص 168.

(3) وسيم حسام الدين الأحمد، المرجع السابق، ص 134.

(4) أردلان نور الدين محمود، المرجع نفسه، ص ص: 168-169.

مضمونها، فمنها من تتناول بشكل حصري نظام تسليم المجرمين ومنها ما يكون عاما يتناول كل مواضيع وزوايا التعاون القضائي التي يكون التسليم جزء منها⁽¹⁾.

وتعد الجزائر من مصاف الدول التي بادرت بإبرام العديد من الاتفاقيات التي تعنى بتنظيم تسليم المجرمين، والظاهر مما وقع بين أيدينا من هذه الاتفاقيات أن الجزائر مع نظرائها قد اعتمدت نظام التخصيص، حيث قامت بتخصيص موضوع التسليم باتفاقيات منفردة كما هو الحال مثلا باتفاقية تسليم المجرمين بينها وبين مملكة إسبانيا التي تم توقيعها بالجزائر بتاريخ 12 ديسمبر 2006⁽²⁾، وتلك المعاهدة التي أبرمتها مع حكومة جمهورية نيجيريا الاتحادية، الموقع عليها بالجزائر في 12 مارس 2003⁽³⁾، كما اعتمدت أيضا أسلوب التضمن، حيث يكون موضوع التسليم جزء من معاهدة أو اتفاقية متعلقة بالتعاون القضائي، كما هو الحال باتفاقيتها الموقعة سنة 1970 في بروكسل مع المملكة البلجيكية المتعلقة بتسليم المجرمين والتعاون القضائي في المواد الجنائية⁽⁴⁾، واتفاقيتها سنة 1984 مع المجر والمتعلقة بالتعاون القضائي والعدلي في المواد المدنية والتجارية والعائلية والجزائية، حيث تناولت موضوع التسليم في المواد من 40 إلى 55 منها⁽⁵⁾.

أما على المستويين الدولي والإقليمي فهناك العديد من الاتفاقيات والمعاهدات المبرمة والتي تتناول تنظيم مسألة تسليم المجرمين، ولاسيما في موضوع الإجرام السيبراني، كما هو الحال في اتفاقية بودابست التي تعرضت لهذه المسألة من خلال نص المادة 24 منها، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تناولت مسألة التسليم من خلال نص المادة 31 منها.

ثانيا: آراء الفقهاء في مسألة تسليم المجرمين:

أ- مبدأ التسليم بين القبول والرفض:

انقسم الفقهاء في مسألة جواز التسليم إلى فريق يرفض هذا المبدأ ويؤكد أن أنصار هذا الاتجاه أن التسليم يشكل مظهرا من مظاهر التنازل عن السيادة الوطنية، وأن مقتضيات العدالة

(1) محمد عبيد، المصادر القانونية لنظم تسليم المجرمين، المعهد المصري للدراسات، 11 مارس 2019، تم الاطلاع عليه بتاريخ 12 سبتمبر 2020 على الساعة 00:09، مختصر الرابط: <https://n9.cl/0pgd>

(2) المرسوم الرئاسي رقم 08-85 المؤرخ في 09 مارس 2008، يتضمن التصديق على اتفاقية تسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا، الموقعة بالجزائر في 12 ديسمبر 2006، ج.ر عدد 14، لسنة 2008.

(3) المرسوم الرئاسي رقم 05-193 المؤرخ في 28 مايو 2005، يتضمن التصديق على المعاهدة المتعلقة بتسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية وحكومة جمهورية نيجيريا الاتحادية، الموقعة بالجزائر في 12 مارس 2003، ج.ر عدد 38، لسنة 2005.

(4) أمر رقم 70-61 المؤرخ بتاريخ 8 أكتوبر 1970 يتضمن المصادقة على الاتفاقية بين الجمهورية الجزائرية الديمقراطية الشعبية والمملكة البلجيكية، المتعلقة بتسليم المجرمين والتعاون القضائي في المواد الجنائية، الموقعة ببروكسيل في 12 يولي 1970.

(5) مرسوم رقم 84-25 المؤرخ بتاريخ 11 فبراير 1984 يتضمن المصادقة على اتفاقية التعاون القضائي والعدلي في المواد المدنية والتجارية والعائلية والجزائية بين الجمهورية الجزائرية الديمقراطية الشعبية والجمهورية الشعبية المجرية، الموقع عليها بالجزائر بتاريخ 07 فبراير 1976.

توجب أن يكون الجاني خاضعا للمحاكمة وتنفيذ العقوبة في موطنه لما في ذلك من سهولة استقصاء ظروفه الشخصية والدافع التي كان وراء إقدامه على ارتكاب الجريمة، كما أن نظام التسليم يخلق عدم الاطمئنان في الجهات القضائية في الدول المطلوب منها التسليم في أن الدولة الطالبة ستحقق مقتضيات العدالة، لكن هذا الاتجاه قد تعرض إلى العديد من الانتقادات في حجه، فأما حجة الأولى فهي واهية، كون التسليم هو عمل من أعمال السيادي وبالتالي فهو لا يمس بها، أما عن مقتضيات العدالة فهي تقتضي التسليم لا رفضه كون الأدلة وإجراءات التحقيقات تكون في البلد الذي وقع فيه الجرم⁽¹⁾.

وفي مواجهة هذا الفريق، هناك فريق داعم لفكرة التسليم وذلك استنادا إلى أن التسليم يعبر عن ضمان أفضل للعدالة، حيث يتم تسليم المجرمين إلى موقع الجرم الذي تتوفر فيه المادة الاستدلالية خاصة حال وجود تشارك في الجرم، لذلك تكون أفضلية المحاكمة أمام جهات قضائية واحدة، ويعمل التسليم أيضا إعادة السكانية الاجتماعية من خلال محاكمة الجاني وعقابه في المكان الذي تسببت فيه جريمته باضطراب⁽²⁾.

ب- الطبيعة القانونية لنظام التسليم:

يوجد خلاف كبير حول الطبيعة القانونية لتسليم المجرمين بين فقهاء القانون، إذ أن فريقا منهم يرى أن الدولة حينما تقوم بتسليم المجرم الفر فإنها بذلك تقوم بمباشرة عملا من الأعمال القضائية إذ بمقتضاه تتم محاكمته وتنفيذ العقاب عليه⁽³⁾، فالطبيعة القضائية للتسليم تنشأ حينما تكون السلطة القضائية هي صاحبة الاختصاص في البت في طلب التسليم، والتقرير بشأنه بموجب حكم أو قرار قابل لأحكام الطعن، فتحديد الطبيعة القضائية للتسليم يمكن وفق ثلاث معايير أولها المعيار العضوي أين تسند المهمة للجهات القضائية، ومعيار موضوعي أين تخضع فيه إجراءات التسليم إلى القواعد المقررة في الدعوى العمومية، والمعيار الأخير متعلق بحق الدفاع وضمن الحقوق للشخص محل التسليم⁽⁴⁾.

(1) رقية عواشيرة، نظام تسليم المجرمين وحدوده في تحقيق التعاون الدولي لمكافحة الجريمة المنظمة، مجلة الفكر، المجلد 04، العدد 04، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، أبريل 2009، ص ص: 17-27:

<https://www.asjp.cerist.dz/en/article/62771>

(2) رقية عواشيرة، المرجع السابق.

(3) آمال بن صويلح، التعاون الدولي وقوانين مكافحة الإرهاب الدولي، مذكرة ماجستير في القانون الدولي العام، كلية الحقوق والعلوم السياسية، جامعة مننوري، قسنطينة، الجزائر، السنة الجامعية 2008-2009، ص ص: 137-138.

(4) فيصل بن زحاف، تسليم مرتكبي الجرائم الدولية، رسالة دكتوراه في القانون الدولي والعلاقات السياسية الدولية، كلية الحقوق والعلوم السياسية، جامعة وهران، السنة الجامعية 2011-2012، ص ص: 27-28.

في حين يرى جانب آخر من الفقهاء أن نظام تسليم المجرمين يندرج ضمن الأعمال السياسية، إذ أن الدولة في التسليم تكون بعيدة كل البعد عن سلطة القضاء، بل إن سلطتها التقديرية ورغبتها هي التي يقوم عليها نظام التسليم، فطلبات التسليم لا تعرض أمام الجهات القضائية، وهي بذلك لا تخضع لأحكام الدعاوى والخصومات القضائية كأحكام قانون الإجراءات الجزائية⁽¹⁾، يوجد العديد من الدول التي تعتمد هذا النظام وبينها الولايات المتحدة الأمريكية وبعض القضاة في محكمة العدل الدولية، الذين يرون أن التسليم هو من القرارات السيادية للدولة التي يوجه إليها طلب التسليم، فلا وجود في إطار القانون الدولي إقرار أو توقع عقوبة في حالة عدم الامتثال لطلب التسليم⁽²⁾.

وهناك مذهب آخر من الفقهاء يرون أن النشأة الأولى لنظام التسليم كان فيها ضمن دائرة أعمال السيادة، وبعدها أخذ في التوجه نحو الطبيعة القضائية ليعد عملاً من أعمال القضاء، ويعود ذلك لما في مصالح الدول والشعوب من تشابك وترابط، والسعي في التعاضد فيما بينها، فنظام التسليم هو نظام يجمع بين أعمال السيادة والقضاء معاً، ويستجيب مطلباً من لاحد مطالب المصلحة العامة المشتركة للدول المتحضرة في هذا العصر، وأما عن الراجح في الأقوال الثلاث، فجو القول التي يقضي بأن تسليم المجرمين ضمن دائرة أعمال السيادة لا القضاء، حتى وعن كان القضاء هو الذي يبت في الطيب، إلا أن القرار النهائي القاضي بالتسليم يكون من اختصاص السلطة السياسية، فلها كامل السلطة في الموافقة عليها أو رفضه⁽³⁾.

وتبعاً لهذه الطبيعة القانونية يمكن لعملية تسليم المجرمين أن تتخذ ثلاث آليات أو أنظمة وهما؛

• النظام الإداري:

وفيه يتم توجيه طلب التسليم من وزارة الخارجية إلى وزارة العدل التي تقوم بدراسته من خلال النظر في استوائه للشروط القانونية ثم تفصل في أمره بالقبول أو الرفض، ثم بعدها يتم إطلاع وزارة الخارجية بهذا القرار، وحينها تقوم هذه الأخيرة بإشعار الممثل الدبلوماسي التابع للدولة الطالبة، وهو نظام يمتاز بالسرعة والبساطة إلا أنه في الوقت ذاته يهضم حقوق الأفراد ولا يوفر ضمانات الدفاع عنهم⁽⁴⁾.

(1) موساوي فتحي رشدي، مبدأ تسليم المجرمين في القانون الدولي الاتفاقي، مذكرة ماجستير في القانون الدولي والعلاقات الدولية، كلية الحقوق، جامعة الجزائر 01، بن يوسف بن خدة، السنة الجامعية 2012-2013، ص 43.

(2) آمال بن صويلح، المرجع السابق، ص ص: 137-138.

(3) المرجع نفسه، ص ص: 137-138.

(4) عويض بن محمد بن هزال النياي، أحكام تسليم المجرمين في الفقه الإسلامي والاتجاهات المعاصرة وتطبيقاتها في المملكة العربية السعودية، رسالة ماجستير، تخصص التشريح الجنائي الإسلامي، برنامج مكافحة الجريمة، المعهد العالي للعلوم الأمنية، المركز العربي للدراسات الأمنية والتدريب، 1995، ص ص: 43-44.

ويرى بعض الباحثين أن النظام الإداري في التسليم قد أخذت شمسه في المغيب، ليترك المجال للنظام القضائي ليحل محله، أو في أقل الأحوال سيحل النظام المختلط محله، وذلك لما شهدته الآونة الأخيرة من تطورات خاصة ظاهرة العولمة القانونية على مساوئ التعاون القضائي الدولي حتى ولو كان على حساب بعض القضايا المتعلقة بالسيادة⁽¹⁾.

• النظام القضائي:

يحال طلب التسليم بموجب هذا النظام من السلطة التنفيذية إلى السلطة القضائية، وفي بعض الدول يحال طلب التسليم من جهة قضائية في دولة طلب التسليم أيضاً، ويصدر القضاء في حق الشخص محل طلب التسليم أمر بالقبض الاحتياطي، ويحدد ميعاد المرافعة، أين يحاكم علنياً وفقاً لسائر أدلة الإثبات التي يناقشها هو ومحاميه، ولا يمكن أن توقيف هذا الشخص أو تسليمه إلا بناء على قناعة القاضي بضلوعه في الجريمة سبب التسليم، ويجوز أن يخضع قرار القاضي في هذا الشأن للطعن بالاستئناف⁽²⁾.

• النظام المختلط:

يتميز النظام المختلط بين النظام الإداري والنظام القضائي، فيستفيد من المحاسن والسمات التي يتميز بها كل من هذين النظامين، فالسلطة القضائية أن تبدو رأيها شريطة أن يكون ذلك على سبيل الاستشارة، ويكون للسلطة التنفيذية اختصاص التقرير في طلبات التسليم كونه عملاً سيادياً⁽³⁾.

ج- القوة الإلزامية لأحكام التسليم:

اختلاف الفقه أيضاً في مسألة القوة الملزمة لأحكام التسليم، ففي الحين الذي يرى اتجاه من اتجاهات الفقه أن أحكام التسليم ترد على وجه الإلزام وأن الدولة تكون ملزمة بتسليم المجرمين، وليس لها خيار إلا أن تقوم هي بنفسها بتنفيذ العقوبة عليه، وإلا فهو ملزمة بتسليمه إلى الدولة التي مارس شكلاً من أشكال الانتهاك ضد قوانينها، يرى اتجاه آخر من الفقه أن التسليم واجب قانوني صريح وبصفة خاصة في الجرائم الموصوفة بالخطورة، ويرى البعض من الفقهاء أن التسليم يعد التزاماً ناقصاً، أو هو واجب سياسي، أو واجب تفرضه الأخلاق السياسية، ويجب على الدولة أن تنقيد به⁽⁴⁾.

(1) موساوي فتحي رشدي، المرجع السابق، ص 45.

(2) عويض بن محمد بن هذال الذيابي، المرجع السابق، ص 45.

(3) المرجع نفسه، ص 48.

(4) مازن خلف الشمري، موانع تسليم الإرهابيين: (دراسة مقارنة)، مجلة كلية الحقوق، المجلد 14، العدد A1، كلية الحقوق، جامعة النهر، العراق، 2012، ص ص: 280-300.

<https://www.iasj.net/iasj?func=article&aid=59527>

ويتعارض مع كل ما سبق، اتجاه آخر من الفقهاء، الذين قرروا أن التسليم لا يعد واجبا قانونيا في حالة ما إذا لم يكن هناك معاهدة تنظمه، بل هو من الواجبات الأدبية، وينجم عن عدم الالتزام به مساس بواجب أدبي بالقصور والإخلال، كما أن هناك من يرى أن التسليم هو عمل سيادي، غير جنوح هذه الآراء إلى تقييد الأساس القانوني للتسليم بالمعاهدات يعد من المآخذ، إذ أن هناك مصادر أخرى يتأسس عليها التسليم قانونيا، فيمكن حينها القيام بالتسليم دون وجود معاهدة، فعلى الدول القيام بتسليم المجرمين الفارين إليها سواء أكان ذلك بناء على معاهدة أم لا، وذلك نظرا لمقتضيات وضروريات التعاون الدولي، والراجح أن التسليم هو واجب قانوني لا أدبي⁽¹⁾.

أما فيما يتعلق بجريمة الإرهاب الإلكتروني وسائر الجرائم المرتبطة بتقنية المعلومات والاتصال فإن التسليم فيها يعد واجبا قانونيا ملزما، وذلك بمقتضى نص المادة 2/24 والتي تنص على أنه: (تعتبر الجرائم الجنائية الواردة في الفقرة ١ من هذه المادة مدرجة كجرائم يجب فيها التسليم في أي معاهدة بشأن تسليم المجرمين قائمة بين الأطراف، وتتعهد الدول الأطراف بتضمين هذه الجرائم على أنها جرائم يجب فيها تسليم المجرمين في أي معاهدة بشأن تسليم المجرمين يتم إبرامها فيما بينهم)⁽²⁾، غير أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لم تنص على هذا الوجوب، بل جعلت من التسليم في هذا النوع من الجرائم مقبولا فقط، حيث نص على أنه: (إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبر جرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف)⁽³⁾.

الفرع الثاني: نظام تسليم المجرمين: الإجراءات والشروط:

ورثت إجراءات سير عمليات تسليم المجرمين الخلاف القائم في طبيعتها، إذ يحتفظ كل تشريع داخلي وكل معاهدة أو اتفاقية بالإجراءات التي يتعين السير وفقها في هذا المجال، ومع هذا يمكن أن نلمح نقاط تقاطع بينها، وإجراءات مشتركة تجمع حولها (أولا)، وبالإضافة إلى الإجراءات واجبة اتخاذ، فإن لنظام التسليم شروطه، إذ يتعين لتسليم أي مجرم من مجرمي الإرهاب الإلكتروني استثناء جملة من الشروط التي أحالت إليها الاتفاقيات المتخصصة في هذا الباب (ثانيا).

(1) مازن خلف الشمري، المرجع السابق.

(2) المادة 2/24 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية، المرجع السابق.

(3) المادة 2/31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق.

أولاً: إجراءات تسليم:

تختلف إجراءات التسليم من دولة لأخرى على حسب النظام المعتمد فيها، فغالبية الدول تسير وفق نظام التسليم عبر السلطة التنفيذية، إذ هي التي تقوم بالبت في طلبات التسليم، في حين نجد بعض الدول تأخذ بالنظام القضائي للتسليم، والبعض الآخر منها يعتمد على النظام المختلط، غير أن هناك بعض الإجراءات قد أجمعت الدول بقطع النظر عن نظام التسليم المعتمد فيها⁽¹⁾، وهي التي سنسوقها على الشكل الآتي:

1- طلب التسليم:

يعرف طلب التسليم على أنه: (الأداة التي تعبر بها الدولة الطالبة صراحة عن رغبتها في استلام الشخص المطلوب، إذ أنه بدون هذا الطلب لا يمكن أن ينشأ الحق في التسليم)، ويجب أن يكون هذا الطلب كتابيا على ما اشترطت به الغالبة من الاتفاقيات، متضمنا طرعا مستقيضا لهوية الشخص محل التسليم بما في ذلك أوصافه وجنسيته وصورته إن كان ذلك ممكنا، ولما نسب إليه من وقائع وما نسب إليه من فعل مجرم وتاريخه ونسخة من القوانين والتشريعات المنطبقة على هذا الفعل، وما أتخذ بشأنه من إجراءات وفي حالة طلب تسليم مجرم من أجل توقيع العقاب، فيجب أن يشتمل الطلب أيضا على نسخة من الحكم الصادر بالعقوبة⁽²⁾.

ولما كان التسليم من أعمال السيادة -على أرجح الآراء- فإن مباشرته تكون من اختصاص حكومة الدولة الطالبة، إذ توجهه بدورها إلى حكومة المطلوب منها التسليم، ويكون ذلك من خلال القنوات الدبلوماسية إذ هي المنوط بها دوليا عملية الاتصال بين الحكومات، وهو المعمول به والمنصوص عليه في غالبية المعاهدات والاتفاقيات الدولية⁽³⁾، ومن أمثلة ذلك ما نص عليه المشرع الجزائري في نص المادة 702 من قانون الإجراءات الجزائية والتي تقضي بتوجيه طلب التسليم إلى الحكومة الجزائرية عن طريق دبلوماسي.

2- إجراءات الدولة المطلوب منها التسليم:

تجري الدولة المطلوب منها تسليم مجرم بمجرد إبلاغها بالطلب بالتحري عن الشخص الذي طلب إلقاء القبض عليه، إذ تقوم بإصدار أمر للقبض عليه استنادا إلى الوثائق التي تضمنها ملفه، ويكون ذلك في خلال 60 يوما على أقصى تقدير، والغالب في تحديد المدة المتعلقة بعملية تسليم

(1) آمال بن صويلح، المرجع السابق، ص 140.

(2) فافة لحر، المرجع السابق، ص: 99-100.

(3) آمال بن صويلح، المرجع نفسه، ص 140.

هذا الشخص بشهر من التاريخ الذي أبلغت فيه الدولة الطالبة بموافقتها على التسليم، غير أنه من الممكن القيام بتأجيل التسليم إذا كان محل محاكمة أمام الجهات القضائية للدولة المطلوب منها أو كان محكوم عليه بعقوبة يجب عليه قضاؤها⁽¹⁾.

ثانياً: شروط التسليم:

تعتبر شروط التسليم في الجرائم المتعلقة بتقنيات المعلومات بما في ذلك جريمة الإرهاب الإلكتروني مختلفة باختلاف التشريعات والمعاهدات والاتفاقيات المتعلقة بتسليم المجرمين، وهذا طبقاً لنص المادة 5/24 من اتفاقية بودابست التي تنص على أنه: (يخضع تسليم المجرمين للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها التسليم أو معاهدات تسليم المجرمين واجبة التطبيق)⁽²⁾، وعليه فإننا سنتناولها على النحو الآتي:

1- شرط الجنسية:

يعتبر مبدأ "حظر تسليم الرعايا" من بين الأسس والركائز الراسخة والثابتة ضمن التعاون القضائي المنصب على تسليم المجرمين، وهناك خلاف كبير بين الدول في مجال تسليم الرعايا تبعاً للوضعية القانونية للرعية المطلوب تسليمه، فإن كان الشخص المطلوب تسليمه يعتبر من رعايا الدولة الطالبة، فإنه لا يكون محل نزاع في هذه الحالة، فيتعين حينها تسليمه إلى الدولة الطالبة فور استيفاء طلب التسليم لشروطه وإجراءاته الموضوعية والشكلية، أما إذا كان الشخص محل طلب التسليم من رعايا الدولة التي يطلب منها التسليم، فإن الفقه في هذه الحالة قد جادل فيه على نطاق واسع، وانقسم فيه بين داعم ورافض، أما من الناحية العلمية فإن ذلك واقف على مضمون المعاهدات الخاصة بالتجريم وقوانين الجنسية لكل بلد، وقد يكون الشخص محل التسليم لا من رعايا الدولة الطالبة والمطلوب منها، بل يكون من رعايا دولة أخرى، ففي هذه الحالة يتوقف التسليم على ما تضمنته المعاهدات أو الاتفاقيات المبرمة بين الدول، فإن تضمنت وجوب استشارة الدولة الثالثة تكون حينها واجبة. وإن لم تتضمنها فتعد حينها الاستشارة مجاملة دولة أو رعاية لمبدأ المعاملة بالمثل⁽³⁾.

يمكن أيضاً أن يكون الشخص محل طلب التسليم متعدد الجنسيات، وفي هذه الحالة يجب العودة إلى التشريعات الوطنية والاتفاقية المبرمة بين الدول، فعلى سبيل المثال نجد المشرع

(1) آمال بن صويلح، المرجع السابق، ص 141.

(2) المادة 5/24 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية.

(3) عمر زغودي، المرجع السابق.

الجزائري في مثل هذه المسألة يميز بين حالتين، أولهما إذا كانت كل تلك الجنسيات ثابتة لشخص أجنبي ففي هذه الحالة وطبقا لنص المادة 1/22 من القانون المدني ينظر إلى الجنسية الفعلية له وفقا للمعيار الواقعي والاعتبارات العلمية، والحالة الثانية هي تعدد الجنسيات المثبتة لشخص يحمل الجنسية الجزائرية، فإن المادة 2/22 من ذات القانون تنظر إلى أحكام التسليم من منظور الجنسية الجزائرية⁽¹⁾، وعلى أساسها يكون الطلب.

كما يمكن أيضا أن يكون الشخص محل طلب التسليم عديم الجنسية، وفي هذه الحالة فإن الاختلاف في القانون الواجب التطبيق بين، فهناك من يوصي بتطبيق قانون الدولة التي كان في السابق يحمل جنسيتها، كما أن هناك من يرى تطبيق قانون دولة الميلاد، غير أن الراجح في ذلك تطبيق حسب الترتيب؛ قانون موطنه، أو محل إقامته، أو قانون القاضي المعروض أمامه النزاع، كما هو الحال بالتشريع الجزائري⁽²⁾ الذي ينص على أنه: (و في حالة انعدام الجنسية يطبق القاضي قانون الموطن أو قانون محل الإقامة)⁽³⁾، وكما نصت المادة 15 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية على أنه: (...2- رهنا بأحكام المادة 4 من هذه الاتفاقية، يجوز للدولة الطرف أن تؤكد أيضا سريان ولايتها القضائية على أي جرم من هذا القبيل في الحالات التالية: ...ب- عندما يُرتكب الجرم أحد مواطني تلك الدولة الطرف أو شخص عديم الجنسية يوجد مكان إقامته المعتاد في إقليمها)⁽⁴⁾.

و هناك أيضا حالة ما إذا كان المطلوب تسليمه شخصا يتمتع بالحصانة، ففي هذه الحالة نصت المادة 03/أ من الاتفاقية النموذجية لتسليم المجرمين على عدم جواز التسليم حيث نصت على أنه: (لا يجوز التسليم متى كان الشخص المكلوب -يتمتع- وفقا لقانون طرفي التسليم بالحصانة من المقاضاة والعقاب لأي سبب كان)، والظاهر من خلال هاذ النص أن الحصانة عامة وشاملة، وبذلك يمكن النص شاكلا لكل الحصانات⁽⁵⁾.

(1) بوعلام خندق، تسليم المجرمين، بحث ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق بن عكنون، جامعة الجزائر بن يوسف بن خدة، السنة الجامعية 2008-2009، ص ص: 48-49.

(2) المرجع نفسه، ص 49.

(3) المادة 3/22 من الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

(4) المادة 15 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 نوفمبر 2000.

(5) فريدة شبري، تحديد نظام تسليم المجرمين، مذكرة ماجستير في القانون الدولي لحقوق الإنسان، كلية الحقوق بودواو، جامعة أمحمد بوقرة، بومرداس، الجزائر، السنة الجامعية 2007-2008، ص 70.

وأخيراً، يجب الإشارة إلى حالة ما إذا كان الشخص محل طلب التسليم لاجئاً سياسياً، ففي هذه الحالة فإن اتفاقية جنيف لسنة 1951 في مادتها 1/33 تنص على حظر قيام الدولة بطرد أو إبعاد اللاجئين إلى دولة يمكن أن تتعرض فيها حياتهم أو حريتهم لتهديدات نظراً لانتماءاتهم العرقية أو الدينية أو الجنسية، أو نظراً لما يتبنونه من آراء سياسية، أو لانتمائهم لجماعة معينة، غير أن هذا النص يتناول مسألة الطرد والإبعاد، وأنه لمن العسير إسقاط هذا المضمون على مضمون نظام تسليم المجرمين⁽¹⁾، إلا أن هناك نصوص دستورية تقضي صراحة بعدم جواز التسليم، كما هو الحال في الدستور القطري الذي ينص على أن: (تسليم اللاجئين السياسيين محظور)⁽²⁾، والدستور الإماراتي القاضي بأن: (تسليم المواطنين، واللاجئين السياسيين، محظور)⁽³⁾.

ونظراً لكون هذا المبدأ القاضي بعدم جواز تسليم الرعايا قد ينجم عنه إن تم تطبيقه على وجه الإطلاق انفلات المجرم من العقاب، فإن هناك بديلاً يتمثل في مبدأ " التسليم أو المحاكمة" المنصوص عليه في المادة 10/16 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية⁽⁴⁾ الآتي نصها: (إذا لم تقم الدولة الطرف التي يوجد الجاني المزعوم في إقليمها بتسليم ذلك الشخص فيما يتعلق بجرم تنطبق عليه هذه المادة، لسبب وحيد هو كونه أحد رعاياها، وجب عليها، بناء على طلب الدولة الطرف التي تطلب التسليم، أن تحيل القضية دون إبطاء لا مبرر له إلى سلطاتها المختصة بقصد الملاحقة. وتتخذ تلك السلطات قرارها وتضطلع بإجراءاتها على النحو ذاته كما في حالة أي جرم آخر ذي طابع جسيم بمقتضى القانون الداخلي لتلك الدولة الطرف. وتتعاون الدول الأطراف المعنية، خصوصاً في الجوانب الإجرائية والمتعلقة بالأدلة، ضماناً لفعالية تلك الملاحقة)⁽⁵⁾، وكما نصت عليه أيضاً المعاهدة الجزائرية النيجرية المتعلقة بتسليم المجرمين في مادتها الثالثة⁽⁶⁾ القاضية بجواز تسليم الطرفين لرعاياها إذا كان قانونها يسمح بذلك، وإلا فإن الطرفان يتعهدان بمتابعة رعاياها على الجرم المرتكب وفق تشريعاتها

(1) عمر زغودي، المرجع السابق.

(2) المادة 58 من الدستور القطري، الصادر في الديوان الأميري بتاريخ 8 جوان 2004.

(3) المادة 38 من دستور الإمارات العربية المتحدة، الصادر عام 1971 شاملاً تعديلاته لغاية عام 2009.

(4) عمر زغودي، المرجع السابق.

(5) المادة 10/16 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

(6) المادة 03 من المرسوم الرئاسي رقم 193-05.

الوطنية، وبما أن الجزائر لا تسمح تشريعها الداخلي بتسليم رعاياها⁽¹⁾ فإن تقديمه للمحاكمة هو الذي سيتم توظيفه في هذه الحالة.

2- ازدواجية التجريم:

يراد بازدواجية التجريم: (أن يكون الفعل سبب التسليم مجرما في قانون كل من الدولتين الطالبة والمطلوب منها التسليم)⁽²⁾، ويعتبر هذا الشرط شرطا أصيلا في الكثير من المعاهدات والاتفاقيات الدولية ثنائية كانت أم متعددة اطراف وتتضمنه أيضا تشريعات وطنية، فنجد على سبيل المثال في المادة 695 من قانون الإجراءات الجزائية الجزائري، كما نصت عليه أيضا اتفاقية بودابست في مادتها 1/24/أ والتي تنص على أنه: (تطبق هذه المادة على تسليم المجرمين بين الدول الأطراف بالنسبة للجرائم المنصوص عليها في المواد من 02 إلى 11 من هذه الاتفاقية، شريطة أن يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين، بعقوبة سالبة للحرية لمدة سنة على الأقل أو بعقوبة أشد)⁽³⁾، والمادة 1/31/أ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المشار إليها آنفا.

ويعد هذا الشرط أعمالا لمبدأ الشرعية الجنائية في الجرائم والعقوبات، والقاضي بألا جريمة ولا عقوبة إلا بمورد نص قانوني يقرها، ويمثل هذا أيضا ضمانا لحفظ لهيبة القضاء وإقرار باحترامه، مع اقتران ذلك كله بحماية حقوق الإنسان وصونها من الاعتداء عليها، فمثل هذا الشرط يعمل على الوفاء بمقتضيات العدالة بأن يكون العقاب على الجاني، ومنعا لعرض الشخص البريء أمام المحكمة⁽⁴⁾، فهو يجمع بين مقتضيات العدالة من جانب، وحفظ حريات الناس وحقوقهم من جانب آخر.

ويمكن تقسم هذا الشرط إلى شطرين؛ أولهما مرتبط بالفعل سبب التسليم، فلا يجوز إجماعا القيام بالتسليم إلا إذا كان سببه فعل معاقب عليه في الدولة الطالبة، سواء تضمن طلب التسليم المحاكمة أو قضاء العقوبة، لكن الخلاف يبرز في كون الفعل سبب التسليم معاقب عليه في الدولة المطلوب منها، والراجح من بين الآراء أنه يجب أن يكون الفعل مجرما فيها أيضا، وهو مناط تعريف ازدواجية التجريم، كما يجب أن يكون التجريم ساري المفعول في كلا الدولتين، فبالنسبة

(¹) المادة 1/698 من الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، المرجع السابق: (لا يقبل التسليم في الحالات الآتية: 1- إذا كان الشخص المطلوب تسليمه جزائري الجنسية...)

(²) عمر زغودي، المرجع السابق.

(³) المادة 1/24/أ من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية.

(⁴) نسيب نجيب، التعاون القانوني والقضائي الدولي في ملاحقة مرتكبي جرائم الإرهاب الدولي، المرجع السابق، ص ص: 120-121.

للدولة الطالبة فلا شك أنه يجب أن يكون نص التجريم سابقا للفعل وإلا عد خرقا لمبدأ عدم رجعية القانون الجنائي، أما بالنسبة للدولة الطالبة فلا يشترط ذلك، لان الازدواجية حنيها متوفرة -عند تقديم الطلب- حتى وإن كان الفعل سابقا لنص التجريم، وإما إذا تم إلغاء نص التجريم بعد وقوع الفعل وقبل البت في طلب التسليم فحينها ينتفي الازدواج ويحظر التسليم، ومع هذا فإن هذه الأحكام جميعا مرهونة بالنصوص التشريعية الداخلية أو الاتفاقية بين الدول، أما الشرط الثاني فيتعلق بسقوط العقاب، فلا يجوز التسليم في جريمة سقطت المحاكمة فيها لمضي الأجل القانوني أو سقطت العقوبة بالتقادم⁽¹⁾، وبما أن جرائم الإرهاب الإلكتروني نوع من أنواع الإرهاب، وبما أن جرائم الإرهاب لا تسقط المحاكمة والعقوبة فيها بالتقادم فلا مجال لتطبيق هذا الشق من الشرط.

3- شرط الجسامة الإجرامية:

تختلف أصناف الجرائم تبعا لجسامتها إلى عدة أصناف، فمن الجرائم ما يعد جنایات في غاية الجسامة والعظم، ومن أجل كبها وردعها يتوقع عليها أكبر العقوبات وأكثرها شدة كالسجن المؤبد أو الإعدام، ومنها ما يكتسب صفة الجرح، ومن أجل ردعها تتخذ عقوبات أقل شدة وحدة من الجنایات، كما يمكن أيضا أن تتخذ هذه الجرائم صورة مخالفات خفيفة أو طفيفة وحينها لا يوقع لردعها إلا عقوبات ضئيلة⁽²⁾.

ولما كان تسليم المجرمين من بين الإجراءات التي تتسم بالتعقيد وبالكلفة الباهظة على الدولة، فإن اللجوء إليها لا يكون إلا في الحالات التي يكون فيها الجرم على قد بلغ من الجسامة والخطر قدرا معينا، فليس من المقبول أن يتم اللجوء على مثل هذه الإجراءات المعقدة والمكلفة إذا كان الشخص محل التسليم مرتكبا لجرم بسيط⁽³⁾، فمن المحذور أن يتم اللوذ أو الاستعانة بنظام التسليم إلا في الحالات التي تكون الجريمة على قدر محدد من الأهمية والجسامة، كما أنه من غير الجائز القيام بإلقاء مؤسسات الدولة الطالبة والمطلب منها بطلبات التسليم في المسائل التي لا تحوز أي أهمية أو يترتب عنه ضرر يتسم بالعموم والخطر، أو في أشكال التصرفات التي يطغها عليها الطابع الخاص لضررها عن الطابع العام⁽⁴⁾، وهذا الشرط يعتبر شرطا بديها، إذ ليس

(1) هادي نعيم المالكي وسارة ظافر عبد الحميد، الشروط الخاصة بالجريمة في تسليم المجرمين طبقا لأحكام القانون الدولي والقانون العراقي، مجلة العلوم القانونية، كلية الحقوق، جامعة بغداد، المجلد 33، العدد 6، العدد الخاص بالتدريسين وطلبة الدراسات العليا، 2018، ص: 151-150: <https://jols.uobaghdad.edu.iq/index.php/jols/issue/view/19>

(2) هادي نعيم المالكي وسارة ظافر عبد الحميد، المرجع السابق.

(3) نسيب نجيب، التعاون القانوني والقضائي الدولي في ملاحقة مرتكبي جرائم الإرهاب الدولي، المرجع السابق، ص 121.

(4) فريد علوش، التعاون الدولي عن طريق نظامي تسليم المجرمين والتسليم المراقب، مجلة الفكر، المجلد 12، العدد 14، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، جانفي 2017، ص: 165-179: <https://www.asjp.cerist.dz/en/article/62385>

من المقبول أن مثلاً مباشر السير في هذا الإجراء الطويل والمعقد والباهض من أجل تسليم مرتكب مخالفة عدم دفع ثمن المشروبات والمأكولات، أو عدم دفع ثمن غرفة في فندق الأفعال المعاقبة عليها في المادة 366 من قانون العقوبات الجزائري.

يعتمد في تحديد جسامة وخطورة الجرائم الخاضعة للتسليم عن طريق ثلاث أساليب وهي:

أ- أسلوب الترتيب:

وتكمن آلية العمل في هذه الطريقة في صياغة وإنشاء لائحة أو جدول يتم فيه بيان للجرائم التي من شأنها أن تكون موضوع التسليم فيها بحيث يتم تعدادها وحصرها وتحديدتها، وهي من بين الطرق أو الأساليب التي يتم الاعتماد عليها كثيراً في المعاهدات، في حين أن هذه الآلية على صعيد التشريعات الوطنية تكون صعبة غير ميسرة، لما في اللغة والاصطلاحات والتكييف القانوني للأفعال ودرجة جسامتها من اختلافات⁽¹⁾.

لكن هذا الأسلوب في تحديد جسامة الجريمة سبب التسليم قد تعرض للعديد من الانتقادات، فهو أسلوب جامد لا يمكنه أن يساير التطورات أو التحديثات التي يمكن أن تستجد في ظواهر الإجرام كما ونوعاً، ويمكن للدول القيام بإضافة جرائم جديدة خاضعة للتسليم غير أن ذلك يستوجب القيام بإبرام معاهدة جديدة أو ملاحق بالمعاهدة القائمة وهذا متعارض من السرعة التي يتطلبها نظام التسليم لما تأخذه تلك المعاهدات والملاحق من وقت⁽²⁾، خاصة في جرائم الإرهاب الإلكتروني التي يلعب عنصر الوقت في كشفها ومكافحتها والتصدي لها دوراً محورياً.

كما أنه أسلوب يتميز بالصعوبة إذ ليس من اليسير وضع جداول أو لوائح للجرائم الخاضعة لنظام التسليم، وفي حالة ما إذا كان ذلك ممكناً فالاختلاف في مهم المراد من تلك الجرائم موضع اختلاف وتباين، ناهيك عما للغة القانونية ومدلولاتها وقواعد التجريم والمجتمعات الإنسانية وما يحيط بها من تفسيرات لأنواع السلوك من اختلافات وتباين فيما بينها⁽³⁾.

ب- أسلوب الشرط العام:

تعتمد آلية العمل في هذا الأسلوب لتحديد جسامة الجرائم الخاضعة لنظام التسليم على تحديد الحد الأدنى للعقوبة المقررة لتحديد الجرائم التي يجوز فيها التسليم، فالجسامة في هذا الأسلوب

(1) سعاد بوخالفة، مبدأ التسليم أو المحاكمة على ضوء أعمال لجنة القانون الدولي، مذكرة ماجستير في إطار مدرسة الدكتوراه في فرع الدولة والمؤسسات العمومية، كلية الحقوق بن عكنون، جامعة الجزائر 01، السنة الجامعية 2014، ص 33.

(2) نسيب نجيب، التعاون القانوني والقضائي الدولي في ملاحقة مرتكبي جرائم الإرهاب الدولي، المرجع السابق، ص 121.

(3) عويض بن محمد بن هذال الذياي، المرجع السابق، ص ص: 72-73.

ينظر إليها من منظور الحد الأدنى المقرر في الجانب الموضوعي لعقوبة الجناية أو الجنحة، وقد أخذت بهذا الأسلوب التشريعات المعاصرة وبشكل خاص على المستوى الوطني⁽¹⁾.

ج- أسلوب الاستبعاد:

تستند آلية عمل هذا الأسلوب على تحديد العقوبة ومقدورها، فتكون حينها العقوبة حينها؛ هي القاعدة الذي تتبني عليه عملية بيان أنواع الجرائم التي تخضع لنظام التسليم، وذلك بإدراج الحد الأدنى أو الأقصى للجرائم التي تكون موجبة للتسليم بموجبها في التشريعات والقوانين المتصلة بتسليم المجرمين سواء أكانت تشريعات داخلية أم اتفاقيات ومعاهدات دولية⁽²⁾، وهو الأسلوب المعتمد في الاتفاقيات الخاصة بالجرائم المتصلة بتكنولوجيا المعلومات والاتصال كما بينت ذلك المادة 1/24/أ من اتفاقية بودابست لمكافحة الجريمة الإلكترونية حين نصت على أن: (...شريطة أن يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين، بعقوبة سالبة للحرية لمدة سنة على الأقل أو بعقوبة أشد)⁽³⁾.

ويمكن أن ينقسم المطلوب تسليمهم استنادا إلى هذا المعيار إلى قسمين؛

- "المطلوب تسليمه على خلفية تهمة منسوبة إليه فر قبل صدور الحكم عليه، ففي هذه الحالة يشترط لتسليمه ألا يقل الحد الأقصى للعقوبة المنصوص عليها على تلك الجريمة عن حد معين تقرر وفقا للتشريع الداخلي للدولة الطالبة أو الدولتين معها؛
- المطلوب تسليمه على خلفية حكم صادر عليه استنادا إلى إجراءات تمت مباشرتها عقب ارتكاب الفعل المجرم وانفلات الجاني قبل أن يستوفي العقوبة المحكوم بها عليه، ففي هذه الحالة يقوم التسليم فيها على شرط عدم تخطى العقوبة المحكوم بها عن الحد الأدنى الذي تم تحديده"⁽⁴⁾.

4- شرط اندراج الجريمة ضمن الجرائم التي يجوز فيها التسليم:

كثيرا ما تقوم الدول في قوانينها الداخلية ومعاهداتها بتعيين وحصر الجرائم التي يجوز فيها تسليم المجرمين، - وكما أسلفنا الذكر - لا يجوز التسليم في الغالب إلا في الجرائم الجسمية سواء أكانت جنائيات أو جنح، أما في غيرها من الجرائم التي تعد جرائم خطيرة فلا يجوز فيها التسليم، غير أن ذلك لا يحول دون التسليم في الجرائم غير الواردة والمحددة في النصوص القانونية

(1) سعاد بوخالفه، المرجع السابق، ص 33.

(2) المرجع نفسه، ص 33.

(3) المادة 1/24/أ من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية.

(4) عويض بن محمد بن هزال الذيابي، المرجع السابق، ص ص: 74-75.

الداخلية أو الاتفاقيات والمعاهدات الدولية، إذا ما كان لذلك مقتضا ظرفيا، أو بناءً على التبادل بين الدول، ما لم تمتع التشريعات الداخلية من ذلك⁽¹⁾.

وقد حددت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، الجرائم التي يجب فيها التسليم في نص المادة 1/16 والتي أحالت إلى المادة الفقرة 01/أ أو ب من ذات الاتفاقية، وهي تلك المرتبطة بالإسهام في جماعة إجرامية منظمة، غسل عائدات تبيض الأموال، الفساد، إعاقة سير العدالة، وذلك عندما تكون هذه الجرائم ذات طابع عبر وطني وتضلع في ارتكابها جماعة إجرامية منظمة، أما المشرع الجزائري فقد حددها في نص المادة 697 من قانون الإجراءات الجزائية التي تنص على أن⁽²⁾ (الأفعال التي تجيز التسليم سواء كان مطلوبا أو مقبولا هي الآتية:

1 - جميع الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جنائية،

2 - الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جنحة إذا كان الحد الأقصى للعقوبة المطبقة طبقا لنصوص ذلك القانون سنتين أو أقل أو إذا تعلق الأمر بمتهم قضى عليه بالعقوبة إذا كانت العقوبة التي قضى بها من الجهة القضائية للدولة الطالبة تساوي أو تجاوز الحبس لمدة شهرين. ولا يجوز قبول التسليم في أية حالة إذا كان الفعل غير معاقب عليه طبقا للقانون الجزائري بعقوبة جنائية أو جنحة⁽³⁾.

أما فيما يتعلق بالإرهاب الإلكتروني فإن الصور التي يتخذها من الجرائم التي يجب أو يجوز فيها التسليم، فبالنسبة للإرهاب الإلكتروني الهجين الذي تستغل فيه نوافذ وخدمات الفضاء الإلكتروني في صور الإرهاب التقليدي كتجنيد الإرهابيين، والتدريب، والإعلام الإرهابي، وتمويل الجماعات الإرهابية فلا ريب من وجهة نظرنا أنها خاضعة لأحكام التسليم بموجب التشريعات والمعاهدات والاتفاقية الدولية والثنائية لمكافحة الإرهاب والإجرام المنظم.

أما فيما يتعلق بالإرهاب الإلكتروني الحقيقي والذي يستهدف الفضاء الإلكتروني وما تعلق به من بنى تحتية فإنه خاضع لأحكام التسليم بموجب نص المادة 1/24 أ من اتفاقية بودابست لمكافحة الجريمة الإلكترونية، وبمقتضى الفقرة الثانية من ذات المادة والتي تنص على وجوب

(1) هادي نعيم المالكي وسارة ظافر عبد الحميد، المرجع السابق.

(2) عمر زغودي، المرجع السابق.

(3) المادة 697 من الأمر رقم 66-155 المتضمن قانون الإجراءات الجنائية.

التسليم في الجرائم المنصوص عليها من 2 إلى 11 من الاتفاقية وهي مظاهر وصور الجرائم الإلكترونية المختلفة والتي سلف ذكرها في بحثنا.

يجوز التسليم أيضا في الإرهاب الإلكتروني بمقتضى نص المادة 1/31 من الاتفاقية العربية لمكافحة الجرائم المتعلقة بتقنية المعلومات حيث نصت على أنه: (هذه المادة تنطبق على تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية) كما نصت الفقرة الثانية من نفس المادة على أنه: (إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبر جرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف).

الفرع الثالث: التسليم بين ما ينتجه من آثار وما يواجه من تحديات:

يترتب عن تنفيذ تسليم المجرمين شأنه شأن غيره من الإجراءات القانونية ذات الطابع الدولي جملة من الآثار والنتائج، سواء في جانبها الموضوعي أو الإجرائي، وكلها ترنو إلى تحقيق العدالة والتكافؤ وخدمة وتيسير التعاون الدولي (أولا)، غير أن هناك العديد من العقبات والتحديات التي توجه نظام التسليم بشكل عام في تحقيق هذه الغاية التي يصبو إليها، وتظهر هذه العقبات بشكل واضح ومعقد في الجرائم المتعلقة بالإرهاب الإلكتروني (ثانيا).

أولا: آثار التسليم:

1- تسليم الشخص محل الطلب:

يستتبع قبول طلب التسليم باتصال بين الدولة الطالبة والمطلوب منها من أجل العمل على التفاهم على كيفية التسليم، تاريخه ومكانه، ويتعين أن يكون التسليم في مدة أقصاها شهر بداية من تاريخ قبول التسليم على ما ذهب إليه المشرع الفرنسي، والأمر في تحديد المدة عائد إلى ما اتفقت عليه الدول، إذ يجوز أن تتوافق على مدة أخرى⁽¹⁾.

وتفاديا لقيام الدول بالتحايل والاستتار على الأوضاع والملابسات التي تكتنف الجريمة والتي قد تكون مانعا من التسليم لو اطلعت عليها الدولة المطلوب منها، فقد تم إقرار مبدأ التخصيص الذي يقضي بحظر قيام الدولة الطالبة بمعاينة الشخص محل التسليم إلا على ما أسند إليه من فعل قام على إثره التسليم⁽²⁾.

(1) فريدة شيري، المرجع السابق، ص 121-122.

(2) آمال بن صويلح، المرجع السابق، ص 141.

ويقوم مبدأ التخصيص على أساس حق اللجوء، فالدولة حينما تقوم بتسليم شخص لجأ إليها فإنها بذلك تقوم بالتنازل عن شطر من حقها لخدمة مقتضيات التعاون الدولي في التصدي للجريمة، وعليه فإن الدولة الطالبة خاضعة في محاكمة الشخص المسلم لمضمون الوقائع التي تضمنها طلب التسليم والتي وافقت عليها الدولة المطلوب منها⁽¹⁾، في حين يرى بعض الفقه أن التسليم يقوم على أساس عقدي، فالتسليم يمثل من وجه عقدا بين الدولة الطالبة والمطلوب منها، ولا يجوز لطرفيه الإخلال بما تضمنه من التزامات⁽²⁾.

2- لائحة المصاريف:

المصاريف التي يشار إليها هنا، هي: (تلك التي تدفع لنقل الشخص المطلوب ومتحصلات الجريمة، وأحيانا تكون لترجمة الوثائق والمستندات والطلب، وهي المصروفات عادة ما تكون على نفقة الدولة الطالبة ما لم تحدد الاتفاقيات غير ذلك)⁽³⁾، ومن الجدير أيضا أن نوضح أن مسألة تحديد عبء تلك المصاريف لم يكن محل اتجاه واحد، فهناك اتجاه يرى أن عبئها واقع على الدولة الطالبة ويمكن أن يتم تعويض الدولة المطلوب منها التسليم عن كل ما تم إنفاقه في العملية إلى غاية إتمام التسليم، وهناك اتجاه آخر يرى أن عبء هذه المصاريف يقع على كل دولة فيما يقع في حدود إقليمها من إجراءات⁽⁴⁾.

3- إعادة التسليم:

يعرف إعادة التسليم على أنه: (تصرف صادر من طرف الدولة التي حازت على الشخص المطلوب تسليمه تقوم بمقتضاها بتسليم هذا الشخص مرة ثانية لدولة أخرى بعد قيامها بمحاكمته، وترى من المحتمل إدانته)، ويكون ذلك على حالتين، أولهما أن تطلب الدولة التي سلمته بإعادة تسليمه إليها إثر جرائم ارتكبها أو لأحكام قضائية محكوم بها عليه، والاستجابة في مثل هذه الحالة تكون مؤقتة، و يجب أن تكون أيضا مؤسسة على مبررات جدية، وثانيهما أن يعاد تسليمه إلى دولة أخرى غير تلك التي سلمته بادئ الأمر، ويعرف هذا الإجراء بأنه: (الإجراء الذي تقوم من خلاله الدولة الطالبة بإعادة تسليم الشخص المطلوب -بعد تسليمه- إلى دولة ثالثة تكون قد طلبت تسليمه من قبل)⁽⁵⁾.

(1) موساوي فتحي رشدي، المرجع السابق، ص ص: 73-74.

(2) بوعلام خندق، المرجع السابق، ص 97.

(3) فريدة شبري، المرجع السابق، ص 122.

(4) بوعلام خندق، المرجع نفسه، ص 104.

(5) فريدة شبري، المرجع نفسه، ص ص: 123-124.

ثانيا: تحديات نظام التسليم:

يتفق ويجمع أغلب المهتمين والمتخصصين في علمي السياسة والقانون على أن نظام تسليم المجرمين من بين أهم الآليات التي يتمظهر فيها التعاون القضائي الدولي لمكافحة الجريمة بشكل عام، والإرهاب الإلكتروني بشكل خاص، غير أن هناك إقرار منهم بأن نظام التسليم بأحكامه المتعارف عليها في عصنا هذا لا يخلو من عيوب وتحديات تواجهه، ولاسيما في مواجهة الإرهاب الإلكتروني، وسنسوق في بحثنا هذا شيئا من التحديات والعوائق التي تواجهه في ذلك، وسيكون ذلك على النحو الآتي:

1- رفض التسليم:

يعد رفض التسليم من بين الأجوبة أو الردود التي يمكن للدولة أن تجيب بها عن طلب التسليم، فالدولة إذا ما رأت بأن قبول طلب التسليم سيكون سببا لملاحقة أو معاقبة الشخص المسلم بسبب قائم على اعتبارات عنصرية وقناعات سياسية، أو إذا ما كانت الاستجابة ستقضي إلى إحداث ضرر بمركزه أثناء المحاكمة، أو إذا تضمن مساسا أو خرقا بالمبادئ الدولية لحقوق الإنسان، فإنه من الممكن أن ترفض طلب التسليم بناء على هذه الأسباب⁽¹⁾.

وقد كان هناك حالات كثيرة لرفض التسليم، كرفض حكومة جنوب إفريقيا تسليم منجستو هيل ماريما وهو دكتاتور أثيوبي، كما رفضت السودان أيضا تسليم المتهمين على خلفية محاولة اغتيال الرئيس المصري في العاصمة الإثيوبية " أديس أبابا "، كما امتنعت فرنسا عن تسليم أبو داود إثر مصرع الفريق الأولمبي التابع للكيان الإسرائيلي في دولة ألمانيا، كما سمحت النمسا لعزة إبراهيم نائب الرئيس العراقي بالخروج من فيينا على الرغم من أنه كان متهما في ارتكاب إبادة جماعية بحق الكرد في العراق، وكان ذلك لما تمليه المصلحة السياسية للنمسا مع العراق⁽²⁾.

ولا ريب أن امتناع بعض الدول عن تسليم بعض المجرمين لاعتبارات سياسية ومصلحية يعد شكلا صارخا من أشكال الانتهاك للاتفاقيات المتعلقة بتسليم المجرمين، فالتسليم يندرج ضمن الإجراءات القانونية التي تخضع في أحكامها لنصوص المعاهدات، لذلك يتعين أن يكون ساريا تحت سلطة قانونية وقضائية، كما يتعين أيضا على الدول الالتزام به⁽³⁾.

(1) فافة لحمر، المرجع السابق، ص 27.

(2) يوسف حسن يوسف، حقوق تبادل المسجونين بين الدول وفق الاتفاقيات الدولية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015، ص 240.

(3) المرجع نفسه، ص 240.

2- الدفع بالحصانة:

تعرف الحصانة على أنها: (امتياز يقرره القانون الدولي العام أو القانون الداخلي يؤدي إلى إعفاء المتمتع من عبء أو تكليف يفرضه القانون العام على جميع الأشخاص الذين يوجدون على إقليم الدولة أو يعطيه ميزة عدم الخضوع لأحكام سلطة عامة في الدولة، وخاصة السلطة القضائية أو بعض أوجه مظاهرها)⁽¹⁾.

فاللجوء إلى الدفع بهذه الحصانة يمثل عقبة كبيرة تقف لاعتراض أحكام العدالة الدولية، وتعمل على خفض وتثدي الجهود التي تم وضعها من قبل المشرع الدولي لضمان حماية حقوق الإنسان، ولذلك فإنه من الضروري بمكان، العمل على إعادة تقييم وتنقيح بصورة عميقة لمبدأ الحصانة التي يتمتع بها الرؤساء والقادة العسكريين وكل المنتمين إلى السلطة العليا، والموظفين الدوليين⁽²⁾.

3- الدفع بحق اللجوء السياسي:

يتضح لنا من الاستتارة بما تتضمنه التشريعات الدولية المعمول بها والسارية المفعول والمتعلقة بحق اللجوء وحظر تسليمهم، أن حق اللجوء يعد عائقاً من العوائق التي تعرقل نظام تسليم المجرمين، والتي ترتب عنها ارتفاع في معدل حرص الهاربين من العدالة على طلب اللجوء بناءً على تبريرات سياسية، ومع ذلك فإن التعاون الدولي قد دعت ضرورياته ومقتضياته إلى صياغة وتشكيل استثناء على مبدأ حضر تسليم اللاجئين السياسيين، ولاسيما في الجرائم الدولية⁽³⁾.

وتعد الجرائم الإرهابية الدولية من الجرائم غير المسيّسة، وذلك بناء على الاتفاقيات المعنية بمكافحة الجريمة الإرهابية المصنفة ضمن الجيل الثاني، والتي تنص على أنه: (لا يجوز لأغراض تسليم المجرمين أو المساعدة القانونية المتبادلة، اعتبار أي جريمة من الجرائم الإرهابية المنصوص عليها في هذه الاتفاقية جريمة سياسية أو جريمة ارتكبت بدوافع سياسية، وبالتالي، لا يجوز رفض طلب تسليم المجرمين أو المساعدة القانونية المتبادلة مؤسس على مثل هذه الجريمة لمجرد أنه يتعلق بجريمة سياسية أو جريمة متصلة بجريمة سياسية أو جريمة ارتكبت بدوافع سياسية)⁽⁴⁾.

غير أن حق اللجوء السياسي يثير إشكالية كبيرة وخطيرة في تسليم الجناة والمتورطين في

(1) عبد الله بن حسين آل هادي، ضمانات الحصانة الدبلوماسية في الفقه الإسلامي والقانون الدولي: (دراسة تأصيلية مقارنة)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2016، ص 47.

(2) عبد الحق لخداري، مبدأ تسليم المجرمين ودوره في تفعيل قواعد القانون الدولي الجنائي، مجلة الباحث للدراسات الأكاديمية، المجلد 06، العدد 01، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، الحاج لخضر، جانفي 2019، ص ص: 507-525: <https://www.asjp.cerist.dz/en/article/82081>

(3) فيصل بن زحاف، المرجع السابق، ص 302.

(4) نسيب نجيب، المرجع السابق، ص ص: 129-130.

أعمال إرهابية إلكترونية، وهذا الأمر عائد إلى اختلاف النهج في التعامل مع ظاهرة الإرهاب الإلكتروني التي أشرنا إليها سابقاً، فإن كان التعامل معها وفق المعاهدات والاتفاقيات المعنية بالجريمة الإلكترونية، فإن هذه الأخيرة تسمح للدول الأطراف برفض طلبات المساعدة المتبادلة إذا كانت تتعلق بجريمة يعتبرها الطرف المطلوب منه جريمة سياسية أو جريمة مرتبطة بجريمة سياسية استناداً إلى نص المادة 3/27 أ والتي تنص على أنه⁽¹⁾: (للدولة الطرف المطلوب منها المساعدة، علاوة على أسس الرفض الواردة في الفقرة 4 من المادة 25، أن ترفض تقديم المساعدة في حال: أ- كان الطلب يتعلق بجريمة تعتبرها الدولة الطرف المطلوب منها المساعدة جريمة سياسية أو جريمة لها علاقة بجريمة سياسية...) ⁽²⁾، واستناداً إلى نص المادة 35 التي تنص على أنها: (يجوز للدولة الطرف المطلوب منها المساعدة- بالإضافة إلى أسس الرفض المنصوص عليها في المادة الثانية والثلاثون الفقرة (4) أن ترفض المساعدة إذا: 1- كان الطلب متعلقاً بجريمة يعتبرها قانون الدولة المطلوب منها المساعدة جريمة سياسية) ⁽³⁾، ولا شك أن التسليم ضمن إطار هذا النص باعتباره مظهراً من مظاهر المساعدة القانونية الدولية، أما إن كان النهج المتبع هو توظيف التشريعات الدولية المتعلقة بمكافحة الإرهاب والتصدي للظاهرة الإرهابية، فحينها يكون الإرهاب الإلكتروني مانعاً لاستعمال حق اللجوء كدفع في مواجهة طلبات التسليم بناءً على ما تضمنته من نصوص تزيح وتزيل الطابع السياسي عن جرائم الإرهاب الدولي. ومن أجل الخروج من هذه الحلقة فإن هناك من اقترح إدخال حكم خاص بشأن الإرهاب السيبراني المرتكب عن طريق الهجمات ضد البنى التحتية الحاسوبية، وذلك بالنص على عدم خضوع جرائم الإرهاب السيبراني لاستثناء الجرائم السياسية، كما أن هناك خيار آخر يقضي باستبعاد استثناء الجريمة السياسية لأفعال خطيرة يتم تحديدها سلفاً في اتفاقية الجرائم الإلكترونية، فهذا الاقتراح من شأنه أن يدفع بدفة التعاون الدولي إلى الأمام، كما أنه مقترح يسير نحو اتجاه استثناء الجريمة السياسية في القضايا الخطيرة للإرهاب، ومع ذلك تبقى هناك مشكلة فيما يتعلق باستبعاد الجريمة السياسية من قضايا الإرهاب، والتي تقرها حتى الاتفاقيات التي تستبعد الاستثناء، ألا وهي إشكالية الانسحاب منه عبر آلية التحفظ⁽⁴⁾.

(1) Marco GERCKE, Op.cit. P.220.

(2) المادة 3/27 أ من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

(3) المادة 1/35 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

(4) Ulrich SIEBER, Coopération internationale contre l'utilisation terroriste d'Internet, « Revue internationale de droit pénal », 2006/3 Vol. 77, PP. 395-449; DOI: 10.3917 / Radep.773.0395: <https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-395.htm>

ومن الجدير أن نشير إلى أن هناك دعوات مطلقة تدعو إلى إلغاء أو تضيق مبدأ حظر التسليم، ونحن نؤيد ما ذهبت إليه الأستاذة ماجدة شهباز بدوح في رجحان منطقية التضيق من المبدأ عن إلغائه، في حين أننا لا نوافقها على ما ذهبت إليه من استحسان تعداد وتحديد للأفعال التي لا تعتبر جرائم سياسية وبالتالي تخضع للتسليم والتي توجهت إليها بعض التشريعات والاتفاقيات⁽¹⁾، ذلك أن التحديد لا يتوافق أبداً مع الطبيعة المتطورة للظاهرة الإجرامية والتي تتطلب تعديلاً متصلاً لتلك النصوص والاتفاقيات، كما أن مثل هذا التحديد على مستوى التشريعات الوطنية لا يمكن أن يخدم التعاون الدولي في إطار مكافحة الجريمة بصفة عامة، إذ لا يمكن البتة أن يرد إجماع في تحديدها بين الدول، نظراً لاختلاف الأنظمة السياسية والإيديولوجيات القائمة في كل دولة، وهي أصلاً نواه الخلاف في تعريف الجرائم السياسية والتي ستسحب حتماً على تحديدها وتجري عليه.

4- الدفع بدعم ازدواجية التجريم:

يعتبر الشرط القاضي بازدواجية التجريم في الدولة الطالبة والمطلوب منها التسليم عقبة من عقبات التعاون الدولي في تسليم المجرمين، فكثير من يكون هذا الشرط غير محققاً نظراً للتباين الحاصل بين النظم القانونية من دولة لأخرى في سياسة التجريم والعقاب، إذ يمكن أن يكون الفعل المجرم مختلف التكييف القانوني بين الدولة الطالبة والمطلوب منها، وهذا ما طرح فكرة التخفيف من الاستجابة لهذا الشرط، والتي تقضي بأنه يكفي لاستقاء الشرط أن تجرم النصوص القانونية تلك الأفعال بقطع النظر عما تكيفها عليه من وصف، إلا أن هذا لا يذلل العقبة بشكل كامل، فقط تكون هناك أفعال يجرمها قانون دولة ولا يجرمها قانون دولة أخرى⁽²⁾.

فتبادل المساعدة القضائية ولاسيما تسليم المجرمين مع استقاء شرق التجريم المزدوج تقتضي توحيد التجريم، أي توحيد الجانب الموضوعي فيه، ففي مجال الجرائم الإلكترونية هناك اتفاق بين بعض الأنظمة والتشريعات الجنائية حول بعض الجرائم المترتبة بالفضاء الإلكتروني، ولكن ليس على كافتها، وحتى في ظل وجود اتفاق على تجريم بعض أشكال الإجرام السيبراني، هناك اختلاف

(1) أنظر: ماجدة شهباز بدوح، مبدأ عدم تسليم المجرمين في الجرائم السياسية، مجلة الفكر، المجلد 12، العدد 14، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، جانفي 2017، ص ص: 229-323: <https://www.asjp.cerist.dz/en/article/62393>

(2) كريمة تدرست، معوقات نظام تسليم المجرمين كآلية للتعاون القضائي الدولي لمكافحة الجريمة المنظمة عبر الوطنية، المجلة النقدية للقانون والعلوم السياسية، المجلد 02، العدد 02، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، نوفمبر 2016، ص ص: 30-57:

<https://www.asjp.cerist.dz/en/article/22163>

في العقوبات التي تقررها لها من دولة لأخرى، وهذا بطبيعة الحال سيكون عائقا حقيقيا في مسار التعاون القضائي ولاسيما ذاك التعاون الذي يكون موضوعه تسليم المجرمين⁽¹⁾.

أما فيما يتعلق بشرط ازدواجية التجريم في جريمة الإرهاب الإلكتروني فإن الأمر يضحى أكثر تعقيدا وأعمق خلافا، فبقطع النظر عن مدى توافق التشريعات الوطنية في أطروحة الإرهاب عموما والأفعال التي تتدرج ضمن دائرة الأعمال الإرهابية، وعن مدى فصل القوانين والتشريع بين الإرهاب وغيره من المفاهيم التي أشرنا إليها في سابق عناصر بحثنا، فإن هناك دولا لا تعترف أصلا بوجود إرهاب إلكتروني ولا أي شكل من أشكال الإجرام السيبراني، وفي هذه الحالة يعد التسليم في القضايا المتعلقة بالإرهاب الإلكتروني مستحيلا لانتفاء شرط التجريم المزدوج.

(¹) Jason **BARKHAM**, *Cyber Warfare, Cybercrime, and Cyber Terrorism: A Bibliographic Essay*, in : *American Society of International Law*. 2001:
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.4646&rep=rep1&type=pdf>

خاتمة

أحدث الفضاء الإلكتروني الذي طغى على المجتمع المعاصر ثورة كبرى في حياة إنسان العصر الحديث، فهو من الفضاءات التي لا يمكن بحال من الأحوال الاستغناء عنها في الكثير من المجالات الحيوية للأفراد والجماعات، فهو عماد الاقتصاديات المعاصرة للدول، وهو الآلية والسبيل إلى تحقيق المزيد من الرفاهية والتطور والازدهار في الكثير من الميادين، كما يمثل أيضا الأسلوب الأكثر فعالية وكفاءة في إدارة وتسيير العديد من البنى التحتية والقطاعات الحساسة، وصفوة ما يمكن قوله في أهمية هذا الفضاء أنه عصب الحياة الإنسانية في العصر الحديث، ولا يمكن الاستغناء عنه ولا التقليل من مهمته ومجالات استعماله، لما قد ينجر ويترتب عن ذلك من مفسد وأضرار عظيمة، وتبعات خطيرة على العديد من القطاعات الحيوية في البلاد.

لكن ظهور الفضاء الإلكتروني والاعتماد عليه بهذا الشكل الكبير والرئيسي قد عمل على خلق حالات جديدة وصورة حديثة من الصراعات الخطيرة، حيث أصبح هذا الفضاء مجالا جديدة من مجالات الحروب والصراعات بين الفواعل الدولية، وتحول عن مقصده ليكون ساحة وغى توظف فيها جميع الأساليب المعقدة في الحروب القذرة ولاسيما الإرهاب الإلكتروني الذي كما رأينا قد أثار جزعا كبيرا للدول بسبب ما يثيره من تهديدات لأمنها القومي والسلامة والأمن العالميين.

و لذلك، سعت الدول بشكل فردي وجماعي في إطار المنظمات الدولية إلى تبني سياسات واستراتيجيات لمكافحته، فعمدت إلى خلق هياكل تنظيمية لذلك، كما قامت بدعم التكنولوجيا المعاصرة لسد الثغرات الأمنية التي يمكن أن ينفلت منها المهاجمون على الفضاء الإلكتروني، كما سعت أيضا إلى بناء صرح قانونية لتجريم صور الإرهاب الإلكتروني بشكله الفعلي والهجين، وعملت أيضا على تعزيز التعاون القضائي الدولي لتحقيق هذا الغرض.

غير أن معظم السياسات التي تم وضعها في هذا المجال إلى حد الآن لا تزال قاصرة على إدراك التأمين الكامل للفضاء الإلكتروني ذلك أن الفضاء الإلكتروني هو فضاء رحب واسع، يتخطى كل الحدود ويتجاوز كل السيادة، ولا يمكن على الإطلاق أن يتم وضع سياسات أمنية داخلية إلا في إطار سياسة دولية عامة، فمشكلة الإرهاب الإلكتروني ليست مشكلة محلية، وهي تتجاوز أخطار الجريمة المنظمة، لذلك فإنه من الضروري العمل على تنسيق الجهود الدولية، ولا يمكن لهذا أن يحصل إلا إذا تقاربت وجهات النظر حول مفهوم هذه الظاهرة، وآليات مكافحتها.

ولعل تقريب هذه الجهات والرؤى الدولية هو أصعب تحدي تواجهه المساعي والجهود الدولية لمواجهة هذه الظاهرة الخطيرة، فالدول كثيرا ما تغلب عليها النزعة الفردية والنظر إلى العلاقات الدولية من منظور المصلحة من جهة، ومنطلق القوة وفرض الهيمنة من جهة أخرى، كما أن هناك دول تمتلك عداً تاريخياً قديماً مما يجعل كل طرف يتعصب لرأيه ويسفه رأي الآخر، وذلك كله على حساب الأمن والسلم العالميين.

فمكافحة الإرهاب الإلكتروني في الوضع الراهن ليست بالفعالية التي يمكن بها أن تتصدي لظاهرة كظاهرة الإرهاب الإلكتروني، فإذا أخذنا المواجهة التقنية وجدناها هشّة أمام أبسط الهجمات الإرهابية، فضلا من أن الإرهابيين قد يطورون قدراتهم الفنية في التعامل مع تلك التقنيات المستعملة، كما يمكنهم أيضا الاستعانة بالهاكرز الذين يملكون معرفة مستفيضة في مجال تقنيات ونظم المعلومات، مما يجعل الوقوف في وجه نشاطاتهم أمر بالغ الصعوبة، إن لم يكن مستحيلا.

يشكل الاستدلال على الجرائم المعلوماتية كلها وبشكل خاص جريمة الإرهاب الإلكتروني أهم آلية لمكافحة، فهو الذي يتيح للأجهزة الأمنية تقديم المتورطين في العمليات الإرهابية أمام القضاء لمحاكمتهم وإنفاذ القانون فيهم، لكن غياب أو نقص الخبرة الفنية والتقنية اللازمة لتحصيل هذه الأدلة في الكثير من دول العالم يمنح للإرهابيين الفرصة للإفلات من العقاب وهذا لعدم صحة الأدلة المستخلصة أو لعدم أصالتها وموثوقيتها، كما أن هناك غياب شبه تام للمعايير الدولية لقبول مثل هذه الأدلة أمام القضاء، كما أن الكثير من الدول لا تعترف أصلا بهذا النوع من الأدلة في أنظمتها القانونية والقضائية وهذا بلا شك يمثل منفاذا يفر منه الإرهابيون من نيل الجزاء والعقاب المستحق ويعيق التعاون القضائي بين الدول.

تعرقل حيابة القطاع الخاص على شريحة كبيرة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك للأجهزة وخدمات الاتصال الشبكي، عمليات المواجهة والحسم الأمني للنشاطات الإرهابية السيبرانية، ومع غياب الثقة المتبادلة والشفافية بين القطاع العام والخاص، فإن عمليات التنسيق تكون في حالة ركود والشلل، وهذا يعيق بشكل كبير للمواجهة الفاعلة للإرهاب الإلكتروني إذ يحول دون تقديم البيانات والمعلومات إلى الجهات الأمنية والقضائية المختصة التي تطلبها سواء لتقديم المجرمين أمام العدالة أو لتطوير الدولة لسياساتها الأمنية والدفاعية ضد اعتداءات وهجمات الإرهاب الإلكتروني.

أظهرت الدراسات أن من بين أهم الآليات الفعالة في مواجهة الإرهاب الإلكتروني هي إشراك المجتمع المدني في سياسات المواجهة، وتفعيل أدواره الأساسية، غير أن ذلك ليس بالأمر الميسر،

فالكثير من الدول ولا سيما تلك التي تتبنى أنظمة شمولية واستبدادية لا تتيح للمجتمع المدني لعب دور كبير في ذلك، خوفا منها من مزاحمتها على السلطة، كما أن منظمات المجتمع المدني في غالبيتها لا تمتلك الموارد والقدرات اللازمة لتقديم الدعم الكافي في تنفيذ سياسات مواجهة الإرهاب الإلكتروني، ضم إلى ذلك أن هناك إمكانية كبيرة لاختراق هذه المنظمات من قبل أفراد يدينون بالولاء لجماعات إرهابية، وقد حدث هذا فعلا في الكثير من الدول التي تصنف جماعة الإخوان المسلمين كجماعة إرهابية، حيث سيطرت هذه الأخيرة على الكثير من الجمعيات والأحزاب ولاسيما في جمهورية مصر العربية معقل الإخوان.

أما من الناحية التشريعية فالجهود المبذولة إلى حد الآن تعاني من قصور شديد رغم مساعي بعض الدول لوضع تشريعات خاصة بالجرائم المعلوماتية وتحديد إجراءات التحقيق فيها، فالتشريعات في جملتها لا تنص إلا فيما ندر عن جريمة الإرهاب الإلكتروني، ومع أنه من الممكن جدا تطبيق النصوص الجنائية المعنية بمكافحة الإرهاب أو تلك المعنية بالجرائم المعلوماتية إلا أن ذلك ليس بالأمر اليسير، فالقواعد الجنائية لا تفسر إلا في أضيق حدودها، ولا يجوز فيها القياس مطلقا، وهذا بكل تأكيد يجعل هيئات إنفاذ القانون في حرج حال تنفيذ مهامها، ويصعب على القضاة والمدعين للعامين تكييف الوقائع، فأزمة الشرعية الجنائية هي من بين أهم الأزمات التي تواجه جهود مكافحة الإرهاب الإلكتروني.

تتجلى المعضلة أيضا في التعاون القانوني على الصعيد الدولي في عدم توافق الدول وإجماعها على اتفاقية لمواجهة الجرائم الإلكترونية، فضلا عن الاتفاق والتوافق على اتفاقية خاصة بالإرهاب الإلكتروني، فالمصالح السياسية والتوجهات الإيديولوجية بلا شك دور مهم في عرقلة مساعي المنظمات الدولية لإيجاد صيغة قانونية متكاملة لمواجهة الإرهاب الإلكتروني، فرغم ما لاتفاقية مكافحة الجريمة الإلكترونية لمجلس أوروبا من دور كبير ومهم في إلهام للتشريعات الداخلية إلا أنها لا تعد محط إجماع بين الدول، وإذا ما تم اقتراح صك دولي متعلق بالإرهاب الإلكتروني فإن الأمر سيكون بلا شك أكثر تعقيدا، وأدعى للخلاف أكثر، لعدم اتفاقها أساسا على مفهوم الإرهاب بشكل عام والإلكتروني منه بشكل خاص، وبذلك يكون الصك الجديد غير قابل للتطبيق والإنفاذ من قبل الكثير من الدول وهذا يتنافى بشكل مطلق مع اعتبارات التعاضد ومقتضيات التآزر في مواجهة هذه الظاهرة.

كما تعد جهود هيئة للأمم المتحدة أيضا جهودا محدودة إذا ما نظرنا إلى حجم الخطر الذي يديق ناقوسه يوما بعد يوم تزايد الهجمات الإجرامية والإرهابية على الفضاء الإلكتروني، فبالمقارنة

مع ما تبذله هيئة الأمم المتحدة من جهود في الوقت الراهن وبين الأخطار التي تتهدد الفضاء الإلكتروني وعدد الهجمات اليومية والنشاطات الإرهابية التي تم رصدها، نجد أنه ما من تناسب بينها، فالكفة غالبية ومائلة للإرهابيين على حساب هيئة الأمم المتحدة التي لم يصدر عنها أي وثيقة قانونية ملزمة بشأن الإرهاب الإلكتروني، ويعد مجلس الأمن الهيئة الأممية التي تمتلك صلاحية إصدار قرارات ملزمة، وهي شبه غائبة عن واقع ما يحدث من إرهاب وعنف إلكتروني.

يصعب التعاون القضائي الدولي في الجرائم عموماً، فالإجراءات القانونية التي يتعين اتخاذها والمنافذ التي يجب النفاذ منها تتفاوت صعوبتها من نظام قانوني لآخر، وتتزايد هذه الصعوبة أمام هذا النوع المستحدث من الجرائم، فالتعاون القضائي الدولي في مجال مكافحة الإرهاب الإلكتروني لا يزال في طوره الأول، لذلك فإن هناك صعوبات دولية قائمة فيما يتعلق بأسس التعاون القضائي الدولي والمساعدات القضائية.

إن المساعدة والتعاون للقضائية في مجال الإرهاب الإلكتروني كثيراً ما يكون عديم الجدوى إذا ما تم وفقاً للقواعد القانونية التي تتضمنها التشريعات الداخلية واتفاقيات التعاون القضائي الجماعية والثنائية، فالتعاون القضائي في جوهره وفي صلب أهدافه يرمي إلى ضمان تقديم الجناة أمام المحاكم لاستفتاء حق المجتمع في العقاب، ومن أجل ذلك يجب أن يكون هناك من الأدلة ما يضمن هذا الحق، وفي غياب تعاون سريع وعاجل يضمن سلامة الأدلة الجنائية الإلكترونية فإن جهود التعاون تؤول إلى الفشل.

يعترض التعاون القضائي أيضاً في مجال توفير الأدلة الرقمية سواء عن طريق الإنابة القضائية أو من خلال تقديم المعلومات الاستدلالية لمشكلة كبيرة، وهي أن كل قواعد تنفيذ الإنابات وأشكال التعاون الأخرى خاضعة للقوانين الوطنية، وليست كلها مجمعة على حجية الأدلة الرقمية، ولا تعترف كلها بقوتها الثبوتية في المواد الجنائية، ضم إلى ذلك أن الكثير من الأجهزة القضائية ومؤسسات إنفاذ القانون لا تمتلك الموارد التقنية والفنية لاستخلاص مثل هذه الأدلة وحفظها، وهذا يؤثر بشكل رئيسي على جهود التعاون للقضائي الدولي في مجال مكافحة الإرهاب الإلكتروني.

يؤثر عدم التوافق على المفاهيم الأساسية ولاسيما مفهوم الإرهاب الإلكتروني بشكل مباشر على وتيرة التعاون للقضائي الدولي وسرعته، فالخلاف القائم بين الدول حول الأفعال والأنشطة الداخلة في دائرة الإرهاب هي محل خلاف شديد بين الدول مع إجماعها على تجريم الإرهاب، فالأفعال التي تعتبر عند الكيان الإسرائيلي إرهاباً هي عند الفلسطينيين دفاعاً شرعياً وكفاحاً ضد الاستعمار، والجماعات التي تصنفها مصر على أنها تنظيمات إرهابية وتخريرية لا تعدّها قطر

وتركيا كذلك، وما نراه في تركيا من وصف لحزب العمال الكردستاني إرهابا لا توافق عليه للكثير من الدول، وبالتالي فإن أي هجوم إلكتروني أو أي نشاط على الفضاء الإلكتروني من تلك الجماعات والتنظيمات لن يكون أبدا محل إجماع بين الدول، وهذا ما يعرقل بالفعل عملية التعاون القضائي الدولي.

وبناء على ما سبق، فإنه من الضروري بمكان، العمل على بذل جهد أكبر، وإعادة تنظيم الصف الدولي للقيام بما يحفظ الأمن والسلم العالميين من التهديدات التي يشكلها الإرهاب في الوسط الإلكتروني، ويجب على الدول أن تعي أن الخلافات السياسية يجب ألا تكون سببا لتقديم ملاذات آمنة للمتورطين في أعمال إرهابية، ويجب أن تدرك أيضا أن الإرهاب الذي يمارسه تنظيم أو فرد ضد دولة معينة لا يستبعد أن تكون في يوم من الأيام ضحاياه من الدول الراعية لذلك الإرهاب أو تلك التي تقدم له ملاذا آمنا بدعوى حرية التعبير والحق في حرية الرأي.

ومما تقدم ذكره، نرى أنه من الضروري أن يكون هناك:

1/ إجماع على تعريف موحد للإرهاب الإلكتروني، وبداية ذلك بالاتفاق على اصطلاح واضح الدلالة على هذه الظاهرة بدلا من التشتت بين اصطلاح الإرهاب الإلكتروني والإرهاب السيبراني، وذلك تقاديا لتمجيع دعم الأبحاث والدراسات الفنية والتقنية التي تعنى بإيجاد حلول عملية لتأمين الفضاء الإلكتروني، ثم بعد ذلك يتعين الوصول إلى تعريف دولي موحد ومجمع عليه من كافة الدول في إطار جهة قانونية دولية معترف بها، أو جهة قانونية دولية ملزمة، لما يعود به من وحدة على نصوص التجريم، والحيلولة دون تسييس هذه الظاهرة، ودفعاً للبس الذي يمكن أن يقع بين الظاهرة وبين غيرها من المفاهيم المشروعة كالدفاع الشرعي الإلكتروني، والنضال الإلكتروني في تقرير المصير، والاحتياجات الإلكترونية وما إلى ذلك من المفاهيم الأخرى.

2/ بناء هيكل أو جهاز أو منظمة أو أي كيان آخر تشرف عليه هيئة الأمم المتحدة للقيام بأعمال حوكمة الإنترنت، وحوكمة الأمن الإلكتروني بشكل خاص، وذلك بمشاركة جميع الفواعل الدولية، سواء أكانت منظمات أو دول، لقطع دابر الخلاف والتنازع بين أصحاب المصالح، ودرء لتحكم وسيطرة جهة معينة على عمليات إدارة الإنترنت، ليكون التركيز بعد ذلك على أساليب وآليات التصدي والمواجهة لهذه الظاهرة وكل صور الاستغلال الإجرامي للفضاء السيبراني.

3/ العمل على بناء هيكل آخر مستقل ومنظم تتناط به مسؤولية التحقيق في الجرائم المعلوماتية بما في ذلك جريمة الإرهاب الإلكتروني، أو إلحاقها بمراكز التحقيقات الجنائية أو

معاهد الطب الشرعي كفروع متخصصة في مثل هذه الجرائم الخطيرة، ومن الملاحظ أن هذه النقطة تأتي أهميتها من تفاقهم حالات الإفلات من العقاب وعطيل العدالة بسبب عدم وجود متهم تسند إليه مسؤولية تنفيذ هذه الجرائم لما عالجناه من مميزات وخصائص لهذه الظاهرة والتي تقتضي استحداث أجهزة متخصصة للتحقيق فيها وجمع الأدلة على مرتكبيها.

وجدير بالإشارة إلى أن هيكلا كهذا يجب أن يكون تأسيسه لا على الصعيد الوطني فقط، بل يجب أيضا أن يكون على الصعيدين الدولي والإقليمي، ولعل المنظمات الشرطية الدولية والإقليمية كمنظمة الإنتربول واليوروبول والأفريبول هي أحسن وسط يمكن أن تتأسس فيه هياكل مثل هذه، إذ هي المنافذ الأكثر مواءمة للعناية بالجوانب التحقيقية في جرائم الإرهاب الإلكتروني.

4/ تعزيز الشراكة بين القطاع العام والخاص لمواجهة هذه الظاهرة عبر تعزيز الثقة وتبادلها بين القطاعين، وخلق آليات للتعاون فيما بينها ولاسيما الآليات القانونية التي تضمن الحقوق وتحدد المسؤوليات، والتفعيل الحقيقي لمبادئ وأسس الحوكمة، بما في ذلك تحديد المسؤوليات التي تقع على كل قطاع في إطار سياسة محددة المعالم لحماية الفضاء الإلكتروني، ودعم الشفافية والنزاهة في ذلك، خاصة فيما يتعلق بتقديم كامل البيانات والمعلومات المتعلقة بالمخاطر التي تهدد هذا الفضاء، وأحدث الهجمات التي تعرض لها، وذلك من أجل المساهمة في بناء سياسات أمنية موائمة لما يستجد من أشكال وصور الاعتداء على الأنظمة، وتحديث استراتيجيات وخطط المواجهة، وأيضا تقديم المعلومات الاستدلالية إلى جاهد إنفاذ القانون.

5/ القيام بتحديث التشريعات الوطنية بما يتناسب مع طبيعة الجرائم الإلكترونية، حيث يجب أن تتضمن نصا صريحا في تجريم الإرهاب الإلكتروني أو تخصيص تشريعات جنائية خاصة تتناول بصفة خاصة هذه الجريمة وتحدد أركانها وصورها وأشكالها والأفعال التي تندرج تحت وصفها، كما يجب أيضا القيام بصياغة معاهدات ذات نطاق دولي تركز بشكل خاص على معالجة ظاهرة الإرهاب الإلكتروني على غرار سائر الصكوك الدولية المعنية بمكافحة الظاهرة الإرهابية، ويجب على مجلس الأمن أن يتعامل بموجب قراراته بالجدية الكاملة في توجيه العمل الدولي لمواجهتها وتوحيدها بموجب قرار ملزم للدول الأعضاء فيه شأنه في ذلك شأن القرارات الصادرة في الإرهاب التقليدي بعد أحداث الحادي عشر من سبتمبر.

6/ توجيه الجهود نحو بناء أنظمة وبرامج لإحباط الهجمات الإرهابية السيبرانية على الصعيد الوطني من جهة، وعلى الصعيدين الدولي والإقليمي من جهة أخرى، وهذا من خلال تشجيع البحث التقني والبرمجي وتوفير الوسائل والموارد اللازمة لذلك، بالإضافة أيضا إلى تكوين الخبرات

الفنية للعمال والموظفين في المنظومات والمؤسسات وبصفة خاصة في تلك التي تعتمد بشمل رئيسي على نظم المعلومات والاتصالات، وتوفير التوعية اللازمة للموظفين بأساليب الحماية التقنية المتاحة، وأسس التعامل مع الفضاء الإلكتروني، العادات غير السليمة التي يتم القيام لها والتي تعرض الأجهزة والشبكات لمخاطر الاختراق والهجمات الفيروسية الحادة، وما إلى ذلك من صور النشاط الإرهاب على الفضاء السيبراني.

7/ بناء الوعي وتنقيف أصحاب المصلحة والمستخدمين الأفراد بخطورة هجمات الإرهاب الإلكتروني، ووضع مجموعة من التوصيات والتوجيهات التي يمكن بواسطتها حماية أجهزتهم وشبكات الاتصال الخاصة بهم، ووضع بين أيديهم أرقام خضراء للاتصال على وجه الاستعجال بالأجهزة الأمنية في حالة تعرضهم لهجوم أو نشاط مشبوه، أو الاتصال بخبراء الطب الشرعي الرقمي الذين يعملون على وقف الهجوم واسترداد البيانات التي يمكن استردادها وجمع المعلومات الاستدلالية لعرضها أمام القضاء متى دعت الضرورة إلى ذلك.

8/ السهر على تشكيل أقطاب أمنية متخصصة في الجرائم المعلوماتية، كتشكيل لجان الشرطة الإلكترونية التي تراقب حركات مرور المعلومات والبيانات، وفلترة محتويات الإنترنت غير المشروعة، وتزويد هذه اللجان الأمنية بكل الآليات والموارد التقنية التي تمكنهم من القيام بعملهم على أكمل وجه، كما يجب على الدولة السهر على إنشاء جيوش إلكترونية تتاط بها مهام الدفاع العسكري الإلكتروني ضد أي عدوان إرهابي ضد مصالحها وبنائها التحتية.

9/ تعزيز عمل المنظمات الشرطة الدولية والإقليمية في مكافحة الإرهاب الإلكتروني من خلال تمكينها من الاستفادة في إطار عملها بكل ما يستحدث من تقنيات وبرمجيات إلكترونية، ومنحهم الغطاء القانوني اللازم الذي يضيف على إجراءاتهم الشرعية الجنائية، وضمان حماية موظفيها وأعضائها من أي شكل من أشكال الابتزاز الإلكتروني.

10/ تعزيز التعاون القضائي الدولي، وذلك من خلال استحداث اتفاقيات جديدة بالإضافة إلى تعديل القوانين الوطنية لتتناسب مع الاعتبارات التي يطرحها الفضاء الإلكتروني، إذ يجب العمل على صياغة نصوص تشريعية تكفل الاستجابة السريعة لطلبات الإنابة القضائية وتقديم المعلومات الاستدلالية وطلبات تسليم الإرهابيين الإلكترونيين، ويجب فض هذا التناقض الحاصل بين الإجراءات المعمول بها في الوقت الراهن والطبيعة الاستثنائية لجريمة الإرهاب الإلكتروني.

قائمة المراجع

قائمة المراجع

أولاً: باللغة العربية:

1- الكتب:

1. أ. ي. بالي، ن. ب. مارين، موسوعة الحرب الإلكترونية، ترجمة: (يوسف إبراهيم الجهماني)، الطبعة الأولى، دار الحوار، سورية، 1992.
2. إبراهيم الحيدري، سوسيولوجيا العنف والإرهاب، الطبعة الأولى، دار الساقى، لبنان 2015.
3. إبراهيم جابر السيد، الاتجاهات الحديثة في الإعلام الصحفي، الطبعة الأولى مؤسسة طيبة للنشر والتوزيع، القاهرة، 2015.
4. إبراهيم جودة علي العاصي، دور التشريعات الدولية الخاصة بحقوق الإنسان في الحد من سيادة الدولة، الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، مصر، 2019.
5. أبو العلا ماضي، جماعات العنف المصرية وتأويلاتها للإسلام: (الجزور التاريخية- الأسس الفكرية-المراجعات)، الطبعة الأولى، مكتبة الشروق الدولية، القاهرة، 2006.
6. أبو بكر محمود الهوش، أدوات البحث عن المعلومات في البيئة الرقمية، الطبعة الأولى، دار حميثرا للنشر، مصر، 2018.
7. أحمد عطية الله، القاموس السياسي، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1968.
8. أحمد فايز صالح، دور المحافظين الجدد في السياسة الخارجية الأمريكية، الطبعة الأولى باحث للدراسات الفلسطينية والاستراتيجية، بيروت، لبنان، 2011.
9. أدولف هتلر، كفاحي، ترجمة: (لويس الحاج)، الطبعة الثانية، منشورات بيسان (د.م.ن)، 1995، ص 162.
10. أردلان نور الدين محمود، المسؤولية الجزائية لرئيس الدولة في التشريعات الداخلية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2014.

11. أزهـر عبد الأمير الفتلاوي، العمليات العدائية طبقا لقواعد القانون الدولي الإنساني الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، مصر، 2018.
12. أسامة سمير حسين، الاحتيال الإلكتروني:(الأسباب والحلول)، الطبعة الأولى الجنادرية للنشر والتوزيع، الأردن، 2011.
13. أسامة سمير حسين، ثورة الحاسوب والاتصالات، الطبعة الأولى، الجنادرية للنشر والتوزيع، الأردن، 2012.
14. أسامة عبد السلام السيد، الاقتصاد الرقمي، الطبعة الأولى، دار غيداء للنشر والتوزيع، الأردن، 2019.
15. إسماعيل أحمد ياغي، الإرهاب والعنف في الفكر الصهيوني، الطبعة الأولى، مكتبة العبيكان، الرياض، 2003.
16. ألكسندر سولجيتسين، أرخبيل غولاغ، ترجمة(نجم سلمان الحجار)، دار علاء الدين ودار ومؤسسة رسلان، دمشق، سوريا، 2017.
17. أنتوني أرنوف، العراق:(منطق الانسحاب)، ترجمة:(محمود برهوم ورعدة محمد حسن عزيزية)، الطبعة الأولى، المؤسسة العربية للدراسات والنشر، بيروت، 2006.
18. إيريك جنسن، الفقر والتعليم:(ماذا يفعل الفقر بمخ أطفالنا؟ وماذا تفعل المدرسة لتصلح ما أفسده الفقر؟)، ترجمة(صفاء الأعسر)، الطبعة الأولى، المركز القومي للترجمة القاهرة، 2015.
19. إيلاف فاخر كاظم علي، مخاطر العمليات المصرفية الإلكترونية:(دراسة مقارنة)، الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، القاهرة، مصر، 2019.
20. إيمان بن سالم، جريمة التجنيد الإلكتروني وفقا لقانون العقوبات الجزائري، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2018.
21. أيمن عبد الله فكري، الجرائم المعلوماتية:(دراسة مقارنة في التشريعات العربية والأجنبية) الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2014.
22. إيهاب أبو العزم، مفاهيم تكنولوجيا المعلومات، الرخصة الدولية لقيادة الحاسب الآلي الإصدار الرابع، الطبعة الأولى، دار الحكمة للطباعة والنشر والتوزيع، ليبيا، 2012.

23. إيهاب خليفة، القوة الإلكترونية: (كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت)، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2017.
24. إيهاب خليفة، مجتمع ما بعد المعلومات: (تأثير الثورة الرابعة على الأمن القومي) الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2019.
25. برامود كيه نايار، مقدمة إلى وسائل الإعلام الجديدة والثقافات الإلكترونية، ترجمة (جلال الدين عز الدين علي)، مؤسسة هنداي سي آي سي، المملكة المتحدة، 2017.
26. بروس شنابير، المعلومات وجالوت: (المعارك الخفية لتجميع بياناتك والسيطرة على عالمك)، ترجمة: (أحمد مغربي)، الطبعة الأولى، منتدى العلاقات العربية والدولية، قطر 2017.
27. بسام اسخيطه، قصة محاكم التفتيش في العالم، الطبعة الأولى، دار هيا للنشر والتوزيع، دمشق، 2000.
28. بشرى حسين الحمداني، القرصنة الإلكترونية: (أسلحة الحرب الحديثة)، الطبعة الأولى، دار أسامة للنشر والتوزيع ونبلاء ناشرون وموزعون، الأردن، 2014.
29. بطاينة، فواد، الأمم المتحدة: (منظمة تبقي ونظام يرحل)، الطبعة الأولى، المؤسسة العربية للدراسات والنشر ودار الفارس للنشر والتوزيع، الأردن، 2002.
30. بلقاسم سلاطينية وآخرون، علم الاجتماع الإعلامي، الطبعة الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2012.
31. بهاء المري، موسوعة المري الجنائية، الجرائم الاقتصادية الشائعة، الجزء الأول الطبعة الثانية، العربية للنشر والتوزيع، (د.ب.ن)، 2019.
32. جاسم محمد البصيلي، الحرب الإلكترونية: (أسسها وأثرها في الحروب)، الطبعة الثانية، المؤسسة العربية للدراسات والنشر، بيروت، 1989.
33. جاك فرجيس، جرائم الدولة: (الكوميديا القضائية)، ترجمة: (حسين حيدر)، الطبعة الأولى، دار عويدات للنشر والطباعة، لبنان، 2004، ص 93.
34. جلاء أحمد يس، الحوسبة السحابية للمكتبات: (حلول وتطبيقات)، الطبعة الأولى العربي للنشر والتوزيع، القاهرة، 2014.

35. جهاد عودة، هيكل العلاقات العربية الأمريكية في مجال مكافحة الإرهاب، المكتبة الأكاديمية، القاهرة، مصر، 2010.
36. جوانيتا إلياس وبيتر ستش، أساسيات العلاقات الدولية، ترجمة: (محيي الدين حميدي)، الطبعة الأولى، دار الفرقد للطباعة والنشر والتوزيع، سورية، 2016.
37. جورج ريتزر، العولمة: (نص أساس)، ترجمة: (السيد إمام)، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2015.
38. جوزيف إس. ناي، مستقبل القوة، ترجمة: (أحمد عبد الحميد نافع)، مراجعة: (السيد أمين شبلى)، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2015.
39. جوزيف س. ناي، القوة الناعمة: (وسيلة النجاح في السياسة الدولية)، ترجمة: (محمد توفيق البجيرمي)، الطبعة العربية الأولى، مكتبة العبيكان، المملكة العربية السعودية، 2007.
40. جوزيف فرانكل، العلاقات الدولية، ترجمة: (غازي عبد الرحمن القصيبي)، الطبعة الثانية، مطبوعات تهامة، جدة، المملكة العربية السعودية، 1984.
41. جون ميرشايمر، مأساة سياسة القوى العظمى، ترجمة: (مصطفى محمد قاسم) النشر العلمي والمطابع، جامعة الملك سعود، المملكة العربية السعودية، 2012.
42. جويل كرتمن، موت النقود، ترجمة: (محمد بن سعود بن محمد العصيمي)، الطبعة الأولى، دار الميمائن للنشر والتوزيع وبنك البلاد، الرياض، المملكة العربية السعودية 2010.
43. حسن ظاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.
44. حسن عماد مكاي، تكنولوجيا الاتصال الحديثة في عصر المعلومات، الطبعة الثانية، الدار المصرية اللبنانية، القاهرة، 1997.
45. حسن فراج حسن، تكنولوجيا الإقناع في تصميم مواقع الصحف الإلكترونية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر.
46. حسين العزاوي، موقف القانون الدولي من الإرهاب والمقاومة المسلحة، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2013.

47. **حسين عماد مكايي**، تكنولوجيا الاتصال الحديثة في عصر المعلومات، الطبعة الأولى، الدار المصرية اللبنانية، القاهرة، 1993.
48. **حسين مصطفى هلالى**، إيمان صالح حسن عبد الفتاح، ريم الألفي، غريب جبر غنام، محمد محمد الألفي، الإدارة الإلكترونية، الطبعة الأولى، دار السحاب للنشر والتوزيع مصر، 2010.
49. **حسين هاشمي**، الإرهاب بين الفقه الإسلامي والقانون الدولي، الطبعة الأولى مركز الحضارة لتنمية الفكر الإسلامي، بيروت، 2014.
50. **حنان يوسف**، الإعلام والسياسية: (مقاربة ارتباطية)، الطبعة الثانية، أطلس للنشر والإنتاج الإعلامي، القاهرة، 2006.
51. **حيدر أدهم عبد الهادي**، دراسات في قانون حقوق الإنسان، دار حامد للنشر والتوزيع الطبعة الأولى، 2009.
52. **خالد أحمد علي محمود**، اقتصاد المعرفة وإدارة الأزمات المالية في إطار المؤسسات الاقتصادية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2019.
53. **خالد أحمد علي محمود**، اقتصاد المعرفة وإدارة الأزمات المالية في إطار المؤسسات الاقتصادية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2019.
54. **خالد بن سليمان الغنبر وسليمان بن عبد العزيز بن هيشة**، الاصطياد الإلكتروني: (الأساليب والإجراءات المضادة)، الطبعة الأولى، مركز التمييز لأمن المعلومات، جامعة الملك سعود، الرياض، 2009.
55. **خالد بين سليمان الغنبر ومحمد بن عبد الله القحطاني**، أمن المعلومات بلغة ميسرة، الطبعة الأولى، مركز التمييز لأمن المعلومات، جامعة الملك سعود، الرياض، 2009.
56. **خالد محمد غازي**، الأصابع الخفية: (التوظيف الإعلامي السياسي لشخصية الجاسوس)، وكالة الصحافة العربية، الجيزة، مصر، 2015.
57. **خالد مرزوق سراج العتيبي**، الجوانب الإجرائية في الشروع في الجرائم المعلوماتية الطبعة الأولى، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2012.

58. خضر مصباح إسماعيل طيطي، إدارة المعرفة: (التحديات والتقنيات والحلول) الطبعة الأولى، دار الحامد للنشر والتوزيع الأردن، 2010..
59. دفيد كين، حرب بلا نهاية: (وظائف خفية للحرب على الإرهاب) ترجمة (معين الإمام)، الطبعة العربية الأولى، العبيكان للنشر، الرياض، المملكة العربية السعودية، 2008.
60. دون إيبرلي، نهوض المجتمع المدني العالمي: (بناء المجتمعات والدول من أسفل إلى أعلى)، ترجمة: (لميس فؤاد يحيى)، الطبعة العربية الأولى، الأهلية للنشر والتوزيع الأردن، 2011.
61. نياض موسى البدانة، الإرهاب المعلوماتي: (التعريف-المفهوم-المجالات-النتائج) الحلقة العلمية: الإنترنت والإرهاب، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، القاهرة، 2008.
62. نياض بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية الرياض، المملكة العربية السعودية، 2015.
63. رامي عطا صديق وفاطمة شعبان أبو الحسن، الإعلام والتنمية في مواجهة الإرهاب: (دليل مصطلحات)، الطبعة الأولى، أطلس للنشر والإنتاج الإعلامي، 2017.
64. راني محمد خريس، الخطاب الصحفي الفلسطيني تجاه المقاومة الفلسطينية، الطبعة الأولى، مركز الزيتونة للدراسات والاستشارات، بيروت، لبنان، 2016.
65. راي بوش، الفقر والليبرالية الجديدة: (الاستمرارية وإعادة الإنتاج في جنوب العالم) ترجمة: (إلهام عيداروس ووليد سليم)، الطبعة الأولى، المركز القومي للترجمة، القاهرة 2015، ص 114.
66. رضوى الخولي، حوكمة الإنترنت، سلسلة أوراق الحق في المعرفة، مركز دعم لتقنية المعلومات، القاهرة، (د.س.ن.).
67. رفيق عبد السلام، الولايات المتحدة الأمريكية بين القوة الصلبة والقوة الناعمة، الطبعة الرابعة، مركز صناعة الفكر للدراسات والأبحاث، لبنان، 2015.

68. زروال معزوزة، بلغازي نور الدين، الإرهاب الإلكتروني للأمن المعلوماتي، المصنف الجماعي: الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، الجزء الأول، الطبعة الأولى المركز الديمقراطي العربي، ألمانيا، جويلية 2020.
69. زياد محمد السبعراوي ومجيد خضر السبعراوي، جريمة قتل الحسين وآل بين النبوة عليهم السلام: (رؤية معاصرة في القانون الجنائي الداخلي والخارجي)، الطبعة الأولى المركز العربي للنشر والتوزيع، القاهرة، مصر، 2018.
70. ستيفن إم. آر. كوفي، ريبكا آلا. ميريل، سرعة الثقة: (الشيء الذي يغير كل شيء) ترجمة (نشوى ماهر كرم الله)، الطبعة العربية الأولى، مكتبة العبيكان، المملكة العربية السعودية، 2014.
71. السعيد مبروك إبراهيم، المعلومات: (ودورها في دعم واتخاذ القرار الاستراتيجي) الطبعة الأولى، المجموعة العربية للتدريب والنشر، مصر، 2012.
72. سلمان علي حمادي الحلبوسي، المسؤولية المدنية الناشئة عن إفشاء السر المهني: (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012.
73. سليمان الطعاني، الوجيز في التربية الإعلامية، الطبعة الأولى، دار الخليج للنشر والتوزيع، عمان، الأردن، 2020.
74. سمية بو مروان، الحكومة الإلكترونية ودورها في تحسين أداء الإدارات الحكومية: (دراسة مقارنة)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2014.
75. سميرة بيطام، حجية الدليل البيولوجي أمام القاضي الجنائي، أمواج للنشر والتوزيع عمان، الأردن، 2015.
76. سيجموند فرويد، الأنا والهو، ترجمة (محمد عثمان نجاتي)، الطبعة الرابعة، دار الشروق، بيروت والقاهرة، 1982.
77. سيجموند فرويد، الحب والحرب والحضارة والموت، ترجمة (عبد المنعم الحفني) الطبعة الأولى، دار الرشاد للطبع والنشر والتوزيع، القاهرة، 1992.

78. سيد حسب الله، أحمد محمد الشامي، الموسوعة العربية، المجلد الأول، المكتبة الأكاديمية، مصر، 2001.
79. سيف الهرمزي، مقتربات القوة الذكية الأمريكية كآلية من آليات التغيير الدولي: الولايات المتحدة الأمريكية (نموذجاً)، الطبعة الأولى، المركز العربي للأبحاث ودراسة السياسات، قطر، 2016.
80. شفيق حسنين، الإعلام الجديد والجرائم الإلكترونية: (التسريبات، التجسس الإلكتروني، الإرهاب)، دار فكر وفن للطباعة والنشر والتوزيع، مدينة السادس من أكتوبر 2014.
81. صابر منصور، حروب الجيل الرابع، الطبعة الأولى، مؤسسة دار الفرسان للنشر والتوزيع، القاهرة، 2016.
82. صباح نوري علوان العجيلي، استراتيجية حروب التحرير، الطبعة الأولى، مركز الكتاب الأكاديمي، الأردن، 2015.
83. صفاء فتوح جمعة، مسئولية الموظف العام في إطار تطبيق نظام الإدارة الإلكترونية الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2014.
84. صلاح محمد عبد الحميد ويمنة عاطف، الإعلام والفضاء الإلكتروني، الطبعة الأولى، أطلس للنشر والإنتاج الإعلامي، الجيزة، 2015.
85. صمويل هنتجتون، القوة العظمى الانفرادية: (البعد الجديد للقوة)، الطبعة الأولى مركز فلسطين للدراسات والبحوث، قطاع غزة، 1999.
86. ضرغام جابر عطوش آل مواش، جريمة التجسس الإلكتروني: (دراسة مقارنة) الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2017.
87. ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي: (دراسة مقارنة) الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، مصر، 2017.
88. طارق عفيفي صادق أحمد، نظرية الحق، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2016.
89. طلعت جواد لحي الحديدي، مبادئ القانون الدولي العام في ظل المتغيرات الدولية: (العولمة)، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2012.

90. طلعت مصطفى السروجي، رأس المال الاجتماعي، الطبعة الأولى، مكتبة الإنجلو المصرية، القاهرة، مصر، 2009.
91. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني سلسلة أوراق، العدد 23، وحدة الدراسات المستقبلية، مكتبة الإسكندرية، الإسكندرية، مصر 2016.
92. عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2009.
93. عامر قنديلجي، التوثيق الإعلامي والأرشيف الصحفي، دار اليازوري للنشر والتوزيع، الأردن، 2014.
94. عبد الصبور عبد القوي علي المصري، التجارة الإلكترونية والقانون، الطبعة الأولى دار العلوم للنشر والتوزيع، القاهرة، 2009.
95. عبد العال الديربي ومحمد صادق إسماعيل، الجريمة الإلكترونية: (دراسة قانونية قضائية مقارنة: مع أحد التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت) الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.
96. عبد العزيز بن سعد الغانم، المحكمة الإلكترونية: (دراسة تأصيلية مقارنة)، دار جامعة نايف للنشر، الرياض المملكة العربية السعودية، 2017.
97. عبد القادر بن عبد الله الفتوخ، الإنترنت: (للمستخدم العربي)، الطبعة الأولى مكتبة العبيكان، الرياض، 2001.
98. عبد القادر بن عبد الله الفتوخ، الجريمة في الأنترنت: وطرق الحماية منها، مكتبة العبيكان، الرياض، 2012.
99. عبد القادر زهير النقوزي، المفهوم القانوني لجرائم الإرهاب الداخلي والدولي منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2008.
100. عبد القادر محمد الأسطة، أساسيات الإدارة الاستراتيجية الحديثة، الطبعة الأولى الأكاديميون للنشر والتوزيع، الأردن، 2016.

101. عبد الله بن حسين آل هادي، ضمانات الحصانة الدبلوماسية في الفقه الإسلامي والقانون الدولي: (دراسة تأصيلية مقارنة)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض المملكة العربية السعودية، 2016.
102. عبد الله بن عبد العزيز الموسى، مقدمة في الحاسب الآلي، الطبعة الأولى، مكتبة الملك فهد الوطنية، الرياض، 2010.
103. عبد الله جعفر كوفلي، العمل الأمني الناجح: (دراسة نظرية-تحليلية)، الطبعة الأولى، دار الخليج للصحافة والنشر، الأردن، 2019.
104. عبد الله حسن، إدارة المعرفة وتكنولوجيا المعلومات، الطبعة الأولى، دار المعترف للنشر والتوزيع، الأردن، 2015.
105. عبد المجيد مبلغ، الإرهاب تعريفه وآليات مكافحته، الطبعة الأولى، مركز الحضارة لتنمية الفكر الإسلامي، بيروت، 2015.
106. عبد الناصر موسى، مرض الوسواس القهري: (الأسباب-الأعراض-الوقاية والعلاج)، الطبعة الأولى، دار خالد اللحياني للنشر والتوزيع، الأردن، 2017.
107. عزة علي محمد الحسن، الحماية القانونية لبرامج الحاسب الآلي، الطبعة العربية الأولى، دار الجنان للنشر والتوزيع، الأردن، 2011.
108. عصام عبد الفتاح، القيصر: (التحدي.. الإرادة.. صناعة عالم جديد)، الطبعة الأولى، كنوز للنشر والتوزيع، القاهرة، 2015.
109. علاء بن محمد صالح الهمص، وسائل التعرف على الجاني، الطبعة الأولى، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2012.
110. علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، الطبعة الثانية، دار المناهج للنشر والتوزيع، سلطنة عمان، 2002.
111. علي عبود المحمداوي، الفلسفة والإرهاب أو في سلم السؤال وعنف الجواب: (سرد في الجريمة المنظمة ضد العقل)، الطبعة الأولى، دار ومكتبة عدنان، بغداد، 2016.
112. علي بن عبد الله عسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، الطبعة الأولى مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

113. علي بن عبد الله عسيري، الإرهاب والإنترنت، الإرهاب والقرصنة البحرية، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2006.
114. علي حرب، ثورات القوة الناعمة في العالم العربي: (من المنظومة إلى الشبكة) الطبعة الثانية، الدار العربية للعلوم ناشرون، لبنان، 2012.
115. علي زياد العلي، المرتكزات النظرية في السياسة الدولية، الطبعة الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2017.
116. علي عباس مراد، الأمن والأمن القومي: (مقاربة نظرية)، الطبعة الأولى، ابن النديم للنشر والتوزيع ودار الروافد الثقافية ناشرون، الجزائر-لبنان، 2017.
117. علي محمد الحاج حسين، الحرب الناعمة الأسس النظرية والتطبيقية، الطبعة الأولى، المركز الإسلامي للدراسات الاستراتيجية العتبة العباسية المقدسة، دون بلد النشر 2018.
118. عماد الدين الجبوري، الفكر الإسلامي بين النظرية والواقع، الطبعة الثانية، " E- Kutub Ltd " للنشر، لندن، إنجلترا، يوليو 2015.
119. عمر أحمد أبو هاشم الشريف، أسامة محمد عبد العليم، هشام محمد بيومي الإدارة الإلكترونية: (مدخل إلى الإدارة التعليمية الحديثة)، الطبعة الأولى، دار المناهج للنشر والتوزيع، الأردن، 2013.
120. عمرو العروسي، الشرطة والحرب الأهلية: (دراسة تطبيقية في القانون الدولي الإنساني)، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014.
121. عودة يوسف سلمان الموسوي، جريمة استهداف إثارة الحرب الأهلية عبر الإعلام: (دراسة مقارنة)، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2018.
122. فايز بن عبد الله الشهري، الخطاب الفكري على شبكة الإنترنت: (رؤية تحليلية لخصائص وسمات التطرف الإلكتروني)، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن الفكري، جامعة الملك سعود، الرياض، 1429 هجـرية.
123. فايز جمعه النجار، نظم المعلومات الإدارية: (منظور إداري)، الطبعة الثالثة، دار الحامد للنشر والتوزيع، الأردن، 2010.

124. فراس محمد أحمد الجحيشي، التوازنات الاستراتيجية الجديدة في ضوء بيئة أمنية متغيرة، الطبعة الأولى، الاكاديميون للنشر والتوزيع، الأردن، 2015.
125. فرج محمد لاه، إعادة اختراع الإرهاب بعد 11 سبتمبر، مؤسسة البراق للنشر والتوزيع، الأردن، 2015.
126. فرد كابلان، المنطقة المعتمدة: (التاريخ السري للحرب السيبرانية)، ترجمة (لوي عبد المجيد)، عالم المعرفة، رقم الإصدار 470، المجلس الوطني للثقافة والفنون والآداب الكويت، مارس 2019.
127. فردوس محمد عبد الباقي، العلاقات بين الكوريتين ومصالح القوى الكبرى، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2019.
128. فرغلي على تسن هريدي، هذا هو الإرهاب: (دراسة في محاكم التفتيش قديما وحديثا)، الطبعة الأولى، دار روابط للنشر وتقنية المعلومات، القاهرة، مصر، 2018.
129. فريج بن سعيد العويضي، حروب تقنية المعلومات: (كيف يشنها القراصنة والإرهابيون على البنية التحتية العالمية؟ وكيفية مواجهتها؟)، الطبعة الأولى، دار العلوم العربية للنشر والإعلام، مصر، 2016.
130. فريد بايبر وشون ميرفي، علم التشفير: (مقدمة قصيرة جدا)، ترجمة (محمد سعد طنطاوي)، الطبعة الأولى، مؤسسة هندواي للتعليم والثقافة، القاهرة، مصر، 2016.
131. فهمي النجار، الحرب النفسية: (أضواء إسلامية)، الطبعة الأولى، دار الفضيلة السعودية، 2005.
132. فيصل محمد عبد الغفار، الحرب الإلكترونية، الطبعة الأولى، الجنادرية للنشر والتوزيع، الأردن، 2016.
133. كريج ستيل، الشيزوفرينيا: (انقسام الشخصية: العلاج السلوكي المعرفي للمرض والتدخلات القائمة على الأدلة والتوجيهات المستقبلية)، ترجمة (مراد على عيسى)، الطبعة العربية الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2014.
134. كيث بوكس وأن ماري توماس، المرجع في روايات الخيال العلمي، ترجمة (عاطف يوسف محمود)، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2010.

135. لورانس أوتول وكينيث مائير، كتاب كامبردج في الإدارة العامة: (المنظمات والحوكمة والأداء)، ترجمة: (عبد الحكم أحمد الخزامي)، الطبعة العربية الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2013.
136. لورنس لسيج، الكود المنظم للفضاء الإلكتروني، الإصدار الثاني، مؤسسة هنداي للتعليم والثقافة، القاهرة، مصر، 2014.
137. لوري أندروز، أعرف من أنت ورأيت ماذا فعلت: (مواقع التواصل الاجتماعي وفقدان الخصوصية)، مكتبة العبيكان للنشر، الرياض، 2015.
138. لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي وحجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي وعوامل حجية الصورة والصوت في الإثبات الجنائي: (دراسة مقارنة)، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2018.
139. ليث عبد الله القهوي، زياد كامل اللالا، بلال محمود الوادي، جودة المعلومات والذكاء الاستراتيجي في بناء المنظمات المعاصرة، الطبعة الأولى، دار ومكتبة الحامد للنشر والتوزيع، الأردن، 2013.
140. ماجد مورييس إبراهيم، الإرهابي: (شهوة الدم ولغز الانتحار)، الطبعة الأولى، دار النهضة العربية، بيروت، لبنان، 2018.
141. مارتن غريفيثس وتيري أوكالاها، المفاهيم الأساسية في العلاقات الدولية، مركز الخليج للأبحاث، دبي، الإمارات العربية المتحدة، 2008.
142. مازن محمد علي، جيوبوليتيكا الأمن القومي العربي: (أمن الخليج العربي "مرتكزا") مقال ضمن المنصف الجماعي: الأمن القومي الإماراتي والخليجي والجزر الإماراتية المحتلة، الطبعة الأولى، مركز المزملة للدراسات والبحوث، الإمارات العربية المتحدة 2014.
143. ماهر ملندي وماجد الحموي، القانون الدولي العام، منشورات الجامعة الافتراضية السورية، سوريا، 2018.

144. مايكل ج. دوريس، جون م. كيلي، جيمس ف. ترينر، التخطيط الاستراتيجي الناجح ترجمة سمة عبدربه، الطبعة العربية الأولى، مكتبات ونشر العبيكان، المملكة العربية السعودية، 2006.
145. محمد أركون، أين هو الفكر الإسلامي المعاصر، ترجمة(هاشم صالح)، الطبعة الثانية، دار الساقى، بيروت، لبنان، 1995.
146. محمد الأمين البشري، علم ضحايا الجريمة وتطبيقاته في الدول العربية، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2005.
147. محمد الجندي، متاهة الإرهاب:(الشرق الأوسط من الخلافة إلى الإرهاب في الفضاء الإلكتروني)، الطبعة الأولى، مجموعة النيل العربية، القاهرة، 2020.
148. محمد الرازقي، محاضرات في القانون الجنائي:(القيم العام، - الأحكام العامة- الجريمة-المسؤولية الجنائية-)، الطبعة الثالثة، دار الكتاب الجديد المتحدة، لبنان، 2002 ص 43.
149. محمد السيد الصياد، أهل السنة في إيران:(دراسة في التأسيسيات الإيديولوجية والسياسية المذهبية تجاه أهل السنة)، المعهد الدولي للدراسات الإيرانية، الرياض، 1440 هجري.
150. محمد العوض محمد وداعة الله، مواقع التواصل الاجتماعي وقضايا الشباب الجامعي، الطبعة الأولى، دار الخليج للنشر والتوزيع، الأردن، 2020.
151. محمد جمال عبد الله، التخطيط الاستراتيجي، الطبعة الأولى، دار المعتر للنشر والتوزيع، الأردن، 2016، ص 259.
152. محمد جمال مظلوم، الأمن غير التقليدي، الطبعة الثانية، مركز الدراسات والبحوث جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2012.
153. محمد خليل موسى، الآخر والحرب على الإرهاب:(نحو نموذج تفسيري للنظام القانوني الدولي المعاصر)، الطبعة الأولى، دار الفكر، دمشق، 2009.
154. محمد عبد الرحمن الحيدر، اتصالات الألياف البصرية، الطبعة الأولى، مكتبة العبيكان، الرياض، 1995.

155. محمد عبد الله شاهين محمد، الاقتصاد المعرفي وأثره على التنمية الاقتصادية للدول العربية، الطبعة الأولى، دار حميثرا للنشر، مصر، 2018.
156. محمد عصام لعروسي، النزاعات المسلحة ودينامية التحولات الجيوسياسية في منطقة الشرق الأوسط وشمال إفريقيا، الطبعة الأولى، مجموعة النيل العربية، القاهرة 2020.
157. محمد مسعود قيراط، الإرهاب: (دراسة في البرامج الوطنية واستراتيجيات مكافحته – مقارنة إعلامية-)، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2011.
158. محمد نبهان سويلم، مدخل إلى علوم الحاسب، الطبعة الأولى، المكتبة الأكاديمية مصر، 2001.
159. محمود أحمد طه، التصنت والتلصص على سرية الاتصالات الشخصية بين التجريم والمشروعية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2014.
160. محمود عرابي، الإرهاب: (مفهومه-أنواعه-أسبابه-آثاره-أساليب مواجهته)، الطبعة الأولى، الدار الثقافية للنشر، القاهرة، مصر، 2007.
161. مروة فكري، مدخل إلى العلاقات الدولية: (أزمة العولمة وآفاق العالمية)، الطبعة الأولى، مركز الحضارة للدراسات والبحوث، دار الكتاب المصري، دار الكتاب اللبناني مصر، لبنان، 2021.
162. مصطفى يوسف كافي، الإدارة الإلكترونية: (إدارة بلا أوراق-إدارة بلا مكان-إدارة بلا زمان-إدارة بلا تنظيمات جامدة)، دار ومؤسسة رسلان للطباعة والنشر والتوزيع، دمشق سوريا، 2011.
163. مصطفى يوسف كافي، الحكومة الإلكترونية: (في ظل الثورة العلمية والتكنولوجية المعاصرة)، دار ومؤسسة رسلان للطباعة والنشر والتوزيع، دمشق، سوريا، 2009.
164. مصلح الصالح، ظاهرة الإرهاب المعاصر: (طبيعتها وعواملها واتجاهاتها)، مركز الملك فيصل للبحوث والدراسات الإسلامية، الرياض، المملكة العربية السعودية، 2002.
165. معتز الخطيب، العنف المستباح: (الشرعية في مواجهة الأمة والدولة)، الطبعة الأولى، دار المشرق، القاهرة، 2017.

166. منصور عمر المعاينة، الطب الشرعي في خدمة الأمن والقضاء، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2007.
167. منى الأشقر جبور، السيبرانية: (هاجس العصر)، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، (د.م.ن)، (د.ت.ن).
168. مؤيد عبيد حسن العزي، حق المتهم في محاكمة عادلة: (دراسة مقارنة وتطبيقية) الطبعة الأولى، المركزي العربي للدراسات والبحوث العلمية للنشر والتوزيع، مصر، 2020.
169. ميثاق بيات الضيفي، أكسجين الحرية، الطبعة الأولى، " E-kutub Ltd " للنشر لندن، بريطانيا، 2019.
170. ميق بايرن كرانجل، تغلب على الخوف من الطيران، ترجمة: (سيم هاشم)، الطبعة العربية الأولى، مكتبة العبيكان، الرياض، المملكة العربية السعودية، 2002.
171. ميكل هيل، أثر المعلومات في المجتمع: دراسة لطبيعتها وقيمتها واستعمالها، مركز الإمارات للدراسات والبحوث الإستراتيجية، الإمارات العربية المتحدة، الطبعة الأولى 2004.
172. ميلود ولد الصديق، مكافحة الإرهاب بين مشكلة المفهوم واختلاف المعايير عند التطبيق: (أوراق بحثية مقدمة في إطار ندوة علمية، الجزء الأول، الطبعة الأولى، مركز الكتاب الأكاديمي، عمان، الأردن، 2018).
173. نادية محمود مصطفى، القوة الذكية في السياسة الخارجية: (دراسة في أدوات السياسة الخارجية الإيرانية تجاه لبنان 2005-2013)، الطبعة الأولى، دار البشير للثقافة والعلوم، مصر، 2014.
174. نبيل علي، العرب وعصر المعلومات، عالم المعرفة، الإصدار رقم الإصدار 184 المجلس الوطني للثقافة والفنون والآداب، الكويت، أبريل 1994.
175. نزيه علي منصور، حق النقض (الفيتو) ودوره في تحقيق السلم والأمن الدوليين الطبعة الأولى، دار الكتب العلمية، لبنان، 2009.
176. نسيم بهلول وآخرون، التطرف الديني: (رؤى دينية أمنية سياسية)، الطبعة الأولى أمواج للنشر والتوزيع، عمان، الأردن، 2014.

177. نعوم تشومسكي، الدولة الفاشية: (إساءة استعمال القوة والتعدي على الديمقراطية) ترجمة: (سامي الكعكي)، دار الكتاب العربي، لبنان، 2007.
178. نعوم تشومسكي، الهيمنة أم البقاء: (السعي الأمريكي إلى السيطرة على العالم) ترجمة: (سامي الكعكي)، دار الكتاب العربي، لبنان، 2004.
179. هال أبلسون، هاري لويس، كين ليدين، الطوفان الرقمي: (كيف يؤثر على حياتنا وحریتنا وسعادتنا)، ترجمة: (أشرف عامر)، مؤسسة هنداوي للتعليم والثقافة، مصر، 2014 ص ص: 227-228.
180. هایل عبد المولى طشطوش، الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2012.
181. هشام بشير وإبراهيم عبد ربه إبراهيم، غسل الأموال بين النظرية والتطبيق الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011.
182. هشام بن عبد الله العباس، تسويق خدمات المعلومات عبر الإنترنت، مكتبة الملك فهد الوطنية، الرياض، المملكة العربية السعودية، 2009.
183. الهواري عبد الرحمن رشدي، التعريف بالإرهاب وأشكاله، أعمال ندوة الإرهاب والعولمة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2002.
184. هيثم عبد الرحمن البقلي، الجرائم الإلكترونية الواقعة على العرض: (بين الشريعة والقانون المقارن)، الطبعة الأولى، دار العلوم للنشر والتوزيع، القاهرة، 2010.
185. هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، الطبعة الأولى، دار الكتب العلمية، بيروت، لبنان، 2005.
186. وائل عبد العال، الدبلوماسية الرقمية ومكانتها في السياسة الخارجية الفلسطينية، سلسلة أبحاث وسياسات الإعلام، مركز تطوير الإعلام، جامعة بيرزيت، فلسطين، 2018.
187. وديع محمد العززي، التقنيات الحديثة للإنتاج التلفزيوني والعمل في القنوات الفضائية، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2021.

188. وسيم حسام الدين الأحمد، مكافحة الجريمة المنظمة عبر الوطنية في ضوء أحكام الشريعة الإسلامية والأنظمة السعودية، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض المملكة العربية السعودية، 2016.
189. وليم هـ داتن، آنا دوباتكا، مايكل هيلز، غينيتت لو، فيكتوريا ناش، حرية الإتصال حرية التعبير: (تغيير البيئة القانونية والتنظيمية الداعمة للإنترنت، منظمة الأمم المتحدة التربية والعلم والثقافة، فرنسا، 2013.
190. ياتشيا بنكلر، ثورة الشبكات: (كيف يغير الإنتاج الاجتماعي الأسواق والحريات)، ترجمة (فريج سعيد العويضي)، الطبعة العربية الأولى، مكتبة العبيكان، الرياض، المملكة العربية السعودية، 2012.
191. اليمين زرواطي، التجربة الجزائرية في مكافحة الإرهاب: (1978-2008) مطبوعات إي-كتب، لندن، 2014.
192. يوسف حسن يوسف، حقوق تبادل المسجونين بين الدول وفق الاتفاقيات الدولية الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015.
193. يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الاستراتيجية، السلیمانية، 2007.

2- الرسائل الجامعية:

أ- مذكرات جامعية:

1. أحمد بن علي عبد الله طارش، رؤية استراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية، رسالة ماجستير في العلوم الاستراتيجية، كلية العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية 2015.
2. أسامة بن يطو، حماية برامج الحاسب الآلي بين نظامي حقوق المؤلف وبراءة الاختراع مذكرة ماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة¹ (الحاج لخضر سابقا)، السنة الجامعية 2014-2015.

3. إسماء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني: (دراسة مقارنة)، مذكرة ماجستير في القانون العام: كلية الحقوق، جامعة النهرين، العراق، 2012.
4. آمال بن صويلح، التعاون الدولي وقوانين مكافحة الإرهاب الدولي، مذكرة ماجستير في القانون الدولي العام، كلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، الجزائر السنة الجامعية 2008-2009.
5. أمال ديلمي، التنظيم القانون الدولي للعلاقات الدبلوماسية، مذكرة ماجستير في القانون العام كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2012.
6. أميمه عثمان حسن عبد الرحيم، دور نظام البصمة الآلي (AFIS) في التعرف على مجهولي الهوية: (دراسة حالة: ولاية الخرطوم)، بحث لنيل درجة الماجستير في علوم الأدلة الجنائية كلية الدراسات العليا والبحث العلمي، جامعة الرباط الوطني، يناير 2017.
7. إيمان العاني، البنوك التجارية وتحديات التجارة الإلكترونية، مذكرة ماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، السنة الجامعية 2006-2007.
8. أيمن محمد فارس الدنف، واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، رسالة ماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية، غزة 2013.
9. بدر الدين بلمولاي، استعمال تكنولوجيا الإعلام والاتصال الحديثة في العلاقات الاجتماعية: دراسة ميدانية بجامعة بسكرة حلو استخدام الانترنت والهاتف النقال في اختيار الزوج - مذكرة ماجستير في علوم الاعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، السنة الجامعية 2011-2012.
10. بوعلام خندق، تسليم المجرمين، بحث ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق بن عكنون، جامعة الجزائر بن يوسف بن خدة، السنة الجامعية 2008-2009.
11. ثيان ناصر آل ثيان، إثبات الجريمة الإلكترونية: (دراسة تأصيلية تطبيقية)، رسالة ماجستير في السياسة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية الرياض، 2012.

12. جميلة سالم عطية، الثورة المعلوماتية وإشكالية بناء وتداول الخطاب اللغوي البصر: (دراسة تحليلية سيميولوجية على عينة من الخطابات اللغوية والبصرية في مواقع شبكات التواصل الاجتماعي - الفيسبوك نموذجاً -)، مذكرة ماجستير في علوم الإعلام والاتصال، كلية الإعلام والاتصال، جامعة الجزائر، 2013-2014.
13. جويذة حمزاوي، التصور الأمني الأوروبي: (نحو بنية أمنية شاملة)، مذكرة ماجستير في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2010-2011.
14. حورية بولعويديات، استخدام تكنولوجيا الاتصال في المؤسسات الاقتصادية الجزائرية: (دراسة ميدانية بمؤسسة سونغاز فرع تسيير شبكة نقل الغاز بالشرق "GRTG" قسنطينة) مذكرة ماجستير في الاتصال والعلاقات العامة، كلية العلوم الإنسانية والعلوم الاجتماعية جامعة منتوري، قسنطينة، السنة الجامعية 2007-2008.
15. خالد محمد سليمان محمد، تقييم فاعلية الإدارة الأمنية في تأمين المنشآت الهامة: (دراسة حالة رئاسة قوات الشرطة)، بحث تكميلي لنيل درجة الماجستير في العلوم الأمنية والجنائية، كلية الدراسات العليا والبحث العلمي، جامعة الرباط الوطني، يونيو 2018.
16. خديجة غرداين، إشكالية السيادة والتدخل الإنساني (حالة الدول العربية)، مذكرة ماجستير في القانون العام المعمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2014-2015.
17. سر الختم عثمان نصر الشيخ، مفاهيم حماية المنشآت بين النظرية والتطبيق: (بالتطبيق على إدارات ومؤسسات حماية المنشآت)، بحث ماجستير في الدراسات الجنائية والأمنية، كلية الدراسات العليا والبحث العلمي، جامعة الرباط الوطني، 2016.
18. سعاد بوخالفة، مبدأ التسليم أو المحاكمة على ضوء أعمال لجنة القانون الدولي مذكرة ماجستير في إطار مدرسة الدكتوراه في فرع الدولة والمؤسسات العمومية، كلية الحقوق بن عكنون، جامعة الجزائر 01، السنة الجامعية 2014.
19. سعاد شحات، استخدامات تكنولوجيا المعلومات والاتصال والفعالية التنظيمية للمؤسسات الاقتصادية: دراسة للمؤسسات الصغيرة والمتوسطة بالجزائر، مذكرة ماجستير في علم

- الاجتماع والاتصال، كلية الآداب والعلوم الاجتماعية، جامعة 08 ماي 1945، السنة الجامعية 2009.
20. **سفيان العاقب**، الدولة والعولمة: نهاية السيادة (فرانسيس فوكوياما نموذجاً)، مذكرة ماجستير في الفلسفة، كلية العلوم الاجتماعية، جامعة وهران 02، السنة الجامعية 2015-2016.
21. **سمية ديمش**، التجارة الإلكترونية: حقيقتها وواقعها في الجزائر، مذكرة ماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، السنة الجامعية 2010-2011.
22. **سهيلة خطابي**، مقاهي الإنترنت بقسنطينة ودورها في التنمية العلمية والثقافية للمجتمع، مذكرة ماجستير في علم المكتبات، كلية العلوم الإنسانية والعلوم الاجتماعية جامعة منتوري، قسنطينة، السنة الجامعية 2008-2009.
23. **سيدي محمد لبشير**، دور الدليل الرقمي في إثبات الجرائم المعلوماتية: (دراسة تحليلية تطبيقية)، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.
24. **صالح خلف زيد المطيري**، دور القيادة الأمنية في مواجهة الحدث الإرهابي: (دراسة تطبيقية على قوات الطوارئ الخاصة وقوات الأمن الخاصة بمنطقة الرياض)، رسالة ماجستير في قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية الرياض، 2005.
25. **صالح عبد الله محمد راشد الوارد**، الإنابة القضائية في قانون الإجراءات الجنائية القطري: (دراسة تحليلية مقارنة)، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة قطر، يونيو 2017.
26. **صالح عمر سرور**، الدبلوماسية الفلسطينية تجاه القوى المؤثرة في عملية السلام منذ أوسلو، رسالة ماجستير في الدراسات الدولية، كلية الدراسات العليا، جامعة بيرزيت، فلسطين العام الجامعي 2002-2003.
27. **صالح لبيد**، إشكالية سيادة الدولة في ظل العولمة، رسالة ماجستير في العلوم السياسية، كلية العلوم السياسية والإعلام، جامعة بن يوسف بن خدة، الجزائر، 2008-2009.

28. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي: (دراسة مقارنة)، رسالة ماجستير في الحقوق، كلية الحقوق، جامعة الإسكندرية، 2009.
29. عبد الله بن حسين آل جراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية: (دراسة تطبيقية على المحققين في هيئة التحقيق والادعاء العام بمدينة الرياض)، رسالة ماجستير في قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014.
30. عبد الله بن عبد العزيز بن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي: (دراسة تطبيقية)، رسالة ماجستير في العدالة الجنائية، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.
31. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية: (دراسة مقارنة)، مذكرة ماجستير في القانون العام، جامعة الشرق الأوسط، 2014.
32. عبير بهلولي، النظرية الواقعية البنيوية في الدراسات الأمنية: (دراسة لحالة الغزو الأمريكي للعراق في 2003)، مذكرة ماجستير في العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية والإعلام، جامعة الجزائر 03، السنة الجامعية 2013-2014.
33. علي بن عبد الله بن زيد الشيماني، أهمية استخدام الهواتف الذكية والحاسب اللوحية في دعم تعلم اللغة الإنجليزية لدى طلاب المرحلة الثانوية، رسالة ماجستير في المناهج وطرق تدريس اللغة الإنجليزية، كلية التربية، جامعة أم القرى، المملكة العربية السعودية، الفصل الدراسي الثاني، 2013.
34. عمر بن خزام بن ناصر بن عمر بن قرملة، دور مؤسسات المجتمع المدني في الوقاية من الإرهاب، رسالة ماجستير في العدالة الجنائية، السياسة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 10 جوان 2007.
35. عويض بن محمد بن هزال الذيابي، أحكام تسليم المجرمين في الفقه الإسلامي والاتجاهات المعاصرة وتطبيقاتها في المملكة العربية السعودية، رسالة ماجستير، تخصص التشريع الجنائي الإسلامي، برنامج مكافحة الجريمة، المعهد العالي للعلوم الأمنية، المركز العربي للدراسات الأمنية والتدريب، 1995.

36. فافة لحر، إجراءات تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية، مذكرة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة وهران الجزائر، السنة الجامعية 2013-2014.
37. فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، السنة الجامعية 2011-2012.
38. فرج بن مزنان العتيبي، فاعلية خطط الحماية الخارجية للمنشآت الحيوية لصد الهجمات الإرهابية: (دراسة مسحية على الضباط المكلفين بأمن وحماية المنشآت الحيوية) دراسة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية 2007.
39. فريدة شبري، تحديد نظام تسليم المرجمين، مذكرة ماجستير في القانون الدولي لحقوق الإنسان، كلية الحقوق بودواو، جامعة أحمد بوقرة، بومرداس، الجزائر، السنة الجامعية 2007-2008.
40. قاطفي حكيم، حرب المعلومات: (المفهوم والتطبيق)، مذكرة ماجستير في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر، السنة الجامعية 2005-2006.
41. كريمة صراع، واقع وآفاق التجارة الإلكترونية في الجزائر، مذكرة ماجستير في العلوم التجارية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، وهران الجزائر، السنة الجامعية 2013-2014.
42. محمد الشايب، الحكومة الإلكترونية كآلية لتوطيد الحكم الجيد: (دراسة في تطبيقات العالم المتقدم والنامي)، مذكرة ماجستير في العلوم السياسية والعلاقات الدولية، كلية الحقوق، جامعة الحاج لخضر، باتنة، السنة الجامعية 2008-2009.
43. محمد براي، وسائل الاتصال الحديثة وأثرها على التغير الاجتماعي في المجتمع الجزائري: (دراسة ميدانية على أساتذة التعليم الثانوي ببئر العاتر ولاية تبسة)، مذكرة ماجستير في علم اجتماع الاتصال والعلاقات العامة، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خضير، السنة الجامعية 2011-2012.

44. محمد عبد الرحمن أبو حمام، دور نظم المعلومات الإدارية في تحقيق الأمن المعلوماتي في جهاز الشرطة الفلسطينية، رسالة ماجستير في برنامج القيادة والإدارة، أكاديمية الإدارة والسياسة للدراسات العليا، جامعة الأقصى، 2014.
45. مريم ماضي، تأثيرات الهاتف النقال على أنماط الاتصال الاجتماعي لدى الطالب الجامعي: دراسة جامعة قسنطينة نموذجاً، مذكرة ماجستير في الإعلام وتكنولوجيا الاتصال الحديثة، كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية، جامعة الحاج لخضر باتنة السنة الجامعية 2012-2013.
46. منال محمود كريم حموري، أثر الثورة المعلوماتية وثورة الاتصالات على التحولات السياسية والأمنية في المنطقة العربية 2010-2017: (الأردن حالة دراسة)، رسالة ماجستير في العلوم السياسية، كلية الآداب والعلوم، جامعة الشرق الأوسط، أيار 2018.
47. موساوي فتحي رشدي، مبدأ تسليم المجرمين في القانون الدولي الاتفاقي، مذكرة ماجستير في القانون الدولي والعلاقات الدولية، كلية الحقوق، جامعة الجزائر 01، بن يوسف بن خدة، السنة الجامعية 2012-2013.
48. نسيب نجيب، التعاون الدولي في مكافحة الإرهاب، مذكرة ماجستير في قانون التعاون الدولي، كلية الحقوق، جامعة مولود معمري، تيزي وزو، نوقشت بتاريخ 2009/07/19.
49. نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة ماجستير في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، السنة الجامعية 2012-2013.
50. نور الحلو حسن عزيز، الإرهاب في القانون الدولي: (دراسة قانونية مقارنة)، أطروحة ماجستير في القانون العام، الأكاديمية العربية المفتوحة في الدنمارك، هلسنكي، فنلندا 2007.
51. هاشم بن عوض بن أحمد آل إبراهيم، سيادة الدولة بين مفهومها التقليدي وظاهرة التدويل، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، يونيو 2013.
52. وسام كامل ياسين العقاد، مدى إمكانية استخدام تطبيقات الهاتف النقال في تطوير العمل (دراسة حالة عيادات وكالة الغوث في قطاع غزة)، رسالة ماجستير في إدارة الأعمال كلية التجارة، الجامعة الإسلامية، غزة، 2013.

53. وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي أطروحة ماجستير في التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح نابلس، فلسطين، 2013.

54. ياسر لطفي العلي، الإرهاب: (مفهومه وأحكامه في الشريعة الإسلامية: دراسة فقهية مقارنة)، رسالة ماجستير في الفقه الإسلامي وأصوله، كلية الشريعة، جامعة دمشق، دمشق، 2007.

55. ياسع ياسمين، دراسة إقتصادية قياسية لأثر تكنولوجيا المعلومات والاتصالات على الأداء الاقتصادي للمنظمة - دراسة حالة شركة القطن الممتص " SOCOTHYD "، مذكرة ماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية، جامعة أمحمد بوقرة، بومرداس، السنة الجامعية 2010-2011.

56. يوسف خليل يوسف عبد الجابر، مدى فعالية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية، رسالة ماجستير في المحاسبة كلية الأعمال، جامعة الشرق الأوسط، كانون الثاني، 2013.

57. يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 06 مارس 2013.

ب- رسائل جامعية:

1. أحمد ضيف، تكنولوجيا المعلومات والاتصال كمدخل لتفعيل إدارة التغيير بالمؤسسة الاقتصادية: حالة المؤسسة الجزائرية (مجمع اتصالات الجزائر نموذجاً)، أطروحة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة أبي بكر بلقايد، تلمسان، السنة الجامعية 2012-2013.

2. أسماء فيلاي، مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثيره بطبيعة التهديدات وطبيعة الحماية المطبقة، أطروحة دكتوراه في الإدارة الاستراتيجية والذكاء الاقتصادي، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2018-2019.

3. أكسوم عيلام رشيدة، المركز القانوني للمستهلك الإلكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.

4. أمينة قدايفة، أثر تكنولوجيا المعلومات على المزيج التسويقي: (دراسة حالة عينة من المؤسسات الاقتصادية الجزائرية)، أطروحة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير. جامعة أحمد بوقرة، بومرداس، السنة الجامعية 2013-2014.
5. بلقاسم أمين بن عمرة، دور الوسائط الاتصالية في تشكيل الفضاءات العمومية الهامشية النسائية داخل الحيز الافتراضي، أطروحة دكتوراه في الطور الثالث في علوم الإعلام والاتصال، كلية العلوم الاجتماعية، جامعة عبد الحميد بن باديس، السنة الجامعية 2017-2018.
6. بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة دكتوراه في العلوم القانونية، كلية العلوم الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2014-2015.
7. بلقيدوم صباح، أثر تكنولوجيا المعلومات والاتصالات الحديثة على التسيير الاستراتيجي للمؤسسات الاقتصادية، رسالة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة قسنطينة 2، الجزائر، السنة الجامعية 2012-2013.
8. جودي سامية، مساهمة نظم المعلومات الحديثة في إعادة الهندسة بالمؤسسة الاقتصادية الجزائرية: (دراسة حالة مؤسسة اتصالات الجزائر)، أطروحة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد خيضر، بسكرة، السنة الجامعية 2016-2017.
9. جيدر حاج بشير، أثر وسائل التواصل الاجتماعي في عملية التحول الديمقراطي في الدول العربية: (دراسة مقارنة)، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، السنة الجامعية 2016-2017.
10. حجار ماجدة، العولمة والعنف: مقارنة سوسيولوجية لظاهرة العنف في ظل العولمة أطروحة دكتوراه في التنمية وتسيير الموارد البشرية، كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة منتوري، قسنطينة، السنة الجامعية 2009-2010.
11. حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، الجزء الثاني، أطروحة دكتوراه في العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، السنة الجامعية 2013-2014.
12. خيرة روابحي، البحث الوثائقي ولغات التوثيق في البنية الرقمية (دراسة ميدانية حول استخدام ادوات البحث ونماذجه في الواب من لدن اساتذة جامعة تيارت: مقارنة وصفية تحليلية)،

- أطروحة دكتوراه في علم المكتبات والعلوم الوثائقية، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة أحمد بن بلة، وهران 01، السنة الجامعية 2018-2019.
13. رابح عمار، الصحافة الإلكترونية وتحديات الفضاء الإلكتروني، دراسة ميدانية للصحافة الإلكترونية الجزائرية، أطروحة دكتوراه في علوم الإعلام والاتصال، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة أحمد بن بلة، وهران 01، السنة الجامعية 2016-2017.
14. رحيمة لدغش، سيادة الدولية وحققها في مباشرة التمثيل الدبلوماسي، أطروحة دكتوراه في القانون العام، كلية الحقوق، جماعة أبي بكر بلقايد، تلمسان، السنة الجامعية 2013-2014.
15. سفيان عيساوي، مكافحة الإرهاب الدولي في منطقة الساحل الإفريقي، أطروحة دكتوراه في القانون الدولي الجنائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، السنة الجامعية 2017-2018.
16. صافية أمينة، آثار استعمال التكنولوجيا الحديثة على أفراد الأسرة الجزائرية، دراسة للتأثيرات النفسية والاجتماعية والأخلاقية والصحية لاستعمال الإنترنت على أبناء الأسرة الجزائرية نموذجاً (دراسة على عينة مراهقين مستخدمين للانترنت بمدينة أم البواقي، أطروحة دكتوراه في علم النفس الأسري، كلية العلوم الاجتماعية، جامعة وهران 02، محمد بن أحمد السنة الجامعية 2015-2016).
17. عباس شافعة، الظاهرة الإرهابية بين القانون الدولي والمنظور الديني، أطروحة دكتوراه في القانون الدولي والعلاقات الدولية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2010-2011.
18. عبد الوهاب ملياني، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر السنة الجامعية، 2016-2017.
19. عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2017-2018.

20. علي عماري، مساهمة تكنولوجيا المعلومات في تنمية الكفاءات: (دراسة حالة مطاحن الأوراس باتة)، أطروحة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد خيضر، بسكرة، السنة الجامعية 2017-2018،
21. علي لونيبي، آليات مكافحة الإرهاب الدولي بين فعالية القانون الدولي وواقع الممارسات الدولية الانفرادية، رسالة دكتوراه في القانون، كلية الحقوق والعلوم السياسية جامعة مولود معمري، تيزي وزو، 04 جويلية 2012.
22. فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01-بن يوسف بن خدة-، السنة الجامعية 2017-2018.
23. فيصل بن زحاف، تسليم مرتكبي الجرائم الدولية، رسالة دكتوراه في القانون الدولي والعلاقات السياسية الدولية، كلية الحقوق والعلوم السياسية، جامعة وهران، السنة الجامعية 2011-2012.
24. كمال عايد، تكنولوجيا الإعلام والاتصال وتأثيرها على قيم المجتمع الجزائري - الشباب الجامعي لتلمسان نموذجا -، أطروحة دكتوراه ل.م.د، كلية العلوم الإنسانية والاجتماعية، جامعة أبي بكر بلقايد، تلمسان، السنة الجامعية 2016-2017.
25. محمد الأخضر كرام، فعالية الدبلوماسية في توجيه مسار العلاقات الدولية، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01، السنة الجامعية 2012-2013.
26. مرابط عياش عزوز، دور تكنولوجيا المعلومات في تنمية الكفاءات المهنية للعامل أطروحة دكتوراه في علم الاجتماع، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، السنة الجامعية 2016-2017.
27. مراد كريم، مجتمع المعلومات وأثره في المكتبات الجامعية: مدينة قسنطينة نموذجا أطروحة دكتوراه في علمو المكتبات، كلية العلوم الإنسانية والاجتماعية، جامعة منتوري قسنطينة، فيفري 2008.
28. مشري محمد الناصر، سبل تفعيل دور تكنولوجيا المعلومات والاتصال في دعم التنمية المستدامة في المؤسسات الصناعية الجزائرية: (دراسة عدد من المؤسسات في الشرق الجزائري)،

رسالة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والعلوم الاجتماعية وعلم التسيير، جامعة فرحات عباس، سطيف 01، الجزائر، السنة الجامعية 2016-2017.

29. **مليلة عطوي**، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت: (دراسة وصفية تحليلية)، أطروحة دكتوراه في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة دالي براهيم، الجزائر، السنة الجامعية 2009-2010.

30. **منير بودردابن**، جهود الدبلوماسية العامة الأمريكية في تنفيذ السياسة الخارجية وتحسين الصورة ضمن معايير الترتيبات والمصالح الأمنية تجاه العالم العربي، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، السنة الجامعية 2017-2018.

31. **نسيمة ضيف الله**، استخدام تكنولوجيا المعلومات والاتصال وأثره على تحسين الجودة العملية التعليمية: (دراسة عينية من الجامعات الجزائرية)، أطروحة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الحاج لخضر، باتنة 1 السنة الجامعية 2016-2017.

3 - مقالات:

1. **إبراهيم رمضان إبراهيم عطايا**، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية: (دراسة تحليلية تطبيقية)، مجلة كلية الشريعة والقانون بطنطا، المجلد 30 العدد 02، كلية الشريعة والقانون، جامعة الأزهر، طنطا، أبريل 2015، ص: 360-403.

2. **أحلام محمد شواي**، الإدارة الإلكترونية وتأثيرها في تطوير الأداء الوظيفي وتحسينية مجلة جامعة بابل للعلوم الإنسانية، المجلد 24، العدد 4، جامعة بابل، العراق، سنة 2016 ص 2388-2411:

3. **أحمد حشاني**، دور تكنولوجيا المعلومات والاتصال في ترقية البحث العلمي، مجلة روافد للبحوث والدراسات، المجلد 04، العدد 01، مخبر الجنوب الجزائري للبحث في التاريخ والحضارة الإسلامية، جامعة غرداية، 2019، ص: 39-57.

4. أحمد عبد الكريم موسى الصرايرة، الطبيعة القانونية لبرامج الحاسب الآلي في التشريع العماني: (دراسة مقارنة)، مجلة جامعة تكريت للحقوق، السنة 8، المجلد 3، العدد 29 كلية الحقوق، جامعة تكريت، العراق، آذار 2016، ص ص 308-326.
5. أحمد عبد المجيد، الأساليب الاتقاعية لتنظيم داعش في تجنيد الأفراد: (مقاربة علمية)، مجلة الباحث الإعلامي، المجلد 08، العدد 31، كلية الإعلام، جامعة بغداد العراق، 2016، ص ص: 89-106.
6. إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد 01، العدد 01، المدرسة العليا العسكرية للإعلام والاتصال، الجزائر ديسمبر 2019، ص ص: 100-123.
7. أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، جامعة نايف العربية للعلوم الأمنية نوفمبر-ديسمبر 2013، ص ص: 85-132.
8. أسماء فيلاي، عبد اللطيف شليل، تهديدات أمن المعلومات وسبل التصدي لها، مجلة البشائر الاقتصادية، المجلد 04، العدد 03، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة طاهري محمد، بشار، فيفري 2019، ص ص: 163-177.
9. إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، جامعة الشهيد حمّة لخضر، الوادي، الجزائر أفريل 2019، ص ص 1016-1031.
10. أشرف عبد المحسن الشريف، أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية، مجلة اعلم، الاتحاد العربي للمكتبات والمعلومات بالتعاون مع مكتبة الملك عبد العزيز العامة بالرياض، يناير 2016، ص ص: 87-114.
11. إكرام بلباي، آليات المجتمع المدني العالمي في رصد وتوثيق وقمع انتهاكات حقوق الإنسان مجلة حقوق الإنسان والحريات العامة، المجلد 02، العدد 01، جامعة بن باديس، مستغانم جانفي 2017، ص ص: 173-202.

12. آلاء محمد صاحب وتبارك ناصر عزوز الزامل، ماهية التجريم المزدوج في نظام تسليم المجرمين: (دراسة مقارنة)، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 01 العدد 1/44، كلية الحقوق، جامعة الكوفة، العراق، ص ص: 347-376.
13. إلهام حسن عزيز ووفاء محمود جاسم، تصميم خوارزمية تشفير باستخدام الأرقام السومرية، مجلة جامعة كركوك، المجلد 12، العدد 03، جامعة كركوك، العراق، 2017 ص ص: 40-63.
14. إلهام شهرزاد رواج، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، المجلد 05، العدد 02 جامعة لونيبي علي، البلدة 02، جوان 2016، ص ص: 184-198.
15. آمال عبد الجبار حسوني ونادية كعب جبر، كاميرات المراقبة بين دواعي الاستعمال وانتهاك الخصوصية، مجلة الحقوق، المجلد 01، العدد 29-30، كلية الحقوق، الجامعة المستنصرية، 2017، ص ص: 01-18.
16. أمين ودرار، الشرطة الجنائية الإفريقية " الأفيبول "، حوليات جامعة الجزائر 1 المجلد 34، العدد 01، جامعة بن يوسف بن خدة، الجزائر، مارس 2020، ص ص: 135-149.
17. أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني المجلد 09، العدد 01، جامعة عبد الرحمان ميرة، بجاية، جويلية 2018، ص ص: 721-744.
18. بصائر علي محمد ومروى عبد الواحد حسن، الدليل الإلكتروني في مجال الإثبات الجنائي، مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية، المجلد 03، العدد 27 جامعة واسط، 2017، ص ص: 271-285.
19. بلقاسم شابي، النزوع إلى المغالاة في الممارسات الدينية عبر المواقع الإلكترونية الإسلامية: موقع البراق ومنبر التوحيد والجهاد أنموذجاً، مجلة التواصل، المجلد 21 العدد 04، جامعة باجي مختار، عنابة، الجزائر، ديسمبر 2015 ص ص: 205-219.
20. توفيق مجاهد، طاهر عباس، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، مجلة العلوم القانونية والسياسية المجلد

- 09، العدد 03، كلية الحقوق والعلوم السياسية، جامعة الشهيد حقه لخضر، الوادي الجزائر، ديسمبر 2018، ص ص: 76-103.
21. جمال معتوق ونور الهدى قدوح، مساهمة الضحايا في السلوكيات الإجرامية والعنفية الواقعة عليهم في المجتمع الجزائري، مجلة الآداب والعلوم الاجتماعية، المجلد 08 العدد 13، جامعة البليدة 02، الجزائر، جويلية 2015، ص ص: 11-28.
22. جمال منصر، تحولات في مفهوم الأمن: (من أمن الوسائل إلى أمن الأهداف)، مجلة دفاتر السياسة والقانون، العدد الأول، جامعة قصدي مرياح، ورقلة، جانفي 2009 ص ص: 125-139.
23. جميلة سلايمي، يوسف بوشي، التحول الرقمي بين الضرورة والمخاطر، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 02، سبتمبر 2019، ص ص: 944-967.
24. جيلالي ماينو، دور قواعد بيانات منظمة الشرطة الجنائية الدولية (الإنتربول) في التحقيقات الجنائية والكشف عن الجرائم، معالم للدراسات القانونية والسياسية، المجلد 03، العدد 02، المركز الجامعي، تندوف، الجزائر، ديسمبر 2019، ص ص: 73-92.
25. حديد نوفيل وحنان كريبط، أمن المعلومات ودورها في مواجهة الاعتداءات الإلكترونية على نظام معلومات المؤسسة، مجلة المؤسسة، المجلد 03، العدد 03، جامعة الجزائر 03، الجزائر، سبتمبر 2014، ص ص: 186-207.
26. حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية: (تصور مقترح)، المجلة العربية للدراسات الأمنية والتدريب، المجلد 27 العدد 53، جامعة نايف العربية للعلوم الأمنية، الرياض، رجب 1432، ص ص 05-54.
27. حسين حسيني جامع وأميرة رضا مسعد السعيد ومنال عبد العال مبارز، تطوير تدريس منهج الكمبيوتر وتكنولوجيا المعلومات لطلاب المرحلة الإعدادية في ضوء متطلبات الوعي بأخلاقيات للتكنولوجيا المعاصرة، مجلة العلوم التربوية، المجلد 24، العدد 04، الجزء 03، معهد الدراسات التربوية، جامعة القاهرة، القاهرة، مصر، أكتوبر 2016، ص ص: 377-402.
28. حكيم غريب، الإرهاب السيبراني والأمن الدولي: (التحديات العالمية الجديدة وأساليب المواجهة)، المجلة الجزائرية للدراسات السياسية، المجلد 05، العدد 02، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، ديسمبر 2018، ص ص: 104-119.

29. حكيم غريب، شرقي صبرينة، تداعيات الحرب الإلكترونية على العلاقات الدولية: (دراسة في الهجوم على إيران "فيروس ستنكست")، مجلة دفاثر السياسية والقانون، المجلد 12، العدد 03، جامعة قصدي مرياح، ورقلة، الجزائر، جوان 2020، ص ص: 92-107.
30. حكيم نشاد، المستهلك الإلكتروني وآليات حمايته في عصر الاقتصاد الرقمي مجلة البحوث القانونية والاقتصادية، المجلد 01، العدد 02، المركز الجامعي، أفلو، جوان 2018، ص ص: 209-223.
31. حميد حمد السعدون، الاستخدام الأمريكي للقوة الصلبة والقوة الناعمة في السياسة الخارجية، مجلة الدراسات الدولية، العدد 64-65 (عدد مزدوج)، جامعة بغداد، العراق 2016، ص ص: 1-16.
32. حميد عبد الكريم يونس وأنور صالح سليمان، تطور السرية في نظام التشفير الانسيابي اللاخطي من نوع (J-K)، مجلة البصرة للعلوم، المجلد 25، العدد 1/أ، جامعة البصرة، 2007، ص ص: 44-55.
33. حيدر محمد عبد النبي ورعد عبد الحسن مهجر ونهلة عباس فليح، تشفير الملفات النصية باستعمال المفتاح المتناظر ومفتاح مستنبط من معلومات النص الصريح مجلة أبحاث البصرة، المجلد 32، العدد 3B، جامعة البصرة، العراق، ص ص: 25-33.
34. خديجة خالدي، آلية الاتحاد الإفريقي للتعاون الشرطي -أفريبول-، مجلة العلوم الاجتماعية والإنسانية، المجلد 11، العدد 01، جامعة العربي التبسي، تبسة، الجزائر جوان 2018، ص ص: 65-79.
35. خليفة إبراهيم عودة التميمي، الأمن والمجتمع: (دراسة في العلاقات بين المؤسسات الاجتماعية والمؤسسات الأمنية)، مجلة كويه، العدد 08، كلية القانون، جامعة كويه، أربيل العراق، 2008، ص ص 352-382.
36. ربيع محمد يحيي، إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط، مجلة رؤى استراتيجية، المجلد الأول، العدد 03، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبوظبي، الإمارات العربية المتحدة، يونيو 2013، الصفحة 65-89.

37. رزيقة حيزير، واقع مكافحة الجريمة الإلكترونية، مجلة الحكمة للدراسات الإعلامية والاتصالية، المجلد 05، العدد 10، مؤسسة كنوز الحكمة للنشر والتوزيع، الجزائر، جوان 2017، ص ص: 80-95.
38. رقية عواشيرة، نظام تسليم المجرمين وحدوده في تحقيق التعاون الدولي لمكافحة الجريمة المنظمة، مجلة الفكر، المجلد 04، العدد 04، كلية الحقوق والعلوم السياسية جامعة محمد خيضر، بسكرة، الجزائر، أبريل 2009، ص ص: 17-27.
39. رؤى يونس، دراسة واقع إدارة أمن نظم المعلومات في المؤسسات السورية، مجلة جامعة البعث للعلوم الهندسية، المجلد 39 العدد 31، جامعة البعث، حمص، سوريا 2017 ص ص: 61-90.
40. زينة حازم خلف الجبوري، طرق تنفيذ الإنابة القضائية الدولية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 06، العدد 22، الجزء الأول، كلية الحقوق، جامعة كركوك، العراق، 2017، ص ص: 36-93.
41. سامر مؤيد عبد اللطيف، الإرهاب الإلكتروني وسبل مواجهته، مجلة جامعة كربلاء العلمية، المجلد 14، العدد 03، جامعة كربلاء، العراق، 2016، ص ص: 57-72.
42. سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي: (رؤية مستقبلية)، مجلة رسالة الحقوق، المجلد 07، العدد 02، كلية القانون، جامعة كربلاء، العراق، 2015، ص ص: 74-121.
43. سراح حليتم، خصوصية التوقيع الرقمي في توثيق العقود الإلكترونية، مجلة الباحث للدراسات الأكاديمية، المجلد 05، العدد 02، جامعة باتنة 01، الحاج لخضر، باتنة، جويلية 2018، ص ص: 737-752.
44. سعد محمد خضير، اتجاهات الجمهور العراقي أزاء المنطق الدعائي للتنظيمات الإرهابية: (دراسة ميدانية)، مجلة الباحث الإعلامي، المجلد 07، العدد 30، كلية الإعلام، جامعة بغداد، العراق، 2015، ص ص: 125-146.
45. سعيد عبيدي، الإرهاب الإلكتروني، مجلة العلوم الإنسانية، المجلد 01، العدد 02، المركز الجامعي علي كافي، تندوف، الجزائر، سبتمبر 2017، ص ص: 32-43.

46. سعيدي عزو وخالد رامول، الأمن التقني للدفع الإلكتروني أي فعالية؟، مجلة معالم للدراسات القانونية والسياسية، المجلد 01، العدد 02، المركز الجامعي، تندوف، ديسمبر 2017، ص ص: 112-129.
47. سليمة ذياب، بلال بوترعة، الجريمة الإلكترونية: (الأسس والمفاهيم)، مجلة تطوير العلوم الاجتماعية، المجلد 13، العدد 01، جامعة زيان عاشور، الجلفة، الجزائر، نوفمبر 2020، ص ص: 07-20.
48. سمير بارة، الأمن السيبراني (CYBER SECURITY) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 01 الحاج لخضر، العدد 04 جويلية 2017، ص ص 255-280.
49. سميرة شرايطية، السيادية السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي، المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 16، جامعة باتنة 1 باتنة، الجزائر، جانفي 2020، ص ص 396-410.
50. سميرة ناصري وبسمة ترغيني، دور المجتمع المدني في مكافحة الجريمة المنظمة، مجلة الحقوق والعلوم السياسية، المجلد 01، العدد 02، جامعة عباس لغرور، خنشلة أكتوبر 2014، ص ص: 159-171.
51. سهيلة بضياف وأمنة حمراي، أمن المعلومات في الجزائر: (الإجراءات والتحديات)، المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 01، جامعة باتنة 1 الحاج لخضر، الجزائر، جانفي 2020، ص ص: 177-190.
52. سهيلة هادي، آليات تعزيز حق الإنسان في الأمن المعلوماتي، المجلة الجزائرية للعلوم القانونية، السياسية والاقتصادية، المجلد 54، العدد 05 (خاص)، كلية الحقوق جامعة الجزائر 01، بن يوسف بن خدة، مارس 2017، ص ص: 223-251.
53. شامل سليمان عسله، الإشكالية القانونية للمحل في عقود إعداد البرامج الإلكترونية في التشريع المدني المصري والتشريعات المدنية المقارنة، حولية كلية الدراسات الإسلامية والعربية للبنات، المجلد الثاني، العدد 33، جامعة الأزهر، الإسكندرية، ص ص 259-296.

54. صالح زياتي، موقع مؤسسات المجتمع المدني في إطار التنمية المحلية في الجزائر مجلة العلوم الاجتماعية والإنسانية، المجلد 08، العدد 16، جامعة باتنة 1 حاج لخضر الجزائر، جوان 2007، ص ص: 255-274.
55. صباح كزيز وأمال كزيز، الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي مجلة التراث، المجلد 07، العدد 05، جامعة زيان عشور، الجلفة، الجزائر، جوان 2018 ص ص: 312-328.
56. صباح محمد عبد الكريم كلو، أخلاقيات مجتمع المعلومات في عصر الإنترنت مجلة الملك فهد الوطنية، المجلد 13، العدد 01، مكتبة الملك فهد الوطنية، الرياض، يناير-يوليو 2007، ص ص: 286-305.
57. صباح مصباح محمود الحمداني ونادية عبد الله الطيف أحمد، ماهية السياسة الوقائية الجزائرية، مجلة جامعة تكريت للعلوم القانونية والسياسية، المجلد 2، العدد 1 الجزء 1، جامعة تكريت، العراق، 2017، ص ص: 35-80.
58. صليحة محمدي وشفيعه حداد، الإرهاب الإلكتروني والأمن القومي للدول: (نمط جديد وتهديدات مختلفة)، المجلة الجزائرية للأمن والتنمية، المجلد 08، العدد 2، جامعة الحاج لخضر، باتنة، الجزائر، جوان 2019، ص ص: 65-77.
59. الطاهر سواكري، خصائص ضحايا الإجرام: (محاولة للتحليل السوسيولوجي)، مجلة الآداب والعلوم الاجتماعية، المجلد 07، العدد 11، جامعة البليدية 02، الجزائر، جوان 2014، ص ص: 01-09.
60. طوبي بحري ودلال بحري، آليات مواجهة الإرهاب الإلكتروني في ظل العولمة مجلة البحوث والدراسات، المجلد 13، العدد 01، جامعة حمة لخضر، الوادي، الجزائر، سبتمبر 2017، ص ص: 187-208.
61. عايدة حوشي، التشفير والمال وراء لسانية في رواية: (التفكيك) لـ رشيد بوجدر الملتقي الوطني الأول حول: النقد الأدبي الجزائري، 21-22 ماي 2006.
62. عباس أحمد الباز، البصمة البصرية والصوتية ودورها في الإثبات الجنائي شرعا وقانونا، الندوة العلمية: (الجوانب الشرعية والقانونية لاستخدام الوسائل العلمية الحديثة في

التحقيق الجنائي)، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، عمان 23-25 أفريل 2007.

63. عباس زبون عبيد العبودي، الإطار القانوني للحكومة الإلكترونية، مجلة العلوم القانونية والسياسية، مجلة العلوم القانونية والسياسية، العدد 01، كلية القانون والعلوم السياسية، جامعة ديالى، العراق، 2012، ص ص 84-102.

64. عبد الحفيظ سعيد مقدم، تقرير عن ندوة: دور مؤسسات المجتمع المدني في التصدي للإرهاب، المجلة العربية للدراسات الأمنية والتدريب، المجلد 30، العدد 60، جامعة نايف العربية للعلوم الأمنية، الرياض، أغسطس 2014، ص ص: 319-330.

65. عبد الحق لخداري، مبدأ تسليم المجرمين ودوره في تفعيل قواعد القانون الدولي الجنائي، مجلة الباحث للدراسات الأكاديمية، المجلد 06، العدد 01، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، الحاج لخضر، جانفي 2019، ص ص: 507-525.

66. عبد الرحمن بن معلا اللويحق، الإرهاب والغلو: (دراسة في المصطلحات والمفاهيم)، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، جامعة الملك محمد بن سعود الإسلامية، المملكة العربية السعودية، 1425 هجرية، ص ص: 93-133.

67. عبد الرحمن خلف العنزي، دور مؤسسات المجتمع المدني في مكافحة التطرف والإرهاب، متوفر على الموقع الإلكتروني للمندوبية السامية للتخطيط، المملكة المغربية.

68. عبد المجيد رمضان، الديمقراطية الرقمية كآلية لتفعيل الديمقراطية التشاركية: (حالة الجزائر)، دفا تر السياسة والقانون، جامعة قصدي مرباح، ورقلة، الجزائر، المجلد 09 العدد 16، جانفي 2017، ص ص: 75-88.

69. عثمان مداحي، أهمية ودور المعلومات في إتخاذ القرارات، مجلة الإدارة والتنمية والدراسات، المجلد 07، العدد 01، جامعة علي لوني سي البلدية 02، الجزائر، جوان 2018 ص ص: 234-244.

70. عزة حازم زكي، نمذجة نظام برمجي للتحقق من الهوية عن طريق بصمة العين، المجلة العراقية للعلوم الإحصائية، المجلد 12، العدد 22، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق، 2012، ص ص: 149-166.

71. عقباوي محمد عبد القادر ومنصوري المبروك، تأثير الصفة الخاصة للضحية في وقوع الجريمة وأثرها على عقوبة الجاني في التشريع الجزائري: (دراسة مقارنة)، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 07، العدد 06، المركز الجامعي لتمرّاست، 2018، ص: 209-232.
72. علاء الدين أحمد عباس، صناعة الخوف في خطاب الصورة الدعائي لتنظيم "داعش" الإرهابي عبر الإنترنت، مجلة الباحث الإعلامي، المجلد 09، العدد 38، كلية الإعلام جامعة بغداد، العراق، 2017، ص: 67-94.
73. علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 03، كلية الحقوق والعلوم السياسية، جامعة حمة لخضر، الوادي، ديسمبر 2019، ص: 88-107.
74. علي جاسم محمد التميمي، الإرهاب الإلكتروني وأثره على المجتمع، المجلة السياسية والدولية، مجلد 2016، العدد 33-34، كلية العلوم السياسية، الجامعة المستنصرية، العراق، 2016، ص: 89-106.
75. عمر زغودي، الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، المركز الجامعي لأفلو، الجزائر، ماي 2020، ص: 101-118.
76. عمر محمود أعر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة دراسات علوم الشريعة والقانون، المجلد 46، العدد 03، الجامعة الأردنية، 2019، ص: 134-155.
77. عنتر بن مرزوق ومحمد الكر، البعد الإلكتروني للسياسة الأمنية الجزائرية، مجلة العلوم الإنسانية والاجتماعية، جامعة باتنة 01 الحاج لخضر، الجزائر، العدد 38، جوان 2018، ص: 29-50.
78. عنتر بن مرزوق ومحي الدين حرشاي، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، المنشورات العلمية لجامعة قصدي مرباح، ورقلة، 2017، ص: 65-80.

79. عنترة بن مرزوق، جريمة الإرهاب الإلكتروني: (الأسباب وآليات العلاج)، مجلة الحقوق والعلوم الإنسانية، المجلد 11 العدد 02، جامعة زياد عشور، الجلفة، الجزائر جوان 2018، ص ص: 509-520.
80. عنترة مرزوق وعبد المؤمن سي حمدي، الانتقال إلى الحوكمة المحلية في الجزائر: (دراسة فب التحديات والآليات)، مجلة التراث، المجلد 07، العدد 05، جامعة زيان عاشور الجلفة، جوان 2018، ص ص: 214-230.
81. العايشي زرزار، من الحوكمة المحلية إلى الحوكمة الإلكترونية للإدارات المحلية مجلة القانون والمجتمع، المجلد 03، العدد 01، جامعة أحمد دراية، أدارار، جوان 2015 ص ص: 84-112.
82. العبد نويب، مفهوم الأمن في الفكر الديني: (دراسة لأبعاد الأمن الإنساني في الإسلام)، مجلة الدراسات القانونية والسياسية، العدد 05، المجلد 01، كلية الحقوق والعلوم السياسية، جامعة عمار التليجي، الأغواط، جانفي 2017، ص ص 244-268.
83. عيسي تركي خلف، تمويل جهود مكافحة الإرهاب الإلكتروني، مجلة الجامعة العراقية، المجلد 34، العدد 03، مركز البحوث والدراسات الإسلامية الجامعة العراقية 2015، ص ص: 471-498.
84. فاتن سعيد بامفلح، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: (دراسة حالة)، الاتجاهات الحديثة في المكتبات والمعلومات، العدد 18، المكتبة الأكاديمية القاهرة، مصر، 2002، ص ص: 249-282.
85. فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحول الرقمي: (السن نموذجاً)، المجلة الجزائرية للأمن الإنساني، السنة الخامسة، المجلد 05، العدد 01، جامعة باتنة 01، الحاج لخضر، جانفي 2020، ص ص: 789-216.
86. فانز ذنون جاسم، تأثير الإنترنت على مبدأ السيادة، مجلة كلية الحقوق، المجلد 17، العدد 02، جامعة النهروان، العراق ، 2015، ص ص 331-348.
87. فريد رناي، واجب تحفظ الأعوان العموميين في القانون الجزائري، مجلة القانون المجتمع والسلطة، المجلد 04، العدد 02، جامعة محمد بن أحمد، وهران 02، 2018 ص ص: 173-182.

88. فريد علوش، التعاون الدولي عن طريق نظامي تسليم المجرمين والتسليم المراقب مجلة الفكر، المجلد 12، العدد 14، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، جانفي 2017، ص ص: 165-179.
89. فريدة صغير عباس ورضوان رياح، التفاعل الافتراضي نحو مقارنة المفهوم في ظل المجتمعات الافتراضية، مجلة الصورة والاتصال، المجلد 07، العدد 02، جامعة وهران السانية، وهران، الجزائر، ديسمبر 2018، ص ص: 119-127.
90. فضيلة تومي، تكنولوجيا الاتصال: (التفاعلية وعلاقتها بالبحث العلمي في الجامعة الجزائرية)، مجلة الباحث في العلوم الإنسانية والاجتماعية، ورقة، عدد خاص، المجلد 03، العدد 6، جامعة قصدي مرباح، مارس 2011، ص ص: 486-521.
91. فوزية حاج شريف والساجي علام، واقع الإرهاب الإلكتروني وآليات مكافحته المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 03، العدد 01، جامعة عمار تليجي، الأغواط، الجزائر، 2019، ص ص: 158-172.
92. كريم رقولي، أحلام وغليسي، الحرب الإلكترونية بين الولايات المتحدة وروسيا مجلة أكاديمية للعلوم السياسية، المجلد 06، العدد 02، جامعة حسية بن بوعلي، شلف، الجزائر، جويلية 2020، ص ص: 134-143.
93. كريمة تدريست، معوقات نظام تسليم المجرمين كآلية للتعاون القضائي الدولي لمكافحة الجريمة المنظمة عبر الوطنية، المجلة النقدية للقانون والعلوم السياسية، المجلد 02، العدد 02، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، نوفمبر 2016، ص ص: 30-57.
94. كنزة تنيو ومحمد دهان، دور الاقتصاد الرقمي في تحقيق جودة الحياة: (دراسة مقارنة بين الجزائر والإمارات)، مجلة الاستراتيجية والتنمية، العدد 03 مكرر (الجزء الأول)، المجلد 09، كلية العلوم الاقتصادية، التجارية وعلوم التسيير، جامعة عبد الحميد بن باديس، مستغانم، 2019، ص ص: 364-385.
95. لخضر دلال وإسماعيل بن ديلمى، المورد البشري خطر أم حصن للمنظمة: (مدخل أمن المعلومات في ظل الذكاء الاقتصادي)، الأفاق للدراسات الاقتصادية، المجلد 05، العدد 01،

كلية العلوم الاقتصادية والعلوم الاجتماعية وعلوم التسيير، جامعة العربي التبسي تبسة، أفريل 2020، ص ص: 124-136.

96. لهيب محمد الزبيدي وريا جاسم العطيوي، تطبيق أسلوب التشفير الانسيابي المبني على الشبكة العصبية الاصطناعية، مجلة علوم الرافدين، المجلد 17، العدد 02/أ، جامعة الموصل، 2006، ص ص: 105-123.

97. لورنس سعيد الحوامدة، الجريمة الإلكترونية، أركانها وآلية مكافحتها، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد 04، العدد 01، الجامعة الإسلامية العالمية، عمان الأردن، كانون الثاني 2017، ص ص 187-220.

98. ليلى عصماني، نظام التقاضي الإلكتروني آلية لإنجاح الخطط التنموية، مجلة الفكر العدد 13، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، فيفري 2016، ص ص 215-225.

99. ليندة شرايشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية: (الاتجاهات الدولية في مكافحة الجريمة الإلكترونية)، مجلة دراسات وأبحاث، المجلد 01 العدد 01، جامعة زياد عاشور، الجلفة، الجزائر، سبتمبر 2009، ص ص: 241-253.

100. ماجدة شهيناز بدوح، مبدأ عدم تسليم المجرمين في الجرائم السياسية، مجلة الفكر المجلد 12، العدد 14، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، جانفي 2017، ص ص: 229-323.

101. مازن خلف الشمري، موانع تسليم الإرهابيين: (دراسة مقارنة)، مجلة كلية الحقوق المجلد 14، العدد A1، كلية الحقوق، جامعة النهروان، العراق، 2012، ص ص: 280-300.

102. مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة العلوم الاقتصادية والإدارية والقانونية، المجلد 02 العدد 07، غزة، فلسطين، مايو 2018، ص ص: 56-67.

103. المجيد لخذاري وفطيمة بن جدو، الأمن القانوني والأمن القضائي: (علاقة تكامل) مجلة الشهاب، المجلد 04، العدد 02، معهد العلوم الإسلامية، جامعة الشهيد حمه لخضر الوادي، جوان 2018، ص ص 387-406.

104. محمد الأمين البشري، الأدلة الجنائية الرقمية: (مفهومها ودورها في الإثبات) المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد 33، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، نوفمبر 2000، ص ص: 91-147.
105. محمد بن فردية، الدليل الجنائي الرقمي وحجتيه أما القضاء الجزائي: (دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني، المجلد 05، العدد 01، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، جوان 2014، ص ص: 276-286.
106. محمد رحيموني، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة للعلوم الإنسانية والاجتماعية، المجلد 16، العدد 03، جامعة أحمد دراية، أدرار، الجزائر سبتمبر 2017، ص ص: 432-451.
107. محمد طوالبية، أيدولوجية الفضاء الرقمي: (دراسة في الخلفيات المرجعية)، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 11، العدد 01، جامعة حسيبة بن بوعلي، شلف، الجزائر، جانفي 2019، ص ص: 47-58.
108. محمد عبد الكريم الحوراني، المجتمع المدني ضرورة وظيفة للدولة، مجلة علوم الإنسان والمجتمع، المجلد 02، العدد 08، جامعة محمد خيدر، بسكرة، ديسمبر 2013 ص ص: 43-78.
109. محمد عقوني وإبراهيم بلمهدي، الآليات التقنية والقانونية لحماية التوقيع الإلكتروني، مجلة الفكر، المجلد 14، العدد 01، جامعة محمد خيضر، بسكرة، فيفري 2019، ص ص: 300-313.
110. محمد فرحات، دور البرلمان في حوكمة الإنترنت، مجلة اتجاهات سياسية، تحليلات سياسية، المركز الديمقراطي العربي، المجلد 03، العدد 11، برلين، ألمانيا، يونيو 2020 ص ص: 137-152.
111. محمود أديب فتاح أغا الكاكه، اختصاصات مجلس الأمن في التصدي للإرهاب الدولي الإلكتروني، مجلة دراسات علوم الشريعة والقانون، المجلد 47، العدد 01، عمادة البحث العلمي وضمان الجودة، الجامعة الأردنية، الأردن، 2020، ص ص: 644-659.

112. مختار يحيوي، تطور آليات مكافحة الإرهاب وانعكاساتها على فكرة الأمن الدولي والأمن الإنساني، مجلة أبحاث قانونية وسياسية، العدد 06، كلية الحقوق والعلوم السياسية جامعة الصديق بن يحي، جيجل، الجزائر، جوان 2018، ص ص 279-289.
113. مخلوف ساحل، المقاربة الجزائرية في مجال مكافحة الإرهاب: (الأس والآليات) مجلة الدراسات القانونية والسياسية، المجلد 02، العدد 01، جامعة عمار تليجي الأغواط جانفي 2016، ص ص: 42-57.
114. مراد قريبيز وفاطمة الزهراء تيشوش، الإنترنت في مواجهة تحديات الجريمة المنظمة، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، المركز الجامعي لأفلو، الجزائر، ماي 2020، ص ص: 119-129.
115. مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، المجلد 12، العدد 02، جامعة غرداية، الجزائر، ديسمبر 2019، ص ص: 703-726.
116. مصطفى بوعقل، آليات وقاية المعاملات الإلكترونية في ظل حوكمة تكنولوجيا المعلومات، مجلة دفاتر MECAS، المجلد 12، العدد 01، جامعة أو بكر بلقايد، تلمسان جوان 2016، ص ص: 380-396.
117. مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: (دراسة مقارنة)، دراسات، علوم الشريعة والقانون، المجلد 45، العدد 04، ملحق 02، عمادة البحث العلمي وضمان الجودة، الجامعة الأردنية، 2018، ص ص: 284-299.
118. معاذ العامودي، الدبلوماسية الرقمية وتأثيرها في السياسة الخارجية، دراسة مقارنة بين فلسطين والاحتلال الإسرائيلي، مجلة رؤية تركية، السنة 07، العدد 04، شتاء 2018 ص ص: 125-149.
119. معمر بن علي وعبد الملك الدح، الوسائل المتاحة لمنظمة الإنترنت لمواجهة الجريمة المنظمة، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، المركز الجامعي لأفلو، الجزائر، ماي 2020، ص ص: 130-143.

120. ملحم خوري نيكولا، تقييم مخاطر تكنولوجيا المعلومات، رحلة التميز في مجال التدقيق الداخلي: (رؤى حول الحوكمة وإدارة المخاطر والرقابة الداخلية)، المدقق الداخلي - الشرق الأوسط -، معهد المدققين الداخليين الدولي، يونيو 2017، ص ص: 10-11.
121. منال قدواح، الإعلام الجديد: (خطوات واعدة نحو بروز مفهوم جديد للديمقراطية وآليات ممارستها الرقمية)، مجلة العلوم الإنسانية، المجلد "ب"، العدد 43، جامعة منتوري قسنطينة، الجزائر، جوان 2015، ص ص: 75-88.
122. منوبة مزوار، أثر الحوافز في الولاء التنظيمي مع دراسة حالة عينة من المؤسسات العمومية الجزائرية، المجلة العلمية المستقبل الاقتصادي، المجلة العلمية المستقبل الاقتصادي، المجلد 01، العدد 01، مخبر مستقبل الاقتصاد الجزائري خارج المحروقات جامعة امحمد بوقرة، بومرداس، الجزائر، ديسمبر 2013، ص ص: 125-157.
123. منيرة عبيزة، التوقيع الإلكتروني كضمانة قانونية لحماية المستهلك الإلكتروني المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 02، العدد 1، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي، الأغواط، مارس 2018، ص ص: 181-202.
124. مولود بلقاسمي وإبراهيم حادي، تحولات مفهوم القوة في الفضاء الإلكتروني: (مقاربة سياسية)، مجلة القانون والعلوم السياسية، المجلد 02، العدد 01، معهد الحقوق والعلوم السياسية، المركز الجامعي صالحى أحمدن نعامة، الجزائر، جانفي 2016، ص ص: 525-539.
125. ميلود حمزاوي، الدبلوماسية الرقمية وتوظيفها عند الرئيس الأمريكي دونالد ترامب المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 01، جامعة الحاج لخضر باتنة 01 الجزائر، جانفي 2020، ص ص: 466-479.
126. ناصر إسماعيل وأمل حسن علوان وتغريد جليل، البطاقة الذكية وأثرها في التقليل من بعض المخاطر المصرفية: (دراسة استطلاعية لعينة من زبائن مصرف الرافدين - فرع الخضراء -)، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد 37، كلية بغداد للعلوم الاقتصادية الجامعة، 2013، ص ص: 77-96.
127. نبيل بن عودة وعائشة بن قارة مصطفى، التعاون القضائي بين الدول ودوره في مكافحة الجرائم المتعلقة بالتميز وخطاب الكراهية في التشريع الجزائري، مجلة الفكر للدراسات

القانونية والسياسية، المجلد 03، العدد 02، جامعة خميس مليانة، جوان 2020 ص ص: 367-357.

128. نجيب بن عمر عوينات، الإرهاب الإلكتروني: (المفهوم والجهود الدولية والإقليمية لمكافحته)، مجلة الأستاذ الباحث، المجلد 02 العدد 02، كلية الحقوق والعلوم السياسية جامعة محمد بوضياف، المسيلة، جوان 2017، ص ص: 9-26.

129. ندى بدر جراح، تقنيات التشفير في التبادل التجاري الإلكتروني، مجلة ميسان للدراسات الأكاديمية، المجلد 07، العدد 14، جامعة ميسان، العراق، 2009، ص ص: 193-210.

130. نسيم تمرنتات، مكافحة الجريمة المنظمة العابرة للأوطان في ظل جهود الإنتربول: (نظرة تقييمية)، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، المركز الجامعي لأفلو، الجزائر، ماي 2020، ص ص: 211-229.

131. نصر قاسمي ومنال عبد الليلة وأسماء بركان، نظم الحوافز والدافعية للإنجاز مجلة التنمية وإدارة الموارد البشرية، المجلد 03، العدد 08، مخبر التنمية التنظيمية وإدارة الموارد البشرية، جامعة البليدة 02، لونيبي علي، الجزائر، فيفري 2017، ص ص: 126-135.

132. نعيمة بن يحيى، الإنابة القضائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم، مجلة الدراسات الحقوقية، المجلد 04، العدد 01، جامعة طاهر مولاي، سعيدة جوان 2017، ص ص: 10-32.

133. نعيمة سداوي، نظام التحفيز لرقى الفرد والمنظمة، مجلة دراسات اقتصادية المجلد 02، العدد 22، جامعة زيان عاشور، الجلفة، أبريل 2014، ص ص: 237-246.

134. نور الدين بن سولة، مجتمع المعلومات في الوطن العربي، مجلة جيل العلوم الإنسانية والاجتماعية، العدد 39، مركز جيل البحث العلمي، الجزائر، فبراير 2018 ص ص: 55-62.

135. نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، المجلد 04، العدد 02، جامعة باتنة 01، الحج لخضر، جوان 2017، ص ص: 908-926.

136. نورة سحري، صعوبات تعريف الإرهاب في القانون الدولي والتي تعيق مكافحته بفعالية، مجلة القانون، المجتمع والسلطة، المجلد 08، العدد 01، جامعة محمد بن أحمد، وهران 02، الجزائر، مارس 2019، ص ص: 175-193.
137. هاجر بوعوة وآمال موترفي، واقع إدارة أمن المعلومات في مؤسسة السويدي إلكترونيك الجزائر، مجلة الريادة لاقتصاديات الأعمال، المجلد 06، العدد 02، جامعة حسيبة بن بوعلي، الشلف، الجزائر، جانفي 2020، ص ص: 199-217.
138. هادي نعيم المالكي وسارة ظافر عبد الحميد، الشروط الخاصة بالجريمة في تسليم المجرمين طبقا لأحكام القانون الدولي والقانون العراقي، مجلة العلوم القانونية، المجلد 33 عدد 06 عدد خاص بالتدريسيين وطلبة الدراسات العليا كلية الحقوق، جامعة بغداد، 2018، ص ص: 151-171.
139. هيبية غربي، نظرية الحرمان النسبي وأسباب التطرف والعنف، مجلة الدراسات الاستراتيجية للكوارث وإدارة الفرص، المجلد 01، العدد 04، المركز الديمقراطي العربي برلين، يناير 2020، ص ص 27-43.
140. وداد سميثي، الحوار الإلكتروني والفضاء العام الافتراضي: (منتديات النقاش الإلكتروني نموذجاً)، مجلة العلوم الإنسانية، العدد 2 المجلد 25، جامعة منتوري، قسنطينة جوان 2014، ص ص 563-578.
141. وداد غزلاني، واقع المجتمع المدني في الجزائر ودوره في تحقيق الرشادة، مجلة القانون، المجتمع والسلطة، المجلد 04، العدد 01، جامعة محمد بن أحمد، وهران 2 فيفري 2015، ص ص: 31-60.
142. وليدة حدادي، الفضاء السيبراني وأزمة القيم الأخلاقية في المجتمعات العربية: (الشبكات الاجتماعية نموذجاً)، مجلة الحقيقة للعلوم الإنسانية والاجتماعية، المجلد 17 العدد 04، جامعة أحمد دراية، أدرار، الجزائر، ديسمبر 2018، ص ص 403-433.
143. ياسمين بونعارة، الجريمة الإلكترونية، مجلة المعيار، المجلد 20 العدد 39، كلية أصول الدين، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، 19 جوان 2015 ص ص 273-314.

4- المواقع الإلكترونية:

أ- مقالات وأبحاث:

1. أحمد السراج الأندلسي، نظام العدالة الجنائية ودور القاضي ورجل القانون في مكافحة الجريمة والوقاية منها، جامعة نايف العربية للعلوم الأمنية، الرياض، 2013، متوفر على الموقع: <https://9anonak.blogspot.com/2016/04/Le-systeme-de-justice-penale-et-le-role-du-juge-et-d-un-homme-de-loi-dans-la-lutte-contre-la-criminalite-et-la-prevention-CDC.html>
2. أحمد السيد، تعريف الاختراق وطرقه وأنواعه وكيفية التصدي له، 06 ديسمبر 2013 تم الاطلاع عليه بتاريخ 16 جانفي 2020، على الساعة 11:32 سا، في الموقع: <https://www.suezbalady.com/index.php/الاختراق-وطرقه-وانواعه-وكيفية-التصدي-له>
3. أحمد صلاح الدين، ازدواجية المعايير والتوظيف السياسي، 25 مارس 2019، تم الاطلاع عليه بتاريخ 15 جانفي 2020، في الموقع: <https://www.omandaily.om/?p=684570>
4. أحمد عبد العليم، اعتبارات الأمن القومي: (لماذا تقاوم روسيا "أمركة" الإنترنت؟)، المستقبل للأبحاث والدراسات المتقدمة، 10 مارس 2015، تم الاطلاع عليه بتاريخ 22 أوت 2020 على الساعة 21:01 سا، في الموقع: <https://n9.cl/z849>
5. أحمد موسى بدوي، الإبادة في بورما: (حين يتحول المسلمون إلى قرابين للعنصرية)، المركز العربي للبحوث والدراسات، 13 يوليو 2015، تم الاطلاع عليه بتاريخ 20 أكتوبر 2019 على الساعة 19:43 سا، في الموقع: <http://www.acrseg.org/39187>
6. أحمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني للين: (قراءة في قانون الأمن السيبراني الصيني)، 27 نوفمبر 2019، تم الاطلاع عليه بتاريخ 05 مارس 2021، على الساعة 22:15 سا، مختص الرابط: <https://cutt.us/hKL4A>
7. آدم مايدة، ليسوا إخواننا: (خطاب الكراهية الصادر عن المسؤولين السعوديين)، مقال منشور على الموقع العربي لهيومن رايتس واتش، 26 سبتمبر 2017، تم الاطلاع عليه بتاريخ 19 ديسمبر 2019 على الساعة 23:25، في الموقع: <https://www.hrw.org/ar/report/2017/09/26/309427>

8. إريك روزنباخ وكاثرين مانستد، رأسمالية البيانات: (تحولات الصراع بين القوى الكبرى على قوة المعلومات)، المستقبل للأبحاث والدراسات المتقدمة، 12 يونيو 2019، تم الإطلاع عليه بتاريخ 17 جانفي 2020، على الساعة 17:36 سا، في الموقع: <https://futureuae.com/ar/Mainpage/Item/4794/> رأسمالية-البيانات-تحولات-الصراع-بين-القوى-الكبرى-على-قوة-المعلومات
9. أشرف دوابة، التجارة الإلكترونية بين الفرص والتحديات، 07 ديسمبر 2019، تم الإطلاع عليه بتاريخ 8 فيفري 2020 على الساعة 18:30 سا، في الموقع: <https://mugtama.com/articles/item/95962-2019-12-07-14-30-38.html>
10. أشرف محمد كشك، الأمن الإستراتيجي والأمن الوطني: (رؤية مستقبلية)، سبتمبر 2019 تم الاطلاع عليه بتاريخ 15 جانفي 2020، على الساعة 15:36 سا، في الموقع: <http://www.akhbar-alkhaleej.com/news/article/1182104>
11. أيمن حسن، دور مواقع التواصل الاجتماعي في نشر الفكر المتطرف، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، 30 سبتمبر 2017، تم الاطلاع عليه بتاريخ 22 جانفي 2020، على الساعة 19:40 سا، في الموقع: <https://www.europarabct.com/> مواقع-التواصل-الاجتماعي-في-نشر-الف
12. إيهاب خليفة، الهجمات الصفرية: (كيف يمكن الاستعداد لليوم الأسود في الإنترنت؟)، 17 مايو 2017، تم الاطلاع عليه بتاريخ 22 جانفي 2020، على الساعة 03:17 سا، في الموقع: <https://futureuae.com/ar/Mainpage/Item/2802/> الهجمات-الصفرية-كيف-يمكن-الاستعداد-اليوم-الأسود-في-الإنترنت
13. إيهاب خليفة، تهديدات سيبرانية: (هل يستطيع القراصنة اختراق المنشأة النووية المستقبل للأبحاث والدراسات المتقدمة)، 07 يناير 2020، تم الاطلاع عليه بتاريخ 28 جانفي 2020، على الساعة 18:55 سا، في الموقع: <https://futureuae.com/ar/Mainpage/Item/5191/> القراصنة-اختراق-المنشآت-النووية
14. إيهاب خليفة، وحدة الأمن السيبراني: الميدان الخامس: الفضاء السيبراني في العقيدة العسكرية لحلف الناتو، المركز المصري للفكر والدراسات الاستراتيجية، 09 فيفري 2020 تم الإطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 16:45 سا، على الموقع: <https://www.ecsstudies.com/8085/>

15. بتول عتوم، ما الفرق بين أمن المعلومات والأمن السيبراني؟، 18 نوفمبر 2019، تم الاطلاع عليه بتاريخ 11 فيفري 2021، على الساعة 17:37 سا، مختصر رابط الموقع: <https://cutt.us/chVCo>
16. جمانة حمدي، الفضاء الإلكتروني يدين خطاب الكراهية المسبب لهجوم نيوزيلندا 15 مارس 2019، تم الاطلاع عليه بتاريخ 28 نوفمبر 2019، على الساعة 19:25 في الموقع: <https://m.arabi21.com/Story/1166783>
17. جورج لبكي، المعاهدات الدولية للإنترنت: حقائق وتحديات، العدد 83، الموقع الرسمي للجيش اللبناني، كانون الثاني 2013، تم الإطلاع عليه بتاريخ 02 جويلية 2020 على الساعة 12:44 سا، مختصر الرابط: <https://n9.cl/w84mw>
18. حسام أبو حامد، إرهاب الدولة ودولة الإرهاب، 6 نوفمبر 2019، تم الاطلاع عليه بتاريخ 28 نوفمبر 2019، على الساعة 23:41 سا، في موقع: <https://blogs.aljazeera.net/blogs/2019/11/6/إرهاب-الدولة-ودولة-الإرهاب>
19. حسام علم الدين، 6 تريليونات دولار خسائر الجرائم الإلكترونية سنوياً.. بحلول 2021، 09 فبراير 2020، تم الإطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 00:39، مختصر الرابط: <https://cutt.us/doNwr>
20. حنان عماد زهران، تشریح مفهوم السيادة، 27 مارس 2019، تم الاطلاع عليه بتاريخ 13 جانفي 2020 على الساعة 22:30 سا، في الموقع: <https://democraticac.de/?p=59802>
21. خالد الغالي، البطالة والإرهاب... ماذا تقول الدراسات؟، 04 ديسمبر 2016، تم الاطلاع عليه بتاريخ 19 ديسمبر 2019 على الساعة 22:23 في الموقع: <https://www.irfaasawtak.com/rights-and-liberties/2016/12/04/البطالة-والإرهاب-تقول-الدراسات؟>
22. ديفيد اغناتيوس، روسيا تحاول السيطرة على الفضاء السيبراني، جريدة الشرق الأوسط: (جريدة العرب الدولية)، العدد 14216، 30 أكتوبر 2017، تم الإطلاع عليه بتاريخ 22 أوت 2020 على الساعة 05:42 سا، مختصر الرابط: <https://n9.cl/14va>

23. رولان مرعب، تداعيات الهجرة غير الشرعية على أوروبا وأبعادها، منشورات، العدد 98، تشرين الأول 2016، موقع الدفاع الوطني اللبناني، تم الاطلاع عليه بتاريخ 18 فيفري 2021، على الساعة 22:58 سا، مختصر الرابط: <https://cutt.us/PF6y6>
24. ريهام عبد الرحمن رشاد العباسي، أثر الإرهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية: (دراسة حالة تنظيم داعش "الدولة الإسلامية")، المركز الديمقراطي العربي، 24 يوليو 2016، تم الاطلاع عليه بتاريخ 27 جانفي 2020، على الساعة 22:19، في الموقع: <https://democraticac.de/?p=34528>
25. زينب مصطفى رويحه، تحديات الدور: (الأمن السيبراني في توجهات روسيا الإفريقية)، قراءات إفريقية، 13 نوفمبر 2019، تم الاطلاع عليه بتاريخ 22 أوت 2020 على الساعة 21:28 سا، مختصر الرابط: <https://n9.cl/vlhao>
26. سعيد علي الحاج بكري، الأمن السيبراني ..و الشراكة بين القطاعين العام والخاص جريدة العرب الاقتصادية الدولية، 11 أكتوبر 2018، تم الاطلاع عليه بتاريخ 02 أوت 2020 على الساعة 16:26 في الموقع: https://www.aleqt.com/2018/10/11/article_1468696.html
27. سعيد علي الحاج بكري، الأمن السيبراني ..و الشراكة بين القطاعين العام والخاص جريدة العرب الاقتصادية الدولية، 11 أكتوبر 2018، تم الاطلاع عليه بتاريخ 02 أوت 2020 على الساعة 16:26 في الموقع: https://www.aleqt.com/2018/10/11/article_1468696.html
28. سمر حسن الباجوري، الأسباب الاقتصادية لتنامي ظاهرة الإرهاب في إفريقيا جنوب الصحراء، المستودع العلمي (MPRA)، 31 ماي 2016، تم الإطلاع عليه بتاريخ 16 فيفري 2020 على الساعة 5:57 سا، في الموقع: <https://mpra.ub.uni-muenchen.de>
29. شفيق نوران، حوكمة الإنترنت: (أبعاد الصراع على إدارة الفضاء الإلكتروني)، موقع المستقبل للأبحاث والدراسات المتقدمة، 12 يوليو 2014، تم الاطلاع عليه بتاريخ 15 جويلية 2020، على الساعة 15:22 سا، مختصر الرابط: <https://n9.cl/9wkq>
30. شيماء عويس، القوة في العلاقات الدولية: (دراسة تأصيلية)، 05 أكتوبر 2018 تم الاطلاع عليه بتاريخ 20 فيفري 2020 على الساعة 15:32 سا، في المواقع: <https://eipss-eg.org/> -العلاقات-الدولية-دراسة-تأصيلية/

31. صالح حميد، المجلس السيبراني في إيران.. يد إلكترونية لقمع الحريات، 12 مارس 2020، تم الاطلاع عليها بتاريخ 22 مارس 2020 على الساعة 08:06 سا، في الموقع: <https://www.alarabiya.net/ar/iran/2020/03/12/الالكترونية-لقمع-الحريات>
32. صباح عبد الصبور، تكتيكات مضادة: (حدود قدرة إيران على توظيف الاختراقات السيبرانية)، المستقبل للأبحاث والدراسات المتقدمة، 02 أبريل 2019، تم الاطلاع عليه بتاريخ 25 جانفي 2020، على الساعة 21:31 سا، في الموقع: <https://futureuae.com/ar/Mainpage/Item/4645/ايران-على-توظيف-الاختراقات-السيبرانية>
33. عادل عبد الصادق، الإرهاب الإلكتروني والصراع الدولي، ندوة المركز الدولي للدراسات المستقبلية والاستراتيجية، أبريل 2012، تم الاطلاع على الندوة بتاريخ 12 نوفمبر 2019 على الساعة 15:35 سا، على الرابط التالي: <https://youtu.be/gB8H4PZWvQk>
34. عادل عبد الصادق، الأمم المتحدة ودعم الاستخدام السلمي للفضاء الإلكتروني المركز العربي لأبحاث الفضاء الإلكتروني، 06 أغسطس 2015، تم الاطلاع عليه بتاريخ 27 أوت 2020، على الساعة 07:38 سا، في الموقع: http://accronline.com/article_detail.aspx?id=22762
35. عبد الفتاح ماضي، العوامل الخارجية والثورات العربية: (أربع إشكاليات للبحث) سياسات عربية، العدد 36، المركز العربي للأبحاث ودراسة السياسية، يناير 2019، تم الاطلاع عليه بتاريخ 19 نوفمبر 2019 على الساعة 01:00 سا، في موقع: <https://siyasatarabiya.dohainstitute.org/ar/issue036/Pages/art01.aspx>
36. عبد المطلب أبو سيف، الحماية ضد الصواعق، الموسوعة العربية، تم الاطلاع عليه بتاريخ 03 جويلية 2020، على الساعة 10:21 سا، على الموقع: <http://arab-ency.com.sy/detail/4924>
37. عبد النبي الشحات، حجب المواقع الإرهابية.. وقانون الجريمة الإلكترونية، صحيفة اليوم السابع، 30 مايو 2017، تم الاطلاع عليه بتاريخ 13 أوت 2020 على الساعة 20:17، مختصر الرابط: <https://n9.cl/yhe5>
38. عبد الوهاب جمال، السيادة: مقوماتها وأركانها، 23 جويلية 2018 تم الاطلاع عليه بتاريخ 13 جانفي 2020 على الساعة 22:12 سا، في الموقع: <https://www.lediplomate.tn/السيادة-مقوماتها-و-أركانها/>

39. عدنان مصطفى البار، خالد على المرحبي، الاقتصاد الرقمي، 21 جانفي 2019، تم الاطلاع عليه بتاريخ 3 فيفري 2020 على الساعة 21:22 سا، في الموقع: <https://www.awforum.org/index.php/en/component/k2/item/208-الرقمي>
40. عزامي بشارة، تنظيم الدولة المكنى "داعش": (أطار عام ومساهمة نقدية في فهم الظاهرة)، المركز العربي للأبحاث ودراسة السياسات، تم الإطلاع عليه بتاريخ 22 ديسمبر 2019 على الساعة 19:23 سا، في الموقع: <https://siyasatarabiya.dohainstitute.org/ar/issue035/Pages/art01.aspx>
41. عزمي بشارة، أصحح أن معادة الصهيونية هي أحد الأشكال الحديثة لمعاداة السامية، المركز العربي للأبحاث ودراسة السياسات، 28 فبراير 2019، تم الاطلاع عليه بتاريخ 18 أكتوبر 2019 على الساعة 18:05 سا، في موقع: <https://www.dohainstitute.org/ar/PoliticalStudies/Pages/Is-Anti-Zionism-a-Form-of-Anti-Semitism-Anti-Zionism-as-a-Jewish-Phenomenon.aspx>
42. عزمي بشارة، قانون القومية: (كم مرة سوف يعلنون قيام إسرائيل)، المركز العربي للأبحاث ودراسة السياسات، 24 يوليو 2018، تم الاطلاع عليه بتاريخ 18 أكتوبر 2019 على الساعة 18:20 سا، في الموقع: <https://www.dohainstitute.org/ar/PoliticalStudies/Pages/Israel-Nation-State-Law-Repeatedly-Declaring-State.aspx>
43. عمرو صلاح، قرصنة الديمقراطية: (الأنماط المتعددة للاختراق الإلكتروني للسياسات الداخلية للدول)، المستقبل للأبحاث والدراسات المتقدمة، 02 فبراير 2017، تم الاطلاع عليه بتاريخ 13 فيفري 2020، على الساعة 15:30 سا، في الموقع: <https://futureuae.com/ar/Mainpage/Item/2439/المتعددة-للاختراق-الإلكتروني-للسياسات-الداخلية-للدول>
44. فاطمة الزهراء عبد الفتاح، سيميوطيقا داعش: (دلائل استخدام الإرهابيين للرموز والشعارات على الإنترنت)، 15 مارس 2017، تم الاطلاع عليه بتاريخ 12 ديسمبر 2019 على الساعة 18:55 سا، في الموقع: <https://futureuae.com/ar/Mainpage/Item/2575/استخدام-الإرهابيين-للمرموز-والشعارات-على-الإنترنت>

45. فرح عصام، استراتيجية "تشي" الثورية.. كيف تغير الصين مستقبل الإنترنت في العالم؟، موقع الجزيرة، 02 جويلية 2020، تم الاطلاع عليه بتاريخ 05 مارس 2021 على الساعة 22:17 سا، مختصر الرابط: <https://cutt.us/E6TqF>
46. كارولين سايج، حرب الأفكار الجديدة: (تأثيرات "التضليل الرقمي" في مكافحة الغرب للإرهاب)، المستقبل للأبحاث والدراسات المتقدمة، 08 يوليو 2019، تم الاطلاع عليه بتاريخ 13 فيفري 2020، على الساعة 16:02 سا، في الموقع: <https://futureuae.com/ar/Mainpage/Item/4838/> حرب-الأفكار-الجديدة-تأثيرات-التضليل-الرقمي-في-مكافحة-الغرب-للإرهاب
47. محمد شوقي عبد العال، رؤية سياسية قانونية: (التطورات المعاصرة في ظاهرة الإرهاب الدولي 1-2)، المركز العربي للبحوث والدراسات، 10 ديسمبر 2015، تم الاطلاع عليه بتاريخ 26 أكتوبر 2019، على الساعة 15:12 سا، في الموقع: <http://www.acrseg.org/39685>
48. محمد عاكف جمال، تداعيات الدفعة الثالثة من وثائق ويكيليكس، 10 ديسمبر 2010، تم الاطلاع عليه بتاريخ 12 أكتوبر 2019، على الساعة 12:55 سا، في الموقع: <https://www.albayan.ae/opinions/2010-12-10-1.595130>
49. محمد عبيد، المصادر القانونية لنظم تسليم المجرمين، المعهد المصري للدراسات 11 مارس 2019، تم الاطلاع عليه بتاريخ 12 سبتمبر 2020 على الساعة 00:09 سا مختصر الرابط: <https://n9.cl/0pgd>
50. محمد عزت هلال، آليات المواجهة: (تهديدات الأمن الإلكتروني في قطاع الطيران المدني)، المستقبل للأبحاث والدراسات المتقدمة، 25 مايو 2017، تم الاطلاع عليه بتاريخ 15 جانفي 2020، على الساعة 21:14 سا، في الموقع: <https://futureuae.com/ar/Mainpage/Item/2827/> آليات-المواجهة-تهديدات-الأمن-الإلكتروني-في-قطاع-الطيران-المدني
51. محمد قيراط، الإرهاب الإلكتروني... التحديات وآليات المواجهة، 20 يونيو 2015 تم الإطلاع عليه بتاريخ 02 سبتمبر 2020 على الساعة 10:36 سا، في الموقع: <https://elaph.com/Web/NewsPapers/2015/6/1017643.html>
52. مروان العشاب، الإنابة القضائية كأحد تجليات التعاون القضائي الدولي، مجلة مغرب القانون، 15 ديسمبر 2015، تم الاطلاع عليه بتاريخ 03 سبتمبر 2020، على الساعة 12:31 سا، مختصر الرابط: <https://n9.cl/9hf2>

53. مروان صالح، مخاطر سيبرانية: (أشكال الإبتزاز الإلكتروني من سرقة الهويات إلى اختراق الصناعات)، المستقبل للأبحاث والدراسات المتقدمة، 07 مايو 2018، تم الاطلاع عليه بتاريخ 16 أكتوبر 2019، على الساعة 19:40، في الموقع: <https://futureuae.com/ar/Mainpage/Item/3897/> الإلكتروني-من-سرقة-الهويات-إلى-اختراق-الصناعات
54. مروة الأسدي، سباق التجسس الإلكتروني وزعزعة النظام العالمي، 20 ديسمبر 2017، تم الاطلاع عليها بتاريخ 18 جانفي 2020، على الساعة 23:12، سا، في الموقع: <https://m.annabaa.org/arabic/informatics/13571>
55. مهدي سلمان الرسام، الإرهاب الرقمي الإلكتروني ناقوس الخطر القادم، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، 12 جوان 2019، تم الاطلاع عليه بتاريخ 16 أكتوبر 2019، على الساعة 19:44، سا، على الموقع: <https://www.politics-dz.com/> الإرهاب-الرقمي-الإلكتروني-ناقوس-الخط
56. نانيس عبد الرزاق فهمي، الحرب السيبرانية: حرب القرن القادم، 15 نوفمبر 2018 تم الاطلاع عليه بتاريخ 17 جانفي 2020 على الساعة 15:47، سا، في موقع: <https://www.raialyoum.com/index.php/> الحرب-السيبرانية-حرب-القرن-القادم
57. نجوى السوداء، بحث الفضاء السيبراني، 15 مايو 2015، تم الاطلاع عليه 12 فيفري 2020 على الساعة 12:42، سا، في الموقع: <https://seconf.wordpress.com/2015/05/15/> بحث-الفضاء-السيبراني
58. نسرین الشحات الصباحي، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول (دراسة حالة إسرائيل)، المركز العربي الديمقراطي، 29 أبريل 2016، تم الاطلاع عليه بتاريخ 28 ديسمبر 2019، على الساعة 19:07، سا، في الموقع: <https://democraticac.de/?p=30962>
59. نضال نعيسة، الاستبداد، (د.ت.ن)، تم الاطلاع عليه بتاريخ 27 مارس 2020 على الساعة 09:39، سا، في الموقع: <http://www.arabtimes.com/A2006/may/9.html>
60. هاجر حسونة، الإرهاب الإلكتروني.. هل يتحول لمصدر التهديد الأول للعالم؟، 04 ماي 2015، تم الاطلاع عليه بتاريخ 17 أكتوبر 2019، على الساعة 18:21، سا، في الموقع: <https://alkhaleejonline.net/> علوم-وتكنولوجيا-الإرهاب-الإلكتروني-هل-يتحول-لمصدر-التهديد-الأول-للعالم؟

61. هدير أبو زيد، السيادة الإلكترونية: اتجاهات تشكيل مناطق سيبرانية تحت سيطرة الدول والشركات، مركز المستقبل للأبحاث والدراسات المتقدمة، 23 سبتمبر 2020، تم الإطلاع عليه بتاريخ 12 فيفري 2021، على الساعة 22:57، مختصر الرابط: <https://cutt.us/qC4B4>
62. هناء الكحلوت، الطفل أكبر ضحايا " إرهاب " الإنترنت.. كيف يستدرج؟، 10 مارس 2017، تم الاطلاع عليه بتاريخ 25 جانفي 2020، على الساعة 00:21 سا، في الموقع: <https://alkhaleejonline.net/مجتمع/الطفل-أكبر-ضحايا-إرهاب-الإنترنت-كيف-يُستدرج؟>
63. رغدة البهي، علاقات متشابكة: كيف تدعم التجارة الرقمية سياسات الأمن السيبراني؟ 02 أكتوبر 2019، تم الإطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 03:23 سا مختصر الرابط: <https://cutt.us/NSZQb>
64. زينب مصطفى رويحه، تحديات الدور: الأمن السيبراني في توجهات روسيا الإفريقية، 13 نوفمبر 2019 تم الاطلاع عليه بتاريخ 12 فيفري 2021، على الساعة 11:23 سا، مختصر رابط الموقع: <https://cutt.us/jMEO2>
65. يوسف الحسن، ثقافة المقاومة، 14 فبراير 2017، تم الاطلاع عليه بتاريخ 12 نوفمبر 2019 على الساعة 17:12 سا، في الموقع: <https://www.alittihad.ae/article/9523/2017/ثقافة-المقاومة>

ب - القواميس:

66. قاموس المعاني: <https://www.almaany.com/ar/dict/ar-ar/> أرهاب
67. قاموس ترجمان: Digital Forensic: <https://torjoman.com/dictionary/search/2-1/Digital+Forensic>
68. القاموس العملي للقانون الإنساني، المحكمة الجنائية الدولية ليوغوسلافيا السابقة والمحكمة الجنائية الدولية لرواندا، موقع أطباء بلا حدود، (د.ت.ن)، تم الاطلاع عليه بتاريخ 25 سبتمبر 2020، على الساعة 01:30 سا، في الموقع: <https://ar.guide-humanitarian-law.org/content/article/5/lmhkm-ljnyy-lwly-lywgwslfy-lsbq-wlmhkm-ljnyy-lwly-lwnd/>

ج- الموسوعات:

69. الموسوعة الحرة: ويكيبيديا.
70. الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، أسلحة المراقبة الشاملة 17 جوان 2019، تم الإطلاع عليه بتاريخ 18 أكتوبر 2019، على الساعة 20:30 سا على موقع: <https://www.politics-dz.com/أسلحة-المراقبة-الشاملة/>
71. الموسوعة الجزائرية للدراسات الاستراتيجية والسياسية، قوة الفضاء السيبراني: (الثقافة والسياسة في الفضاء الإلكتروني والإنترنت)، 27 نوفمبر 2019، تم الاطلاع عليه بتاريخ 15 فيفري 2020، على الساعة 19:17 سا، في الموقع: <https://www.politics-dz.com/الفضاء-السيبراني-الثقافة-والسياس/>
72. الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، الدبلوماسية الرقمية .. القوة الناعمة الجديدة، 22 نوفمبر 2018، تم الاطلاع عليه بتاريخ 06 فيفري 2021، على الساعة 17:23 سا، مختصر الرابط: <https://cutt.us/mgCZg>
73. الموسوعة السياسية، الأمن السيبراني، (د.ت.ن)، تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 16:25، في موقع الموسوعة، مختصر رابط الموقع: <https://cutt.us/Z0R0L>
74. الموسوعة السياسية، عوامل قوة الدولة في المجال الدولي، تم الاطلاع عليه بتاريخ 22 فيفري 2021، على الساعة 08:02 سا، مختصر الرابط: <https://cutt.us/Nm9O6>
- د- مصادر متنوعة في مواقع مختلفة:

75. قناة العربية، بعد عودة الإنترنت... إيران تحجب كل شبكات التواصل الأجنبية، 21 نوفمبر 2019، تم الاطلاع عليه بتاريخ 16 ديسمبر 2019 على الساعة 01:33 سا، في الموقع: <https://www.alarabiya.net/ar/iran/2019/11/21/ايران-تحجب-كل-شبكات-التواصل-الأجنبية>
76. هيئة الأمم المتحدة، حقوق الإنسان، (د.ت.ن)، تم الاطلاع عليها بتاريخ 15 جانفي 2020، على الساعة 22:23 سا، على موقع: <https://www.un.org/ar/sections/issues-depth/human-rights/>

77. موقع قناة الجزيرة، ليبيراسيون:(كيف أسكتت السلطات الإيرانية صوت الاحتجاجات)، 20 نوفمبر 2019، تم الاطلاع عليها بتاريخ 18 فيفري 2020 على الساعة 19:23 سا، في الموقع:

<https://www.aljazeera.net/news/politics/2019/11/20/-إيران-الاحتجاج-القمع-الإنترنت-البنزين-خامنئي>

78. صحيفة الشرق، تقارير عالمية:(أبوظبي تمارس الإرهاب الإلكتروني وتهدد الأمن السيبراني الإقليمي)، 22 مايو 2019، تم الاطلاع عليه بتاريخ 12 جانفي 2020، على الساعة 18:53 سا، في الموقع:

<https://m.al-sharq.com/article/22/05/2019/-تقارير-عالمية-أبوظبي-تمارس-الإرهاب-الكثروني-وتهدد-الأمن-السيبراني-الإقليمي>

79. حملة المركز العربي لتطوير الإعلام الاجتماعي، شبكة مسكتة:(تثلي الشباب الفلسطيني لا يشعرون بالأمان للمشاركة السياسية عبر الإنترنت)، 20 أكتوبر 2019، تم الاطلاع عليه بتاريخ 18 أكتوبر 2019، على الساعة 18:33 سا، على موقع:

<https://7amleh.org/2019/10/20/شبكة-مُسكَّتة-تثلي-الشباب-الفلسطيني/>

80. عربية سكاي نيوز، نساء داعش " الوديعات " .. " الأقوى " في تجديد الإرهابيين، 10 ديسمبر 2018، تم الاطلاع عليه بتاريخ 22 جانفي 2020، على الساعة 20:00 سا، في الموقع:

<https://www.skynewsarabia.com/world/1207068-نساء-داعش-الوديعات-الأقوى-تجديد-الإرهابيين>

81. الإنتربول، بحوث الإنتربول في المجال السيبراني تكشف عن تهديد تشكله البرمجيات الخبيثة على العملات الافتراضية، 26 مارس 2015، تم الاطلاع عليه بتاريخ 16 أكتوبر 2019، على الساعة 19:30، في موقع:

<https://www.interpol.int/ar/1/1/2015/4>

82. وزراء الاتصالات وتقنية المعلومات، تقرير: الجرائم الإلكترونية تكبد الاقتصاد العالمي خسائر بقيمة 445 مليار دولار سنوياً،(د.ت.ن)، تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 00:48، على الموقع الوزارة:

<https://www.mcit.gov.sa/ar/media-center/news/94698> 83.

84. موقع صانعو الحدث، ما هو أثر الجريمة الإلكترونية على اقتصادات الدول؟، 19 أكتوبر 2016، تم الاطلاع عليه بتاريخ 13 فيفري 2021، على الساعة 00:43، مختصر الرابط: <https://cutt.us/e4Akx>
85. فراس اللو، أفضل الأساليب التقنية لتخطي حجب المواقع، نشر على موقع الجزيرة بتاريخ 04 جوان 2017، تم الاطلاع عليه بتاريخ 18 جويلية 2020، على الساعة 18:22 سا، مختصر الرابط: <https://n9.cl/c51e3>
86. إفريقيا تواجه مأزقاً بين مكافحة الجريمة الإلكترونية وضمان حقوق الإنسان، الإمارات اليوم، دبي، نشر بتاريخ 28 أبريل 2015، تم الاطلاع عليه بتاريخ 17 أوت 2020، على الساعة 19:41 سا، في الموقع: <https://www.emaratalyoun.com/technology/electronic-equipment/2015-04-28-1.779166>
87. شبكة الأمم المتحدة للعدالة الجنائية ومنع الجريمة، جامعة نايف العربية للعلوم الامنية: <https://nauss.edu.sa/ar-sa/departments/InternationalCooperation/international-acts/Pages/CrimePrevention.aspx>
88. سوريا: قانون مكافحة الجرائم الإلكترونية يهدد حرية الرأي والتعبير على الإنترنت مركز الخليج لحقوق الإنسان، 16 ماي 2018، تم الاطلاع عليه بتاريخ 02 سبتمبر 2020، على الساعة 10:55 سا، في الموقع: <https://www.gc4hr.org/news/view/1862>
89. التصدي لتهديدات الجريمة السيبرية، موقع الإنتربول: تم الإطلاع عليه بتاريخ 03 سبتمبر 2020 على الساعة 09:56 سا: في الموقع: <https://www.interpol.int/ar/4/6/1>
90. تدريب ضباط ليبين على التصدي لأنشطة الإرهابيين على الإنترنت، الإنتربول، 24 يناير 2020، تم الاطلاع عليه بتاريخ 03 سبتمبر 2020، على الساعة 10:07 سا، في الموقع: <https://www.interpol.int/ar/1/1/2020/4>
91. مراسل آر تي، منفذ العملية الإرهابية في نيس مهاجر غير شرعي يحمل الجنسية التونسية، 29 أكتوبر 2020، تم الاطلاع عليه بتاريخ 18 فيفري 2021، على الساعة 22:55، مختصر الرابط: <https://cutt.us/AQyFv>

92. إنشاء تحالف دولي جديد لمكافحة الجرائم الإلكترونية حول العالم، موقع قناة بي بي سي (BBC)، 05 يوليو 2011، تم الاطلاع عليه بتاريخ 12 سبتمبر 2020 على الساعة 11:36 سا، في الموقع:

https://www.bbc.com/arabic/scienceandtech/2011/07/110705_international_body_cyber_crimes

93. وليد رمزي، الجزائر - 44 بالمائة من الجزائريين محاولات قرصنة إلكترونية، حدث منشور على موقع: TSA عربي، بتاريخ 28 مارس 2018، على الساعة 11:48 تم الاطلاع عليه في 18 فيفري 2020 على الساعة 10:16:

<https://www.tsa-algerie.com/ar/الجزائر-44-بالمائة-من-الجزائريين-واجهو/>

94. موقع: <https://icct.nl/people/dr-alex-p-schmid-visiting-research-fellow/>

95. موقع: <https://faculty.mu.edu.sa/naouinette/mycv>

96. مكافحة الإرهاب .. مهام وصلاحيات اليوروبول، المركز الأوربي لدراسات مكافحة الإرهاب والاستخبارات، 04 يوليو 2019، تم الاطلاع عليه بتاريخ 20 سبتمبر 2020، على الساعة 20:34 سا، في موقع المركز:

<https://www.europarabct.com/%D9%85%D9%87%D8%A7%D9%85-%D9%88%D8%B5%D9%84%D8%A7%D8%AD%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D9%8A%D9%88%D8%B1%D9%88%D8%A8%D9%88%D9%84-%D9%81%D9%8A-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%A7/>

5- النصوص القانونية:

أ. القوانين الوطنية:

أ.1: الدساتير:

1. الدستور القطري، الصادر في الديوان الأميري بتاريخ 8 جوان 2004.
2. دستور الإمارات العربية المتحدة، الصادر عام 1971 شاملا تعديلاته لغاية عام 2009.

أ. 2: قوانين:

3. قانون جنسية الرايخ المؤرخ بتاريخ 15 سبتمبر 1935
4. قانون حماية الدم والشرف الألماني المؤرخ بتاريخ 15 سبتمبر 1935.
5. الأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم.
6. الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.
7. القانون عدد 83 لسنة 2000، مؤرخ في 09 أوت 2000، يتعلق بالمبادلات والتجارة الإلكترونية، ر.ر.ج.ت عدد 64، 11 أوت 2000.
8. القانون رقم 11 لسنة 2007، يتعلق بقانون المعاملات الإلكترونية، صدر بتاريخ 14 جوان 2007.
9. القانون رقم 09-04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر. عدد 47 لسنة 2009.
10. القانون رقم (9) لسنة 2011 المتعلق بتنظيم استخدام كاميرات وأجهزة المراقبة الأمنية، صدر بتاريخ 08 ماي 2011، في الجريدة الرسمية العدد 07، المنشورة بتاريخ 20 جوان 2011.
11. القانون رقم 18-04 المؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر. عدد 27 لسنة 2018.
12. قانون رقم 18-05 المؤرخ في 10 مايو 2018 والمتعلق بالتجارة الإلكترونية المنشورة ب16 مايو 2018، ، الجريدة الرسمية رقم 28.
13. القانون رقم 20-05 المؤرخ بتاريخ 28 أبريل 2020 يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج.ر. عدد 25 لسنة 2020.

أ. 3: المراسيم والقرارات:

14. مرسوم سلطاني رقم 69/2008، بإصدار قانون المعاملات الإلكترونية، صدر ب 17 مايو 2008، ج.ر. عدد 864 لسنة 2008.

15. مرسوم بقانون اتحادي رقم 5 الصادر بتاريخ 13 أوت 2012 في شأن مكافحة جرائم تقنية المعلومات المعدل بموجب القانون الاتحادي رقم 12 الصادر بتاريخ 23 ماي 2016 الجريدة الرسمية رقم 540 ملحق ص 19، الإمارات العربية المتحدة.
16. مرسوم بقانون اتحادي رقم 5 الصادر بتاريخ 13 أوت 2012 في شأن مكافحة جرائم تقنية المعلومات المعدل بموجب القانون الاتحادي رقم 12 الصادر بتاريخ 23 ماي 2016 الجريدة الرسمية رقم 540 ملحق ص 19، الإمارات العربية المتحدة.
17. المرسوم الأميري رقم 07 لسنة 2016، بشأن تنظيم تداول واستخدام أجهزة ومعدات الرقابة على المباني في عجمان
18. القرار الوزاري رقم 260 لسنة 2019 الصادر بتاريخ 27 مارس 2019 في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات المدنية، المنشور الجريدة الرسمية رقم 651.
19. القرار الوزاري رقم 259 لسنة 2019 الصادر بتاريخ 27 مارس 2019 في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات الجزائية، المنشور الجريدة الرسمية رقم 651.

ب. الاتفاقيات الدولية والإقليمية:

20. ميثاق الأمم المتحدة لعام 1945.
21. اتفاقية الرياض العربية للتعاون القضائي، وقعت في الرياض بتاريخ 06 أبريل 1983، ودخلت حيز التنفيذ بداية من 30 أكتوبر 1985.
22. اتفاقية الأمم المتحدة لقانون البحار فتح التوقيع عليها بتاريخ 10 ديسمبر سنة 1982 جامايكا، ودخلت حيز النفاذ بتاريخ 14 نوفمبر 1994.
23. اتفاقية تنفيذ الأحكام والإعلانات القضائية بدول مجلس التعاون لدول الخليج العربية، التي صودق عليها بدول مجلس التعاون لدول الخليج العربية في دورته السادسة عشر، المنعقدة بسلطنة عمان في ديسمبر 1995، أنظر: المرسوم رقم 16 لسنة 1996 المتضمن

تصديق دولة قطر على هذه الاتفاقية الصادر بتاريخ 24 أبريل 1996، ج.ر. عدد 04، المنشورة بتاريخ 20 ماي 1996.

24. اتفاقية مجلس أوروبا المتعلقة بمكافحة الجريمة الإلكترونية، صودق عليها بتاريخ 23 أكتوبر 2001، بالعاصمة بودابست، المجر.

25. معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي، الصادرة بتاريخ 28 جويلية 1999، ج.ر. عدد 07 لدولة قطر، 27 جويلية 2006.

26. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 نوفمبر 2000.

27. اتفاقية مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب، الصادرة بتاريخ 04 ماي 2004، ج.ر. عدد 07 لدولة قطر، 24 جويلية 2008.

28. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقع عليها بالقاهرة بتاريخ 21 ديسمبر 2010، والداخله حيز التنفيذ بتاريخ 06 فيفري 2014.

29. اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المعتمدة في الدورة العادية 23 لقمة رؤساء دول وحكومات الاتحاد الأفريقي غينيا الاستوائية، بتاريخ 27 يونيو 2014.

30. النظام الأساسي لآلية الاتحاد الأفريقي للتعاون الشرطي "آفريبول"، اعتمدته الدورة العادية الثامنة والعشرون للمؤتمر المنعقد بأديس أبابا، إثيوبيا، بتاريخ 30 يناير 2017.

ج. الاتفاقيات الثنائية:

31. أمر رقم 61-70 المؤرخ بتاريخ 8 أكتوبر 1970 يتضمن المصادقة على الاتفاقية بين الجمهورية الجزائرية الديمقراطية الشعبية والمملكة البلجيكية، المتعلقة بتسليم المجرمين والتعاون القضائي في المواد الجنائية، الموقعة ببروكسيل في 12 يولي 1970.

32. مرسوم رقم 84-25 المؤرخ بتاريخ 11 فبراير 1984 يتضمن المصادقة على اتفاقية التعاون القضائي والعدلي في المواد المدنية والتجارية والعائلية والجزائية بين الجمهورية الجزائرية الديمقراطية الشعبية والجمهورية الشعبية المجرية، الموقع عليها بالجزائر بتاريخ 07 فبراير 1976.
33. المرسوم الرئاسي رقم 07-323 المؤرخ في 23 أكتوبر 2007، يتضمن التصديق على اتفاقية التعاون القضائي والإعانات والإنابات القضائية وتنفيذ الأحكام وتسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ودولة الإمارات العربية المتحدة الموقعة بالجزائر بتاريخ 12 أكتوبر 1983، ج.ر. عدد 67، 24 أكتوبر 2007.
34. المرسوم الرئاسي رقم 05-193 المؤرخ في 28 مايو 2005، يتضمن التصديق على المعاهدة المتعلقة بتسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية وحكومة جمهورية نيجيريا الاتحادية، الموقعة بالجزائر في 12 مارس 2003، ج.ر. عدد 38 لسنة 2005.
35. المرسوم الرئاسي رقم 08-85 المؤرخ في 09 مارس 2008، يتضمن التصديق على اتفاقية تسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا، الموقعة بالجزائر في 12 ديسمبر 2006، ج.ر. عدد 14، لسنة 2008.
36. المرسوم رقم 55 لسنة 2016، المتعلق بالتصديق على اتفاقية تعاون بين حكومة دولة قطر وحكومة سلطنة عمان في المجال الأمني، 14 ديسمبر 2016، ج.ر. عدد 01 12 فبراير 2017
37. المرسوم رقم 84 لسنة 2017، المتعلق بالتصديق على اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر وحكومة الجمهورية الجزائرية الديمقراطية الشعبية، 06 نوفمبر 2017، ج.ر. عدد 15، 27 ديسمبر 2017.
38. المرسوم رقم 07 لسنة 2020، المتعلق بالتصديق على اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر ومكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن إنشاء وتمويل مركز الأمم المتحدة الإقليمي لمكافحة الجريمة السيبرانية في الدوحة، 02 مارس 2020، ج.ر. عدد 07، 22 أبريل 2020.

د. قرارات الجمعية العامة للأمم المتحدة:

39. قرار الجمعية العامة رقم 1514، الدورة 15، المتضمن إعلان منح الاستقلال للبلدان والشعوب المستعمرة الصادر بتاريخ 20 ديسمبر 1960.
40. قرار الجمعية العامة رقم 56/183 الصادر بتاريخ 31 جانفي 2002، المتضمن مؤتمر القمة العالمي لمجتمع المعلومات
41. قرار الجمعية العامة للأمم المتحدة رقم 288/60 المتعلقة باستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، المؤرخ بتاريخ 08 سبتمبر 2006.
42. قرار الجمعية العامة في 29 ديسمبر 2014، قرار رقم 69-245: المحيطات وقانون البحار.
43. قرار الجمعية العامة للأمم المتحدة رقم 157/73 المتعلق بمحاربة تمجيد النازية والنازية الجديدة والممارسات الأخرى التي تساهم في إثارة الأشكال المعاصرة من العنصرية والتمييز العنصري وكراهية الأجانب وما يتصل بذلك من تعصب، المؤرخ بتاريخ 17 ديسمبر 2018.
44. قرار الجمعية العامة للأمم المتحدة رقم 264/73 المتعلق بحالة حقوق الإنسان في ميانمار، المؤرخ بتاريخ 22 ديسمبر 2018.

6- وثائق أخرى:

1. محضر مجلس الأمن، الجلسة 4838 المنعقدة بتاريخ 09 أكتوبر 2003، والتي تضمن جدول أعمالها: المحكمة الدولية لمحاكمة الأشخاص المسؤولين عن الانتهاكات الجسيمة للقانون الدولي التي ارتكبت في أقاليم يوغسلافيا السابقة منذ عام 1991، المحكمة الجنائية الدولية لمحاكمة الأشخاص المسؤولين عن أعمال الإبادة الجماعية وغير ذلك من الانتهاكات الجسيمة للقانون الدولي الإنساني المرتكبة في إقليم رواندا والموا كطنين الروانديين المسؤولين عن أعمال الإبادة الجماعية وغيرها من الانتهاكات المماثلة المرتكبة في أراضي الدول المجاورة بين 1 يناير و31 ديسمبر 1994، (نسخة مؤقتة).
2. مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب، الأمم المتحدة، نيويورك، 2009.

3. اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، حوكمة الإنترنت: (تحديات وفرص للبلدان الأعضاء في الإسكوا)، الأمم المتحدة، نيويورك، 2009.
4. الأمم المتحدة، استخدام الإنترنت لأغراض إرهابية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، نيويورك 2013.
5. محضر موجز للجلسة الثالث للجنة السادسة للجمعية العامة المتضمنة التدابير الرامية إلى مكافحة الإرهاب الدولي، الدورة 69، المؤرخ بتاريخ 27 أكتوبر 2014.
6. الأمان في الفضاء السيبراني وومكافحة الجرائم السيبرانية في المنطقة العربية: (توصيات سياسية)، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، الأمم المتحدة نيويورك، 2015.
7. عمل معهد الأمم المتحدة الأقاليمي لأبحاث الجريمة والعدالة، تقرير المجلس الاقتصادي والاجتماعي، الأمم المتحدة، 9 مارس 2015، الوثيقة (E/CN.15/2015/12).
8. جنة منع الجريمة والعدالة الجنائية، الدورة 27، تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عقد في فيينا في الفترة من 03 إلى 05 أبريل 2018، المجلس الاقتصادي والاجتماعي 13 أبريل 2018.
9. تقرير الأمين العام لهيئة الأمم المتحدة رقم 130/47 الصادر عن الجمعية العامة بتاريخ 30 جويلية 2019 والمتضمن مكافحة استخدام تكنولوجيا المعلومات والاتصال الأغراض الإجرامية.
10. منظمة الأمن والتعاون في أوربا، الوقاية من الإرهاب ومكافحة التطرف العنيف والزاديكالية المؤيديين إليه: (مقاربة الشرطة المجتمعية)، فيينا، فبراير 2014.
11. هيئة تنظيم الاتصال، مسودة لائحة الكوابل البحرية، سلطنة عمان:

<https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.tra.gov.om/pdf/submarine-cables-regulation-ar.pdf&ved=2ahUKewi04da1ppboAhV5AWMBHdJEAwUQFjAAegQIAhAB&usg=AOvVaw0ANiCzMuhHrTbm4PPV2tMB>

12. القرار السابع بشأن تعريف مصطلح الإرهاب المنشور بتاريخ 12 مايو 2015 عن مجمع اللغة العربية:

<https://www.m-a-arabia.com/site/15829.html>

13. إغنيو كاكاياردون وآخرون، مكافحة خطاب الكراهية في الإنترنت، ترجمة(صابر طروات) سلسلة اليونسكو حول حرية الإنترنت، فرنسا، 2015،
14. مستشارية الأمن الوطني، أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات استراتيجية الأمن السيبراني العراقي.
15. مشروع حول الجريمة المعلوماتية وشبكة لشبونة، التدريب على الجريمة المعلوماتية للقضاة وأعضاء النيابة العامة:(المفهوم)، المديرية العامة لحقوق الإنسان والشؤون العامة، قسم مجتمع المعلومات والعمل على مكافحة الجريمة، المجلس الأوروبي، فرنسا، 08 أكتوبر 2009.
16. الاتحاد الدولي للاتصالات، المسألة 22/1 تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني(التقرير النهائي)، قطاع تنمية الاتصالات لجنة الدراسات 01، فترة الدراسة الرابعة 2006-2010.
17. مشروع قانون مكافحة الجريمة الإلكترونية المقدم من النائب تامر الشهاوي، التنظيم القانوني والجرائم الإلكترونية:(ما بين أمن المعلومات وتقييد الحريات)، مركز هردو لدعم التعبير الرقمي، القاهرة، 2018.
18. بيان الرياض للأمن السيبراني، المنتدى الدولي للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، الرياض، 05 فبراير 2020.

ثانيا: باللغة الأجنبية:

1- Ouvrages :

A. Français :

1. **Ahmed DAHMANI, Jose DO-NASCIMENTO, Jean-Michel LEDJOU, Jean-Jacques GABAS**, la démocratie à l'épreuve de la société numérique, Editions Karthala, PARIS, 2007.
2. **Arnaud BLIN**, Le Terrorisme, Edition Le Cavalier Bleu(Idées reçues), Paris, 2005.
3. **Camille GRAND, Pierre GROSSER**, Les Relations internationales depuis 1945, Hachette Education(programme ReLIRE), 2000
4. **Didier GODART**, sécurité informatique :(resèques, stratégiques et solutions), 2^{ème} Édition, éditions des Cci de wallonie SA, Belgique, 2005.
5. **Eric FILIOL**, les virus informatiques:(théorie, pratique et applications), deuxième edition, Springer, FRANCE, 2009.

6. **Geneviève VIDAL**, *la sociologie des usages:(continuités et transformations)*, LAVOISIER, 2012.

7. **Patrick ANTOULY**, *surfer sans risque:(protéger votre ordinateur – virus, spywares, chevaux de Troie, spam)*, Éditions ENI, France, 2009.

8. **Roland BERNARD**, *La France, Son Passé Et Notre Avenir, mon petit Édition*, Paris, France, 2010.

B. Anglais :

9. **Andrew JAKUBOWICZ, Kevin DUNN, Gail MASON, Yin PARADIES, Ana-Maria BLIUC, Nasya BAHFEN, Andre ONOLER, Rosalie ATIE, Karen CONNELLY**, *Cyber Racism and Community Resilience:(Strategies for Combating Online Race Hate)*, Switzerland, 2007.

10. **Bernadette SCHELL, Clemens MARTIN**, *Webster's New World Hacker Dictionary*, 1st edition, Wiley Publishing, Inc, USA, 2006.

11. **Camino KAVANAGH, Daniel STAUFFACHER**, *A role for civil society, ICTs norms and confidence building measures in the context of international security*, ICT4 Peace Foundation, GENEVA 2014.

12. **Larry DANIEL, Lars DANIEL**, *Digital Forensics for legal professionals:(understanding digital evidence from the warrant to the courtroom)*, Elsevier, USA, 2011.

13. **Laura DENARDIS**, *The Global War for Internet Governance* Yale University Press, usa, 2014.

14. **Michael G. SOLOMON, Diane BARRET, Neil BROOM** *Computer Forensics:(JumpStart™)*, SYBEX, london, 2005.

15. **Tim MAURER**, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security Science, Technology, and Public Policy Program*, Explorations in Cyber International Relations Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge September 2011.

2. Mémoires et thèses universitaires :

A. Mémoires :

1. **Nadia Nihel BOUAYAD-AGHA**, *Le role de la victime dans le passage à l'acte*, Mémoire de magistère en sciences criminelles et criminologie, Faculté de droit, Université Aboubekr BELKAID Tlemcen, Année universitaire : 2004-2005.

B. Thèses :

1. **Ali Obaid Sultan Alkaabi**, *Combating Computer Crime: An International Perspective*, Thesis submitted in accordance with the regulations

for the Degree of Doctor of Philosophy, Information Security Institute Faculty of Science and Technology, Queensland University of Technology, October 2010.

2. **Alina ANDRONACHE**, *ALIGNING CYBERSECURITY MANAGEMENT WITH ENTERPRISE RISK MANAGEMENT IN THE FINANCIAL INDUSTRY*, A thesis submitted for the degree of Doctor of Philosophy, Brunel Business School, Brunel University, London 2019.

3. **Gary Craig KESSLER**, *Judges' Awareness, Understanding, and Application of Digital Evidence*, A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy Graduate School of Computer and Information Sciences, Nova Southeastern University, Florida, 2010.

4. **Houda BENALIOUCHE**, *Multimodalité Biométrique dans le cadre d'une Application d'Authentification*, Doctorat en science, Option : Informatique, Faculté des Sciences, Université Ferhat Abbas Sétif 1 2016.

5. **Humza Naseer**, *A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility*, Submitted in fulfilment of the requirements of the degree of Doctor of Philosophy, School of Computing and Information System, University of Melbourne, octobre 2018.

6. **Jonathan A. MATUSITZ**, *cyberterrorism : (A postmodern view of networks of terror and how computer law security exper and enforcement officials fight them)*, submitted to the graduate faculty in partial fulfillment of the requirements for the degree of Doctor of Philosophy university of Oklahoma, 2006.

7. **Lalonde Lévesque Fanny**, *prévention des attaques par logiciels malveillants:(perspectives de la santé publique)*, thèse présentée en vue de l'obtention du diplôme de philosophie doctor(génie informatique), école polytechnique de Montréal, université de Montréal, 2018.

8. **Robert Louis Parrillo**, *Extradition: A Test of International Cooperation in the Enforcement of Domestic Criminal Law*, A Dissertation submitted to the Department of Political Science in partial fulfillment of the requirements for the degree of Doctor of Philosophy, COLLEGE OF SOCIAL SCIENCES, FLORIDA STATE UNIVERSITY, 2009.

9. **Romain BOOS**, *La Lutte contre la cybercriminalité au regard de l'action des États*, doctorat de droit privé et sciences criminelles, faculté de droit, sciences économiques et gestion, unevirsité de Lorraine, 2016.

10. **Saleem SHAHZAD**, *Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics*, Academic dissertation for the Degree of Doctor of Philosophy in Computer and Systems

Sciences, Department of Computer and Systems Sciences, Stockholm University, Sweden, 2015.

11. **Yves SCHULIAR**, *La coordination scientifique dans les investigations criminelles. Proposition d'organisation, aspects éthiques, ou de la de la nécessité d'un nouveau métier*, thèse pour obtenir le grade de docteur, Ecole des Sciences Criminelles, UNIVERSITÉ PARIS DESCARTES, Paris, 23 novembre 2009.

3. Articles :

A. Français :

1. **Camille MOREL**, *menace sous les mers: les vulnérabilités du système câblé mondial, la découverte "Hérodote"*, N° 163, 2016, PP.33-43.

2. **Dominique BOULLIER**, *" Internet est maritime: les enjeux des câbles sous-marins"*, RIS, *La Revue Internationale et Stratégique*, n° 95, Automne 2014, pp. 149-158.

3. **Frederick DOUZET, Alix DESFORGES, Kevin LIMONIER**, *Géopolitique du cyberspace :("territoire", frontières et confits)*, *Fronts et frontières des sciences du territoire*, Paris, France, Mar 2014, pp.173-178.

4. **Frédéric DOUZET**, *Géopolitique du cyberspace:(La cyberstratégie de l'administration Obama Geopolitics of cyberspace: the Obama administration's cyberstrategy)*, *Bulletin de l'association de géographes français*, 91-2 | 2014, PP. 138-149.

5. **Frederick DOUZET**, *la géopolitique pour compadre le cyberespace*, *La Découverte « Hérodote »*, 1 n° 152-153, 2eme trimestre, 2014, pp 3-21

6. **Jean-François DAGUZAN**, *La protection des infrastructures critiques:(l'enjeu stratégique du XXIe siècle)*, *AFRI*, Volume XI Centre Thucydide, Université Panthéon-Assas, paris, 2010, PP.1001-1015.

7. **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 agendas institutionnels*, *Revue québécoise de droit international*, Société québécoise de droit international, volume 2-1, Hors-série novembre 2018, PP.25-39.

8. **Taillat STEPHANE, Amaël CATTARUZZA, et Didier DANET**. *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, 2018 PP.22-23.

9. **Thierry BALZACQ**, *Qu'est-ce que la sécurité nationale?* *Revue internationale et stratégique*, Institut de relations internationales et stratégiques, N° 52, 2003, PP. 33-50:

B. Anglais :

10. **A. BOZTAS, A.R.J. Riethoven, M. Roeloffs**, Smart TV forensics: Digital traces on televisions, DFRWS 2015 Europe, **Digital Investigation**, Volume 12, Supplement 1, March 2015, Pages S72-S80.

11. **Ayman Shaaban, Nashwa Abdelbaki**, Comparison Study of Digital Forensics Analysis Techniques; Findings versus Resources, The 5th International Workshop on Privacy and Security in Health Care(PSCare 2018), **Procedia Computer Science**, Volume 141 Elsevier B.V, 2018, Pages 545-551.

12. **Bandr FAKIHA**, Digital Forensics:(Crimes and Challenges in Online Social Networks Forensics), **Journal of the Arab American University**, volume 06, issue 01, American University-Jenin, Palestine 2020, PP: 15-33.

13. **Brian CARRIER**, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, **International Journal of Digital Evidence**, Volume 1, Issue 4, UTICA COLLAEGE, Winter 2003, PP.01-12.

14. **Brian D. CARRIER, Eugene H. SPAFFORD**, Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence, Digital Forensic Research Workshop(DFRWS) 2005, PP.1-10.

15. **Clay SHIELDS, Ophir FRIEDER, Mark MALOOF**, A system for the proactive, continuous, and efficient collection of digital forensic evidence, **Digital Investigation**, Volume 8, Elsevier Ltd Supplement, August 2011, Pages S3-S13.

16. **Clay WILSON**, Botnets, cybercrime, and cyberterrorism:(vulnerabilities and policy issues for congress), Congressional research service, January 29, 2008, PP.16-17.

17. **Daniel T. KUEHT**, From Cyberspace to Cynerpower :(Difining the Problem), **cyber and national Security**, first Edition, centre for techlogogy and national security, national defense university press, fotomac books inc, washington, 2009, pp 24-42.

18. **Darya MAZURTSOVA**, Un legal sources in the field of regulation of online space at the present stage, THE YOUTH OF THE 21ST CENTURY: EDUCATION, SCIENCE, INNOVATIONS Proceedings of VI International Conference for Students Postgraduates and Young Scientists, Publisher: Vitebsk State University named after Masa Masherova(Vitebsk), 2019, PP. 319-321.

19. **David MUGISHA**, digital forensics: (Digital Evidence in judicial System), **International Journal of Cyber Criminology** volume 04, march 2019.

20. **Fahad Nabeel**, Establishment of UN Cyber Peacekeeping Force: Prospects and Challenges, **NUST Journal of International Peace & Stability**, Volume II, Number 2, Edited at the Centre for International Peace and

Stability(CIPS), National University of Sciences and Technology(NUST), July 2019, PP.17-31.

21. **Fatima TALAT**, Transnational Crimes:(Investigatory Challenges), international Conference : Criminal Justice Under Stress, ILI Golden Jubile, Law Institute, New Delhi, Indian, 2007, PP. 302-311.

22. **Galinec DARKO, Moznik DARKO, Boris GUBERINA**, Cybersecurity and cyber defence: national level strategic approach, **Automatika Journal for Control**, Measurement, Electronics Computing and Communications, volume 58, Issue 3, PP.273-286.

23. **Gregor BRUCE**, Definition of Terrorism – Social and Political Effects, *Journal of Military and Veterans' Health, Issues 21*, volume 02, published by the Australasian Military Medicine Association, Australie, may 2013, PP. 26-30.

24. **Hai Thanh LUONG, Huy Duc PHAN**, Cybercrime in Legislative Perspective:(A Comparative Analysis between the Budapest Convention and Vietnam Regulations), **International Journal of Advanced Research in Computer Science**, Volume 10, No. 3, May-June 2019, PP.1-12.

25. **Hamda BARIKI, Mariam HASHMI, and Ibrahim BAGGILI**, Defining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools, Digital Forensics and Cyber Crime:(Second International ICST Conference Abu Dhabi, United Arab Emirates, October 4-6, 2010) Volume Editor: **Ibrahim Baggili**, Springer Heidelberg Dordrecht London NewYork, 2011, PP.78-95.

26. **Hisyam SYARIF**, English about Antivirus Software **International Research Journal of Management, IT & Social Sciences**, Vol.2, No.1, January 2015, PP.17-21.

27. **Janne J. KORHONR, Kari HIEKKANEN, Juha MYKKANEN**, Information Security Governance, Strategic and Practical Approaches for Information Security Governance:(Technologies and Applied Solutions), **IGI Global**, 2012: PP.1-16.

28. **Jeffrey Thomas BILLER**, Cyber-Terrorism :(Finding a Common Starting Point), **Journal Of Law, Technology & THE Internet**, Vol.04, Iss.02. Case Western Reserve University, Cleveland Ohio, 2013, pp.275-351.

29. **Jonathan ZITTRAIN and John PALFREY**, Internet Filtering: The Politics and Mechanisms of Control, publishing in Collective workbook themed: **Access Denied:(The Practice and Policy of Global Internet Filtering)** edited by Ronald Deibert, John Palfrey Rafal Rohozinski, and Jonathan Zittrain, usa, 2008, PP.29.56.

30. **Juhani ERONEN, Kati KARJALAINEN, Rauli RUUPERA Erno KUUSELA, Kimmo HALUNEN, Marko LAAKSO, Juha RÖNING**, *Software Vulnerability vs. Critical Infrastructure - a Case Study of Antivirus Software*, *International Journal On Advances in Security*, vol 2, no 1, IARIA, year 2009, PP.72-89.

31. **Kevin CONLAN , Ibrahim BAGGILI, Frank BREITINGER**, *Anti-forensics:(Furthering digital forensic science through a new extended, granular taxonomy)*, DFRWS USA 2016 d Proceedings of the 16th Annual USA Digital Forensics Research Conference, **Digital Investigation**, Volume 18, Supplément, 7 août 2016, Pages S66-S75.

32. **Laura ANI**, *Cyber crime and national security: the role of the penal and procedural law, .* " Law and Security in Nigeria, 2011, PP. 200-202

33. **Mariua ERBANA, Raluca-Mariana TEFANB, Eduard-Ionel IONECUL**, *Information Protection – Security, Clustering and E-governance*, 21st International Economic Conference 2014, IECS 2014, 16-17 May 2014, Sibiu, Romania, **Procedia Economics and Finance**, Volume 16, Elsevier B.V, 2014, PP. 288-292.

34. **Max MANLEY**, *Cyberspace's Dynamic Duo:(Forging a Cybersecurity Public-Private Partnership)*, **Journal of Strategic Security** , Vol. 8, No. 3, University of South Florida Board of Trustees Supplement: Eleventh Annual IAFIE Conference(Fall 2015), pp. 85-98.

35. **Michael ROBINSON, Kevin JONES, Helge JABICKE Leandros MAGLARAS**, *An Introduction to Cyber Peacekeeping* [Submitted on 26 Oct 2017([v1](#)), last revised 24 Apr 2018(this version v2)].

36. **Michal Tonhauser, Jozef Ristvej**, *Disruptive acts in cyberspace, steps to improve cyber resilience at National Level*, 13th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM 2019), High Tatras, Novy Smokovec – Grand Hotel Bellevue, Slovak Republic, May 29-31, 2019, **Transportation Research Procedia**, Volume 40, Elsevier B.V, 2019, PP. 1591-1596.

37. **Mitko BOGDANOSKI, Drage PETRESKI**, *cyber terrorism –global Security theart, international scientific defence, security and peace journal*, MINISTRY OF DEFENCE OF THE REPUBLIC OF MACEDONIA, 2013, PP.59-72

38. **Mubarak BANISAKHER, Marwan OMAR, Wade CLARE** *Critical Infrastructure - Perspectives on the Role of Government in Cybersecurity*, **Journal of Computer Sciences and Applications** Vol.7, No.1, Science and Education Publishing, US, 2019, PP.37-42.

39. **Nathan E. BUSCH, Austen D. GIVENS**, *Public-Private Partnerships in Homeland Security Opportunities and Challenges* Faculty and Researcher Publications, **Homeland Security Affairs(Journal)**, v.8, article 18, Naval Postgraduate School, October 2012 PP. 1-24.
40. **Nazura Abdul Manap, Pardis Moslemzadeh Tehrani**, *Cyber Terrorism: Issues in Its Interpretation and Enforcement*, **International Journal of Information and Electronics Engineering** Vol. 2, No. 3, May 2012, PP.409-413.
41. **Nikolaos KOUMARTZIS, Andreas VEGGIS**, *Internet regulation:(The need for more transparent Internet filtering systems and improved measurement of public opinion on Internet filtering)* **First Monday(peer-reviewed journal on the internet)**, Volume 16 Number 10 - 3 October 2011.
42. **Oluwafemi Osho, Agada D. Onoja**, *National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis*, **International Journal of Cyber Criminology(IJCC)**, Vol. 9(1), June 2015, PP. 120–143.
43. **Pavan K. JAGALUR, Peter L. LEVIN, Kate BRITTAIN, Matthew DUBINSKY, Kristine Landau JAGALUR, Charlotte LATHROP**, *Cybersecurity for Civil Society*, IEEE International Symposium on Technology in Society(ISTAS) Proceedings Miriam Cunningham and Paul Cunningham(Eds), 2018.
44. **Philippe LAGADEC**, *Filtrage de messagerie et analyse de contenu*, 2004:
45. http://195.154.171.95/SSTIC04/Filtrage_messagerie/SSTIC04-article-Lagadec-Filtrage_messagerie.pdf
46. **Pradipta Nindyan SAPUTRA, Arfin SUDIRMAN, Obsatar SINGA, Wahyu WARDHANA, Nurul HAYANA**, *Addressing Indonesia's Cyber Security through Public-Private Partnership(PPP)*, **Central European Journal of International & Security Studies**, Vol. 13, N° 4, CEJISS, Metropolitan University Prague,(2019), PP.104-120.
47. **Ravneet KAUR, Amandeep KAUR**, *Digital Forensics*, **International Journal of Computer Applications**, Volume 50 – No.5 Foundation of Computer Science, USA, July 2012, PP.5-9.
48. **Ryan HARRIS**, *Arriving at an anti-forensics consensus:(Examining how to define and control the anti-forensics problem)* **Digital Investigation**, Volume 3, Supplement, September 2006, PP. 44-49.
49. **Sam BERNER**, *Cyber-terrorism: reality or paranoia*, South African Journal of Information Management, Volume 5, No.01 African Online Scientific Information Systems(Pty) Ltd t/a AOSIS South Africa, 2003.

50. **Satyabrata DASHA, Subhendu Kumar PANIB**, E-Governance Paradigm Using Cloud Infrastructure: Benefits and Challenges, International Conference on Computational Modeling and Security(CMS 2016), **Procedia Computer Science**, Volume 85, Elsevier B.V 2016, Pages 843-855.

51. **Soltan ALHARBI, Jens WEBER-JAHNKE, Issa TRAORE**, The Proactive and Reactive Digital Forensics Investigation Process:(A Systematic Literature Review), **international Journal of Security and Its Applications**, Vol 05, No 04,, October, 2011, PP.59-72.

52. **Stein SCHJOLBERG**, Terrorism in Cyberspace–Myth or reality?, **Terrorism**, , vol 01, 2006.

53. **Sungmi Park, Nikolay Akatyev, Yunsik Jang, Jisoo Hwang Donghyun Kim, Woonseon Yu, Hyunwoo Shin,, Changhee Han Jonghyun Kim**, A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement, **Digital Investigation**, Volume 24 Supplement, Elsevier Ltd, March 2018, Pages S93-S100.

54. **Tara DAVENPORT**, Submarine cables, cybersecurity and international law:(an international analysis), **Journal of Law and Technology**, volume 24, issue 01, Catholic University of America USA, 2015, article 04.

55. **Tatiana Nascimento HEIM, and Ramses A. WESSEL**, The Global Regulation of Cybersecurity: A Fragmentation of Actors Definitions and Norms, Draft contribution to be published in Lucía Millán Moro(dir.) and Gloria Fernández Ciberataques Arribas(ed.), y *Ciberseguridad en la Escena Internacional*, 2020.

56. **Tuesday REITANO, Troels OERTING, Marcena HUNTER** Innovations in International Cooperation to Counter Cybercrime:(The Joint Cybercrime Action Taskforce(J-CAT)), **The joint cybercrime action taskforce The European Review of Organised Crime**, vol. 2, no 2, 2015 PP. 142-154.

57. **Ulrich SIEBER**, Coopération internationale contre l'utilisation terroriste d'Internet, « Revue internationale de droit pénal », 2006/3 Vol. 77, PP. 395-449: DOI: 10.3917 / Radep.773.0395.

58. **Walter DORN**, Cyberpeacekeeping:(A New Role for the United Nations?), **GEORGETOWN JOURNAL OF INTERNATIONAL AFFAIRS**, Volume 18, No. 3, Fall 2017, PP.138-146.

59. **Zahri Yunos, Rabiah Ahmad and Noor Azwa Azreen Abd Aziz**, The Concept of Cyber Terrorism, **SEARCCT'S sélection of articles**, volume 01, Southeast Asia Regional Centre for Counter-Terrorism, ministry of foreugn affairs, Malaysia, 2013, PP. 68-79.

4. Web site:

A. Article:

1. **Alexis ZEMA**, *Aux États-Unis, s'affranchir des caméras de surveillance chinoises vire au casse-tête*, Publié le 8 août 2019, vu le 20 juillet 2012 à 22:43h, sur le lien: <https://www.lefigaro.fr/secteur/high-tech/aux-etats-unis-s-affranchir-des-cameras-de-surveillance-chinoises-vire-au-casse-tete-20190808>

2. **Andrew TILLET**, *Deal with ISPs to block terror attack websites*, Mar 25, 2020, Accessed on 13/08/2020, at 20:03h, in: <https://www.afr.com/politics/federal/deal-with-isps-to-block-terror-attack-websites-20200323-p54d0t>

3. **Andrijana GAVRILOVIC**, [Webinar summary] *What is the role of civil society and communities towards a peaceful cyberspace?*, Posted on 11 Dec 2018, Accessed on 30 July 2020, at 19:14h, In: <https://www.diplomacy.edu/blog/webinar-what-role-civil-society-and-communities-towards-peaceful-cyberspace>

4. **Celia LOUIE**, *U.S.-China Cybersecurity Cooperation*, SEPTEMBER 8, 2017, Accessed on 20/08/2020 at 01:01 in: <https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/>

5. **Walter O. BAGGETT**, *reating a culture of security: The OECD standards for systems security provide internal auditors with a tool for operationalizing tone at the top*, "Internal Auditor", vol. 60, no. 3, June 2003, p. 37+. Gale Academic OneFile, Accessed 1 Sept. 2020, at 09:45h in: <https://link.gale.com/apps/doc/A103194416/AONE?u=maine&sid=AONE&xid=4280cb74>

B. Various web sites:

6. *Federal Rules of Evidence Rule 702. Testimony by Expert Witnesses*, legal information Institute, cornelle law school, Accessed on 09/08/2020 at 15:55h, in: https://www.law.cornell.edu/rules/fre/rule_702:

7. *Significant Cyber Incidents*, center dor stratefic & international studies(CSIS), Accessed on 18/08/2020, at 21:48H, in: <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>

8. CCDCOE: <https://ccdcoe.org/organisations/un/>

9. *Fact Sheet, G8 Counter-Terrorism Cooperation Since September 11, G-7/8 Kananaskis Summit, Kananaskis, Canada, June 26, 2002*: <https://2001-2009.state.gov/e/eeb/rls/fs/11477.htm>

10. G8 Communiqué Okinawa 2000, Okinawa, Japan, July 23, 2000:
<http://www.g8.utoronto.ca/summit/2000okinawa/finalcom.htm>
11. G8 Summit Declaration on Counter-Terrorism, St. Petersburg, July 16, 2006:
<http://www.g8.utoronto.ca/summit/2006stpetersburg/counterterrorism.html>
- G8 Declaration on Counter Terrorism, L'Aquila Summit, July 9, 2009:
<http://www.g8.utoronto.ca/summit/2009laquila/2009-counterterrorism.html>
12. G8 Leaders Statement on Countering Terrorism, Muskoka, June 26 2010:
<http://www.g8.utoronto.ca/summit/2010muskoka/counterterrorism.html>
13. G8 Declaration: Renewed Commitment for Freedom and Democracy, Deauville, 26-27 mai 2011(publiée le 27 mai 2011):
<http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-fr.html>
14. cybercrime law: <https://www.cybercrimelaw.net/OECD.html>
15. Europol website, european cybercrime center- EC3,:(Combating crime in a digital age):
<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>
16. Europol website, new european cybercrime centre- EC3, 21 January 2013, Accessed on 05/09/2020, At 15/50H, in:
<https://www.europol.europa.eu/newsroom/news/new-european-cybercrime-centre-ec3-opens-europol>
17. Cyber security in the spotlight, Official Website of Eurojust, 04/17/2015, Been watched on 05/09/2020 At 15:21H, in:
<http://www.eurojust.europa.eu/press/News/News/Pages/2015/2015-04-16-Cyber-security-in-the-spotlight.aspx>
18. Eurojust Meeting on Cybercrime-Towards a Judicial Cybercrime Network, Official Website of Eurojust, 11/26/2015, Been watched on 05/09/2020 At 15:23H, in:
<http://www.eurojust.europa.eu/press/News/News/Pages/2015/2015-11-26-Eurojust-Meeting-on-Cybercrime-Towards-a-Judicial-Cybercrime-Network.aspx>
19. cyberspace, oxford dictionary :
<https://www.oxfordlearnersdictionaries.com/definition/english/cyberspace?q=cyberspace>
20. oxford dictionary, Digital
<https://dictionary.cambridge.org/fr/dictionnaire/anglais/digital>

21. oxford dictionary, forensics:
<https://dictionary.cambridge.org/fr/dictionnaire/anglais/forensics>
22. UKESSAYS, Proactive and Reactive Cyber Forensics Investigation Process, 12th Mar 2018 Accessed on 02 August 2020, at 04:41H, in:
<https://www.ukessays.com/essays/computer-science/proactive-reactive-cyber-forensics-investigation-1756.php>
23. cyber monde, dictionnaire Larousse :
<https://www.larousse.fr/dictionnaires/francais/cybermonde/21258>
24. terrorisme, dictionnaire Larousse sur web :
<https://www.larousse.fr/dictionnaires/francais/terrorisme/77478>
25. oxford learner's dictionaries; governance:
<https://www.oxfordlearnersdictionaries.com/definition/english/governance?q=governance>
26. larousse; gouvernance;
<https://www.larousse.fr/dictionnaires/francais/gouvernance/37692?q=gouvernance#431601>
27. Le cabinet JURISLITIS, CABLES SOUS MARINS – QUEL DROIT APPLICABLE , 24 octobre 2018, vu le 03 juillet 2020, à 06:13H, sur le site:
<http://www.delplanqueparis.fr/fr/nos-publications/cables-marins-droit-applicable/>
28. Rédaction 7seizh.info, Nantes / Cyber-guerre islamique : les hackers s'attaquent aux sites chrétiens, publier le 10 janvier 2015, vu le 02/11/2020 à 00:55 sur le site: <http://7seizh.info/2015/01/10/cyber-guerre-islamique-les-hackers-sattaquent-aux-sites-chretiens/>
29. Are religious organizations at risk of being hacked? Seven steps you can take to battle cyber crime, October 1, 2018, Accessed in 24/11/2020 At 22:21 in: <https://blog.24by7security.com/are-religious-organizations-at-risk-of-being-hacked-seven-steps-you-can-take-to-battle-cyber-crime>
30. How many power plants are there in the United States?, Frequently asked questions, U.S. Energy Information Administration, Last updated: November 18, 2020, Accessed on 24/11/2020 At 00:93 in: <https://www.eia.gov/tools/faqs/faq.php?id=65&t=2#:~:text=As%20of%20December%2031%2C%202019,plants%20in%20the%20United%20States>
31. Serge Krasavin, What is Cyber-terrorism, Computer Crime Research Center, accessed in 05/02/2021, at 10:55, in: <https://www.crime-research.org/library/Cyber-terrorism.htm#:~:text=In%20the%20same%20year%20Mark,national%20groups%20or%20clandestine%20agents.%22>

6. Textes juridiques :**A. Convention :**

1. Convention pour la prévention et la répression du terrorisme, société des nations 1937.
2. Convention de l'OUA sur la prévention et la lutte contre le terrorisme, adopté en 01 juillet 1999, entrée en vigueur le 06 décembre 2002.
3. Déclaration Africaine des Droits et Libertés de l'Internet dernière mise à jour 28 août 2014.

B. Textes de lois:

4. title 18, U.S. Code, This title was enacted by act June 25, 1948, ch. 645, § 1, 62 Stat. 683, With the latest modifications.
5. Title 34 U.S. Code, This title was enacted by act June 25, 1948, ch. 645, § 1, 62 Stat. 683, With the latest modifications.
6. Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3(V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002, Abrogé par Loi n°2004-575 du 21 juin 2004 - art. 40(V) JORF 22 juin 2004.
7. Orrin Grant Hatch, A BILL To prevent cyberterrorism, S. 1568, 107th CONGRESS, 1st Session, October 18, 2001.
8. John Edwards, A BILL To protect against cyberterrorism and cybercrime, and for other purposes, S. 1900, 107th CONGRESS, 2d Session, January 28, 2002
9. PUBLIC LAW 113-283, Federal Information Security Modernization Act of 2014, 113th Congress, DEC. 18, 2014.

C. Décisions & Résolutions :

10. Décision-cadre du conseil du 13 juin 2002 relative à la lutte contre le terrorisme,(2002/475/JAI), J.O.U.E L 164 du 22. Juin 2002.
11. Décision du Conseil sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI du Conseil instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, conseil de l'union européenne, bruxelles, 15 juillet 2009.
12. Décision 2009/426/JAI DU CONSEIL du 16 décembre 2008 sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, J.O.U.E L138 du 04/06/2009

13. Résolution du Parlement européen du 12 mars 2015 sur les relations entre l'Union européenne et la Ligue des États arabes et sur la coopération dans la lutte contre le terrorisme(2015/2573(RSP)) J.O.U.E/ C316 du 30/08/2016.

14. Résolution du Parlement européen du 21 mai 2015 sur l'incidence des évolutions des marchés européens de la défense sur les capacités de sécurité et de défense en Europe(2015/2037(INI)), 21 mai 2015, J.O.U.E C 353, 27.09.2016.

15. Résolution du Parlement européen du 8 septembre 2015 sur la situation des droits fondamentaux dans l'Union européenne(2013-2014)(2014/2254(INI)), 8 septembre 2015, J.O.U.E C 316/2, 2017.

16. Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité(2017/2068(INI)), 3 octobre 2017, J.O.U.E C 346 DU 2018.

17. Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense(2018/2004(INI)), Mercredi 13 juin 2018, Journal officiel de l'Union européenne, J.O.U.E/C28/6 du 27.1.2020

D. Autres documents :

18. Réponse de M. Vitorino au nom de la Commission(8 mars 2001), J.O.U.E/C235E

19. Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection(Texte présentant de l'intérêt pour l'EEE), 23 décembre 2008.

20. Avis du Comité économique et social européen sur la «Proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information(ENISA)», J.O.U.E/C107/12 du 06.04.2011.

21. communication conjointe au parlement européen, au conseil, au comité économique et social européen, et au comité des régions, commission européenne, la haute représentante de l'union pour les affaires étrangères et la politique de sécurité, Bruxelles, le 18.11.2015, P.16.

22. Joaquin PUEYO, Marie-Louise FORT, rapport d'information déposé par la commission des affaires européennes sur la nouvelle politique européenne de voisinage, assemblée nationale, No3364, 16 décembre 2015, France.

23. MINISTÈRE DE L'INTÉRIEUR, la réponse du ministère de l'intérieure de la menace liée au numérique en 2019, Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, Rapport n° 3, France, Mai 2019.

24. *Avis du Comité économique et social européen sur «L'avenir de l'UE: avantages pour les citoyens et respect des valeurs européennes»*(avis exploratoire à la demande de la présidence roumaine du Conseil de l'Union européenne), 05 juillet 2019, J.O.U.E: C228/08/2019.

25. *Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services* issued on: February 12, 2020.

7. Ouvrages divers:

1. *A Simplified Guide To Digital Evidence*, National Forensic Science Technology Center, under a cooperative agreement from the Bureau of Justice Assistance(BJA), Florida, 2009.

2. **Alexander SEGER**, *The Budapest Convention on Cybercrime 10 years on: (Lessons learnt or the web is a web)*, *Selected papers and contributions from the International Conference on "Cybercrime: Global Phenomenon and its Challenges"* Courmayeur Mont Blanc Italy 2-4 December 2011 Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, Milan, Italy 2012, PP. 167-177.

3. *BACKGROUND GUIDE*, INTERPOL, Specialized Committee, tmun 2018

4. **Bruce W. MCCONNELL, Pavel SHARIKOV, Maria SMEKALOVA**, *Suggestions on Russia-U.S. Cooperation in Cybersecurity*, POLICY BRIEF, No. 11, Russian International Affairs Council (RIAC), Moscow, May 2017.

5. **Camino KAVANAGH**, *The United Nations, Cyberspace and International Peace and Security: (Responding to Complexity in the 21st Century UNIDIR RESOURCES)*, United Nations Institute for Disarmament Research(UNIDIR), 2017.

6. **Carlo KOPP**, *The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction*, *Air & Space Power Journal – Chronicles Online Journal*, US Air Force.

7. **Charletta ANDERSON**, *Cyber Security and the Need for International Governance*, April 24, 2016.

8. **Cristin Flynn GOODWIN, J. Paul NICHOLAS**, *Developing a National Strategy for Cybersecurity: (foundations for Security) growth and innovation*, Microsoft Corporation, 2013.

9. **Cristin GOODWIN, J. Paul NICHOLAS**, *A framework for cybersecurity information sharing and risk reduction*, Microsoft Corporation, 2015.

10. **Félix BLANC**, *Géopolitique des câbles: une vision sous-marine de l'internet, les carnets du CAPS, N°26, technologies et puissance France*, juin 2018. PP.31-50.

11. **Franz-Stefan GADY, Greg AUSTIN**, Russia, The United States, And Cyber Diplomacy:(Opening the Doors), The EastWest Institute, New York, USA, 2010.
12. **Gary C. KESSLER**, Anti-Forensics and the Digital Investigator, 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western, Australia, December 3rd 2007.
13. *Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face*, Vienne, 25-28 février 2013, UNODC/CCPCJ/EG.4/2013/2, 23 janvier 2013.
14. *Guide pour la bonne gouvernance de la cybersécurité*, Le Centre pour la gouvernance du secteur de la sécurité, Genève, 2019.
15. *Information Technology Industry Council, The IT Industry's Cybersecurity Principles for Industry and Government*, Information Technology Industry Council(ITI), Washington, Version 3.0, 2011.
16. ISFS, Computer Forensics, Part 1:(An Introduction to Computer Forensics), Information Security and Forensics Society(ISFS), April 2004.
17. Jason BARKHAM, Cyber Warfare, Cybercrime, and Cyber Terrorism: A Bibliographic Essay, in : American Society of International Law. 2001
18. **Jeetendra Pande, Ajay Prasad**, Digital Forensics, Post-Graduate Diploma in Cyber Security Digital Forensics, Uttarakhand Open University, Haldwani, 2016.
19. **Laviero BUONO**, Fighting cybercrime through prevention, outreach and awareness raising, " **ERA Forum**. Vol. 15. No. 1. Springer Berlin Heidelberg, 2014.
20. **Louise Marie HUREL, Luisa Cruz LOBATO**, A Strategy for Cybersecurity Governance in Brazil, INSTITUTO IGARAPÉa think and dotank, strategic note 30, Rio de Janeiro, Brasil, SEPTEMBER 2018.
21. **M.B. RAQIB**, Combating Cybercrime in Bangladesh:(A Critical Analysis in the context of Legal ramification of Law) Research paper presented to Department of Law, Daffodil International University, 11 December, 2018.
22. **Marco GERCKE**, Understanding cybercrime:(Phenomena, challenges and legal response), the ITU publication telecommunication Development Sector, Geneva, Switzerland September 2012.
23. **Marie BAEZNER**, Cybersecurity in Sino-American Relations, center for security studies(SCC), analyse in Security Policy, ETH Zurich, N0 224, April 2018, PP.01-04.
24. **Mayssa ZERZRI**, The Threat of Cyber Terrorism and Recommendations for Countermeasures, Center for Applied Policy Research, C·A·Perspectives on Tunisia, 2017.
25. Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, Implementation Plan for the OECD

Guidelines for the Security of Information Systems and Network :(Towards a Culture of Security), 02 jul 2003(DSTI/ICCP/REG(2003)5/REV1).

26. Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, the Promotion of a culture of security for information systems and networks in OECD countries, 16 dec 2005,(DSTI/ICCP/REG(2005)1/FINAL):

27. Organization for Economic Co-operation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD PUBLICATIONS, France, 2002.

28. **Roberto FLOR**, Cyber-criminality:(finding a balance between freedom and security), Selected papers and contributions from the International Conference on “Cybercrime: Global Phenomenon and its Challenges” Courmayeur Mont Blanc, Italy 2-4 December 2011 Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, Milan, Italy, 2012, PP. 13-20.

29. **Richard HORNE**, Governing cyber security risk: It's time to take it seriously:(Seven principles for Boards and Investors), PricewaterhouseCoopers LLP, 2007.

30. **Samantha A. Adams, Marlou Brokx, Lorenzo Dalla Corte, Maša Galič, Kaspar Kala, Bert-Jaap Koops, Ronald Leenes, Maurice Schellekens, Karine e Silva, Ivan Škorvánek**, The Governance of Cybersecurity:(A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK), TILT – Tilburg Institute for Law, Technology, and Society Tilburg University, The Netherlands, November 2015.

31. **Sean E. GOODISON, Robert C. DAVIS, Brian A. JACKSON** Digital Evidence and the U.S. Criminal Justice System:(Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence), Priority criminal justice, NEEDS INITIATIVE, RAND Corporation, 2015

32. **Sophie JOISSAINS et Jacques BIG**, RAPPORT D'INFORMATION FAIT au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale et de la commission des affaires européennes sur la lutte contre la cybercriminalité, Enregistré à la Présidence du Sénat le 9 juillet 2020, N° 613.

33. **Judge Stein SCHIOLBERG**, An International Criminal Tribunal for Cyberspace(ICTC) Prosecution for the Tribunal Police investigation for the Tribunal, Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes, A paper for the EastWest Institute(EWI) Cybercrime Legal Working Group, March 2012.

34. *The IT Industry's Cybersecurity Principles for Industry and Government*, Information Technology Industry Council(ITI), Washington, Version 3.0, 2011.

35. **Theresa HITCHENS, Nilsu GOREN**, *International Cybersecurity Information Sharing Agreements, phase I Study Report*, Center for International & Security Studies, U. Maryland, 2017.

36. **Thomas REMINGTON, Chris SPIRITO, Elena CHERNENKO, Oleg DEMIDOV, Vitaly KABERNIK**, *Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity*, Working Group Paper 7, WORKING GROUP ON THE FUTURE OF U.S.- RUSSIA RELATIONS, Kathryn W. and Shelby Cullom Davis Center for Russian and Eurasian Studies Harvard University, MAY 2016.

37. U.S. DEPARTMENT OF THE TREASURY, *G7 fundamental elements of cybersecurity for the financial sector*, , Treasury and Federal Reserve, U.S. DEPARTMENT OF THE TREASURY 10/nov/2016.

38. Union internationale des télécommunications, *Guide de la cybersécurité pour les pays en développement*, Bureau de développement des télécommunications, Union internationale des télécommunication, Genève, Suisse, 2007.

39. United States. Federal Bureau of Investigation, 17/10/2008 Homeland Security Digital Library.

40. UNODC, *Rapport sur la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité*, tenue à Vienne du 27 au 29 mars 2019.

41. **UROJUST**, *Cybercrime*, UROJUST News, European Union Agency for Criminal Justice Cooperation, Issue No. 7 - October 2012.

42. **Wayne SANSEN, Rick AYERS**, *Guidelines on Cell Phone Forensics:(Recommendations of the National Institute of Standards and Technology)*, Technology Administration, National Institute of Standards and Technology, Sponsored by the Department of Homeland Security, USA, May 2007.

43. Gouvernement de canada, *Stratégie de cybersécurité du Canada :(renforcer le canada et accroître sa prospérité)*, canada, 2010, P.02.

44. **LCol J.M.F. Robichaud**, *le cyberespace et les forces armées canadiennes*, collèges des forces canadiennes, défense nationale canada, 2016.

1 مقدمة

الباب الأول:

الإرهاب الإلكتروني في ظل محوالة الفضاء الإلكتروني

الفصل الأول:

الفضاء الإلكتروني والتحويلات الكبرى في المفاهيم الاستراتيجية

12 المبحث الأول: ماهية الفضاء الإلكتروني

12 المطلب الأول: مفهوم الفضاء الإلكتروني

13 الفرع الأول: تعريف الفضاء الإلكتروني

13 أولاً/ تعريف الفضاء الإلكتروني

18 ثانياً: حدود الفضاء الإلكتروني

21 الفرع الثاني: خصائص الفضاء الإلكتروني

21 أولاً: خصائص خدمات الفضاء الإلكتروني

25 ثانياً: الخصائص التنظيمية للفضاء الإلكتروني

27 الفرع الثالث: أهمية الفضاء الإلكتروني

27 أولاً: أهمية الفضاء الإلكتروني لعمل الحكومة ومرفق القضاء

30 ثانياً: الاقتصاد الرقمي

34 ثالثاً: الثقافة والتعليم الإلكترونيين

35 المطلب الثاني: البنية التكوينية للفضاء الإلكتروني

36 الفرع الأول: الطبقة المادية للفضاء الإلكتروني

36 أولاً: الحاسوب

39 ثانياً: الهاتف النقال

40 ثالثاً: الكوابل البحرية

42	الفرع الثاني: الطبقة المنطقية للفضاء الإلكتروني
43	أولاً: تعريف برامج الحاسب الآلي
46	ثانياً: أنواع برامج الحاسب الآلي
48	الفرع الثالث: شبكات الحاسب الآلي
48	أولاً: الشبكات المعلوماتية
49	ثانياً: الشبكة العالمية للإنترنت
53	الفرع الرابع: الطبقة الإعلامية للفضاء الإلكتروني
53	أولاً: مجتمع المعلومات كطبقة بشرية في تكوين الفضاء الإلكتروني
54	ثانياً: البنية المعلوماتية
60	المبحث الثاني: الآثار المترتبة عن عولمة الفضاء الإلكتروني
60	المطلب الأول: أثر الفضاء الإلكتروني في إعادة تشكيل العلاقات الدولية
61	الفرع الأول: أثر الفضاء الإلكتروني على سيادة الدولة
61	أولاً: الإطار العام للسيادة
66	ثانياً: أثر الفضاء الإلكتروني على سيادة الدول
68	الفرع الثاني: الفضاء الإلكتروني والتحول الاستراتيجي في مفهوم القوة
69	أولاً: القوة في العلاقات الدولية
74	ثانياً: القوة الإلكترونية في التفاعلات الدولية
77	الفرع الثالث: ظهور الدبلوماسية الرقمية على الساحة السيبرانية
77	أولاً: الإطار المفهومي للدبلوماسية
79	ثانياً: الدبلوماسية الرقمية على ساحة الفضاء الإلكتروني
85	المطلب الثاني: الفضاء الإلكتروني والتحول في مفهوم الأمن
85	الفرع الأول: أثر الفضاء الإلكتروني في تغيير مفهوم الأمن
85	أولاً: التطور المفهومي للأمن

89		ثانيا: الأمن في الفضاء السيبراني
92		الفرع الثاني: الأمن السيبراني: المكونات والأبعاد
93		أولا: مرتكزات أمن الفضاء الإلكتروني
95		ثانيا: أبعاد الأمن السيبراني
99		الفرع الثالث: مهددات الأمن السيبراني
99		أولا: الجرائم الإلكترونية
105		ثانيا: الحرب السيبرانية

الفصل الثاني:

الإرهاب الإلكتروني: خطر يهدد الأمن الدولي

111		المبحث الأول: ماهية الإرهاب الإلكتروني
111		المطلب الأول: مفهوم الإرهاب الإلكتروني
111		الفرع الأول: إشكالية تعريف الإرهاب الإلكتروني
112		أولا: إشكالية تعريف الإرهاب
117		ثانيا: تعريف الإرهاب الإلكتروني
122		الفرع الثاني: تمييز الإرهاب الإلكتروني عن غيره من المفاهيم
123		أولا: تمييز الإرهاب الإلكتروني عن المقاومة الإلكترونية
127		ثانيا: التمييز بين الإرهاب الإلكتروني وحرب المعلومات
128		ثالثا: التمييز بين الإرهاب الإلكتروني والجريمة الإلكترونية
129		الفرع الثالث: خصائص الإرهاب الإلكتروني
129		أولا: الخصائص المتعلقة بطبيعة الجريمة
132		ثانيا: الخصائص المتعلقة بطبيعة الهجمات
133		ثالثا: الخصائص المتعلقة بتقييم طبيعة التهديد
134		المطلب الثاني: أسباب الإرهاب الإلكتروني

الفرع الأول: الأسباب النفسية والاجتماعية.....	134
أولاً: الأسباب النفسية	135
ثانياً: الأسباب الاجتماعية.....	138
الفرع الثاني: الأسباب السياسية والاقتصادية.....	140
أولاً: الأسباب السياسية.....	140
ثانياً: الأسباب الاقتصادية.....	144
الفرع الثالث: الأسباب الإيديولوجية والمذهبية.....	147
أولاً: التطرف الإيديولوجية	147
ثانياً: التطرف العقائدي	152
الفرع الرابع: الأسباب التقنية والفنية	156
أولاً: الأسباب التقنية	156
ثانياً: الأسباب الفنية	159
المبحث الثاني: الإرهاب الإلكتروني: الهجمات والتداعيات	161
المطلب الأول: هجمات الإرهاب الإلكتروني.....	161
الفرع الأول: مصادر الهجمات الإرهابية الإلكترونية	162
أولاً: إرهاب الدولة	162
ثانياً: إرهاب الأفراد والجماعات	166
الفرع الثاني: أسلحة الهجمات الإرهابية الإلكترونية.....	167
أولاً: الأسلحة الإلكترونية الهجينة	168
ثانياً: الأسلحة الإلكترونية الفعلية	169
ثانياً: الهجوم إلى البيئة الإلكترونية	178
المطلب الثاني: تداعيات الإرهاب الإلكتروني.....	184
الفرع: تداعيات الإرهاب الإلكتروني على الأفراد	185

أولاً: تداعيات الإرهاب الإلكتروني على حقوق الإنسان الرقمية	185
ثانياً: تداعيات الإرهاب الإلكتروني على الأمن الفكري	189
الفرع الثاني: تداعيات الإرهاب الإلكتروني على الأمن القومي للدول	191
أولاً: تداعيات الإرهاب الإلكتروني على البنية التحتية الحرجة	191
ثانياً: تداعيات الإرهاب الإلكتروني على أمان المعلومات وسريتها	195
الفرع الثالث: تداعيات الإرهاب الإلكتروني على العلاقات الدولية	196
أولاً: التوظيف الصلب الإرهاب الإلكتروني في الصراع الدولي	196
ثانياً: التوظيف الناعم الإرهاب الإلكتروني في العلاقات الدولية	199

الباب الثاني:

المواجهة الدولية لظاهرة الإرهاب الإلكتروني

الفصل الأول:

الجهود الأمنية الدولية لمواجهة الإرهاب الإلكتروني

المبحث الأول: التنظيم الوظيفي لبحر الإرهاب الإلكتروني	207
المطلب الأول: حوكمة الأمن السيبراني	207
الفرع الأول: مفهوم حوكمة الأمن السيبراني	208
أولاً: تعريف الحوكمة الأمنية في مجال الفضاء الإلكتروني	208
ثانياً: مرتكزات حوكمة الأمن السيبراني	213
الفرع الثاني: تفعيل دور المجتمع المدني في الوقاية من الإرهاب الإلكتروني	219
أولاً: لمحة عامة عن المجتمع المدني ودوره في تحقيق الأمن والسلم العالميين:	219
ثانياً: إسهامات المجتمع المدني في مكافحة الإرهاب الإلكتروني وتحقيق الأمن السيبراني:	222
الفرع الثالث: التعاون بين القطاع العام والخاص	227
أولاً: إطار بناء الشراكة بين القطاع العام والخاص في الأمن السيبراني	228

229	ثانيا: اتجاهات التعاون بين القطاع العام والخاص
234	المطلب الثاني: الطب الشرعي الرقمي
235	الفرع الأول: الإطار المفهومي للطب الشرعي الرقمي
235	أولا: تعريف الطب الشرعي الرقمي
238	ثانيا: الطب الشرعي الرقمي: المكانة والأنواع
242	الفرع الثاني: الأدلة الرقمية في الطب الشرعي الرقمي
243	أولا: مفهوم الدليل الرقمي
248	ثانيا: إجراءات بناء وتكوين الدليل الرقمي
252	الفرع الثالث: تحديات الطب الشرعي الرقمي
252	أولا: التحديات التقنية والتنظيمية
256	ثانيا: التحديات القانونية
258	المبحث الثاني: الاستراتيجية الوقائية لحماية الفضاء الإلكتروني
258	المطلب الأول: ديناميكيات التأمين التقني للفضاء الإلكتروني
259	الفرع الأول: التشفير
259	أولا: تعريف عملية التشفير
263	ثانيا: أنواع التشفير
267	الفرع الثاني: الجدران النارية وبرامج مكافحة الفيروسات
267	أولا: الجدران النارية
273	ثانيا: برامج مكافحة الفيروسات
277	الفرع الثالث: نظام الحجب والمراقبة
277	أولا: الحجب والترشح
282	ثانيا: المراقبة الإلكترونية
285	المطلب الثاني: حماية الأصول المادية للفضاء الإلكتروني

285.....	الفرع الأول: حماية المباني
285.....	أولاً: ضبط حدود المباني ومكانها
288.....	ثانياً: ضبط الدخول والخروج
291.....	الفرع الثاني: حماية الموظفين والحماية منهم
291.....	أولاً: حماية الموظفين
296.....	ثانياً: الحماية من الموظفين
299.....	الفرع الثالث: حماية الأجهزة والمعدات
299.....	أولاً: حماية الكوابل البحرية
303.....	ثانياً: حماية الحواسيب والمعدات الحساسة الدقيقة

الفصل الثاني:

الجهود القانونية الدولية لمواجهة الإرهاب الإلكتروني

307.....	المبحث الأول: الإطار القانوني الدولي في التصدي للإرهاب الإلكتروني
307.....	المطلب الأول: الجهود التشريعية الوطنية والإقليمية
308.....	الفرع الأول: التشريعات الوطنية في مكافحة الإرهاب الإلكتروني
308.....	أولاً: السياسة التشريعية الجزائرية في مواجهة الإرهاب الإلكتروني
314.....	ثانياً: السياسة التشريعية الأمريكية لمكافحة الإرهاب الإلكتروني
319.....	الفرع الثاني: الجهود الإقليمية
319.....	أولاً: جهود الاتحاد الأوروبي
324.....	ثانياً: الاتحاد الإفريقي
328.....	الفرع الثالث: الاتفاقيات الثنائية لتحقيق الأمن السيبراني
328.....	أولاً: الصين
329.....	ثانياً: الولايات المتحدة
331.....	ثالثاً: روسيا

332.....	رابعاً: قطر
336.....	المطلب الثاني: جهود الهيئات الدولية
336.....	الفرع الأول: جهود منظمة هيئة الأمم المتحدة
336.....	أولاً: إطار الحوار الدولي في مواجهة الإرهاب الإلكتروني
344.....	ثانياً: الأمم المتحدة وثقافة الأمن السيبراني
348.....	الفرع الثاني: جهود مجموعة الثمانية
349.....	أولاً: سياق الأمن السيبراني في مجموعة الثمانية
354.....	ثانياً: أهم القمم التي تناولت موضع مكافحة الإرهاب الإلكتروني
356.....	الفرع الثالث: دور منظمة التعاون الاقتصادي والتنمية
356.....	أولاً: نشاطات منظمة التعاون الاقتصادي لتحقيق الأمن السيبراني
359.....	ثانياً: توصيات منظمة التعاون الاقتصادي والتنمية
366.....	المبحث الثاني: التعاون القضائي الدولي في التصدي للإرهاب الإلكتروني
366.....	المطلب الأول: المساعدة القضائية الدولية
367.....	الفرع الأول: قنوات المساعدة القضائية
367.....	أولاً: على الصعيد الدولي
372.....	ثانياً: على الصعيد الإقليمي
379.....	الفرع الثاني: المساعدة الإجرائية
379.....	أولاً: الإنابة القضائية
386.....	ثانياً: تنفيذ الأحكام الأجنبية
388.....	الفرع الثالث: المساعدة الفنية
388.....	أولاً: تبادل المعلومات
391.....	ثانياً: التدريب والتكوين
393.....	المطلب الثاني: تسليم مجرمي الإرهاب الإلكتروني

393.....	الفرع الأول: مفهوم تسليم المجرمين
393.....	أولاً: تعريف التسليم
397.....	ثانياً: آراء الفقهاء في مسألة تسليم المجرمين
401.....	الفرع الثاني: نظام تسليم المجرمين: الإجراءات والشروط
402.....	أولاً: إجراءات تسليم
403.....	ثانياً: شروط التسليم
411.....	الفرع الثالث: التسليم بين ما ينتجه من آثار وما يواجه من تحديات
411.....	أولاً: آثار التسليم
413.....	ثانياً: تحديات نظام التسليم
418.....	خاتمة
425.....	قائمة المراجع
509.....	الفهرس

الملخص:

أفضت الثورة الصناعية إلى إحداث طفرة عظيمة في المجال التكنولوجي والتقني ولاسيما فيما يتعلق بمجال تكنولوجيا المعلومات والاتصال وما ارتبط بهما من نظم مختلفة، الأمر الذي ترتب عنه بزوغ الفضاء الإلكتروني كمجال حيوي أدى إلى إحداث تغييرات محورية وجذرية في المجال السياسي والاقتصادي والاجتماعي والعسكري فضلا عن آثاره على الصعيد القانوني، فقد نتج عنه وبشكل منقطع النظير تغيير نمط حياة البشر أفرادا وجماعات، كما غير من طبيعة قوى الدول وعلاقاتها بعضها ببعض، وأعاد تشكيل التوازنات الدولية للقوى، ورغم ما لهذا الفضاء الإلكتروني من محامد إلا أنه قد غير من مفهوم الأمن وأعاد صياغة مفهوم الحرب، وأصبح ساحة صراع ومصدر تهديد مؤرق للبشرية لاسيما بعدما أصبح يوظف لأغراض إرهابية، إذ تحول الفضاء الإلكتروني لساحة يمارس فيها الإرهابيون نشاطات إرهابية إلكترونية ذات أهداف متفاوتة الخطورة.

Abstract :

The industrial revolution led to a great boom in the technological and technical field, especially with regard to the field of information and communication technologies and the various systems associated with them, which resulted in the emergence of cyberspace as a vital area which has led to radical changes in the political and economic sphere. And socially and militarily, as well as its legal effects, it has brought about an unprecedented change in the way of life of human beings, individuals and groups, as well as in the nature of state power. and its relations with each other, and reshaped the international balance of power Although this cyberspace is having a positive effect, it has changed the concept of security and redefined the concept of war, and it has become an arena of conflict and a source of alarming threat to humanity, especially after being used for terrorism. Because cyberspace has become an arena in which terrorists engage in electronic terrorist activities with objectives of varying severity.