جريمة الإرهاب السيبراني في النظام السعودي

الباحث/ منصور حمد عبد الكريم الحميد

ماجستير القانون الجنائي- جامعة نايف العربية للعلوم الامنية

تحت إشراف

الدكتور/ علي مصطفى الأمين جبر

أستاذ مشارك بقسم القانون الجنائي بجامعة نايف العربية للعلوم الأمنية

(ISSN: 2537 - 0758)

جريمة الإرهاب السيبراني في النظام السعودي

الباحث/ منصور حمد عبد الكريم الحميد

مستخلص الدراسة:

تواجه المملكة العربية السعودية، كغيرها من الدول، تحديات متنامية نتيجة تصاعد جريمة الإرهاب السيبراني، التي باتت تمثل تهديدًا للأمن الوطني نظرًا لطبيعتها الرقمية المعقدة، وتداخلها مع الأنظمة التقنية والقانونية على حد سواء. وقد هدفت هذه الدراسة إلى تحليل الأركان الموضوعية والإجرائية لجريمة الإرهاب السيبراني في النظام السعودي، مع التركيز على التكييف النظامي والتحديات العملية المرتبطة بضبط الجريمة وتنفيذ القانون. اعتمدت الدراسة المنهج التحليلي، وذلك من خلال استقراء النصوص النظامية ذات الصلة في المملكة، والرجوع إلى الأدبيات الجنائية والأمنية والدراسات المحكمة الحديثة. كشفت النتائج عن استمرار الفراغ التشريعي الجزئي حيال جريمة الإرهاب السيبراني، حيث لا تتضمن الأنظمة الحالية نصوصًا صريحة توضح أركان الجريمة بشكل مفصل، بالإضافة إلى وجود تعدد مؤسسي في الجهات المعنية دون تنسيق فعّال في مواجهة التهديدات، مما يضعف من القدرة الوطنية على الاستجابة الفورية. كما برزت صعوبات فنية وقانونية في جمع الأدلة الرقمية واعتمادها قضائيًا، في ظل تطور أدوات التمويه الرقمي ونقص الكوادر المؤهلة تقنيًا.

وفي ضوء ما سبق، توصي الدراسة بضرورة استحداث فصل خاص في نظام مكافحة الإرهاب يتناول جريمة الإرهاب السيبراني بنصوص واضحة ومباشرة، ووضع لائحة تنفيذية متخصصة ضمن نظام مكافحة الجرائم المعلوماتية، بالإضافة إلى إصدار تنظيم مستقل للمسؤولية الجنائية للمنصات الرقمية، سواء عند التورط أو الإهمال في الوقاية من الجريمة. إن تبني هذه التوصيات من شأنه تعزيز فعالية المواجهة النظامية والتقنية لهذه الظاهرة، والارتقاء بقدرة المملكة على حماية أمنها السيبراني ضمن إطار تشريعي متكامل وواضح.

الكلمات المفتاحية: الإرهاب السيبراني، الأمن السيبراني، إنفاذ القانون، الجرائم الرقمية، النظام السعودي.

The crime of cyberterrorism in the Saudi regime

Researcher/ Mansour Hamad Abdulkarim Al-Hamid
Master of Criminal Law - Naif Arab University for Security Sciences
Supervision
Dr. Ali Mustafa Al-Amin Jabr
Associate Professor at the Criminal Law Department at Naif Arab University for Security Sciences

Study Abstract:

Like many other countries, the Kingdom of Saudi Arabia faces growing challenges due to the rise of cyberterrorism crimes, which have become a threat to national security because of their complex digital nature and their intersection with both technical and legal systems. This study aims to analyze the substantive and procedural elements of cyberterrorism crime in the Saudi legal system, focusing on its legal characterization and the practical challenges related to crime detection and law enforcement. The study adopts an analytical approach by examining relevant Saudi legal texts and drawing upon related criminal and security literature as well as recent peer-reviewed studies. The findings reveal a persistent legislative gap concerning cyberterrorism, as the current legal framework lacks explicit provisions that clearly define the elements of the crime. In addition, the existence of multiple institutional stakeholders without effective real-time coordination weakens the nation's immediate response capabilities. The study also highlights technical and legal difficulties in collecting and judicially admitting digital evidence, particularly amid the evolution of digital obfuscation tools and a shortage of technically qualified personnel in some law enforcement bodies.

In light of these findings, the study recommends establishing a dedicated section within the Anti-Terrorism Law that explicitly addresses cyberterrorism with clear and direct provisions, enacting a specialized executive regulation within the Anti-Cybercrime Law, and issuing an independent regulation concerning the criminal liability of digital platforms in cases of involvement or negligence in crime prevention. The adoption of these

(ISSN: 2537 - 0758)

recommendations is expected to enhance the effectiveness of the regulatory and technical response to this phenomenon and strengthen the Kingdom's ability to protect its cybersecurity within a clear and comprehensive legislative framework.

Keywords: Cyberterrorism, cybersecurity, law enforcement, digital crimes, Saudi legal system.

مقدمة الدراسة:

شهد مفهوم الإرهاب تطورًا جذريًا في العصر الحديث، حيث انتقل من كونه تهديدًا تقليديًا يرتكز على استخدام العنف المادي المباشر إلى ظاهرة أكثر تعقيدًا ترتكز على الوسائل التقنية المتقدمة. وقد أدى هذا التحول إلى نشوء ما يُعرف بالإرهاب السيبراني، الذي بات يمثل أحد أخطر التهديدات للأمن القومي والسيادة الرقمية للدول، نظرًا لقدرة مرتكبيه على تنفيذ عمليات تخريبية من خلف الشاشات دون حدود جغرافية، وبوسائل يصعب تتبعها أو مواجهتها بالإجراءات التقليدية.

وفي ظل الطفرة التكنولوجية التي يشهدها العالم، تزايد الاعتماد على البنية التحتية الرقمية في إدارة شؤون الدولة، لا سيما في المجالات الاقتصادية والأمنية والإدارية، الأمر الذي أدى إلى نشوء بيئة خصبة للجماعات الإرهابية لاستغلال الفضاء السيبراني في تنفيذ أهدافهم. فقد أصبحت الشبكات الإلكترونية أداة مركزية للتجنيد، والدعاية، والتخطيط، بل والتنفيذ الفعلي للهجمات، مما أكسب الإرهاب السيبراني طابعًا متطورًا وشديد الخطورة[١].

فلقد استغلت الجماعات الإرهابية المزايا التكنولوجية كعنصر حيوي لدعم وتحقيق أهدافها ومنفذ لوجستي داعم وحاضن للنشاط الإعلامي لها في مناطق مختلفة من العالم، فمن خلال شبكات الإنترنت تستطيع الجماعات الإرهابية تصوير أنفسهم وأعمالهم في الضوء والسياق الذي يريدونه، دون أن يعرقل ذلك تفحص وسائل الإعلام الرسمية لذلك التصوير أو غربلته أو تحويره، وقد بدأ الإرهابيون بالفعل في استخدام الفضاء الإلكتروني في التأثير على الرأي العام وتجنيد أعضاء جدد وجمع الأموال[٢].

---

[١] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، الجريمة السيبرانية والإيقاع الإجرامي التقليدي بالضحايا، دراسة شاملة عن الجريمة السيبرانية، مسودة فبراير، جينيف، ٢٠١٩، ص ١٢٢.

[٢] أحمد عبيس الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،مجلة المحقق للعلوم القانونية والسياسية، الجزائر، ٢٠١٧، ص ٥٥.

وتُعد المملكة العربية السعودية من الدول التي أولت اهتمامًا بالغًا بهذا النوع من الجرائم، إدراكًا منها لخطورتها المتزايدة على الأمن الوطني، والمؤسسات الحيوية، واستقرار المجتمع. فقد بادرت المملكة إلى إصدار الأنظمة ذات الصلة، وتأسيس الهيئات المختصة، وإطلاق الاستراتيجيات الوطنية للأمن السيبراني، غير أن الواقع العملي يُظهر استمرار وجود ثغرات قانونية ومؤسساتية تتطلب المعالجة الفورية والدقيقة[٣].

ويكتسب موضوع الإرهاب السيبراني أهمية متزايدة في ضوء تداخله مع عدد من الجرائم المنظمة، مثل تمويل الإرهاب وغسل الأموال الرقمية، واستخدام العملات المشفرة في تنفيذ عمليات معقدة، فضلًا عن علاقته الوثيقة بجرائم المعلومات والاعتداء على الأنظمة المعلوماتية الحكومية. مما يجعل دراسته من منظور قانوني وأمني أمرًا ضروريًا لفهم أركانه، وتحديد وسائل مواجهته، والوقوف على حدود المسؤولية الجنائية لمرتكبيه[٤].

مشكلة الدراسة:

رغم التطور المذهل في تقنيات المعلومات والاتصالات، وما حمله من فرص لتعزيز التنمية والإدارة الحكومية الحديثة، إلا أن هذه التطورات فتحت في الوقت ذاته آفاقًا جديدة لارتكاب أنماط إجرامية مستحدثة، في مقدمتها جريمة الإرهاب السيبراني، التي تمثل تحديًا مركبًا يتقاطع فيه البعد الأمني مع البعد التقني. وقد أصبح الفضاء الرقمي بيئة خصبة لاستغلاله من قبل الجماعات الإرهابية في التخطيط والتجنيد، وتمويل العمليات، والترويج لأفكارها المتطرفة بعيدًا عن الرقابة الأمنية التقليدية.

وفي هذا السياق، تواجه المملكة العربية السعودية تحديات حقيقية في رصد هذه الأنشطة ومواجهتها تشريعيًّا ومؤسسيًّا، في ظل التطور المتسارع لوسائل تنفيذ الجرائم السيبرانية، وتعقيد إثباتها، وامتداد آثارها إلى البنية التحتية والأمن الوطني. ومن ثمّ، تنبع مشكلة الدراسة من الحاجة إلى تحليل الطبيعة القانونية لجريمة الإرهاب السيبراني، وتقييم

---

[٣] عبد الرزاق المرجان وآخرون، الأساليب والاتجاهات الحديثة للجرائم السيبرانية والوقاية منها، دار جامعة نايف للنشر، الرياض، ٢٠٢٥م، ص ٤٤

[٤] جبور على الأشقر، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٦، ص ١٦.

(ISSN: 2537 - 0758)

مدى كفاية السياسات والنصوص النظامية السعودية القائمة لمكافحتها، وبيان الثغرات التي قد تُعيق فاعلية المواجهة، وذلك في ضوء التجارب الوطنية الحالية والجهود المتعددة المبذولة في هذا المجال.

تساؤلات الدراسة:

١. ما هي الأركان القانونية المميزة لجريمة الإرهاب السيبراني في النظام السعودي، وكيف تختلف عن الجرائم التقليدية؟
٢. ما مدى كفاية العقوبات النظامية المقررة لمواجهة جريمة الإرهاب السيبراني في ظل طبيعتها المركبة والمتجددة؟
٣. ما هي أبرز الجهات والمؤسسات الوطنية المختصة بمكافحة الإرهاب السيبراني، وما حدود أدوارها؟
٤. ما هي أبرز الإجراءات الجنائية الخاصة بضبط جريمة الإرهاب السيبراني، وما الإشكاليات التي تعيق إنفاذ القانون فيها؟

أهداف الدراسة: **تسعى الدراسة لتحقيق الأهداف الآتية:**

١. تحديد الأركان القانونية المميزة لجريمة الإرهاب السيبراني في النظام السعودي، وكيف تختلف عن الجرائم التقليدية.
٢. توضيح مدى كفاية العقوبات النظامية المقررة لمواجهة جريمة الإرهاب السيبراني في ظل طبيعتها المركبة والمتجددة.
٣. عرض أبرز الجهات والمؤسسات الوطنية المختصة بمكافحة الإرهاب السيبراني، وما حدود أدوارها.
٤. توضيح أبرز الإجراءات الجنائية الخاصة بضبط جريمة الإرهاب السيبراني، وما الإشكاليات التي تعيق إنفاذ القانون فيها.

أهمية الدراسة:

تتضح أهمية الدراسة من خلال ما يلي:

أولًا: **الأهمية النظرية:**

تنبع الأهمية النظرية لهذه الدراسة من طبيعة الموضوع الذي تتناوله، والمتمثل في جريمة الإرهاب السيبراني، وهي من أبرز صور الجرائم المعاصرة التي تستلزم إعادة النظر في المفاهيم الجنائية التقليدية، خاصة ما يتعلق بالأركان القانونية، والعقوبات،

والمساهمة الجنائية، وهو ما يُبرز أهمية الإسهام النظري الذي تقدمه الدراسة في بناء إطار قانوني متكامل لهذا النوع من الجرائم. كما تُعد الدراسة إثراءً للمكتبة العربية والسعودية في ميدان الجرائم السيبرانية.

ثانياً: الأهمية العملية:

تتجلّى الأهمية العملية للدراسة في كونها تُسلّط الضوء على التحديات الواقعية التي تواجه الجهات المختصة في مكافحة جريمة الإرهاب السيبراني، وذلك في ظل تعقيد الأدلة الرقمية وتداخل الاختصاصات المؤسسية. وتبرز أهمية الدراسة أيضًا في تحليلها للإجراءات الجنائية السعودية، وتقديمها مقترحات عملية قابلة للتطبيق لتطوير إنفاذ القانون في هذا المجال. كما تُعد هذه الدراسة مرجعًا مهمًا لصنّاع القرار، وللقضاة، ورجال الضبط الجنائي، والمحققين، والباحثين في ميدان الأمن السيبراني، لما تتضمنه من رؤية نقدية وحلول واقعية لسد الثغرات النظامية والإجرائية.

منهج الدراسة:

من خلال توظيف المنهج الوصفي التحليلي: يمكن للباحث تعقب ورصد الإنجازات القانونية ومن التشريعات والتحليل المعمق لنصوص القرارات الدولية، وتتبع الخطط والاستراتيجيات المحلية والإقليمية والدولية لمواجهة الإرهاب السيبراني.

مفاهيم ومصطلحات الدراسة:

(أ) مفهوم الجريمة:

لغة: في اللغة بمعنى الكسب والقطع، والحرم والجريمة بمعنى الذنب و (الجرم) بالكسر الجسد و(جرم) أيضا كسب وبابهما ضرب[٥].

اصطلاحاً: الجريمة هي محظورات شرعية زجر الله تعالى عنها بحد أو تعزير "وعرفها أبو يعلى بن الفراء بتعريف شبيه به بأنها محظورات بالشرع، زَجَرَ اللَّهُ تَعَالَى عَنْهَا بحد أو تعزيز"[٦].

كما تعرف الجريمة بأنها كل فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرًا احترازيًا[٧].

---

[٥] محمد بن مكرم ابن منظور، لسان العرب، دار الكتب العلمية، بيروت، ط ٢، ١٤٣٠هـ، ص١٥٩٥.

[٦] عبد القادر عودة، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، دار الكاتب العربي، بيروت، لبنان، ج١، ٢٠١٣، ص٦٦.

(ISSN: 2537 - 0758)

(ب) مفهوم الإرهاب السيبراني وما يتصل به:

١- التعريف اللغوي للإرهاب السيبراني:

أ- تعريف الإرهاب:

لغةً: اتفقت معاجم اللغة العربية على أن لفظة (إرهاب) تعني الفزع والخوف والرعب فهي مشتقة من فعل ثلاثي مزيد بحرف (أرهب) فتقول: (أرهب فلاناً، أي خوفه وفزعه وأخافه)[٨]. وأما (أرهبه واسترهبه) فيعني: (أخافه وأفزعه)[٩].

وفي المعاجم الأجنبية المترجمة ورد لفظ الإرهاب بدلالة المصطلح (Terrorism) المشتقة من الفعل (Terror) بما يعني: الفزع والذعر والهلع والتخويف أو إشاعة الهلع[١٠].

٢- التعريف الاصطلاحي للإرهاب السيبراني:

هو هجوم غير مشروع أو تهديدات بهجمات ضد أجهزة الحاسب الآلي والشبكات أو البيانات والمعلومات المخزنة بطريقة إلكترونية، يتم توجيهها للانتقام أو التهديد أو الإجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأكمله لتحقيق أهداف سياسية أو دينية أو اجتماعية[١١].

والاتفاقية العربية لمكافحة جرائم تقنية المعلومات ٢٠١٠ لم تقدم تعريفًا مستقلاً للإرهاب الإلكتروني، بل ركزت على تحديد الأفعال المرتبطة بالإرهاب عند استخدام تقنية المعلومات، حيث تشير المادة ١٥ من هذه الاتفاقية إلى "الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات"، **وتحددها بالآتي**[١٢]:

١. نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

---

[٧] محمود طه جلال، أصول التجريم والعقاب في السياسة الجنائية المعاصرة "دراسة مقارنة"، رسالة ماجستير، كلية الحقوق، جامعة عين شمس،١٤٢٥هـ، ص٧٣.

[٨] محمد بن مكرم ابن منظور، مرجع سابق، ص ٨٣٥.

[٩] آبادي محمد بن يعقوب الفيروز، القاموس المحيط، مؤسسة الرسالة، بيروت، ط٢، ١٩٨٧م، ص١١٨.

[١٠] حارث سليمان الفاروقي، المعجم القانوني، مكتبة لبنان، بيروت، ط٥، ٢٠١٣، ص ٦٩٠.

[١١] هشام بشير، مرجع سابق، ص ٥٥.

[١٢] الاتفاقية العربية لمكافحة الجرائم السيبرانية، جامعة الدول العربية، ٢٠١٠، ص ٢٤.

٢. تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
٣. نشر طرق صناعة المتفجرات التي تستخدم خاصة في عمليات إرهابية.
٤. نشر الفتن والاعتداء على الأديان والمعتقدات.

ويعرفه مركز حماية البنية التحتية القومية الأمريكية" بأنه: "عمل إجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية وينتج عنه تدمير أو تعطيل الخدمات لبث الرعب والخوف لإرباك السكان والتأثير السلبي عليهم لخدمة أجندة سياسية أو اجتماعية أو أيديولوجية[١٣].

بينما يعرفه مكتب التحقيقات الفيدرالي الأمريكي بأنه: الهجوم المتعمد ذو الدوافع السياسية ضد أنظمة المعلومات، وبرامج الكمبيوتر والبيانات المخزنة من قبل مختلف الفاعلين[١٤].

كما يُعرف الإرهاب "السيبراني" "Cyber Terrorism" بأنه تلك الجرائم التي لا تعرف الحدود الجغرافية Crime Trans Boarder والتي يتم ارتكابها بالحاسب الآلي عن طريق شبكة الإنترنت، وبواسطة شخص على دراية فائقة بها، ولذا أطلق عليه (الإرهاب الإلكتروني)[١٥].

وتخلص الدراسة بعد استعراض المفاهيم المختلفة للإرهاب السيبراني، إلى أن هذا النوع من الجرائم يمثل هجمات متعمدة تحمل أهدافًا سياسية، وتهدف إلى التأثير في قرارات حكومة المملكة العربية السعودية أو توجيه الرأي العام داخل المجتمع. ويتم تنفيذ هذه الهجمات عبر الفضاء السيبراني، الذي يُستخدم كوسيلة أساسية في تنفيذ الأعمال الإرهابية.

---

[١٣] عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، ٢٠١٤م، ص٥.

[١٤] محمد مجاهد، تضارب المصالح "عقبات تشكيل تحالف عسكري ضد داعش، اتجاهات الأحداث، مجلة مركز المستقبل للأبحاث والدراسات المتقدمة، ع ٨، أبوظبي، ٢٠١٥، ص ٢٣٥.

[١٥] شمان ناجي الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٦، ص ٣٥.

(ISSN: 2537 - 0758)

وقد تأخذ هذه الهجمات شكلًا تقنيًا مباشرًا يستهدف البنية التحتية للمنشآت الحساسة، أو تسريب المعلومات السرية، وقد تكون على شكل حملات تحريضية تستهدف إثارة الفتن، أو نشر الكراهية الدينية، أو استهداف الرموز والمقدسات، وغالبًا ما تكون هذه الأعمال مدعومة من جهات خارجية معادية.

كما تشمل بعض أشكال الإرهاب السيبراني استخدام أدوات متطورة مثل الطائرات المسيرة "الدرون"، التي تُدار عبر الشبكات الرقمية، وتنفذ عمليات قد تقتصر على البنية التقنية، أو تمتد لتصيب أهدافًا مادية حقيقية داخل الدولة.

(ج) النظام:

النظام في اللغة: الجمع: "نُظُمٌ، وأَنْظِمَةٌ، وأَناظيمُ" مصدر "نظَمَ" **النِّظَامُ:** "الترتيبُ والاتِّساق". "والنظم: التأليف، يقال: نظم الأشياء نظما ونظاما أي: ألفها وضم بعضها إلى بعض فانتظمت.

والنظام: ما نظمت فيه الشيء من خيط وغيره، فكل شيء قرنته بآخر، أو ضممت بعضه إلى بعض فقد نظمته. والنظام الهدية، والسيرة، والطريقة، يقال: ليس لأمرهم نظام، أي: ليس له هدي ولا متعلق ولا استقامة، ومازال على نظام واحد أي: على طريقة واحدة"[١٦]، ومن هذا يتضح أن النظام في اللغة: يُفيد تأليف الشيء على نسق واحد.

النظام في الاصطلاح: يُعرف النظام في الاصطلاح باعتبارين هما:

- **الاعتبار الأول:** من الناحية الموضوعية، فهو عبارة عن مجموعة من الأحكام التي تتعلق بموضوع محدد، وتعرض في صورة مواد متتالية[١٧].
- **الاعتبار الثاني:** من الناحية الشكلية، فهو عبارة عن وثيقة مكتوبة من الملك بعد اتفاق مجلس الوزراء ومجلس الشورى[١٨].

النظام إجرائياً:

القواعد العامة الملزمة الصادرة من السلطة التنظيمية والموافق عليها بمرسوم ملكي.

---

[١٦] محمد بن مكرم ابن منظور، مرجع سابق، ص ١٣٥٦.

[١٧] محمد عبد الله المرزوقي، السلطة التنظيمية في المملكة العربية السعودية، دار العبيكان، الرياض، ١٤٢٥هـ، ص ٨٦.

[١٨] عبد المجيد الحفناوي، أصول التشريع في المملكة العربية السعودية، دار الكتب، القاهرة، ط٢، ٢٠١٥، ص ٩٣.

الدراسات السابقة:

١- دراسة (عبدالرزاق المرجان وآخرون، ٢٠٢٥)[١٩].

بعنوان الأساليب والاتجاهات الحديثة للجرائم السيبرانية والوقاية منها.

هدفت هذه الدراسة إلى استكشاف الأنماط التقنية المعقدة للجرائم السيبرانية الحديثة، وتحليل الأساليب المستجدة المستخدمة في تنفيذ الهجمات الرقمية، من خلال عينة إحصائية وتحليلية شملت ١٢ دولة عربية. اعتمد الباحثون المنهج التحليلي المقارن، مع الاستناد إلى منهج الرصد الميداني لتحديد اتجاهات التهديدات السيبرانية.

وقد كشفت الدراسة عن سبعة أنماط رئيسية للهجمات، أبرزها: الهجمات المؤتمتة، وهجمات الذكاء الاصطناعي، وتشفير الفدية. ومن أبرز النتائج أن مستوى الجريمة السيبرانية يشهد تحولًا نوعيًا نحو التعقيد الهيكلي في تصميم الهجوم، وضعف القدرة التنظيمية لدى بعض الجهات الأمنية الإقليمية في المتابعة الوقائية. كما أظهرت الدراسة قصورًا في التشريعات العربية بشأن الجرائم السيبرانية المتقدمة.

وأوصت الدراسة بتأسيس وحدة استخبارات رقمية عربية مشتركة، وتطوير المنصات الوطنية لرصد الهجمات السيبرانية المتزامنة، وتحديث البنية التشريعية لتشمل الجرائم التقنية القائمة على الذكاء الاصطناعي والرموز المشفرة.

وتتميّز هذه الدراسة عن الدراسة السابقة بتركيزها الحصري على جريمة الإرهاب السيبراني، دون الخلط بينها وبين الجرائم المعلوماتية العامة. بينما تناولت بعض الدراسات السابقة الجريمة الرقمية بشكل شامل، ركّزت هذه الدراسة على البنية القانونية الخاصة بالإرهاب السيبراني في المملكة العربية السعودية، وناقشت أركان الجريمة وعقوباتها والنصوص المنظمة لها بشكل تفصيلي، وهو ما يُعد جانبًا لم يُسلّط عليه الضوء بهذا العمق من قبل.

كما أن هذه الدراسة تميّزت بدمج الجوانب النظرية مع الواقع الإجرائي، من خلال تحليل الإجراءات المتبعة في الضبط والتفتيش والإثبات الرقمي، وتقييم أدوار الجهات الرسمية المعنية. وقدمت توصيات عملية قابلة للتنفيذ، مما يمنح الدراسة بُعدًا تطبيقيًا يعزز من قيمتها العلمية في دعم الجهود الوطنية لمكافحة الإرهاب السيبراني.

---

[١٩] عبد الرزاق المرجان وآخرون، الأساليب والاتجاهات الحديثة للجرائم السيبرانية والوقاية منها، دار جامعة نايف للنشر، الرياض، ٢٠٢٥م.

(ISSN: 2537 - 0758)

٢- دراسة (سعيد بن زعل الخريصي، ٢٠٢٣)[٢٠].

بعنوان: جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية في مواجهتها من منظور الأمن الوطني والقانون الدولي.

سعى الباحث إلى تحليل التهديدات السيبرانية على الأمن الوطني السعودي من زاوية السياسة الخارجية، من خلال استعراض المواقف الدبلوماسية للمملكة، وتفاعلها مع الأطر القانونية الدولية. اعتمد المنهج الوصفي التحليلي، بالتركيز على آليات الردع الخارجية.

أبرزت النتائج أن المملكة تبنت سياسة متوازنة تقوم على تفعيل التحالفات الأمنية الإقليمية، والتوقيع على اتفاقيات مشتركة لمكافحة الإرهاب السيبراني، كما طوّرت منظومتها الدبلوماسية الرقمية في المحافل الدولية. كما أظهرت الدراسة وجود فجوة في التنسيق القانوني بين الأنظمة المحلية والدولية فيما يتعلق بتعريف الإرهاب السيبراني.

وأوصت الدراسة بإنشاء مجلس وطني للتنسيق السيبراني الخارجي، وتفعيل الشراكة مع الإنتربول الإلكتروني، وتوسيع الجهد القانوني السعودي للمساهمة في صياغة اتفاقية دولية موحدة حول مكافحة الإرهاب السيبراني.

ورغم القيمة التحليلية لدراسة الخريصي في تسليط الضوء على البُعد الدبلوماسي والسياسة الخارجية للمملكة في مواجهة الإرهاب السيبراني، إلا أن دراستنا الحالية تتميّز عنها بالتركيز الداخلي الدقيق على المنظومة القانونية السعودية ذاتها، من حيث تحليل أركان الجريمة، والتكييف النظامي، والعقوبات المقررة، والإجراءات العملية للضبط والتفتيش والإثبات، وهو ما لم تتطرق إليه دراسة الخريصي بشكل مفصل، حيث اكتفت بتناول السياسات الخارجية دون تفكيك البنية النظامية الداخلية للجريمة.

كذلك فإن الدراسة الحالية توسّعت في استقراء الواقع المؤسساتي والأمني السعودي، وحددت التحديات التنفيذية أمام الجهات المختصة، مع تقديم توصيات عملية قابلة للتطبيق على المستوى الوطني، في حين أن توصيات الخريصي تمحورت حول الشراكات الدولية والتوصيف الدبلوماسي، مما يُظهر أن الدراسة الحالية تُكمل النقص في

---

[٢٠] سعيد بن زعل الخريصي، جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية في مواجهتها من منظور الأمن الوطني والقانون الدولي، مجلة جامعة الأندلس للعلوم الإنسانية والاجتماعية، العدد ٧٣، المجلد ١٠، ٢٠٢٣م.

الجانب الداخلي الذي لم تُعالجه الدراسات السابقة بنفس القدر من التخصص والعمق القانوني.

٣- دراسة (سهل بن زعل الخريصي، ٢٠٢٣)[٢١].

بعنوان (جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية في مواجهتها من منظور الأمن الوطني والقانون الدولي)

استهدفت الدراسة بيان كيف يمكن للأدوات الدبلوماسية والاتفاقيات الأمنية الإقليمية أن تشكّل حائط صد قانوني وأمني أمام الهجمات السيبرانية الموجهة للمملكة. اعتمد الباحث المنهج التحليلي المقارن، بالتركيز على التجارب الدولية في مواجهة الإرهاب السيبراني.

أظهرت النتائج أن السعودية عززت من وجودها في اتفاقيات الحماية السيبرانية الثنائية والجماعية، وساهمت في تفعيل مبادرة "التحالف السيبراني العربي"، كما أظهرت الدراسة الحاجة إلى دمج هذه الجهود بالسياسات الأمنية الوطنية، ووأوصى الباحث بإنشاء منصة وطنية لتبادل المعلومات السيبرانية بين الأجهزة الحكومية والدبلوماسية، وربط الهيئات القانونية بالتقنية داخل منظومة الأمن الوطني، ووضع إستراتيجية لتعزيز الردع القانوني الخارجي في الجرائم العابرة للحدود.

وتختلف الدراسة الحالية عن دراسة الخريصي من حيث المجال والتركيز؛ إذ توجهت دراسة الخريصي إلى تحليل الأطر الخارجية والدبلوماسية لمكافحة الإرهاب السيبراني من منظور السياسة الخارجية السعودية، متناولة الاتفاقيات الدولية والتحالفات الإقليمية، بينما ركزت دراستنا الحالية على البنية القانونية الداخلية، وخصّت بالتحليل النصوص النظامية ذات الصلة، وأوضحت أركان الجريمة، والعقوبات، والإجراءات، والإشكالات العملية المرتبطة بإنفاذ القانون، ما يجعلها دراسة متخصصة في الأبعاد النظامية والجنائية المحلية.

كما تتميّز هذه الدراسة بالتركيز على الجوانب التطبيقية والواقعية في الضبط والتحقيق والإثبات، من خلال ربط الإشكالات الإجرائية بمواد نظام الإجراءات الجزائية

---

[٢١] سهل بن زعل الخريصي، جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية في مواجهتها من منظور الأمن الوطني والقانون الدولي، مجلة أبحاث العلوم الإنسانية والاجتماعية، الجامعة الإسلامية بالمدينة المنورة، العدد ٧٣، ٢٠٢٣م.

(ISSN: 2537 - 0758)

السعودي، في حين لم تتناول دراسة الخريصي سوى مستويات السياسات والردع الخارجي، دون التعمق في الممارسات القانونية الداخلية أو عرض آليات الضبط والضمانات القضائية. ومن ثمّ، تُعدّ دراستنا استكمالًا تكميليًا للبُعد الداخلي الذي أهملته الأدبيات السابقة.

٤- دراسة (حازم الجمل، ٢٠٢٢)[٢٢].

بعنوان الحماية الجنائية للأمن السيبراني في المملكة العربية السعودية.

هدفت الدراسة إلى تحليل البنية التشريعية السعودية في مواجهة الجرائم السيبرانية، خاصةً في ضوء نظام مكافحة الجرائم المعلوماتية، مع مقارنة بالتشريعات المقارنة في أوروبا والولايات المتحدة. استخدم الباحث المنهج التحليلي القانوني، مدعومًا بتحليل الحالات القضائية ذات الصلة.

أوضحت النتائج وجود قصور تشريعي في توصيف بعض الأنماط السيبرانية المعقدة مثل اختراق الشبكات السيادية وهجمات المعلومات المالية المشفّرة، كما بينت الحاجة لتحديث الإجراءات الجنائية المتعلقة بالتحقيق الرقمي، وأوصت الدراسة بإنشاء دائرة قضائية سيبرانية متخصصة، وتعديل المادة الثالثة والسادسة من نظام مكافحة الجرائم المعلوماتية لتوسيع نطاق التجريم، إضافة إلى اعتماد ضوابط فنية قضائية بشأن الإثبات الرقمي.

وفي ضوء المقارنة مع هذه الدراسة، يمكن بيان أوجه تمايز الدراسة الحالية على النحو التالي:

تركّزت دراسة الجمل على الحماية الجنائية للأمن السيبراني عمومًا، من منظور نظام مكافحة الجرائم المعلوماتية، مع مقارنة بالقوانين الغربية، وخلصت إلى الحاجة لتحديث بعض المواد النظامية وتوسيع نطاق التجريم. بينما تميّزت الدراسة الحالية بتخصصها الدقيق في "الإرهاب السيبراني" كجريمة نوعية قائمة بذاتها، وبالتحليل المفصل لأركانها، وطبيعتها المركبة، وتكييفها وفق نظام مكافحة الإرهاب وتمويله، إضافة إلى إبراز العلاقة بين النصوص القانونية والممارسات الإجرائية داخل المملكة، دون اعتماد المقارنات الخارجية.

---

[٢٢] حازم الجمل، الحماية الجنائية للأمن السيبراني في المملكة العربية السعودية، مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية، العدد ١٦٣٧، ٢٠٢٢م، ص ١

ومن جهة أخرى، انطلقت الدراسة الحالية من إشكالات واقعية مرتبطة بضبط الجريمة السيبرانية الإرهابية، وإثباتها قضائيًا، وتقصّي حدود فاعلية المؤسسات الوطنية، ما جعلها أكثر ارتباطًا بالتطبيق القضائي والضبط الأمني المحلي، مقارنة بدراسة الجُمَل التي حافظت على طابع نظري تحليلي عام. ومن ثمّ، فإن الدراسة الحالية تمثّل نقلة نوعية في التناول الإجرائي والنظامي للجرائم السيبرانية ذات الطبيعة الإرهابية، في سياق وطني سعودي خالص.

التعليق على الدراسات السابقة:

تُظهر الدراسات السابقة قاسمًا مشتركًا يتمثل في الاعتراف بخطورة الإرهاب السيبراني على الأمن الوطني للمملكة العربية السعودية، وضرورة التصدي له من خلال منظومة متكاملة تشمل التشريع، والتنظيم المؤسسي، والتعاون الإقليمي والدولي، والتقنيات الحديثة. وقد تنوعت اتجاهات هذه الدراسات بين ما ركز على الأبعاد التقنية والهجمات المعاصرة (المرجان وآخرون)، وما ركز على الجوانب الدبلوماسية والسياسية في الرد على الإرهاب السيبراني (الخريصي وسهل الخريصي)، بينما انصبّ تركيز دراسة الجمل على البنية التشريعية للنظام الجنائي في المملكة.

وتتقاطع الدراسة الحالية مع تلك الدراسات من حيث المنطلق، إذ تتفق معها في التأكيد على الطابع التهديدي المتصاعد للإرهاب السيبراني، وحاجة المملكة إلى أطر نظامية دقيقة، وممارسات تنفيذية فعالة. غير أن هذه الدراسة تنفرد بأنها تناولت الموضوع من زاوية جنائية متخصصة، تدمج بين التحليل الموضوعي لأركان الجريمة وتحليل إجرائي لمسار التحقيق والمحاكمة، بما يعكس خصوصية التناول من منظور إنفاذ القانون في النظام السعودي.

لقد مثّلت الدراسات السابقة ركيزة تأسيسية أسهمت في إثراء التصوّر النظري والمنهجي للدراسة الحالية، إذ استفاد الباحث من التحليل المؤسسي والدبلوماسي الوارد في دراسة (الخريصي، ٢٠٢٣) ودراسة (سهل الخريصي، ٢٠٢٣) في دعم التوصيات المتعلقة بتفعيل التنسيق بين الجهات الوطنية، وإنشاء منصات لتبادل المعلومات السيبرانية، وتعزيز الشراكة الدولية في مكافحة الإرهاب السيبراني. كما أمدّت دراسة (حازم الجمل، ٢٠٢٢) الباحث بخلفية قانونية قوية حول الثغرات التشريعية في نظام

(ISSN: 2537 - 0758)

مكافحة الجرائم المعلوماتية، ما ساعد على تدعيم الحاجة الملحّة لتحديث النصوص النظامية وربطها بتوصيف دقيق لجريمة الإرهاب السيبراني.

ومن خلال الاطلاع على هذه الدراسات، تمكّن الباحث من تجاوز الطابع التحليلي العام الذي ميّزها، والتوجه نحو معالجة جنائية دقيقة، تستند إلى فحص الركن المادي والمعنوي والشرعي للجريمة، وتحليل الإجراءات الأمنية والقضائية لضبطها وإثباتها، وهو ما أضفى على الدراسة طابعًا تطبيقيًا يعكس منظور إنفاذ القانون بصورة مباشرة، ويملأ فراغًا بحثيًا لم يُعالج بتفصيل في الدراسات السابقة.

المبحث الأول

جرائم الإرهاب السيبراني وسياسات مكافحتها في المملكة العربية السعودية

تمهيد وتقسيم:

في ظل التطور المتسارع للتكنولوجيا الرقمية، برزت جرائم الإرهاب السيبراني كأحد أبرز التهديدات التي تواجه الدول والمجتمعات في العصر الحديث. فبينما اعتمد الإرهاب التقليدي في الماضي على وسائل عنف مادية، أتاح العصر الرقمي أدوات وأساليب جديدة لتنفيذ الأعمال الإرهابية عبر الفضاء السيبراني، مما جعل الإرهاب السيبراني شكلاً حديثًا وخطيرًا من التهديدات التي تستهدف الأفراد والمؤسسات والدول بأكملها.

ويهدف هذا المبحث إلى تحليل أنماط جرائم الإرهاب السيبراني من خلال دراسة السيناريوهات المختلفة التي يستخدمها الإرهابيون في الفضاء السيبراني، مع التركيز على تقسيم هذه الجرائم وأنواعها وفقًا للأدوات المستخدمة والأهداف المتضررة. كما يتناول المبحث تطور أساليب الإرهاب السيبراني، والتي تشمل الهجمات على البنى التحتية الحيوية والأنظمة المعلوماتية والبيانات الحساسة، مما يجعل الإنترنت والشبكات الرقمية ساحة جديدة للصراع تتميز بالتعقيد والسرية.

إضافة إلى ذلك، يستعرض المبحث السياسات السعودية في مكافحة جرائم الإرهاب السيبراني، حيث يتم تسليط الضوء على الجهود الحكومية والأمنية التي تبذلها المملكة العربية السعودية لمواجهة هذه التهديدات. كما يتم استعراض دور الأمن الوطني في حماية البنية التحتية الرقمية والأنظمة المعلوماتية من الهجمات السيبرانية المدمرة، مع التركيز على التشريعات والتقنيات الحديثة التي تعتمدها المملكة في هذا المجال.

ويتألف المبحث من مطلبين رئيسيين:

الأول: يتناول أنماط جرائم الإرهاب السيبراني وتقسيماتها وأنواعها.

بينما يركز **المطلب الثاني** على السياسات السعودية في مكافحة هذه الجرائم.

المطلب الأول

أنماط (سيناريوهات) جرائم الإرهاب السيبراني

تمهيد وتقسيم:

في عصر تزايد الاعتماد على التكنولوجيا والإنترنت، ظهرت جرائم الإرهاب السيبراني كتهديد كبير للأمن الوطني والدولي. هذه الجرائم، التي تُرتكب عبر الفضاء السيبراني، تختلف في طبيعتها وأساليب تنفيذها، مما يجعل من الصعب تحديد كيفية مواجهتها بشكل شامل. على الرغم من أن العديد من هذه الجرائم تتشابه في تأثيرها على المجتمعات، إلا أن أنماط الإرهاب السيبراني تختلف بشكل كبير من حيث الأسلوب والهدف.

ويتناول هذا المطلب أنماط الجرائم السيبرانية التي يتم استخدامها في تنفيذ الهجمات الإرهابية، حيث سيتعين علينا تقسيمها إلى فئات واضحة تساعد في فهم الأدوات والتقنيات التي يستخدمها الإرهابيون في العصر الرقمي.

وينقسم هذا المطلب إلى فرعين رئيسيين:

الأول يتناول تقسيم جرائم الإرهاب السيبراني إلى عدة أنواع بناءً على الوسائط الرقمية التي يتم استخدامها.

بينما يركز **الفرع الثاني** على أنواع جرائم الإرهاب السيبراني وفقًا لطبيعة الهجمات المستخدمة.

الفرع الأول

تقسيم جرائم الإرهاب السيبراني

يُعَد تقسيم جرائم الإرهاب السيبراني خطوة أساسية لفهم تنوع الأساليب التي يتم استخدامها في تنفيذ الهجمات الإرهابية عبر الفضاء الرقمي. يتطلب هذا التقسيم تصنيف الجرائم بناءً على الوسائط الرقمية المستهدفة، سواء كانت الشبكات، البنى التحتية، أو الأنظمة الحكومية. يسهم هذا التصنيف في تحديد أنماط الهجمات، مما يعزز القدرة على التصدي لها بشكل أكثر فعالية. في هذا الفرع، سنتناول مختلف أنواع

(ISSN: 2537 - 0758)

جـرائم الإرهـاب السـيبراني التـي تحـدث عبـر الوسـائط الرقميـة، مـع توضـيح الأدوات والتقنيات التي يستخدمها الإرهابيون لتنفيذ هذه الجرائم.

أولاً: ما يقع على الوسيط الإلكتروني:

يستهدف هذا النوع من الجرائم الوسائط الإلكترونية والبنية التحتية الرقمية بشكل مباشر. يحدث عندما يقوم الجاني بالتسلل إلى الأنظمة المعلوماتية، قواعد البيانات، أو الخوادم بهدف تعطيلها أو تدميرها أو سرقة البيانات. تشمل هذه الجرائم الهجمات التي تستهدف الأنظمة التقنية مثل **هجمات الحرمان من الخدمة(DDoS)**، أو البرامج الضارة مثل الفيروسات وبرامج التجسس، التي تتسلل إلى الأنظمة لتدمير البيانات أو التلاعب بها. كما تشمل الهجمات على الشبكات الحكومية أو العسكرية بهدف تشويش أو تعطيل التواصل الحيوي[٢٣].

- **أمثلة:**
  - **هجوم:DDoS** هجوم على مواقع الحكومة أو الشركات لتعطيلها.
  - **اختراق الأنظمة الحكومية** :سرقة البيانات الحساسة أو التلاعب بأنظمة الرقابة.
  - **البرمجيات الخبيثة** :استخدام الفيروسات أو برامج التجسس لسرقة بيانات أو إلحاق ضرر بالأنظمة[٢٤].

ثانياً: ما ينتشر عبر الوسائط الإلكترونية:

يشمل هذا النوع من الجرائم الاستخدام المباشر للوسائط الإلكترونية (مثل الإنترنت ووسائل التواصل الاجتماعي) لنقل أو نشر المواد التي تهدد الأمن العام أو تعزز الفكر المتطرف. في هذا السياق، يستخدم الإرهابيون المنصات الرقمية لنشر الدعاية الإرهابية، تجنيد الأعضاء الجدد، جمع التبرعات، والترويج للأنشطة الإجرامية. يزداد خطر هذا النوع من الجرائم بسبب سهولة انتشار المعلومات على الإنترنت وسرعة الوصول إلى جمهور واسع[٢٥].

---

[٢٣] زعل بن سعيد الخريصي، "جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية في مواجهتها من منظور الأمن الوطني والقانون الدولي"، مجلة الأندلس للعلوم الإنسانية والاجتماعية، ع٧٣، ٢٠٢٣ ص ٢٠١..

[٢٤] زعل بن سعيد الخريصي، المرجع السابق، ص٢٠١.

[٢٥] حازم الجمل. مرجع سابق، ص ٣٢٥..

- **أمثلة:**

- **نشر الدعاية الإرهابية عبر الإنترنت:** تحميل فيديوهات دعائية أو منشورات على منصات مثل فيسبوك وتويتر لزيادة الدعم لمجموعات إرهابية.
- **التجنيد الإلكتروني:** استخدام الشبكة العنكبوتية لجذب الشباب والتأثير عليهم للانضمام إلى التنظيمات الإرهابية.
- **التثقيف والتدريب عن بعد:** توفير دروس عبر الإنترنت عن كيفية صناعة الأسلحة أو تنفيذ الهجمات[٢٦].

ثالثاً: ما يقع على الوسيط ثم ينتقل إلى العالم الواقعي:

تُستخدم في هذا النوع من الجرائم الوسائط الإلكترونية كأداة للتخطيط والتنفيذ والتوجيه للجرائم الإرهابية التي تحدث في العالم الواقعي. تشمل هذه الجرائم الهجمات التي يتم التنسيق لها عبر الإنترنت، مثل التخطيط لعمليات التفجير، الهجمات على البنية التحتية الحيوية، أو تنفيذ هجمات عنف جسدي. ينتقل المخططون للجريمة من الفضاء الرقمي إلى العالم المادي لتنفيذ العمليات التي تؤثر بشكل مباشر على المجتمعات[٢٧].

- **أمثلة:**

- **التخطيط لتنفيذ هجمات إرهابية:** استخدام الإنترنت لتنسيق الهجمات الإرهابية على مواقع استراتيجية مثل المنشآت الحيوية أو السفارات.
- **هجمات على البنية التحتية:** شن هجمات على الأنظمة الصناعية أو الشبكات الكهربائية بعد أن تم التخطيط لها عبر الإنترنت.
- **التخريب أو التفجيرات:** استخدام التعليمات والإرشادات عبر الإنترنت لتنفيذ عمليات إرهابية مثل التفجيرات[٢٨].

---

[٢٦] زعل بن سعيد الخريصي، مرجع سابق، ص٢٠١.

[٢٧] سحر جمال زهران، الجوانب القانونية الدولية لجريمة الإرهاب الإلكتروني، مجلة السياسة والاقتصاد، مج٥، ع٤٤، ٢٠١٩، ص ٨٣.

[٢٨] سحر جمال زهران، المرجع السابق، ص ٨٣.

(ISSN: 2537 - 0758)

الفرع الثاني
أنواع جرائم الإرهاب السيبراني

يتناول هذا الفرع أنواع جرائم الإرهاب السيبراني التي تشهد تطورًا مستمرًا بفضل التقدم التكنولوجي. يتميز هذا النوع من الجرائم بتنوع الأساليب والأدوات التي يستخدمها الإرهابيون لتحقيق أهدافهم، والتي تتراوح من الهجمات الرقمية على البنى التحتية إلى التجنيد الإلكتروني ونشر الدعاية المتطرفة. في هذا الفرع، سنستعرض أبرز الأنواع التي تتخذها هذه الجرائم، مع تسليط الضوء على الأمثلة الواقعية لكل نوع، مما يساعد في فهم الأبعاد المختلفة لهذه الجرائم وسبل مكافحتها.

أولاً: الواقع الافتراضي للتدريب الإرهابي:

مع التطور التكنولوجي، أصبح الإرهابيون يستخدمون الواقع الافتراضي كأداة لتدريب أعضائهم على تنفيذ الهجمات. ويوفر هذا النوع من التدريب بيئة محاكاة تمكن الأفراد من تعلم كيفية تنفيذ العمليات الإرهابية، مثل الهجمات على البنى التحتية أو التخطيط لعمليات التفجير، في بيئة آمنة وبأقل تكلفة. يتم ذلك باستخدام محاكاة عبر الإنترنت أو ألعاب الفيديو التي تحاكي الواقع وتعرض سيناريوهات مماثلة للهجمات الحقيقية[٢٩].

- **أمثلة:**
  - **تدريب على الهجمات الإلكترونية:** بعض الجماعات الإرهابية تستخدم محاكيات الهجوم مثل ألعاب الفيديو التي تحاكي تنفيذ الهجمات على البنية التحتية الحيوية أو الأنظمة الإلكترونية.
  - **محاكاة هجمات التخريب:** إنشاء بيئات افتراضية عبر الإنترنت يتمكن فيها الإرهابيون من **محاكاة التفجيرات** أو الهجمات على الأنظمة العسكرية[٣٠].

ثانياً: الطابعات ثلاثية الأبعاد في صناعة المتفجرات والأسلحة:

مع تقدم التكنولوجيا، أصبح الإرهابيون يستخدمون الطابعات ثلاثية الأبعاد لتصنيع الأسلحة والمتفجرات بأقل تكلفة وأسرع وقت. يُعتبر هذا النوع من الجرائم من أخطر

---

[٢٩] زعل الخريصي، مرجع سابق، ص ٢١٠.

[٣٠] زعل الخريصي، المرجع السابق، ص ٢١٠.

الأنماط، حيث يمكن تصنيع أسلحة غير قانونية أو أدوات تفجير بسهولة باستخدام هذه الطابعات[٣١].

- **أمثلة**:
  - **صناعة الأسلحة النارية:** تصنيع أجزاء من الأسلحة باستخدام الطابعات ثلاثية الأبعاد.
  - **إنتاج المواد المتفجرة:** استخدام الطابعات لتصنيع أدوات تفجير بطريقة غير قانونية[٣٢].

ثالثًا: **تنفيذ هجمات بطائرات بدون طيار**:

الطائرات بدون طيار تُعد أداة متطورة يمكن استخدامها لشن هجمات على **المنشآت الحيوية** أو أهداف أخرى في العالم الواقعي. يتضمن هذا النوع من الجرائم استخدام الطائرات غير المأهولة لتوجيه الهجمات عن بُعد، مما يقلل من الخطر على الإرهابيين أنفسهم[٣٣].

- **أمثلة**:
  - **هجمات على المنشآت النفطية:** استهداف المنشآت النفطية في السعودية باستخدام طائرات بدون طيار.
  - **هجمات على المنشآت العسكرية:** تنفيذ هجمات إرهابية على المنشآت العسكرية باستخدام الطائرات بدون طيار.

ففي ١٤ سبتمبر ٢٠١٩، تعرضت منشأتان تابعتان لشركة أرامكو السعودية في بقيق وخريص لهجمات بواسطة طائرات بدون طيار وصواريخ كروز، ما أدى إلى اندلاع حرائق وتوقف مؤقت في إنتاج النفط. أعلنت جماعة الحوثي اليمنية مسؤوليتها عن الهجمات،و تسببت الهجمات في خفض إنتاج النفط السعودي بنحو ٥.٧ مليون برميل يوميًا، ما يعادل حوالي ٥٠% من إنتاج المملكة[٣٤].

---

[٣١] سحر جمال زهران، مرجع سابق، ص ٨٨.

[٣٢] سحر جمال زهران، المرجع السابق، ص ٨٨.

[٣٣] زعل الخريصي، مرجع سابق، ص ٢٢٢.

[٣٤] وكالة الأنباء السعودية. ٢٠١٩. "وزير الطاقة: الهجوم الإرهابي على معملي بقيق وخريص أدى إلى توقف ٥.٧ مليون برميل يوميًا". وكالة الأنباء السعودية (SPA)، ١٤ سبتمبر.

(ISSN: 2537 - 0758)

رابعاً: تنفيذ هجمات بسيارات ذاتية القيادة:

السيارات ذاتية القيادة أصبحت جزءًا من التكنولوجيا المتقدمة التي يمكن استغلالها لتنفيذ الهجمات الإرهابية. يتم استخدام هذه السيارات كأدوات لتنفيذ **هجمات عن بُعد** على أهداف معينة[٣٥].

- **أمثلة:**
  - **هجمات باستخدام السيارات الذاتية القيادة:** تنفيذ الهجمات الانتحارية باستخدام السيارات التي يتم التحكم فيها عن بُعد.
  - **التحكم عن بُعد في السيارات الهجومية:** استهداف مواقع معينة باستخدام السيارات الذاتية القيادة لتفجيرها عند الهدف[٣٦].

خامساً: تحليل بيانات لتحديد الأهداف الإرهابية:

يتم استخدام تحليل البيانات واستخدام تقنيات الذكاء الاصطناعي لتحديد الأهداف المحتملة للعمليات الإرهابية. يشمل ذلك تحليل البيانات التي يتم جمعها عبر الإنترنت أو عبر شبكات التواصل الاجتماعي لتحديد المواقع أو الأفراد المستهدفين[٣٧].

- **أمثلة:**
  - **تحليل البيانات الاجتماعية:** استخدام تحليل البيانات عبر فيسبوك وتويتر لتحديد المواقع التي يمكن أن تكون أهدافًا للهجمات.
  - **تحليل البيانات الحكومية:** استخدام تحليل البيانات المتقدم لاختراق المعلومات الحكومية وتحديد الأهداف الحيوية[٣٨].

سادساً: التهديد السيبراني من خلال طلب الفدية:

في هذا النوع من الجرائم، يقوم المهاجمون باستخدام برمجيات الفدية لتهديد الأفراد أو المؤسسات عبر الإنترنت. يتمكن المهاجمون من تشفير البيانات الحساسة أو تعطيل الأنظمة الحيوية، ثم يطلبون دفع فدية مقابل إعادة فك التشفير أو استعادة البيانات[٣٩].

تم الاسترجاع في [١٢/٩/١٤٤٦هـ الساعة ٩ مساءاً] من https://www.spa.gov.sa/1969112.

[٣٥] زعل الخريصي، مرجع سابق، ص ٢٢٦.

[٣٦] زعل الخريصي، المرجع السابق، ص ٢٢٦.

[٣٧] حازم الجمل، مرجع سابق، ص ٣٢٨.

[٣٨] حازم الجمل، المرجع السابق، ص ٣٢٨.

- **أمثلة**:

- **هجمات الفدية على المستشفيات:** استخدام برمجيات الفدية لتعطيل أنظمة المستشفيات وطلب دفع فدية لاستعادة البيانات.
- **اختراق شبكات الشركات:** سرقة البيانات أو تعطيل الأنظمة في الشركات الكبيرة وطلب فدية مقابل إعادة النظام[٤٠].

سابعاً: **التجنيد والتمويل عبر الإنترنت**:

يعد الإنترنت أداة قوية بالنسبة للجماعات الإرهابية لجذب الأفراد من مختلف أنحاء العالم، وخاصةً من خلال منصات التواصل الاجتماعي، المنتديات، والمواقع الإلكترونية الخاصة بالتنظيمات. يتم استغلال هذه الوسائط في تجنيد الأعضاء الجدد، وجمع التمويلات لتدعيم أنشطتهم الإجرامية. بالإضافة إلى ذلك، يمكن استغلال الإنترنت لتنظيم حملات ترويجية هدفها نشر الفكر المتطرف[٤١].

- **أمثلة**:

- **التجنيد عبر الإنترنت:** تنظيم حملات على الإنترنت لجذب أفراد إلى التنظيمات الإرهابية.
- **جمع التبرعات:** استخدم بعض الجماعات الإرهابية منصات مثل باي بال و كريبتو لجمع الأموال لتمويل الأنشطة الإرهابية[٤٢].

ثامناً: **الهجمات على البنية التحتية الرقمية**:

هذا النوع من الجرائم يشمل الهجمات التي تستهدف **البنية التحتية الرقمية** مثل الشبكات الكهربائية، أنظمة المياه، أو أنظمة الاتصالات. يتم استخدام الإنترنت كأداة لتنفيذ هجمات إلكترونية تؤدي إلى تعطيل الخدمات الأساسية للمجتمعات. يتم ذلك عبر اختراق الأنظمة أو نشر الفيروسات التي تدمر أو تعطل نظم التحكم في البنية التحتية[٤٣].

---

[٣٩] حازم الجمل، مرجع سابق، ص ٣٢٨.

[٤٠] حازم الجمل، المرجع السابق، ص ٣٢٨.

[٤١] حازم الجمل، مرجع سابق، ص ٣٣٣.

[٤٢] حازم حسن الجمل، المرجع السابق، ص ٣٣٣.

[٤٣] سحر جمال زهران، مرجع سابق، ص ٧٥.

(ISSN: 2537 - 0758)

- **أمثلة**:

- **هجوم Stuxnet:** الذي استهدف **البرنامج النووي الإيراني** عن طريق نشر فيروسات تسببت في تدمير أجهزة الطرد المركزي.
- **هجوم على شبكات الكهرباء:** استخدام برامج خبيثة لتعطيل خدمات الكهرباء في دولة معينة[٤٤].

تاسعًا: **نشر الدعاية الإرهابية والتحريض على العنف**:

يتمثل هذا النوع من الجرائم في استخدام الإنترنت والمنصات الرقمية لنشر **الدعاية الإرهابية** وتجنيد الأفراد، فضلاً عن **التحريض على العنف** من خلال نشر أفكار متطرفة أو تعليمات للقيام بالهجمات. يُستخدم الإنترنت كمنصة لنشر مقاطع فيديو، منشورات، أو مقاطع صوتية تحرض على الإرهاب[٤٥].

- **أمثلة**:

- **الدعاية عبر منصات الفيديو:** مثل نشر فيديوهات دعائية على **يوتيوب** و **تويتر** لزيادة التأثير على المتطرفين.
- **التحريض على العنف:** نشر مقاطع تحتوي على تعليمات حول كيفية تصنيع الأسلحة أو تنفيذ الهجمات[٤٦].

عاشراً: **الهجمات الإلكترونية على المؤسسات الحكومية والخاصة**:

هذا النوع من الجرائم يشمل الهجمات التي تستهدف المؤسسات الحكومية أو الشركات الكبرى بهدف سرقة المعلومات الحساسة، التخريب، أو حتى الابتزاز. يمكن استخدام الإنترنت لاختراق الشبكات الخاصة بالمؤسسات، مما يؤدي إلى تسريب المعلومات أو تعطيل العمليات بشكل تام[٤٧].

- **أمثلة**:

- **اختراق شبكات الشركات:** مثل سرقة بيانات العملاء أو المعاملات التجارية لشركات كبيرة عبر الإنترنت.

---

[٤٤] سحر جمال زهران، المرجع السابق، ص ٧٥.

[٤٥] زعل الخريصي، مرجع سابق، ص ٢٣١.

[٤٦] زعل الخريصي، المرجع السابق، ص ٢٣١.

[٤٧] حازم حسن الجمل، مرجع سابق، ص ٣٣٤.

- **الهجوم على الدوائر الحكومية:** مثل تعطيل أنظمة الحكم أو نشر وثائق سرية تضر بالسمعة الأمنية لدولة ما.

وفي الفترة الانتقالية بين نهاية ولاية الرئيس دونالد ترامب وبداية ولاية الرئيس جو بايدن، تعرضت الولايات المتحدة لعدد من الاختراقات السيبرانية البارزة التي أثرت على مؤسسات حكومية وشركات خاصة. **وأهمها ما يلي**[٤٨]:

اختراق SolarWinds (٢٠٢٠): في ديسمبر ٢٠٢٠، تم الكشف عن اختراق واسع النطاق استهدف أنظمة شركة SolarWinds، المزود الرئيسي لبرامج إدارة الشبكات. استغل المهاجمون تحديثًا ضارًا لبرنامج Orion التابع للشركة لاختراق حوالي ١٨,٠٠٠ عميل، بما في ذلك وكالات حكومية أمريكية مثل وزارات الخزانة والتجارة والأمن الداخلي. نُسب هذا الهجوم إلى مجموعة قرصنة مدعومة من الحكومة الروسية.

وفي ختام هذا المطلب، تبين أن جرائم الإرهاب السيبراني تشكل تهديدًا متزايدًا للأمن الوطني والدولي، حيث تتنوع أساليب تنفيذ هذه الجرائم بشكل معقد وتعتمد على تقنيات وأدوات متعددة. لقد استعرضنا الأنماط المختلفة لهذه الجرائم من خلال تقسيمها إلى فئات وفقًا للوسائط الرقمية المستهدفة، مما يسهل فهم طرق الهجوم والاستراتيجيات المتبعة. كما تم توضيح تأثير هذه الجرائم على الأفراد، المؤسسات، والدول، مما يعكس مدى أهمية تبني استراتيجيات فعّالة لمكافحة هذه التهديدات في ظل التقدم التكنولوجي المستمر.

المطلب الثاني

السياسات السعودية في مكافحة جريمة الإرهاب السيبراني ومواجهتها

تمهيد وتقسيم:

يمثّل الإرهاب السيبراني أحد أبرز التحديات التي استدعت من المملكة العربية السعودية بناء منظومة سياسات وطنية متكاملة، تتجاوز المعالجة التشريعية، لتشمل الأبعاد الأمنية، والتقنية، والاستراتيجية، إدراكًا منها لخطورة هذا النمط من التهديدات

---

[٤٨] ويكيبيديا. (2020). 2020 United States federal government data breach. تم الاسترجاع في (١٤٤٦/٩/١٢هـ الساعة ٩ مساءً] من https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

(ISSN: 2537 - 0758)

على أمن الدولة ومؤسساتها الحيوية. وقد برز هذا التوجّه من خلال إصدار عدد من الاستراتيجيات الوطنية والسياسات الحكومية التي تهدف إلى الوقاية من الإرهاب السيبراني، وتجفيف منابعه، وتعزيز الردع القانوني والتقني حياله. ويأتي ذلك ضمن رؤية شاملة تندرج في إطار أهداف رؤية المملكة ٢٠٣٠، التي أولت الأمن السيبراني أهمية قصوى بوصفه ركيزة من ركائز الأمن الوطني.

وتنبثق أهمية هذا المطلب من الحاجة إلى تحليل السياسات السعودية القائمة، سواء على مستوى الاستراتيجيات الحكومية أو من منظور الأمن الوطني، وبيان مدى تكاملها مع الجهود النظامية والمؤسسية الأخرى في مكافحة هذه الجريمة. **ويمكن تقسيم هذا المطلب إلى الفرعين التاليين:**

الفرع الأول: السياسات الحكومية السعودية في مجال مكافحة الإرهاب السيبراني.

الفرع الثاني: مواجهة الإرهاب السيبراني من منظور الأمن الوطني السعودي.

الفرع الأول

السياسات الحكومية السعودية في مجال مكافحة الإرهاب السيبراني.

في ظل النمو المتسارع للتهديدات السيبرانية وتطور أساليب الإرهاب الرقمي، وضعت المملكة العربية السعودية سياسات استراتيجية متكاملة بهدف مواجهة هذه الظاهرة الخطيرة التي تهدد أمنها الوطني والاقتصادي والاجتماعي. وقد شملت تلك السياسات تأسيس هيئات وطنية متخصصة، وإصدار تشريعات دقيقة، وإطلاق استراتيجيات وطنية فعالة لتعزيز الأمن السيبراني. وقد انعكست هذه الجهود في عدة مبادرات تنظيمية وتشريعية، عززت قدرة المملكة على التصدي لهذه التحديات السيبرانية الجديدة، **وذلك على النحو التالي:**

حيث يتناول هذا الفرع الأول أبرز السياسات الحكومية السعودية في مكافحة الإرهاب السيبراني، ويُقسَّم إلى عدة عناصر، هي:

أولًا: تأسيس الهيئة الوطنية للأمن السيبراني:

أولت المملكة العربية السعودية أهمية قصوى لمواجهة التهديدات الإلكترونية والسيبرانية، ما دفعها إلى تأسيس الهيئة الوطنية للأمن السيبراني بموجب الأمر الملكي

رقم (٦٨٠١) بتاريخ ١١ صفر ١٤٣٩هـ الموافق ٣١ أكتوبر ٢٠١٧م[٤٩]. وترتبط الهيئة مباشرة بخادم الحرمين الشريفين، تأكيدًا على أهميتها ومكانتها في سلم الأولويات الوطنية. وتتمثل مهمة الهيئة في حماية الفضاء السيبراني الوطني من التهديدات الداخلية والخارجية، عبر تنسيق الجهود الوطنية وتطوير السياسات والمعايير الخاصة بأمن المعلومات والشبكات، وتقديم الدعم والمساندة للجهات الحكومية والخاصة لرفع مستوى الحماية ضد الهجمات الإرهابية السيبرانية المحتملة.

كذلك تعمل الهيئة على وضع معايير أمنية دقيقة يجب الالتزام بها من قِبل جميع المؤسسات العاملة في المملكة، وتحديد المخاطر السيبرانية وتصنيفها، والتأكد من جاهزية الجهات الحكومية والخاصة لمواجهتها. كما تُشرف على البرامج التدريبية والتوعوية اللازمة لرفع مستوى الوعي حول خطورة التهديدات السيبرانية[٥٠].

ثانياً: إطلاق الاستراتيجية الوطنية للأمن السيبراني:

كما عززت المملكة قدراتها في مجال الأمن السيبراني من خلال إطلاق الاستراتيجية الوطنية للأمن السيبراني بقرار مجلس الوزراء رقم (٥٧٢) بتاريخ ١٢ شوال ١٤٣٩هـ. وتهدف الاستراتيجية إلى توفير بيئة سيبرانية آمنة وموثوقة، وتطوير القدرات الوطنية اللازمة لمواجهة التهديدات السيبرانية والإرهابية، وضمان حماية المصالح الحيوية للدولة، وذلك من خلال بناء قدرات وطنية احترافية في مجال الأمن السيبراني، وتوفير بنية تحتية رقمية آمنة تدعم التحول الرقمي في المملكة[٥١].

بالإضافة إلى ذلك، تضمنت الاستراتيجية محاور رئيسية، منها تعزيز التعاون الدولي في مجال الأمن السيبراني، وبناء الشراكات بين القطاعين العام والخاص، وتطوير

---

[٤٩] الأمر الملكي رقم (٦٨٠١)، بتاريخ ١١ صفر ١٤٣٩هـ، الرياض، هيئة الخبراء بمجلس الوزراء، ١٤٣٩هـ، ص ٣.

[٥٠] الهيئة الوطنية للأمن السيبراني، وثيقة ضوابط الأمن السيبراني الأساسية، الرياض، الهيئة الوطنية للأمن السيبراني، ١٤٤٠هـ، ص ١٢.

[٥١] الاستراتيجية الوطنية للأمن السيبراني، قرار مجلس الوزراء رقم (٥٧٢)، بتاريخ ١٢ شوال ١٤٣٩هـ، الرياض، هيئة الخبراء بمجلس الوزراء، ١٤٣٩هـ.

(ISSN: 2537 - 0758)

الأطر التنظيمية والقانونية لضمان الاستجابة السريعة والفعالة ضد التهديدات الإرهابية عبر الفضاء الرقمي[٥٢].

ثالثاً: إصدار أنظمة وتشريعات متخصصة:

كذلك استكملت المملكة إطارها التنظيمي لمكافحة الإرهاب السيبراني من خلال إصدار عدد من الأنظمة والتشريعات المهمة والمتخصصة. يأتي في مقدمتها نظام مكافحة الجرائم المعلوماتية، الصادر بالمرسوم الملكي رقم (م/١٧) بتاريخ ١٤٢٨/٣/٨هـ، والذي يعد الركيزة الأساسية لمواجهة الجرائم الإلكترونية المرتبطة بالإرهاب السيبراني. إذ يُحدد النظام بوضوح الجرائم المعلوماتية ويُرتب لها عقوبات صارمة تشمل السجن والغرامة، كما يُنظّم إجراءات التحقيق والمحاكمة لتلك الجرائم[٥٣].

من جهة أخرى، صدر نظام مكافحة الإرهاب وتمويله بموجب المرسوم الملكي رقم (م/٢١) بتاريخ ١٤٣٩/٢/١٢هـ، والذي يُعد مكملًا لنظام مكافحة الجرائم المعلوماتية، إذ يحتوي على نصوص خاصة تعالج استخدام التقنيات الحديثة في الأعمال الإرهابية وتمويلها عبر المنصات الرقمية والإلكترونية[٥٤].

بالإضافة لما سبق، فقد عززت هذه الأنظمة من قدرة الجهات المختصة على اتخاذ التدابير اللازمة، من خلال تعريف واضح للإجراءات والعقوبات، مما يُسهم بشكل كبير في تحقيق الردع العام والخاص ضد مرتكبي الجرائم الإرهابية السيبرانية[٥٥].

---

[٥٢] الاستراتيجية الوطنية للأمن السيبراني، مرجع سابق، ص ١١.

[٥٣] نظام مكافحة الجرائم المعلوماتية، الصادر بالمرسوم الملكي رقم (م/١٧)، بتاريخ ١٤٢٨/٣/٨هـ، قرار مجلس الوزراء رقم ٧٩ بتاريخ ١٤٢٨/٣/٧هـ، المنشور بجريدة أم القرى، السنة ٨٣، العدد ٤١٤٤، بتاريخ ٢٥ ربيع الأول ١٤٢٨هـ، الموافق ١٣ إبريل ٢٠٠٧م.

[٥٤] نظام مكافحة الإرهاب وتمويله، الصادر بالمرسوم الملكي رقم (م/٢١)، بتاريخ ١٤٣٩/٢/١٢هـ، قرار مجلس الوزراء رقم ٩٢ بتاريخ ١٤٣٩/٢/١١هـ، المنشور بجريدة أم القرى، العدد ٤٦٩٥ بتاريخ ٢١ صفر ١٤٣٩هـ، الموافق ١٠ نوفمبر ٢٠١٧م، ص ٣-٥.

[٥٥] سعد بن حمد القحطاني، السياسة الجنائية السعودية في مكافحة جرائم تقنية المعلومات، رسالة دكتوراه، قسم العدالة الجنائية، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٢٠، ص ١٠٣-١٠٤.

ومما سبق يرى الباحث أن السياسات السعودية في مجال مكافحة الإرهاب السيبراني جاءت شاملة ومنسقة، تعكس استجابة واعية من قِبل الدولة لمواجهة المخاطر الرقمية المعاصرة. وعلى الرغم من ذلك، فإن الاستمرار في تطوير وتحديث هذه السياسات يظل أمرًا بالغ الأهمية، في ظل التحديات المتجددة والتطور المستمر لأساليب الإرهاب السيبراني.

رابعاً: تأسيس المركز الوطني الإرشادي للأمن السيبراني:

كما حرصت المملكة على استكمال منظومتها المتخصصة في مجال مكافحة الإرهاب السيبراني بإنشاء المركز الوطني الإرشادي للأمن السيبراني، والذي يعد إحدى المبادرات الهامة التي أطلقتها الهيئة الوطنية للأمن السيبراني في عام ٢٠١٩. ويهدف المركز إلى توفير الإرشادات الأمنية المتخصصة التي تُساعد مختلف القطاعات الحكومية والخاصة في تعزيز قدراتها على مواجهة التهديدات والهجمات السيبرانية المحتملة، كما يُقدم المركز تنبيهات أمنية دورية حول الثغرات والمخاطر الجديدة في مجال الأمن الرقمي[٥٦].

كذلك يقوم المركز بتطوير برامج توعية وتثقيف لرفع مستوى الوعي العام تجاه مخاطر الإرهاب السيبراني، والتعريف بأفضل الممارسات العالمية في مجال الحماية الإلكترونية، ما أسهم في تعزيز البنية التحتية الرقمية بالمملكة.

ومما سبق يمكن للباحث القول إن هذا المركز يمثل ذراعًا فنية تنفيذية توفر المعلومات الفورية والتوجيهات الاحترافية لمواجهة التهديدات السيبرانية بفاعلية.

خامساً: دور السياسات الحكومية في تسريع التحقيقات الجنائية الرقمية:

من خلال اعتماد سياسات وطنية موحدة للأمن السيبراني، أصبح بالإمكان توحيد إجراءات التحقيقات الرقمية، خاصة فيما يتعلق بجمع الأدلة وتنسيق البلاغات وتبادل البيانات بين الجهات المختصة. وقد ساهم هذا التنظيم في تسريع الوصول إلى مصادر الجريمة، وتقليل الوقت المستغرق بين حدوث الواقعة وبدء التحقيق الرسمي، ما يعزز فعالية إنفاذ القانون في الجرائم السيبرانية[٥٧].

---

[٥٦] الهيئة الوطنية للأمن السيبراني، تقرير المركز الوطني الإرشادي للأمن السيبراني، الرياض، ٢٠٢٠، ص ١٥.

[٥٧] أماني بهجت، أمن المعلومات، المركز الإقليمي للدراسات، القاهرة، ٢٠١٥م، ص ٣٦.

(ISSN: 2537 - 0758)

ومما سبق يمكن للباحث القول إن السياسات الحكومية لا تقتصر على الأطر الوقائية فقط، بل تُعد أيضًا محفزًا رئيسًا لتسريع أدوات التحقيق الرقمي وتسهيل المهام الجنائية للضبط والاستدلال.

سادساً: تعزيز التعاون الدولي والإقليمي في مكافحة الإرهاب السيبراني

في ذات الإطار، تضع المملكة العربية السعودية التعاون الدولي والإقليمي ضمن أهم أولوياتها في السياسات الحكومية لمكافحة الإرهاب السيبراني. إذ تشارك المملكة بشكلٍ فاعل في المؤتمرات الدولية والإقليمية ذات الصلة بالأمن السيبراني، مثل مؤتمر الأمن السيبراني العالمي الذي تستضيفه المملكة دوريًا بهدف تعزيز الشراكات الاستراتيجية مع الدول والمنظمات الدولية وتبادل المعلومات والخبرات حول التهديدات السيبرانية[٥٨].

كذلك بادرت المملكة بتوقيع اتفاقيات تعاون مع دول مثل الولايات المتحدة الأمريكية والمملكة المتحدة ودول الخليج لتعزيز تبادل الخبرات الفنية والقانونية وتطوير قدراتها في مجال الأمن السيبراني، ما عزز مكانتها كطرف فاعل ومؤثر في الجهود الدولية لمواجهة التهديدات الإرهابية السيبرانية[٥٩].

ومما سبق يمكن للباحث القول إن المملكة تبنت نهجًا دبلوماسيًا وأمنيًا مزدوجًا في مكافحة الإرهاب السيبراني، يجمع بين التحديث الداخلي والتعاون الخارجي المتعدد المستويات.

سابعا: برامج التوعية والتدريب المتخصصة في مجال الأمن السيبراني:

إلى جانب ذلك، خصصت المملكة مجموعة واسعة من البرامج التدريبية والتوعوية المتخصصة في مجال الأمن السيبراني، تُنفذها الجهات الحكومية المختصة بالتعاون مع الجامعات والمراكز التدريبية. ومن أبرز هذه البرامج مبادرة «البرنامج الوطني للتوعية بالأمن السيبراني» الذي أطلقته الهيئة الوطنية للأمن السيبراني بهدف تثقيف المجتمع

---

[٥٨] وزارة الخارجية السعودية، تقرير المملكة حول التعاون الدولي في مجال الأمن السيبراني، الرياض، ٢٠٢١، ص ٨–٩.

[٥٩] وزارة الخارجية السعودية، مرجع سابق، ص ١٢.

السعودي بكافة فئاته حول مخاطر التهديدات السيبرانية، ورفع مستوى الوعي حول سبل الوقاية منها والتعامل معها[٦٠].

كما نظّمت المملكة ورش عمل وبرامج تدريبية مكثفة للعاملين في القطاعات الحكومية والحيوية لتعزيز قدراتهم الفنية في مجال مواجهة الهجمات السيبرانية، والتعامل مع حالات الطوارئ الإلكترونية[٦١].

وفي ضوء ذلك يرى الباحث إن إشراك القطاع الخاص في منظومة الأمن السيبراني يمثل خطوة متقدمة نحو تحقيق شمولية الحماية الرقمية، وزيادة فعالية التدابير المتخذة.

ثامناً: تعزيز الشراكة بين القطاعين العام والخاص

وأخيرًا، ركزت السياسات السعودية على أهمية بناء شراكات استراتيجية بين القطاعين العام والخاص لمواجهة التحديات السيبرانية المعاصرة. وتجلّى ذلك من خلال إطلاق «المركز الوطني للأمن السيبراني» بالتعاون مع القطاع الخاص، والذي يهدف إلى تسريع استجابة الجهات المختلفة للتهديدات السيبرانية، وتطوير الحلول التقنية والفنية التي تعزز من مستوى الأمن الإلكتروني في المملكة[٦٢].

كما وفّرت هذه الشراكة أرضية خصبة لتبادل الخبرات، وتعزيز الابتكار في مجال الأمن السيبراني، ما نتج عنه تطوير حلول تقنية متقدمة قادرة على التعامل مع أحدث أساليب الهجمات السيبرانية التي قد تستهدف البنية التحتية الحيوية للدولة[٦٣].

ومما سبق يرى الباحث أن السياسات الحكومية السعودية في مجال مكافحة الإرهاب السيبراني تميزت بالشمولية والتنوع، وتعزيز التعاون بين القطاعات المختلفة. ورغم ما حققته هذه السياسات من نجاحات، فإن استمرارية تحديثها وتطويرها تظل ضرورية، لمواكبة التحديات التقنية المتجددة والأساليب المبتكرة للهجمات السيبرانية.

---

[٦٠] الهيئة الوطنية للأمن السيبراني، تقرير البرنامج الوطني للتوعية بالأمن السيبراني، الرياض، الهيئة الوطنية للأمن السيبراني، ٢٠٢٢، ص ١٣.

[٦١] جامعة الملك سعود، التقرير السنوي لوحدة الأمن السيبراني، الرياض، جامعة الملك سعود، ٢٠٢١، ص ٢٥-٢٧.

[٦٢] الهيئة الوطنية للأمن السيبراني، وثيقة شراكة القطاعين العام والخاص في الأمن السيبراني، الرياض، الهيئة الوطنية للأمن السيبراني، ٢٠٢٢، ص ٩.

[٦٣] الهيئة الوطنية للأمن السيبراني، مرجع سابق، ص ١٣.

(ISSN: 2537 - 0758)

تاسعًا: الجهود المؤسسية ودور الدولة في حماية المجني عليه من الإرهاب السيبراني:

أولت المملكة العربية السعودية اهتمامًا متزايدًا لحماية الأفراد من الجرائم السيبرانية ذات الطابع الإرهابي، من خلال منظومة مؤسسية متكاملة تشمل الجوانب القانونية والتقنية والتنظيمية.

وقد تجلّى هذا الدور في سنّ الأنظمة المتخصصة مثل نظام مكافحة الجرائم المعلوماتية، الذي تضمن نصوصًا تُجرّم أفعال الإرهاب السيبراني وتحمي ضحاياه.

كما ساهمت الهيئة الوطنية للأمن السيبراني في إنشاء أطر تقنية للإنذار المبكر والاستجابة للحوادث السيبرانية، إلى جانب تقديم الدعم الفني للجهات الحكومية والخاصة(٦٤).

وتتولى رئاسة أمن الدولة متابعة التهديدات التي تستهدف الأمن الوطني عبر الوسائط الإلكترونية، والتنسيق مع الجهات القضائية لملاحقة مرتكبيها. كما تعمل وزارة الداخلية والنيابة العامة على استقبال بلاغات المجني عليهم ومباشرة إجراءات التحقيق والحماية(٦٥).

وتُعد هذه المنظومة المؤسسية بمثابة خط الدفاع الأول في التصدي لهذه الجرائم، لا سيما في ظل التزايد المستمر للهجمات السيبرانية التي تستهدف الأفراد والكيانات الحيوية في المملكة(٦٦).

ومما سبق، يرى الباحث أن المملكة تتبنى نموذجًا مؤسسيًا متقدّمًا لحماية المجني عليه من الإرهاب السيبراني، إلا أن فاعلية هذه الجهود ترتبط بمدى تكامل الأدوار وتحديث الإجراءات واستمرارية الدعم القانوني والتقني المخصص للفئات المستهدفة.

الفرع الثاني

مواجهة الإرهاب السيبراني من منظور الأمن الوطني السعودي

يمثل الأمن الوطني إطار الحماية الشاملة لمقدرات الدولة وسيادتها واستقرارها الداخلي والخارجي، وقد توسع هذا المفهوم في العصر الرقمي ليشمل البُعد السيبراني

---

(٦٤) الهيئة الوطنية للأمن السيبراني، "الاستراتيجية الوطنية للأمن السيبراني"، الرياض، ٢٠٢٠، ص١٩.

(٦٥) وزارة الداخلية، "تقرير الحماية من الجرائم المعلوماتية"، الرياض، ٢٠٢٢، ص١٤.

(٦٦) رئاسة أمن الدولة، "الأمن السيبراني ومكافحة الإرهاب"، الرياض، ٢٠٢١، ص٣٣.

بوصفه أحد أبرز ميادين الصراع العالمي. فالإرهاب السيبراني لم يعد مجرد تهديد إلكتروني محدود الأثر، بل أصبح وسيلة لهدم الثقة في المؤسسات، والتأثير على القرار السيادي، وتعطيل البنى التحتية الحيوية. وفي هذا السياق، تدرك المملكة العربية السعودية أن حماية الأمن الوطني لم تعد ممكنة دون تأمين الفضاء السيبراني، خاصةً مع استهداف المنشآت الحيوية، والمراكز الاقتصادية، والجهات الأمنية بمنظومات هجمات تقنية متطورة.

وتبعًا لذلك، بات من الضروري تحليل طبيعة التحديات التي تواجه الأمن الوطني في المملكة ضمن هذا النطاق، وتقييم مدى كفاءة الآليات الأمنية المتبعة لمكافحة الإرهاب السيبراني، بما يحقق الوقاية والتصدي على حد سواء. **وسوف أوضح ذلك من خلال المحورين التاليين:**

أولاً: تحليل التحديات التي تواجه الأمن الوطني السعودي:

تمثل التحديات المرتبطة بالأمن السيبراني هاجسًا كبيرًا للأمن الوطني السعودي، فهي تشمل مجموعة من المخاطر التي تفرض على المملكة تطوير حلول شاملة ومستدامة. ويتطلب هذا الأمر تحليلًا دقيقًا لهذه التحديات بهدف تحديد الآليات المناسبة للتصدي لها، **وذلك على النحو التالي:**

(١) ضعف التنسيق بين الجهات العدلية والجهات الفنية المختصة

يُعد التنسيق بين جهات إنفاذ القانون (كالنيابة العامة، والشرطة، والمحاكم) وبين الجهات الفنية (مثل الهيئة الوطنية للأمن السيبراني، ووزارة الاتصالات) أمرًا بالغ الأهمية لضمان التعامل الفوري والفعّال مع الجرائم السيبرانية ذات الطابع الإرهابي. لكن في الواقع، لا تزال هناك بعض التحديات التي تعيق تدفق المعلومات والبيانات بين هذه الجهات، كاختلاف أنظمة العمل، أو بطء الإجراءات، أو ضعف التكامل الرقمي، مما يؤدي إلى تأخير الاستجابة وعرقلة سير العدالة[٦٧].

ومما سبق يمكن للباحث القول إن تطوير قنوات الاتصال القضائي والفني، وتوحيد منصات البلاغات، يُمثل ضرورة لتعزيز فعالية المواجهة الجنائية للإرهاب السيبراني.

---

[٦٧] مها حمد القريني، واقع الجرائم المعلوماتية في المملكة العربية السعودية، الدار العالمية لتقنية المعلوماتية، القاهرة، ٢٠٢١، ص٥٦.

(ISSN: 2537 - 0758)

(٢) صعوبة جمع الأدلة الرقمية وإثباتها قضائيًا:

تُواجه أجهزة إنفاذ القانون في المملكة تحديًا جوهريًا يتمثل في كيفية جمع الأدلة الرقمية الناتجة عن الجرائم السيبرانية، وحفظها، وتحليلها، وتقديمها للمحكمة ضمن معايير الإثبات المقبولة. فبعض هذه الأدلة يكون زائلًا أو عابرًا، وبعضها الآخر يتطلب تقنيات متقدمة لتحليله، ما قد يؤدي إلى ضياع الأثر الرقمي أو عدم قبول الدليل أمام المحكمة بسبب خلل إجرائي في جمعه(٦٨).

ومما سبق يمكن للباحث القول إن تطوير قدرات الضبط الجنائي الرقمي، وتأهيل المحققين والقضاة لفهم طبيعة الأدلة السيبرانية، يُعد شرطًا أساسيًا لتحقيق عدالة جنائية فعّالة في هذا النوع من القضايا.

(٣) زيادة التعقيد والتطور في التهديدات السيبرانية:

تعتبر التقنيات المتطورة أحد أبرز التحديات التي تواجه الأمن الوطني السعودي، إذ يتم استخدام تقنيات الذكاء الاصطناعي والبرمجيات الخبيثة بشكل متزايد في الهجمات السيبرانية، مما يزيد من صعوبة كشف هذه التهديدات والتصدي لها(٦٩).

(٤) نقص الوعي الأمني المجتمعي:

يمثل انخفاض الوعي المجتمعي تحديًا مهمًا، إذ يستغل المهاجمون هذه الثغرة لتنفيذ هجمات ناجحة. لذلك، أطلقت الجهات السعودية حملات توعية مكثفة لتعزيز الوعي بالأمن السيبراني ومخاطر الهجمات الإلكترونية(٧٠).

(٥) التحديات المرتبطة بالبنية التحتية:

تمثل البنية التحتية الرقمية أحد المجالات التي يمكن أن تتعرض لأضرار جسيمة جراء الهجمات السيبرانية، لذا فقد ركزت الجهود السعودية على حماية هذه البنية من خلال تعزيز أنظمة الحماية والإنذار المبكر(٧١).

---

(٦٨) محمد المنشاوي وآخرون، الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية، دار جامعة نايف للنشر، الرياض، ٢٠٢٤م، ص ١.

(٦٩) مركز الجرائم السيبرانية والأدلة الرقمية، الملتقى الأول لاستخدامات الذكاء الاصطناعي في المجالات الأمنية: تقرير الملتقى، دار جامعة نايف للنشر، الرياض، ٢٠٢٣، ص ١٣.

(٧٠) هيئة الاتصالات والفضاء والتقنية، التقرير السنوي، الرياض، ٢٠٢٢، ص ١١٦.

(٦) المخاطر القانونية والتنظيمية:

تشمل التحديات القانونية والتنظيمية التعامل مع الثغرات في الأنظمة والتشريعات التي قد يستغلها المهاجمون لتنفيذ جرائمهم، وتعمل المملكة باستمرار على تحديث التشريعات وتوحيد معايير الأمن السيبراني[٧٢].

(٧) الهجمات المتكررة على القطاعات الحساسة:

تعتبر القطاعات الحيوية مثل الاتصالات والطاقة من أبرز أهداف الهجمات السيبرانية، ولذلك نفذت المملكة استراتيجيات مكثفة للحد من تأثير هذه الهجمات، من خلال تطوير قدرات المراقبة والاستجابة الفورية[٧٣].

ومما سبق يرى الباحث إن التعامل مع هذه التحديات يتطلب تطوير استراتيجية شاملة تدمج بين الجوانب التقنية والبشرية والتنظيمية لضمان فعالية الاستجابة.

(٨) التحديات المرتبطة بالعناصر البشرية داخل المؤسسات:

لا تزال الأخطاء البشرية، سواء عن قصد أو غير قصد، تمثل نقطة ضعف في منظومة الأمن السيبراني، إذ يمكن لموظف بسيط فتح رابط خبيث يؤدي إلى تسريب ضخم للبيانات أو شلل في النظام. وتزداد الخطورة عند وجود موظفين غير مدربين على سياسات الأمن الرقمي. وقد كشفت تقارير الهيئة الوطنية للأمن السيبراني أن نسبة عالية من الحوادث تعود إلى سلوكيات بشرية خاطئة، مما يستدعي إنشاء وحدات داخلية في كل مؤسسة لمراقبة الامتثال السيبراني[٧٤].

ومما سبق يمكن للباحث القول إن العنصر البشري يشكل التحدي الصامت في المنظومة السيبرانية، مما يستلزم تحويله من ثغرة إلى خط دفاع من خلال التثقيف والانضباط والرقابة المؤسسية.

---

[٧١] ميليسيا هاشاواي، فهد السويلم، المملكة العربية السعودية "لمحة عن الجاهزية السيبرانية"،معهد بوتوماك للدراسات السياسية،فرجينيا، ٢٠١٧، ص ١٣.

[٧٢] مها حمد القريني، مرجع سابق، ص ٥٨.

[٧٣] هيئة الاتصالات والفضاء والتقنية، مرجع سابق، ص ١١٤.

[٧٤] عبد العزيز بن غرم الله، جرائم الانترنت وعقوباته وفق نظام مكافحة الجرائم المعلوماتية السعودي، دار الكتاب الجامعي للنشر والتوزيع، الرياض، ١٤٣٨، ص ٧٥.

(ISSN: 2537 - 0758)

ثانياً: الآليات الأمنية المتبعة لمكافحة الإرهاب السيبراني:

تقوم المنظومة الأمنية في المملكة العربية السعودية على جملة من الآليات المتكاملة لمواجهة الإرهاب السيبراني، بهدف تحقيق استجابة فعّالة ضد التهديدات الإلكترونية المتزايدة، وحماية البنية التحتية الحيوية، وضمان الأمن الوطني. وتمتد هذه الآليات بين ما هو تنظيمي، وما هو تقني، وما يرتبط بالتنسيق والجاهزية الأمنية، **وسوف أوضح ذلك على النحو التالي:**

(١) تطوير منظومات الأمن السيبراني الوطنية:

حرصت المملكة على بناء مراكز عمليات سيبرانية وطنية ترتبط بشكل مباشر بالجهات الحكومية والأمنية، لتكون نقطة الإنذار الأولى عند وقوع أو محاولة تنفيذ هجوم سيبراني. ومن أبرز هذه المنظومات: مركز الأمن السيبراني الوطني، ومركز الاستجابة للطوارئ الرقمية، والتي تعمل على التحليل الفوري للتهديدات، وتصنيفها، وإصدار تقارير استباقية للجهات ذات الصلة[٧٥].

ومما سبق يمكن للباحث القول إن هذه المنظومات تُعد الأساس الفني الذي ترتكز عليه عملية كشف الهجمات الإلكترونية قبل وقوعها أو الحد من أثرها عند تنفيذها.

(٢) دور رئاسة أمن الدولة في تنسيق المواجهة الأمنية:

تتولى رئاسة أمن الدولة التنسيق الفعلي للجهود الأمنية المرتبطة بالإرهاب السيبراني، سواء من خلال المعلومات الاستخباراتية أو عبر التدخل العملياتي في حالات الهجوم أو التهديدات الجادة. وتقوم الرئاسة بتفعيل غرف عمليات مشتركة، وتنظيم التدخل السريع وفقًا لمستوى التهديد، كما تعتمد على التعاون مع الجهات الدولية في تتبع مصادر الهجمات وتحديد هوية المنفذين[٧٦].

ومما سبق يمكن للباحث القول إن رئاسة أمن الدولة تُشكل الخط الدفاعي الأول في المواجهة العملياتية، مستفيدة من قدراتها التقنية والاستخباراتية المتقدمة.

(٣) دور الهيئة الوطنية للأمن السيبراني في تنفيذ الضوابط الوقائية:

أصدرت الهيئة الوطنية للأمن السيبراني عددًا من الأدلة الإرشادية والضوابط الملزمة التي تُشكّل البنية الإجرائية لأي جهة حكومية أو حيوية في المملكة. **ومن أبرزها:**

---

[٧٥] الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، مرجع سابق، ص ١٧.

[٧٦] عبدالعزيز بن غرم الله، مرجع سابق، ص ٨١.

ضـوابط الأمـن السـيبراني الأساسـية، وضـوابط الأمـن السـيبراني للتشـغيل والتقنيـة، وقـد ألزمت بها جميع الجهات. كما نفذت الهيئة برامج تدريب وورش عمل لرفع التزام الجهات بها وتقييم مستويات الامتثال[٧٧].

ومما سبق يمكن للباحث القول إن الهيئة قامت بتحويل الأمن السيبراني من مفهوم تقني إلى التزام نظامي قابل للتنفيذ والمتابعة.

(٤) التعاون المؤسسي وتبادل المعلومات بين الجهات المختصة:

أنشأت المملكة منصات رقمية مشتركة تسمح بتبادل سريع وآمن للمعلومات المتعلقة بالهجمات السيبرانية بين الجهات الحكومية والأمنية، كما أُنشئت لجان تنسيقية بين الهيئة الوطنية، ووزارة الداخلية، والنيابة العامة، ووزارة العدل، لضمان سير الإجراءات الجنائية بشكل سلس في حال وقوع اعتداء سيبراني إرهابي[٧٨].

ومما سبق يمكن للباحث القول إن التنسيق المؤسسي يُعد حجر الزاوية في منع تعارض الإجراءات وتوفير رد موحّد وسريع عند حدوث تهديد إلكتروني خطير.

(٥) تنفيذ التمارين الافتراضية لقياس الجاهزية:

تعتمد المملكة آلية التمارين السيبرانية المشتركة، وهي محاكاة واقعية لهجمات إلكترونية، تُنفذ بين مختلف الجهات الأمنية والتقنية، بهدف اختبار الجاهزية، وكفاءة الاستجابة، والقدرة على إدارة الأزمات. وقد شملت هذه التمارين قطاعات حيوية مثل الطاقة والمطارات والخدمات المالية، وأسهمت في اكتشاف نقاط الضعف قبل وقوع حوادث حقيقية[٧٩].

ومما سبق يمكن للباحث القول إن التمارين السيبرانية أصبحت أداة معيارية لتقييم الأداء الأمني السيبراني، وقياس مرونة النظام الوطني في مواجهة الإرهاب الرقمي.

(٦) تطوير أدوات التحقيق الرقمي الجنائي

تسعى الجهات الأمنية في المملكة إلى تحديث آليات التحقيق الرقمي، من خلال تأسيس وحدات متخصصة داخل وزارة الداخلية والنيابة العامة، مدعومة بأدوات تحليل

---

[٧٧] الهيئة الوطنية للأمن السيبراني، مرجع سابق، ص ٢١.

[٧٨] غادة الطريف، السياسة الاجتماعية ومكافحة الجرائم الالكترونية في المجتمع السعودي، دار جامعة نايف للنشر، الرياض، ٢٠٢٠، ص ٩٤.

[٧٩] غادة الطريف، المرجع السابق، ص ٩٥.

(ISSN: 2537 - 0758)

الأدلة الرقمية، وتقنيات تتبع مصدر الهجمات، وتوثيق الأدلة الإلكترونية ضمن المعايير القانونية. وقد تم تنفيذ برامج تدريبية بالتعاون مع جهات دولية لتأهيل المحققين على استخراج الأدلة من الهواتف، الخوادم، الشبكات، والمنصات المشفّرة[٨٠].

ومما سبق يمكن للباحث القول إن تطوير التحقيقات الرقمية يُشكل الحلقة الأهم في تحويل الهجوم السيبراني من حادث تقني إلى جريمة جنائية قابلة للإثبات والمساءلة.

(٧) التدخل الميداني السريع لأجهزة إنفاذ القانون:

قامت وزارة الداخلية بإنشاء فرق تدخل سيبراني، قادرة على الانتقال إلى مواقع الهجوم عند الضرورة، وتحليل البيانات الأولية، وحجز الأجهزة المعنية، وتفعيل خطط احتواء إلكترونية وميدانية لحماية الأنظمة. وتعمل هذه الفرق بالتنسيق مع وحدات الجرائم المعلوماتية في الشرطة، ومع الأجهزة القضائية المختصة.

ومما سبق يمكن للباحث القول إن دمج القوة الميدانية مع الاستجابة الرقمية يشكل تطورًا نوعيًا في كيفية تعامل المملكة مع الجرائم الإرهابية السيبرانية[٨١].

المبحث الثاني

الجوانب الإجرائية لمواجهة الإرهاب السيبراني في النظام السعودي

تمهيد وتقسيم:

تُعد المملكة العربية السعودية من الدول التي أولت اهتمامًا بالغًا بهذا النوع من الجرائم، إدراكًا منها لخطورتها المتزايدة على الأمن الوطني، والمؤسسات الحيوية، واستقرار المجتمع. فقد بادرت المملكة إلى إصدار الأنظمة ذات الصلة، وتأسيس الهيئات المختصة، وإطلاق الاستراتيجيات الوطنية للأمن السيبراني، غير أن الواقع العملي يُظهر استمرار وجود ثغرات قانونية ومؤسساتية تتطلب المعالجة الفورية والدقيقة.

ويكتسب موضوع الإرهاب السيبراني أهمية متزايدة في ضوء تداخله مع عدد من الجرائم المنظمة، مثل تمويل الإرهاب وغسل الأموال الرقمية، واستخدام العملات المشفرة في تنفيذ عمليات معقدة، فضلًا عن علاقته الوثيقة بجرائم المعلومات والاعتداء على

---

[٨٠] مركز الجرائم السيبرانية والأدلة الرقمية، الإرهاب السيبراني في المنطقتين الإفريقية والعربية: تقرير استقصائي من ورشة عمل جامعة نايف ومركز الأمم المتحدة لمكافحة الإرهاب، دار جامعة نايف للنشر، الرياض، ٢٠٢٤م، ص ١١.

[٨١] ميليسيا هاثاواي، فهد السويلم، مرجع سابق، ص ١٣.

الأنظمة المعلوماتية الحكومية. مما يجعل دراسته من منظور قانوني وأمني أمرًا ضروريًا لفهم أركانه، وتحديد وسائل مواجهته، والوقوف على حدود المسؤولية الجنائية لمرتكبيه.

وفي ظل هذا السياق، تأتي هذه الدراسة لتقدم تحليلًا قانونيًا شاملًا لجريمة الإرهاب السيبراني في النظام السعودي، من خلال التركيز على عناصرها الموضوعية، وإجراءات مواجهتها، ودور المؤسسات الوطنية المختصة بإنفاذ القانون في التعامل معها، مع بيان مدى كفاية التشريعات والسياسات الراهنة في مكافحة هذا النوع من الجرائم.

ويمكن تقسيم هذا المبحث إلى المطلبين التاليين:

- **المطلب الأول:** التكييف النظامي لجريمة الإرهاب السيبراني وعقوباتها.
- **المطلب الثاني:** إجراءات الضبط الجنائي والإشكاليات العملية في إنفاذ القانون في جرائم الإرهاب السيبراني.

المطلب الأول

التكييف النظامي لجريمة الإرهاب السيبراني وعقوباتها

يُعد التكييف النظامي لجريمة الإرهاب السيبراني ضرورة قانونية لفهم طبيعة هذه الجريمة المعقدة، وتحديد إطارها العقابي وفقًا للأنظمة السارية في المملكة العربية السعودية. فهذه الجريمة تجمع بين الأساليب التقليدية في الاعتداء على الأمن الوطني، والوسائل التقنية الحديثة التي تعقّد من إجراءات إثباتها، مما يتطلب تحليلًا دقيقًا لأركانها وعقوباتها النظامية. **وسوف أوضح ذلك من خلال الفرعيين الآتيين:**

الفرع الأول: أركان جريمة الإرهاب السيبراني في النظام السعودي.

الفرع الثاني: العقوبات النظامية المقررة لجريمة الإرهاب السيبراني

الفرع الأول

أركان جريمة الإرهاب السيبراني في النظام السعودي

تُعد الأركان المكوّنة لجريمة الإرهاب السيبراني في النظام السعودي حجر الأساس في التكييف القانوني لهذه الجريمة المعقّدة، والتي تزاوج بين الطبيعة الرقمية للجريمة والطابع الإرهابي المقصود منها. ويتعين لتوصيف الواقعة بأنها "جريمة إرهاب سيبراني" تحقق مجموعة من الأركان النظامية، تشمل: ركنًا شرعيًا يرتكز على النص النظامي، وركنًا ماديًا يبرز من خلال السلوك الإجرامي الإلكتروني، وركنًا معنويًا يتمثل في القصد

(ISSN: 2537 - 0758)

الجنائي بأنواعه، وركنًا مفترضًا يعكس خصوصية البيئة السيبرانية. وسوف أعرض هذه الأركان تفصيلًا من خلال العناصر الآتية:

أولاً: الركن الشرعي في جريمة الإرهاب السيبراني:

يُعد الركن الشرعي أحد الأركان الجوهرية في البناء القانوني لجريمة الإرهاب السيبراني، حيث لا يمكن مساءلة أي شخص جنائيًا ما لم يكن فعله مؤسسًا على نص نظامي صريح يجرّمه، تطبيقًا لمبدأ "لا جريمة ولا عقوبة إلا بنص"، وهو ما أكده الفقه الجنائي السعودي في سياق التفسير الضيق للنصوص الجزائية.

وقد توافرت في النظام السعودي نصوص متعددة تُشكّل الركن الشرعي لجريمة الإرهاب السيبراني، يأتي في مقدمتها نظام مكافحة الإرهاب وتمويله، حيث نصت المادة الأولى على أن الأعمال الإرهابية تشمل الأفعال التي تُرتكب باستخدام الوسائل التقنية، أو عبر الشبكات المعلوماتية، بهدف زعزعة الأمن الوطني، أو الإضرار بالمصالح السياسية والاقتصادية أو بالبنية التحتية للدولة، أو تهديد النظام العام. وهذا النص يُعد حجر الزاوية في تأسيس البنية القانونية لتجريم الإرهاب السيبراني عبر الوسائل الإلكترونية[٨٢].

كما يُعزز نظام مكافحة الجرائم المعلوماتية هذا التأسيس من خلال ما ورد في المادة السادسة، التي نصت على عقوبة السجن والغرامة لكل من ينتج أو يُرسل أو يُخزن عبر الشبكة المعلوماتية محتوىً من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو الأمن الوطني. وقد أشارت المادة الثالثة والرابعة من ذات النظام إلى تجريم الدخول غير المشروع إلى الأنظمة الحكومية الحساسة، أو إتلاف البيانات أو تدميرها أو تعطيلها، وهي أنماط ترتبط ارتباطًا مباشرًا بالجريمة السيبرانية ذات الطابع الإرهابي[٨٣].

---

[٨٢] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، بتاريخ ١٤٣٩/٢/١٢هـ، قرار مجلس الوزراء رقم ٩٢ بتاريخ ١٤٣٩/٢/١١هـ، المنشور بجريدة أم القرى، العدد ٤٦٩٥ بتاريخ ٢١ صفر ١٤٣٩هـ.

[٨٣] نظام مكافحة الجرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، بتاريخ ١٤٢٨/٣/٨هـ، قرار مجلس الوزراء رقم ٧٩ بتاريخ ١٤٢٨/٣/٧هـ، المنشور بجريدة أم القرى، السنة ٨٣، العدد ٤١٤٤، بتاريخ ٢٥ ربيع الأول ١٤٢٨هـ، الموافق ١٣ إبريل ٢٠٠٧م.

وتتضح أهمية الركن الشرعي في هذه الجريمة من خلال شمول النصوص النظامية لحالات متعددة تشمل: التحريض، الترويج، التخطيط، التنفيذ، التستر، أو المساهمة في أعمال سيبرانية تهدف إلى تقويض استقرار الدولة أو إرهاب المجتمع، وهو ما يُوسع من مظلة التجريم النظامي[٨٤].

ومما سبق يمكن للباحث القول إن الركن الشرعي لجريمة الإرهاب السيبراني قد تم إرساؤه على دعائم نظامية واضحة ومتكاملة في النظام السعودي، من خلال التلاقي بين أحكام نظام مكافحة الإرهاب وتمويله، ونظام مكافحة الجرائم المعلوماتية، مما يُوفّر أساسًا متينًا لتجريم هذه الأفعال، ويُؤكد على التزام المملكة بمواجهة هذا النوع المستحدث من الجرائم بكل حزم.

ثانيا: الركن المادي للجريمة السيبرانية الإرهابية:

يُشكّل الركن المادي الأساس الواقعي للجريمة، حيث يقوم على ترجمة النية الإجرامية إلى فعل مادي ملموس، ينتج عنه ضرر فعلي يهدد الأمن الوطني [٨٥]، وفي جريمة الإرهاب السيبراني، يتخذ هذا الركن صورة خاصة، تتمثل في السلوك الرقمي المنطوي على خطورة عالية، والمرتبط بنتيجة إجرامية تمس استقرار الدولة أو سلامة بنيتها التحتية أو سيادتها الرقمية. وتمتاز هذه الجريمة بخصوصية في تحقق ركنها المادي، لكونها تُرتكب في بيئة افتراضية عبر أدوات رقمية، يصعب ضبطها أو تحديد نطاقها المكاني والزماني بدقة، مما يفرض تحديات خاصة على جهات الضبط والتحقيق.

ويقوم على توافر **ثلاثة عناصر مترابطة**، هي: السلوك الإجرامي، والنتيجة الإجرامية، والعلاقة السببية بينهما. وتكمن خصوصية هذا الركن في كونه يعتمد على وسائط إلكترونية عابرة للحدود، ويتطلب تدخلًا تقنيًا متقدمًا لكشفه. **وسوف يتم تناول هذه العناصر على النحو التالي:**

---

[٨٤] عبد العزيز بن غرم الله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة جرائم الإنترنت، دار الكتاب الجامعي، الرياض، ١٤٣٨هـ، ص ١٢٣.

[٨٥] عبد الله الفقيه، الجريمة في الفقه الجنائي، دار النهضة العربية، القاهرة، الطبعة الثانية، ٢٠١٥، ص ٢٨٩.

(ISSN: 2537 - 0758)

(١) السلوك الإجرامي (الفعل الإجرامي السيبراني):

يُعد السلوك الإجرامي الركن المحوري في البناء المادي لجريمة الإرهاب السيبراني، إذ يمثّل النشاط الخارجي الإرادي الذي يصدر عن الجاني ويُترجم نيته إلى واقع ملموس عبر الفضاء الرقمي، متى كان هذا النشاط مُجرّمًا نظامًا ويُفضي إلى تهديد أمن الدولة أو التأثير في مصالحها الحيوية. ويتمثل هذا السلوك في أي فعل يُرتكب عبر الوسائل التقنية الحديثة، ويستهدف المساس بالأمن الوطني أو النظام العام أو المؤسسات السيادية للدولة، سواءً بشكل مباشر أو غير مباشر.

وتأخذ هذه الأفعال السيبرانية صورًا تقنية متجددة، من أبرزها:

١. **اختراق الأنظمة السيادية أو الأمنية للدولة**، بما في ذلك قواعد البيانات الخاصة بالوزارات، أو منصات الاتصال العسكري أو الأمني المشفر، أو الأنظمة الرقمية للمؤسسات الحيوية، ويُعد هذا الفعل من أخطر أشكال السلوك الإجرامي السيبراني، لما ينطوي عليه من تهديد مباشر للسيادة الرقمية.
٢. **شنّ هجمات حجب الخدمة الموزعة(DDoS)**، التي تُستخدم لإغراق الخوادم الحكومية أو مواقع البنية التحتية بالخوارزميات الكثيفة، مما يؤدي إلى تعطيل تام في خدمات الدولة، وشل قدرتها على التفاعل التقني مع الجمهور.
٣. **زرع برمجيات خبيثة(Malware)**، مثل الفيروسات المتقدمة أو أدوات التجسس (Spyware) داخل أنظمة الحماية أو منصات التحكم المركزية في المنشآت السيادية، بهدف سرقة المعلومات أو تعطيل الأنظمة من الداخل، وهو ما يُعد صورة من صور التسلل الإلكتروني المتعمد لأغراض عدائية.
٤. **تعطيل البنية التحتية الحيوية**، كمنظومات الطاقة والاتصالات والمطارات وشبكات القطارات أو الدفاع المدني، وهي أهداف رئيسية في العمليات الإرهابية السيبرانية لما لها من تأثير مباشر على الحياة العامة والاستقرار الوطني.
٥. **بث دعايات رقمية تحريضية ذات طابع عدائي**، سواء عبر مقاطع مرئية أو نصوص مكتوبة تُنشر في المنصات الرقمية الكبرى، وتستهدف إثارة النعرات الدينية أو القومية، أو التحريض على العنف أو العصيان، أو التشكيك في مؤسسات الدولة، وتُعد هذه الأفعال من الوسائل غير المباشرة للتأثير في النظام العام وزعزعة الثقة المؤسسية.

وقد اعتنى **نظام مكافحة الإرهاب وتمويله** بتحديد صور هذا السلوك بدقّة، حيث نصّ في **المادة (١)** على أن:

"العمل الإرهابي هو كل فعل يقوم به الجاني بقصد الإخلال بالنظام العام، أو زعزعة أمن المجتمع، أو الإضرار بالمصالح الوطنية، أو تهديد الوحدة الوطنية، أو تعريض الموارد الوطنية للخطر، متى ارتكب باستخدام وسائل تقنية أو مادية أو رقمية"[٨٦].

وتكشف هذه الصياغة أن المنظم السعودي لم يُقيّد وصف العمل الإرهابي بالأدوات التقليدية، بل فتح المجال أمام التقنيات الرقمية بوصفها وسيلة يمكن أن تتحقق من خلالها الجريمة، ما دام الفعل يفضي إلى نتيجة ذات طبيعة تهديدية للكيان الوطني أو مكوناته السيادية.

وبالتالي، فإن صور السلوك الإجرامي السيبراني بحسب النظام تشمل على وجه الخصوص:

- اختراق الأنظمة السيادية الرقمية
- إتلاف أو تعطيل قواعد بيانات الوزارات أو الأجهزة الأمنية
- نشر البرمجيات الخبيثة المؤدية إلى انهيار البنية التحتية الحساسة
- الاستخدام العمدي للفضاء السيبراني للتحريض أو الترويج لأعمال عنف جماعي

ومن زاوية مكملة، فقد نصّ نظام مكافحة الجرائم المعلوماتية في المادة (٣) على عقوبة تصل إلى عشر سنوات سجنًا بحق[٨٧]:

"كل من ارتكب فعلًا يؤدي إلى تهديد الأمن الوطني أو الإضرار بالمصالح العامة عبر الوسائل المعلوماتية". كما جرّمت **المادة (٤)** صورة صريحة:

"الدخول غير المشروع إلى المواقع أو الأنظمة الحساسة أو الحكومية".

ومن خلال هذه المواد، يتّضح أن النظام السعودي تبنّى نهجًا مزدوجًا في توصيف السلوك السيبراني، بحيث اعتبر المكان الرقمي (كالموقع السيادي) والوسيلة التقنية (كالاختراق أو الإتلاف) والأثر الناتج، جميعها عوامل تدخل في توصيف السلوك الإجرامي، بما يحقق التكييف النظامي الدقيق للفعل في سياق جريمة الإرهاب السيبراني.

---

[٨٦] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، المادة ١

[٨٧] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، المواد (٣،٤)

(ISSN: 2537 - 0758)

وبالنظر إلى ما تقدّم، فإن السلوك الإجرامي في هذه الجريمة لا يُعد جريمة إرهابية لمجرد كونه رقمياً أو متقنًا من الناحية التقنية، بل متى ما توافرت فيه أربعة شروط نظامية:

١. أن يُرتكب الفعل عبر وسيلة رقمية أو معلوماتية.
٢. أن يكون الفعل موجّهًا ضد مصلحة سيادية أو وطنية.
٣. أن تكون الوسيلة المستخدمة مؤهلة لإحداث أثر تهديدي مباشر أو غير مباشر.
٤. أن يثبت اقتران السلوك بنية إرهابية خاصة، وفق ما نصت عليه المواد الأولى والثالثة من نظام مكافحة الإرهاب.

وهذا الفهم يسمح بتمييز السلوك السيبراني الإرهابي عن الجرائم المعلوماتية التقليدية، حيث لا يكفي مجرد الدخول غير المشروع أو التحايل على النظم لحمل الوصف الإرهابي، بل يجب أن يتجه السلوك نحو إحداث خلل في الأمن الوطني أو الاستقرار السياسي أو وحدة المجتمع.

ويمثل هذا التوافق بين النظامين تعبيرًا واضحًا عن استيعاب المنظم لطبيعة هذه الجرائم المركبة، ومحاولته معالجتها من زاويتين: الأولى أمنية تتعلق بقصد الإضرار بالوطن والمجتمع، والثانية تقنية تتعلق بالوسائل الرقمية المستخدمة.

وتفرض هذه الطبيعة غير التقليدية على المنظّم أن يعتمد سياسة تجريمية مرنة، تُركّز على الأثر والنية بدلًا من الاقتصار على الوسيلة أو الأسلوب، مما يتطلب توسيع دائرة التجريم لتشمل الأفعال التحضيرية والوسائل التقنية، لا مجرد النتيجة المادية[٨٨].

كما أن غياب التحديد المكاني والزماني للسلوك السيبراني، نتيجة استخدام خوادم خارجية أو بنى تشفير متداخلة، يُحتم على جهات الضبط والتحقيق اتباع مناهج تحليل فني متقدم تستند إلى تحليل السياق الرقمي، والربط بين مؤشرات التسلل، والبيانات اللوجستية (Logs)، وسجلات الأحداث الأمنية (SIEM Systems)، وهو ما يختلف جذريًا عن أساليب الإثبات في الجرائم التقليدية.

ومن خلال ما سبق، يتضح أن السلوك الإجرامي في جريمة الإرهاب السيبراني لا يُمثّل مجرد فعل عدائي في الفضاء الرقمي، بل هو بنية إجرامية شديدة التعقيد، تتجاوز

[٨٨] المرجان وآخرون، الأساليب والاتجاهات الحديثة للجرائم السيبرانية، دار جامعة نايف للنشر، الرياض، ٢٠٢٥م، ص ٧٣.

المفهوم التقليدي للفعل المادي، وتستهدف الكيانات السيادية للدولة من خلال اختراقات رمزية لكن ذات أثر حقيقي، ما يجعل من التكييف القانوني مرهونًا بفهم التقنية، لا بالنص المجرد فقط.

(٢) النتيجة الإجرامية:

تُمثّل النتيجة الإجرامية في جريمة الإرهاب السيبراني الأثر المترتب على السلوك الإجرامي، وهي العنصر الذي يُميز بين السلوك الضار والمُجرّم وبين الأفعال التي قد تبدو مشابهة في الوسيلة ولكن لا تُفضي إلى ضرر يستوجب التجريم. ويُشترط في هذه النتيجة أن تكون ضارة بمصالح جوهرية تمس كيان الدولة أو نظامها العام أو بنيتها التحتية الحيوية، مثل تعطيل الدفاع، أو شل الأمن الداخلي، أو إيقاف أنظمة النقل والطاقة أو الاتصالات.

ويتّضح من النصوص النظامية في المملكة العربية السعودية أن المعيار الأساس لاعتبار السلوك الرقمي جريمة إرهابية سيبرانية لا يقف عند حدود الوسيلة التقنية، وإنما يتطلب تحقق "نتيجة إجرامية" تُهدّد فعليًا المصالح الجوهرية للدولة، وتمس النظام العام أو الأمن الوطني أو البنية التحتية الحيوية.

وقد تبنى نظام مكافحة الإرهاب وتمويله هذا الفهم الموسّع للنتيجة الإجرامية، حيث قرر في المادة (١) أن العمل الإرهابي يشمل "كل فعل يقوم به الجاني بقصد الإخلال بالنظام العام، أو زعزعة أمن المجتمع، أو الإضرار بالمصالح الوطنية" [٨٩].

وهذا النص لا يقيّد الوسيلة، بل يُضفي الصفة الإرهابية على النتيجة المترتبة عن أي فعل، سواء أكان ماديًا تقليديًا أو سيبرانيًا رقميًا، ما دام قد نتج عنه مساس مباشر أو غير مباشر بالبنى السيادية أو المكونات الأمنية للدولة.

وتأسيسًا على ذلك، فإن مجرد استخدام الوسائل التقنية لا يكفي لقيام الجريمة الإرهابية، بل يجب أن يُفضي الفعل إلى نتيجة ضارة، تمس بمفاهيم جوهرية مثل:

- الوحدة الوطنية.
- الاستقرار السياسي.
- القدرة الدفاعية أو السيادية.
- البنية التحتية للقطاعات الحيوية.

---

[٨٩] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، المادة ١.

(ISSN: 2537 - 0758)

ولذلك فإن النتيجة تُعد بمثابة *العنصر الفاصل* بين الاستخدام التقني المشروع، أو حتى الجرمي العام، وبين الفعل الذي يُصنّف جريمة إرهابية سيبرانية وفق التكييف النظامي في المملكة.

أما نظام مكافحة الجرائم المعلوماتية فقد أكّد على ذات المفهوم من زاوية أخرى، حيث نص في المادة (٦) على أنه يُعاقب كل من يرتكب فعلاً يؤدي إلى "إتلاف البيانات الحكومية، أو تعطيل الشبكات أو الخدمات العامة، أو المساس بالنظام العام،" بالسجن والغرامة"[٩٠].

ويمكن القول هنا إن المادة السادسة توسّعت في تصوير النتيجة الإجرامية، لتشمل الأثر السيبراني الذي لا يقتصر على التدمير المادي، بل يمتد إلى تعطيل الخدمة العامة، أو التأثير في استقرار النظام العام الرقمي للدولة .وهذا التكييف ينسجم مع الطابع المعاصر لجريمة الإرهاب السيبراني، **التي قد تتمثل نتائجها في:**

- شلّ الخدمات الأمنية أو الدفاعية
- إيقاف منشآت البنية الحيوية
- إثارة الفوضى عبر المنصات الرقمية
- تعطيل الثقة العامة في المؤسسات السيادية

ولذا فإن العلاقة بين النصين تُبرز تكاملًا وظيفيًا في النظام السعودي، حيث يُعنى نظام مكافحة الإرهاب بتجريم النتيجة في سياقها الأمني والسياسي، بينما يُعنى نظام الجرائم المعلوماتية بتفصيل الآثار التقنية، مما يُشكل معًا أساسًا مركبًا لتجريم النتيجة الإجرامية في جرائم الإرهاب السيبراني.

ومن الناحية التحليلية، فإن هذا التلاقي بين النصوص يُبرر الاتجاه الفقهي الداعي إلى إفراد الإرهاب السيبراني بتنظيم نظامي خاص، يجمع بين الاعتبارات الأمنية والتقنية، ويُقدّم صياغة قانونية دقيقة تُراعي النتيجة المحتملة للفعل الرقمي لا وسيلته فقط.

ويمتد أثر النتيجة الإجرامية ليشمل صورًا مباشرة، كتعطيل الخدمات الأمنية أو الهجمات على البنى السيادية، وصورًا غير مباشرة مثل بث الفوضى، وإضعاف الثقة العامة، وترويع المواطنين. وقد أشار المنشاوي إلى أن: "تحقق النتيجة الإجرامية هو ما

[٩٠] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، المادة ٦.

يُميز الفعل العادي عن الجريمة الإرهابية الرقمية، ويشكل الحد الفاصل بين التهديد والتجريم المؤسس[٩١].

(٣) العلاقة السببية:

تُعد العلاقة السببية هي العنصر الثالث في تكوين الركن المادي، وهي التي تربط بين الفعل الإجرامي الذي قام به الجاني والنتيجة الضارة التي تحققت، أي أن يكون الفعل التقني غير المشروع هو السبب المباشر أو غير المباشر في وقوع النتيجة التي تُكوّن الجريمة الإرهابية. وتكمن أهمية هذا العنصر في جرائم الفضاء السيبراني في تعقيد سلاسل السلوك الفني، وصعوبة عزل السبب الفعلي المؤدي إلى النتيجة في بيئة إلكترونية مفتوحة ومتعددة الوسائط.

وقد عالج نظام مكافحة الإرهاب وتمويله هذه المسألة بطريقة موسعة، إذ قرر في المادة (٣٢) أن: "كل من سهّل، أو حرض، أو موّل، أو اشترك بأي صورة كانت في ارتكاب جريمة إرهابية، يُعد فاعلًا أصليًا، متى كانت أفعاله سببًا في النتيجة، ولو لم يتحقق فعله على نحو مباشر"[٩٢].

كما شدد نظام مكافحة الجرائم المعلوماتية في المادة (١١) على أنه: "إذا ترتب على الجريمة المعلوماتية ضرر بالأمن العام أو الاقتصاد الوطني أو النظام الاجتماعي، فتُضاعف العقوبة"، مما يدل ضمنًا على ضرورة وجود صلة بين الفعل المرتكب والضرر المتحقق، وهي الصلة التي لا تثبت إلا من خلال إثبات العلاقة السببية بالوسائل الفنية والتحليلية[٩٣].

ومن الناحية الفنية، يُعد إثبات العلاقة السببية في جرائم الإرهاب السيبراني من أعقد مراحل الإثبات، بسبب اعتماد الجناة على أدوات متقدمة للإخفاء والتشفير، مثل استخدام خوادم VPN، وشبكات Tor، وبرمجيات تمويه الهوية الرقمية، ما يجعل الربط بين الفعل والنتيجة عملية تتطلب تحليلًا معمّقًا لسجلات الخوادم، وأوامر التتبع الرقمي، ومقارنة مخرجات الأجهزة المضبوطة مع الحوادث المبلغ عنها.

---

[٩١] محمد المنشاوي، النظام الجزائي الخاص، دار الكتاب الجامعي، الرياض، ١٤٤٤هـ، ص ١٤٩.

[٩٢] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، المادة ٣٢.

[٩٣] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، المادة ١١.

(ISSN: 2537 - 0758)

ولذلك، يُعد تدخل الخبراء المختصين في الأدلة الرقمية أمرًا حاسمًا في هذه المرحلة، إذ لا يُمكن للقاضي أو المحقق أن يُكوّن قناعته دون تقرير فني مفصّل يُثبت أن الفعل الرقمي الذي ارتكبه الجاني هو الذي أفضى إلى النتيجة الإجرامية، مما يعزز من عدالة التكييف، ويُغلق باب الإنكار أو التملص الفني من المسؤولية الجنائية[٩٤].

وقد خلص الباحث إلى أن وجود السلوك الرقمي لا يكفي لقيام الجريمة، ما لم يقترن بتحقق نتيجة تمس الأمن الوطني، وثبوت علاقة سببية مباشرة، مما يُبرز أهمية تطوير الأدوات الفنية والإجرائية لضبط هذا الركن بدقة.

ثالثًا: الركن المعنوي لجريمة الإرهاب السيبراني:

يُعد الركن المعنوي أحد أبرز الأركان التي تميز جريمة الإرهاب السيبراني عن غيرها من الجرائم المعلوماتية، نظرًا لما تتطلبه من نية إجرامية مركبة تتجاوز مجرد استخدام الوسائل التقنية المحظورة، لتشمل استهدافًا صريحًا لأمن الدولة واستقرارها، وهو ما يُكسبها خصوصية قانونية تتداخل فيها الأبعاد الجنائية والسياسية.

أولًا: القصد الجنائي العام والخاص:

يتحقق القصد الجنائي العام في جريمة الإرهاب السيبراني عندما يتوافر لدى الجاني الإدراك الكامل بحقيقة الفعل المرتكب، وتكون إرادته متجهة نحو ارتكابه، رغم علمه بمخالفته للنظام. ويشمل ذلك أي سلوك تقني أو إلكتروني يؤدي إلى المساس بالأنظمة الوطنية الحساسة، مثل اختراق المواقع السيادية، أو تعطيل الخدمات العامة، أو نشر الفوضى عبر الوسائط الرقمية، مع إدراك الجاني أنه يقوم بفعل غير مشروع.

أما القصد الجنائي الخاص، فيظهر عند اقتران السلوك الإلكتروني بنية محددة تتعلق بأهداف ذات طابع إرهابي، كإحداث الرعب في المجتمع، أو التأثير على القرار السياسي، أو تهديد المؤسسات السيادية للدولة، أو إلحاق الضرر بالأمن القومي. وقد نص نظام مكافحة الإرهاب وتمويله على ضرورة توافر هذا القصد الخاص، حيث عرف الجريمة الإرهابية بأنها "كل فعل يقوم به الجاني بقصد الإخلال بالنظام العام، أو زعزعة الأمن الوطني، أو تهديد وحدة الدولة"[٩٥].

---

[٩٤] السيد شريف، الوجيز في شرح نظام الإجراءات الجزائية السعودي، دار الإجادة، الرياض، ١٤٤٣هـ، ص ٢١٣.

[٩٥] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ١.

وجريمة الإرهاب السيبراني تفترض وجود نية إجرامية مزدوجة، تجمع بين العلم بالفعل المحظور من جهة، والتخطيط لتحقيق أهداف إرهابية من جهة أخرى، ما يجعل إثبات القصد الخاص عنصرًا محوريًا في بناء الإدانة[٩٦].

ثانياً: إثبات النية الإجرامية في الفضاء السيبراني

تُعد مسألة إثبات النية الإجرامية في جرائم الإرهاب السيبراني من أعقد التحديات التي تواجه الجهات القضائية والأمنية، نظرًا للطبيعة التخفيّة للفضاء الرقمي، واعتماد الجناة على أدوات تشفير متطورة تخفي هويتهم وسلوكهم. ولا يكفي مجرد وجود فعل مادي محظور، بل يجب إثبات أن هذا الفعل قد تم بدافع إرهابي، وهو ما يستدعي الاعتماد على القرائن التقنية والدلائل الرقمية والسياقات السلوكية[٩٧].

وتُعد الأدلة الرقمية، مثل سجل الدخول إلى المواقع، أو استخدام أدوات رقمية مصنفة، أو التواصل مع جهات محظورة، مؤشرات قوية على النية الإجرامية الخاصة. كما قد يستدل على القصد الخاص من خلال دراسة نمط التكرار في الأفعال، وتزامنها مع أهداف لجماعات متطرفة، وتحليل محتوى الرسائل المشفرة. لذا أصبح هناك ضرورة إلى الاعتماد على تحليل السياق التقني والسلوكي للفعل الرقمي لإثبات القصد الخاص، خاصة في ظل تطور وسائل التخفي الإلكتروني[٩٨].

وتُعد مسألة إثبات القصد الجنائي– بنوعيه العام والخاص– في جرائم الإرهاب السيبراني من أكثر المسائل تعقيدًا في الممارسة العملية، نظرًا للطبيعة غير المادية للسلوك، واعتماد الجناة على وسائل تقنية متقدمة تُخفي آثارهم الرقمية. ومع ذلك، فإن مناط الإثبات لا يتعلق فقط بتوافر وسيلة تقنية، وإنما بالربط الموضوعي بين السلوك التقني والنية الإرهابية الخاصة.

---

[٩٦] فهد نايف الطريسي، الإجراءات الجزائية في المملكة العربية السعودية، دار الكتاب الجامعي، الرياض، ٢٠١٩م، ص ١١٢.

[٩٧] عباس طفشي، حنان طرشان، الجرائم الالكترونية في الفقه الإسلامي والقانون الوضعي، المركز الديمقراطي العربي، القاهرة، ٢٠٢٢، ص٢١.

[٩٨] إيمان مأمون، متولي عبدالمؤمن، قواعد الإثبات في النظام القانوني السعودي والقانون المقارن، دار الإجادة للنشر والتوزيع، الرياض، ٢٠٢٣م، ص ١٤٥.

(ISSN: 2537 - 0758)

ويُناط بقاضي الموضوع– استنادًا إلى سلطته التقديرية– استخلاص القصد الجنائي من مجمل الأدلة المقدمة في الدعوى، ولا سيما الرقمية منها، بشرط أن تكون هذه الأدلة قد جُمعت بصورة نظامية، وتُفسَّر في ضوء القرائن والسياق العام للفعل الإجرامي.

ومن هنا، يُلقى على جهات التحقيق عبء مضاعف في جمع وتحليل قرائن متعددة، من بينها:

- سجل الاستخدامات الرقمية التي توحي بالاستهداف المقصود لمواقع سيادية أو مؤسسات حساسة.
- تكرار الأفعال الرقمية المتزامنة مع أحداث أو دعوات مرتبطة بجماعات إرهابية.
- تحليل البنية التقنية للأدوات المستخدمة (برمجيات تخفٍ– بروتوكولات تشفير– مسارات وهمية).
- محتوى الاتصالات المشفرة، أو النصوص الرقمية التي تُظهر ميولًا تحريضية أو نيات عدائية.

ولا يُشترط لثبوت القصد الخاص اعتراف صريح أو دليل مباشر، بل يكفي أن تُستشفّ النية من الوقائع المحيطة والسياق التقني العام، وفق ما تقرره المحكمة بناء على مبدأ الاقتناع القضائي، المنصوص عليه ضمن المبادئ العامة في الإثبات الجنائي.

وهنا تبرز الحاجة إلى تعاون وثيق بين الفرق الفنية الجنائية والنيابة العامة، لتقديم ملف إثبات رقمي مُحكم، يُمكِّن القاضي من بناء تصوّر منطقي ومتكامل عن توافر القصد الإجرامي الخاص، دون إخلال بضمانات العدالة أو تجاوز لمبدأ قرينة البراءة.

ومما سبق يمكن للباحث القول إن الركن المعنوي في جريمة الإرهاب السيبراني يمثل أحد أكثر الأركان حساسية وتعقيدًا، إذ يتطلب توافر علم الجاني بالفعل غير المشروع، واقترانه بهدف إرهابي خاص، ويستلزم لإثباته الجمع بين المعايير القانونية التقليدية والوسائل التقنية الحديثة، مما يُحتّم تطوير الأدوات التحليلية والقضائية المختصة بهذه النوعية من الجرائم.

رابعاً: الركن المفترض (البيئة الإلكترونية)

يُعد الركن المفترض في جريمة الإرهاب السيبراني عنصرًا مميزًا عن باقي صور الجرائم الإرهابية التقليدية، إذ يتمثل في البيئة الرقمية التي تُرتكب فيها الجريمة، كشرط

موضوعي لا يتحقق الفعل الجرمي بدونه. فلا يمكن وصف الفعل بأنه إرهاب سيبراني ما لم يقع عبر وسيط إلكتروني مثل الإنترنت أو الشبكات المعلوماتية أو تطبيقات الاتصالات الرقمية. وهذا الركن لا يُعد من الأركان الجوهرية للجريمة بمعناها التقليدي (المادي أو المعنوي أو الشرعي)، لكنه يمثل خصوصية جوهرية تميز هذه الجريمة عن غيرها من الجرائم الإرهابية.

وتتجلى ملامح هذا الركن في عدة عناصر:

أولًا: وسط الجريمة الإلكتروني:

تفترض الجريمة السيبرانية وجود وسيط تقني يُرتكب عبره الفعل الإرهابي، مثل الخوادم الإلكترونية، أو الشبكات المفتوحة أو المغلقة، أو منصات التواصل، أو قواعد البيانات المؤسسية. وهو ما نص عليه نظام مكافحة الجرائم المعلوماتية في عدة مواد، أبرزها المادة الثالثة التي جرّمت الدخول غير المشروع إلى مواقع إلكترونية حكومية أو عسكرية[٩٩].

ثانياً: الأدوات التكنولوجية الحديثة:

يُفترض في هذه الجريمة استخدام وسائل تقنية متقدمة تشمل برمجيات الاختراق، وفيروسات الشبكة، وأدوات التشفير، وتقنيات "التمويه الرقمي" لإخفاء الهوية. وهذا ما أكده نظام مكافحة الإرهاب وتمويله من خلال إدراج الوسائل الإلكترونية ضمن أدوات ارتكاب الجريمة في المادة الأولى، التي توسعت في وصف الوسائل لتشمل كل ما يؤدي إلى تقويض الأمن عبر الفضاء السيبراني[١٠٠].

ثالثاً: امتداد الأثر من الفضاء الرقمي إلى الواقع المادي:

رغم أن الجريمة السيبرانية تقع في بيئة افتراضية، إلا أن نتائجها قد تُصيب الواقع المادي مباشرة، كتعطيل منشآت حيوية (مطارات– محطات كهرباء– أنظمة طبية)، أو إثارة الفوضى العامة. وهذه النتيجة هي ما يعطي الجريمة طابعها الإرهابي الخطير، ويستوجب التعامل معها بمنطق متكامل يشمل الأمن السيبراني والأمن الوطني معًا[١٠١].

---

[٩٩] نظام مكافحة الجرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، المادة ٣.

[١٠٠] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، المادة ١.

[١٠١] عبدالرزاق المرجان وآخرون، مرجع سابق، ص ٧٣.

(ISSN: 2537 - 0758)

رابعاً: تعقيدات الإثبات والاختصاص القضائي:

الطابع العابر للحدود للجريمة السيبرانية يخلق إشكاليات متعددة، أبرزها: تحديد الجهة القضائية المختصة، وجمع الأدلة الرقمية عبر أكثر من دولة، وإثبات العلاقة بين الفعل والفاعل في ظل أنظمة الإخفاء الرقمي. وقد أشارت الأدبيات القانونية السعودية إلى أن البيئة السيبرانية تتطلب أدوات إثبات غير تقليدية، وقدرة قضائية خاصة على التعامل مع الأدلة الرقمية[١٠٢].

ومما سبق، يمكن للباحث القول إن الركن المفترض لجريمة الإرهاب السيبراني– والمتمثل في الفضاء الإلكتروني كبيئة لوقوع السلوك الإجرامي– يفرض تحديات منهجية على مستوى الضبط الفني، والإثبات العدلي، والتنفيذ القضائي.

ويرجع ذلك إلى الطبيعة غير المادية لهذا الوسط، وخصائصه التقنية المتغيرة، بما يستلزم من المنظّم السعودي تطوير أدوات تشريعية وإجرائية تتناسب مع هذه الخصوصية، إلى جانب تأهيل الكوادر الأمنية والقضائية والفنية للتعامل مع هذا النوع من الجرائم، باعتبارها نمطًا مستحدثًا يخرج عن القوالب التقليدية للجريمة الجزائية.

الفرع الثاني

جريمة الإرهاب السيبراني وعقوباتها النظامية المقررة

تمثّل العقوبات الجنائية أداة مركزية في المنظومة القانونية السعودية لمواجهة التهديدات الأمنية المعاصرة، وعلى رأسها جريمة الإرهاب السيبراني، لما تحمله من مخاطر استراتيجية تهدّد أمن الدولة ومؤسساتها الحيوية. وتُظهر الأنظمة السعودية ذات الصلة، وفي مقدمتها نظام مكافحة الإرهاب وتمويله، ونظام مكافحة الجرائم المعلوماتية، سعيًا واضحًا لإرساء توازن بين الردع الفعّال والمرونة التشريعية في مواجهة التطور التقني المتسارع. وتبرز أهمية دراسة هذه العقوبات من خلال الوقوف على طبيعتها، ونطاقها، وآليات تطبيقها، والتحديات التي تواجه إنفاذها، لا سيما في ظل الطبيعة التخفيّة للفاعل السيبراني وتعقيد وسائل الإثبات في هذا المجال. **وسوف أوضح ذلك على النحو الآتي:**

---

[١٠٢] إيمان مأمون، متولي عبدالمؤمن، مرجع سابق، ص ١٤٥.

أولًا: الجرائم والعقوبات في نظام مكافحة الإرهاب وتمويله:

وضع نظام مكافحة الإرهاب وتمويله[١٠٣] إطارًا تشريعيًا شاملاً لتجريم الأفعال الإرهابية السيبرانية، مستوعبًا التهديدات الحديثة المرتبطة باستخدام التقنية في الإخلال بالأمن العام، واستهداف المصالح الحيوية للدولة، وقد تضمّن هذا النظام عدة صور للعقوبات كما يلي:

١) العقوبات الأصلية:

فرض النظام عقوبات أصلية مشددة على مرتكبي الجرائم الإرهابية ذات البعد السيبراني، وتراوحت العقوبات بين السجن لمدد تصل إلى ثلاثين عامًا، أو السجن المؤبد، أو الإعدام في الحالات التي تترتب عليها آثار جسيمة، كقتل الأرواح أو تهديد الأمن القومي أو استهداف منشآت استراتيجية حساسة[١٠٤].

وفي ضوء ذلك يرى الباحث أن لجوء المنظم السعودي إلى تشديد العقوبات على الجرائم الإرهابية ذات الطابع السيبراني يُعد توجهًا مشروعًا ومُبررًا، لما تنطوي عليه هذه الأفعال من تهديد مباشر للسيادة الرقمية الوطنية، وارتباطها المحتمل بأعمال عدائية تماثل في آثارها الهجمات المسلحة التقليدية، مما يقتضي معالجتها بعقوبات رادعة تتناسب مع جسامة الخطر وامتداده غير المرئي عبر الفضاء السيبراني.

٢) تجريم التحريض والتمويل الإلكتروني:

امتد نطاق التجريم ليشمل كل من يحرّض أو يموّل أو يروّج للجريمة الإرهابية عبر الوسائط التقنية، بما فيها المنصات الرقمية والعملات المشفّرة، سواء تم التمويل بصورة مباشرة أو غير مباشرة، وتُقدّر العقوبة بالسجن بين خمس سنوات إلى خمس وعشرين سنة[١٠٥].

ولم يكتفِ النظام بمساءلة الفاعل الأصلي، بل شمل بالعقاب كل من ساهم بأي صورة في ارتكاب الجريمة السيبرانية الإرهابية، سواء بالتحريض أو تقديم العون التقني أو الإيواء أو التسهيل، متى ثبت أن المساهم كان على علم بالغاية الإرهابية للفعل[١٠٦].

---

[١٠٣] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ.

[١٠٤] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ٥٠.

[١٠٥] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ٤٧.

[١٠٦] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ٥١.

(ISSN: 2537 - 0758)

ويُعاقب المساهم بنفس العقوبة المقررة للجريمة التامة، إذا توافرت النية المشتركة بينه وبين الفاعل الأصلي، وهو ما أكد عليه الفقه النظامي باعتبار أن المساهمة الرقمية تُعد من أخطر صور الدعم للجريمة الإرهابية الحديثة [١٠٧].

وفي ضوء ذلك يرى الباحث أن النظام أحسن في تشديد العقوبة على كل من يشارك في الجريمة الإرهابية السيبرانية، حتى لو لم يكن هو من نفّذ الجريمة بنفسه. لأن الجريمة الإلكترونية لا تتم بيد واحدة، بل تحتاج إلى دعم وتمويل وتسهيل، خصوصًا عبر الإنترنت. لذلك، فإن معاملة المحرّض والمموّل مثل الفاعل الأصلي تُعتبر خطوة مهمة لسد الثغرات ومعاقبة كل من يشارك في هذا النوع الخطير من الجرائم.

٣) تشديد العقوبة في حال استخدام الوسائل التقنية:

لم ينص النظام صراحة على اعتبار استخدام الوسائل الإلكترونية ظرفًا مشددًا مستقلًا، إلا أن طبيعة الجريمة السيبرانية بحد ذاتها، وما تفرزه من تعقيدات في التتبع والإثبات وتهديد الأمن السيبراني الوطني، تبرر توقيع العقوبات في حدودها العليا. ويؤخذ ذلك في الاعتبار ضمن السلطة التقديرية للمحكمة، خصوصًا إذا اقترنت الجريمة بوسائل تمويه رقمية أو استهدفت منشآت سيادية أو بنية تحتية رقمية [١٠٨].

وفي ضوء ذلك يرى الباحث أن ترك المنظم السعودي تقدير خطورة الوسائل الإلكترونية للمحكمة يُعدّ نهجًا مرنًا، لكنه قد لا يكون كافيًا في ظل التطور التقني المتسارع. إذ إن الجريمة السيبرانية تُشكّل تهديدًا مضاعفًا عندما تُرتكب بأدوات معقدة يصعب تتبعها، لذا فإن النص على الظرف المشدد صراحة في النظام قد يسهم مستقبلاً في تعزيز الردع وتحقيق الحماية الجنائية المناسبة للبنية التحتية الرقمية الوطنية.

٤) مساءلة الكيانات الاعتبارية:

تضمّن النظام نصوصًا تُحمّل الشركات والمؤسسات التقنية المسؤولية الجنائية حال ثبوت تورّطها في تسهيل أو التستر على الجريمة الإرهابية السيبرانية، ويجوز معاقبتها بالغرامات المالية الكبرى (لا تزيد على (عشرة) ملايين ريال ولا تقل عن (ثلاثة) ملايين ريال)، أو تعليق نشاطها أو إغلاق منصاتها الرقمية عند الاقتضاء[١٠٩].

---

[١٠٧] عبد المجيد الحفناوي، أصول التشريع في المملكة، دار الكتب، القاهرة، ٢٠١٥م، ص ٢٢١

[١٠٨] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ٢/٥٠.

[١٠٩] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ٤٩.

وفي ضوء ذلك يرى الباحث أن تحميل الكيانات الاعتبارية مثل الشركات والمنصات التقنية هذه المسؤولية يُعد خطوة محورية في مواكبة طبيعة الجريمة السيبرانية المعاصرة، خاصةً وأن هذه الجهات قد تُستغل عمدًا أو عن تقصير في تنفيذ الأفعال الإجرامية. ويُعد هذا التوجه النظامي داعمًا لفرض رقابة ذاتية على المنصات الرقمية، وتحفيزها على تطوير أنظمة حماية وتبليغ فعالة، بما يسهم في الوقاية قبل وقوع الجريمة.

٥) صلاحيات المحكمة الجزائية المتخصصة:

فوض النظام المحكمة الجزائية المتخصصة بسلطة تقدير العقوبات وفقًا لظروف الواقعة الإرهابية السيبرانية، وهو ما يعكس مرونة التشريع في تقدير خطورة كل جريمة على حدة، مع مراعاة الطبيعة الفنية والدقيقة لهذه الأفعال.

حيث تتولى المحكمة المختصة الفصل في أي مما يأتي:

١- الجرائم المنصوص عليها في النظام.

٢- دعاوى إلغاء القرارات ودعاوى التعويض المتعلقة بتطبيق أحكام النظام.

وتُستأنف الأحكام الصادرة في شأن الفقرتين (١) و(٢) من هذه المادة أمام محكمة الاستئناف الجزائية المتخصصة"...[١١٠].

وبالرجوع إلى المواد العقابية من الثلاثين حتى الخمسين، نجد أن النظام حدّد نطاقات العقوبة (حد أدنى وحد أعلى)، لكنه لم يُلزم القاضي بحكم معيّن، مما يفتح المجال أمام المحكمة لممارسة سلطتها التقديرية بناءً على[١١١]:

- درجة الخطورة الفنية للفعل السيبراني
- موقع الفعل في البنية التحتية الوطنية
- وجود ارتباط بكيانات أو تمويل إرهابي
- الوسائل المستخدمة (كالتشفير، أو العملات المشفّرة، أو المنصات المجهولة)

وهو ما يُكرّس مبدأ المرونة القضائية في العقاب، ويُحقق الملاءمة بين طبيعة الجريمة ومقدار العقوبة الملائمة لها من حيث الأثر والنية والوسيلة.

---

[١١٠] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ٢٤.

[١١١] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ.

(ISSN: 2537 - 0758)

٦) شمولية التجريم للأفعال التحضيرية والتنسيقية:

أبرز نظام مكافحة الإرهاب وتمويله في عدة مواد منه– خاصة المادة (الثانية عشرة)–[١١٢] أن الجريمة الإرهابية لا تقتصر على الفعل التنفيذي المباشر، بل تشمل أيضًا الأفعال السابقة عليه مثل: التخطيط أو الإعداد أو التنسيق أو المساعدة أو التحريض، حتى وإن لم تكتمل أركان الجريمة. وهذا ما يُعد تأكيدًا على شمولية النظام السعودي في تجريم الأفعال السيبرانية الإرهابية في مراحلها الأولى، مما يُمكّن من التدخل المبكر، ويُعزز مفهوم الوقاية قبل المواجهة.

وفي ضوء ذلك يرى الباحث أن امتداد نطاق التجريم ليشمل الأفعال التحضيرية لجريمة الإرهاب السيبراني يُمثل نقلة نوعية في البنية الوقائية للنظام الجنائي السعودي، ويُعبّر عن وعي المنظم بخطورة المراحل التمهيدية في الجريمة الرقمية، إذ قد تُلحق أضرارًا جسيمة حتى قبل التنفيذ الكامل. كما أن هذا التوسع في التجريم يمنح جهات التحقيق مرونة أكبر في اتخاذ التدابير الاستباقية لقطع الطريق على التهديد قبل تحققه.

٧) العقوبات التكميلية والتدابير الأمنية الوقائية:

نص النظام كذلك على تدابير أمنية مكمّلة للعقوبات الأصلية، مثل :وضع المحكوم عليه تحت الرقابة الأمنية، أو منعه من استخدام الوسائط الرقمية، أو من السفر، أو من ممارسة الأنشطة المهنية المرتبطة بالتقنية، وهو ما يُشكّل إجراءً وقائيًا لحماية الأمن العام من إعادة ارتكاب الجريمة. وهذه التدابير تُطبَّق بناءً على تقدير المحكمة المختصة، بما يتوافق مع طبيعة الجريمة وظروفها، كما ورد في المواد (١٩ و٢٤) من النظام[١١٣].

وفي ضوء ذلك يرى الباحث أن اعتماد النظام لهذه التدابير الأمنية المكمّلة يُجسّد فكرًا جنائيًا حديثًا، لا يكتفي بالعقوبة الأصلية، بل يمتد لحماية المجتمع بعد التنفيذ، خاصةً في الجرائم السيبرانية ذات الخطورة العالية. كما أن المنع من استخدام الوسائط الرقمية يُعدّ تدبيرًا دقيقًا يتناسب مع طبيعة الفعل المجرَّم، ويمنع الجاني من العودة لاستخدام الفضاء الرقمي كأداة لارتكاب الجريمة من جديد.

---

[١١٢] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ١٢.

[١١٣] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، المادة١٩، ٢٤.

ومما سبق يمكن للباحث القول إن نظام مكافحة الإرهاب وتمويله أرسى معالجة نظامية صارمة وشاملة لجريمة الإرهاب السيبراني، لم تقتصر على الفاعل المباشر، بل امتدت لتشمل كل من ساهم أو شارك أو حرّض أو خطط، مع فرض تدابير وقائية مكمّلة لضمان عدم تكرار الخطر.

ثانياً: العقوبات الأصلية الواردة في نظام مكافحة الجرائم المعلوماتية:

يُعد نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/١٧) بتاريخ ١٤٢٨/٣/٨هـ[١١٤]، الإطار النظامي الرئيس الذي يُعنى بتجريم الأفعال الإلكترونية في المملكة العربية السعودية، وقد نص في مواده على عقوبات تطال صورًا متعددة من الإرهاب السيبراني، وفيما يلي أبرز العقوبات ذات الصلة:

١) التهديد والابتزاز الإلكتروني لأغراض إرهابية:

يعاقب النظام بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تتجاوز ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، لكل من قام بتهديد أو ابتزاز الغير لحمله على ارتكاب فعل أو الامتناع عنه[١١٥]، ويُضاعف أثر هذه الجريمة حين يقترن بدوافع إرهابية، كإجبار الموظفين الحكوميين على تنفيذ عمليات رقمية تؤثر في الأمن الوطني.

وفي ضوء ذلك يرى الباحث أن هذا النص يُظهر مدى خطورة التهديد والابتزاز الرقمي، خصوصًا إذا ارتبط بدوافع إرهابية، حيث يتحول السلوك من جريمة معلوماتية عادية إلى فعل يهدد الأمن الوطني. ومن ثمّ، فإن استخدام الفضاء السيبراني في التأثير على إرادة الأفراد أو الجهات الرسمية يُعد من صور الضغط غير المشروع الذي يستوجب تشديد العقوبة وفق تقدير المحكمة.

٢) نشر أو إنشاء محتوى إرهابي أو تحريضي إلكترونيًا:

"يعاقب النظام بالسجن مدة تصل إلى خمس سنوات، وبغرامة تصل إلى ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، على كل من أنشأ موقعًا إلكترونيًا، أو نشر محتوى عبر الشبكة المعلوماتية من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة.

كما يُعد من قبيل الجرائم المعلوماتية المشددة، كل من أنشأ موقعًا إلكترونيًا، أو أحد برامج الحاسب الآلي، أو استخدمها لنشر أفكار الجماعات الإرهابية، أو لتيسير التواصل

---

[١١٤] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ.

[١١٥] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة ٢/٣.

(ISSN: 2537 - 0758)

مع قياداتها، أو لتمويل أنشطتها أو الترويج لها، ويُعاقب مرتكب ذلك بالسجن مدة تصل إلى عشر سنوات، وبغرامة تصل إلى خمسة ملايين ريال[١١٦].

في ضوء ذلك، يرى الباحث أن هذه المادة تُجسّد بوضوح مدى إدراك المنظم السعودي لخطورة الفضاء السيبراني كأداة لنشر الفكر المتطرف وتغذية الجرائم الإرهابية. إذ لم يكتفِ بتجريم الاعتداء على النظام العام أو القيم الدينية، بل شدد العقوبة عند اقتران الفعل بارتباطات إرهابية، وهو ما يعكس توجهًا تشريعيًا وقائيًا لحماية الأمن الفكري والرقمي في آنٍ واحد، ويُبرز الطابع الردعي للنص القانوني.

٣) الدخول غير المشروع إلى مواقع أو أنظمة سيادية:

"يعاقب النظام بالسجن لمدة لا تزيد على عشر سنوات، وبغرامة لا تتجاوز خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، لكل من قام بالدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي سيادي أو أمني أو تابع للدولة، إذا كان القصد من ذلك هو المساس بالأمن الداخلي أو الخارجي، أو التأثير على استقرار الدولة أو مراكز صنع القرار، ويُعد ذلك من أشد صور الجرائم المعلوماتية المرتبطة بالأمن الوطني [١١٧].

وفي ضوء ذلك يرى الباحث أن هذه المادة تُبرز الخط الفاصل بين الجرائم المعلوماتية التقليدية والجرائم السيبرانية ذات الطبيعة السيادية، إذ إن استهداف الأنظمة الحكومية أو السيادية يُعد تهديدًا مباشرًا للأمن الوطني. وفي هذا الإطار، يُثمّن الباحث إدراج المنظم السعودي عقوبات مشددة تراعي جسامة الفعل وأثره في زعزعة الاستقرار العام، مما يعكس وعيًا تشريعيًا بخطورة الهجمات الرقمية الموجهة إلى مراكز القرار والبنية الأمنية للدولة.

٤) إنتاج أو تخزين أو نشر مواد رقمية تمس الأمن الوطني:

يعاقب النظام بالسجن مدة لا تزيد على خمس سنوات وبغرامة تصل إلى ثلاثة ملايين ريال على كل من أنتج أو نشر أو خزن أي مادة عبر الوسائط الإلكترونية، من شأنها تأليب الرأي العام أو تهديد السلم الاجتماعي أو دعم الجماعات الإرهابية[١١٨].

---

[١١٦] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة ٦، ٧.

[١١٧] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة ١/٧

[١١٨] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة ١/٦.

وفي ضوء ذلك يرى الباحث أن توسيع نطاق التجريم ليشمل الأفعال المعلوماتية المرتبطة بالإنتاج أو التخزين أو النشر يوفّر غطاءً قانونيًا مهمًا لحماية الأمن الوطني الرقمي، ويمنح الجهات المختصة القدرة على التدخل المبكر لملاحقة المحتوى التحريضي أو الداعم للإرهاب، حتى قبل تحقّق الضرر المادي المباشر، مما يعزز الطابع الوقائي للنظام.

٥) محاولة ارتكاب الجريمة المعلوماتية أو الشروع فيها:

يشمل نطاق التجريم في نظام مكافحة جرائم المعلوماتية الشروع في ارتكاب أي جريمة من الجرائم المنصوص عليها فيه، حيث نصت المادة العاشرة على أن: "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقرر"[١١٩].

ويعني ذلك أن المحاولة تُعد صورة من صور الركن المادي للجريمة الإلكترونية، وتُعامل بنظام العقوبة التقديرية حسب خطورة الفعل ومدى اقترابه من النتيجة التامة، وذلك بحسب ما تراه المحكمة المختصة من ظروف الواقعة وملابساتها.

وفي ضوء ذلك يرى الباحث أن إدراج الشروع ضمن الأفعال المعاقب عليها يُجسّد توجه المنظم السعودي في تبني سياسة جنائية استباقية، تعزز من كفاءة الحماية السيبرانية، وتتيح للمحكمة الجزائية المختصة مرونة تقديرية في الحكم، تتناسب مع طبيعة الفعل الإجرامي ومستوى تهديده، حتى لو لم يتحقق الضرر الكامل أو النتيجة الإجرامية التامة.

٦) مسؤولية الكيانات الاعتبارية عن الجرائم المعلوماتية:

يُجيز نظام مكافحة جرائم المعلوماتية تحميل المؤسسات والمنصات الرقمية المسؤولية الجنائية متى ثبت تورّطها في ارتكاب أو تسهيل أو التستّر على الجرائم السيبرانية. وقد نصّت المادة (١٣) من النظام على جواز الحكم بمصادرة الوسائل والأجهزة والبرامج المستخدمة، أو إغلاق الموقع الإلكتروني أو مكان تقديم الخدمة إغلاقًا نهائيًا أو مؤقتًا، إذا ثبت أن الجريمة ارتكبت بعلم مالك الجهة التقنية. كما يجوز فرض

[١١٩] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة ١٠.

(ISSN: 2537 - 0758)

العقوبات التبعية، مثل: الغرامة المالية، أو تعليق النشاط، أو سحب الترخيص، أو منع الجهة من مزاولة النشاط التقني نهائيًا أو مؤقتًا، وفقًا لما تقرره المحكمة المختصة[١٢٠].

وفي ضوء ذلك يرى الباحث أن تحميل الكيانات الاعتبارية المسؤولية الجنائية يعكس وعي المنظّم السعودي بخطورة البنية التحتية الرقمية، وما قد يترتب على تقصير المؤسسات التقنية من أضرار تمس الأمن الوطني والمجتمعي. كما أن منح المحكمة سلطة تقدير العقوبة التبعية يُحقق التوازن بين الردع والعقاب من جهة، ومراعاة مصلحة الاستثمار الرقمي من جهة أخرى.

٧) تجريم التحريض والمساعدة على الجريمة الإلكترونية:

"يُعاقب نظام مكافحة جرائم المعلوماتية كل من حرّض أو ساعد أو اتفق مع غيره على ارتكاب أي من الجرائم المعلوماتية، ويُعامل بالعقوبة المقررة للجريمة متى وقعت بناءً على ذلك التحريض أو المساعدة أو الاتفاق، كما يُعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة إذا لم تقع الجريمة الأصلية. وقد أكدت المادة (٩) من النظام على أن هذه المسؤولية تشمل كل من تورط بأي صورة، بما في ذلك مزودو الخدمة، وأصحاب المواقع، ومستخدمي الشبكات الرقمية متى ثبت علمهم بوقوع الفعل وقيامهم بأدوار مساعدة[١٢١].

وفي ضوء ذلك يرى الباحث أن التوسّع في تجريم التحريض والمساعدة يعكس توجه المنظّم السعودي نحو حماية الفضاء السيبراني من الجرائم المعقّدة التي تقوم على التعاون الخفي بين عدة أطراف. كما أن اعتبار مزودي الخدمة وأصحاب المواقع من المشمولين بالعقوبة متى ثبت علمهم، يرسخ مبدأ المسؤولية التشاركية، ويعزز الرقابة الذاتية في البيئة الرقمية.

ثالثًا: ظروف التشديد والتخفيف في الجريمة السيبرانية الإرهابية:

(١) ظروف التشديد في الجريمة السيبرانية الإرهابية:

تمنح الأنظمة السعودية المحكمة الجزائية المتخصصة سلطة تقدير العقوبة بين الحد الأدنى والأعلى وفقًا لظروف كل واقعة، ولكنها تُلزم– في حالات معينة– بتوقيع الحد الأعلى للعقوبة إذا توافرت ظروف مشددة محددة نظامًا. **وتتمثل هذه الظروف فيما يلي:**

---

[١٢٠] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة ١٣

[١٢١] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة ٩.

- إذا تم ارتكاب الجريمة من خلال عصابة منظمة.
- إذا استُغل الجاني منصبه العام أو نفوذه أو سلطته الوظيفية لتنفيذ الجريمة.
- إذا استُخدم في ارتكاب الجريمة القُصَّر أو من في حكمهم.
- إذا كان للجاني سوابق جنائية في جرائم مماثلة.
- إذا اقترنت الجريمة باستخدام وسائل إلكترونية معقدة أو تمويه رقمي أضفى عليها طابعًا خفيًا يصعب اكتشافه.

وقد نصت على هذه الآلية المادة الثامنة من نظام مكافحة جرائم المعلوماتية، التي قررت رفع العقوبة تلقائيًا إلى نصف الحد الأعلى على الأقل متى توافرت هذه الظروف[١٢٢].

وفي ضوء ذلك يرى الباحث أن آلية التشديد تُظهر بُعدًا احترازيًا في المنظومة السعودية، إذ لا تُعاقب فقط على الجريمة بذاتها، بل تُحمّل الجاني تبعة أكبر إذا استخدم أدوات تضاعف من الأثر الإجرامي. كما أن ترك هامش التقدير للمحكمة يُراعي خصوصية كل واقعة، ويمنحها قدرة على التفرقة بين الحالات البسيطة والمُنظّمة.

(٢) ظروف التخفيف في العقوبة:

نصّت المادة الثامنة والخمسون من نظام مكافحة جرائم الإرهاب وتمويله على جواز تخفيف العقوبة في حال توفر ظروف معينة، بشرط ألا تقل العقوبة عن نصف الحد الأدنى المقرر لها، وذلك إذا قدّم الجاني معلومات نوعية ساعدت في منع وقوع الجريمة أو القبض على باقي المشاركين أو كشف الأدلة أو إضعاف الأثر الإجرامي. **ومن أبرز الحالات التي تمنح القاضي سلطة تخفيف الحكم ما يلي[١٢٣]:**

١. إذا بادر الجاني بالإبلاغ عن الجريمة قبل وقوعها أو أثناء التخطيط لها.
٢. إذا تعاون مع الجهات المختصة وأرشد إلى بقية المتهمين أو المتورطين في الشبكة الإرهابية.
٣. إذا أظهر ندمًا صادقًا وقدم اعترافًا تفصيليًا قبل صدور الحكم النهائي.
٤. إذا ساهمت المعلومات التي قدّمها في تجنيب الدولة أضرارًا أو خسائر محتملة.

---

[١٢٢] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة ٨.

[١٢٣] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ١٢، مادة ٥٦.

(ISSN: 2537 - 0758)

وقد قررت المادة ذاتها أن التخفيف مشروط بتقدير المحكمة، ويُراعى فيه مدى جدية التوبة، ومدى فعالية المعلومات المقدمة في حماية الأمن الوطني أو تفكيك التنظيم الإجرامي.

ويمكن القول إن هذه الظروف تُمنح سلطة تقديرها للقاضي وفقًا لملابسات الدعوى وخطورتها الأمنية[١٢٤].

وفي ضوء ذلك يرى الباحث أن منح المحكمة سلطة تخفيف العقوبة في جرائم الإرهاب السيبراني، رغم خطورتها، يعكس توازنًا دقيقًا بين الردع والحوافز القانونية للتعاون. ويُعد ذلك توجهًا ذكيًا من المنظّم السعودي، إذ يُوظف الأدوات الجنائية لمنع الجريمة قبل وقوعها عبر تشجيع التبليغ والتعاون، مما يُعزز الوقاية، ويدعم فعالية إنفاذ القانون في بيئات رقمية معقّدة يصعب اختراقها دون مساعدين داخليين.

رابعا: العقوبات التبعية والمصادرة وحجب المواقع الإلكترونية:

تُعد العقوبات التبعية من الوسائل القانونية الهامة التي يعتمد عليها النظام السعودي لتعزيز الردع العام والخاص، ولضمان عدم إفلات الجناة من الآثار المترتبة على جريمتهم، وحرمانهم من الاستفادة من الأدوات التي استُخدمت في تنفيذ الإرهاب السيبراني. ويُبرز نظاما مكافحة الإرهاب وتمويله، ومكافحة الجرائم المعلوماتية، العديد من التدابير التبعية التي تتميز بطابعها الفني والإجرائي، **والتي يمكن عرضها على النحو الآتي:**

(١) المصادرة القانونية للأموال والأدوات:

نص نظام مكافحة الإرهاب وتمويله على وجوب مصادرة جميع الأموال أو الوسائط أو الأدوات التي استُخدمت أو أُعدت للاستخدام في ارتكاب الجريمة الإرهابية، سواء تعلّق الأمر بأجهزة إلكترونية، أو برامج رقمية، أو حسابات مالية رقمية استخدمت في تمويل العمليات الإرهابية. وقد اعتبر النظام المصادرة إجراءً إلزاميًا في حال ثبت استخدام الوسيلة في الجريمة[١٢٥].

وفي ضوء ذلك يرى الباحث أن نظام مكافحة جرائم الإرهاب وتمويله قد أحسن حين قرّر وجوب المصادرة القانونية للوسائط الرقمية والأموال المرتبطة بالجريمة الإرهابية، لا

---

[١٢٤] كمال محمد عواد، الوسيط في النظام الجنائي السعودي، دار الإجادة، الرياض، ٢٠٢٠م، ص١٤٢.

[١٢٥] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ٥٨.

باعتبارها عقوبة إضافية، بل كإجراء ضروري لحماية الأمن الوطني من إعادة استخدام هذه الوسائل. ويُعد هذا التوجه مواكبًا لطبيعة الجرائم السيبرانية، التي تعتمد في تنفيذها على أدوات تقنية غير تقليدية، مثل العملات المشفرة، أو البنية الرقمية الموازية، مما يفرض على القضاء اتخاذ تدابير غير تقليدية لضمان الردع الفعلي وتجفيف منابع التهديد.

(٢) العقوبات التبعية على الأشخاص الاعتباريين:

يتضمن النظام إمكانية توقيع جزاءات على الشركات أو المنصات التقنية أو مزودي الخدمات الرقمية التي يثبت تواطؤها أو تقاعسها في منع ارتكاب الجريمة، وتتمثل هذه العقوبات في تعليق الترخيص، أو إغلاق المنشأة، أو فرض رقابة حكومية مشددة، أو تغريمها بمبالغ مالية كبيرة. وتُعد هذه التدابير ضرورية في ضوء التوسع العالمي في استخدام المنصات الرقمية لأغراض إرهابية[١٢٦].

وفي ضوء ذلك، يرى الباحث أن العقوبات التبعية المقررة على الأشخاص الاعتباريين تُعد خطوة متقدمة في مواجهة البنية التحتية للجريمة السيبرانية الإرهابية، حيث لم يعد يكفي تتبع الأفراد فقط، بل بات من الضروري مساءلة الكيانات التي وفّرت البيئة أو الوسيلة أو الغطاء. ويمثل ذلك تحولًا مهمًا من العقوبة الفردية إلى المسؤولية المؤسسية، خاصة في ظل ما تشهده الساحة الرقمية من تصاعد استخدام المنصات لأغراض دعائية وتمويلية إرهابية.

(٣) حجب المواقع الإلكترونية الضارة:

تمنح الأنظمة السعودية الجهات المختصة– كالهيئة الوطنية للأمن السيبراني، وهيئة الاتصالات والفضاء والتقنية– صلاحيات فورية في حجب المواقع الإلكترونية التي تُستخدم لأغراض إرهابية، مثل نشر الفكر المتطرف، أو جمع التبرعات، أو التنسيق بين عناصر التنظيمات، أو الترويج للأعمال الإرهابية. وقد تضمّنت السياسات الفنية المعتمدة آلية تقنية للحجب الاستباقي دون اشتراط إذن قضائي فوري في الحالات العاجلة، حفاظًا على الأمن الوطني.

---

[١٢٦] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ، مادة ٤٩.

(ISSN: 2537 - 0758)

تُستمد هذه الصلاحية من المواد التنفيذية واللوائح الصادرة عن الهيئة الوطنية للأمن السيبراني، وهيئة الاتصالات والفضاء والتقنية، والمستندة إلى أحكام نظام مكافحة الإرهاب وتمويله[١٢٧]، ونظام مكافحة جرائم المعلوماتية[١٢٨].

وفي ضوء ذلك، يرى الباحث أن منح الجهات المختصة صلاحية الحجب الفوري للمواقع الإلكترونية ذات الطابع الإرهابي يُجسّد مبدأ "الاستجابة الوقائية" في البيئة السيبرانية، ويعكس إدراك المنظم السعودي لخطورة التأخير في هذا النوع من الجرائم، التي تتسم بسرعة الانتشار والتأثير. كما أن تمكين الهيئات التقنية من التصرف الفوري يعزز من كفاءة المنظومة الأمنية الرقمية دون أن يُخل بحقوق المتقاضين، طالما أن هذه الإجراءات تخضع لاحقًا للرقابة القضائية أو التنظيمية.

(٤) إتلاف البرمجيات والبيانات المحظورة:

يجوز للمحكمة، بناءً على توصية الجهات الأمنية المختصة، إصدار قرار بإتلاف أو حذف أو تعطيل البيانات الرقمية أو البرمجيات الضارة التي تُشكّل خطرًا إرهابيًا محققًا، وذلك بموجب إشراف مباشر من الهيئة الوطنية للأمن السيبراني أو الجهات الفنية المماثلة. ويُعد هذا التدبير من أبرز صور حماية الفضاء السيبراني من إعادة تفعيل الجريمة[١٢٩].

وفي ضوء ذلك، يرى الباحث أن تمكين المحكمة من إصدار قرارات بإتلاف البرمجيات والبيانات الضارة يُعدّ إجراءً وقائيًا ضروريًا في مواجهة الجرائم الإرهابية السيبرانية، خاصة في ظل سهولة إعادة تفعيل الأدوات الرقمية عبر النسخ أو التشفير أو النشر المتكرر. كما يُسهم هذا الإجراء في منع العودة لارتكاب الجريمة، ويُقلّل من احتمالية تسريب محتوى خطر إلى بيئات رقمية جديدة. ويشترط في هذا التدبير أن يتم

---

[١٢٧] نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١)، ١٤٣٩هـ.

[١٢٨] نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨هـ، مادة١٤، والتي تنص على "تتولى هيئة الاتصالات وتقنية المعلومات وفقًا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة".

[١٢٩] هذا الإجراء يندرج ضمن صلاحيات القضاء الواردة ضمن نظام مكافحة جرائم الإرهاب وتمويله، لاسيما في المواد (٥٨) و (٦١)، التي تُجيز للمحكمة مصادرة أو إبطال الوسائط الرقمية أو منع التصرف فيها، متى ثبت ارتباطها بالجريمة الإرهابية أو استخدامها في تنفيذها.

تحت إشراف الجهات الفنية الرسمية المختصة لضمان سلامة التنفيذ وضبط الحذف وفق المعايير التقنية الدقيقة.

(٥) نشر الأحكام القضائية:

أجاز نظام مكافحة الإرهاب للمحكمة المختصة أن تأمر بنشر الحكم النهائي الصادر في جريمة إرهابية سيبرانية، على نفقة المحكوم عليه، في وسيلة إعلامية مناسبة، وذلك تعزيزًا لمبدأ الردع العام، وتحذيرًا من إعادة ارتكاب الجريمة، وحماية للمجتمع من تكرار السلوكيات الإرهابية[١٣٠].

وفي ضوء ذلك، يرى الباحث أن إجازة نشر الأحكام القضائية الصادرة في قضايا الإرهاب السيبراني تمثل أداة مهمة لتعزيز الردع العام، وإيصال رسالة قانونية واضحة بخطورة هذه الأفعال ونتائجها النظامية. كما يُسهم هذا النشر في رفع وعي المجتمع بالمخاطر الرقمية، ويعكس التزام القضاء السعودي بالشفافية في التعامل مع الجرائم ذات الطابع الأمني الحساس، خاصة حين يكون الفعل الإجرامي قد أُرتكب عبر فضاء مفتوح مثل الإنترنت.

خامساً: المقارنة بين نظام مكافحة الإرهاب وتمويله ونظام مكافحة الجرائم المعلوماتية في العقوبات المقررة للإرهاب السيبراني

تُظهر الدراسة أن النظامين– نظام مكافحة الإرهاب وتمويله، ونظام مكافحة الجرائم المعلوماتية– يشتركان في بعض الأهداف المتعلقة بحماية الأمن الوطني من المخاطر السيبرانية، غير أن بينهما اختلافات جوهرية في نطاق التجريم، وطبيعة العقوبات، وظروف التشديد، **على النحو التالي:**

١. من حيث نطاق التجريم:

أ. نظام مكافحة الإرهاب وتمويله:

- يُعالج الأفعال ذات البُعد السياسي أو الأمني، ويُركّز على الأفعال التي تمس الأمن الوطني، أو تسعى إلى الإخلال بالنظام العام، أو ترويع السكان، أو تهديد استقرار الدولة.

---

[١٣٠] هذا الإجراء وارد في المادة (٤٩) من نظام مكافحة جرائم الإرهاب وتمويله، والتي خوّلت المحكمة المختصة صلاحية تضمين الحكم عقوبة النشر الإعلامي، بعد أن يكتسب الحكم الصفة القطعية، على نفقة المحكوم عليه، وفي وسيلة إعلامية تُحدَّد بحسب طبيعة الجريمة ومكان ارتكابها.

(ISSN: 2537 - 0758)

- ويشمل ذلك: التخطيط لعمليات إرهابية عبر الإنترنت، تمويل الإرهاب الرقمي، التحريض على العنف أو التطرف، والتواصل مع الجماعات الإرهابية الإلكترونية.

ب. نظام مكافحة الجرائم المعلوماتية:

- يركز على حماية البنية التحتية المعلوماتية، والحقوق الرقمية للأفراد والجهات، ويُعالج الاختراق، والاحتيال الإلكتروني، والتشهير، والمس بالحياة الخاصة، والدخول غير المشروع على الشبكات، دون اشتراط وجود قصد إرهابي.

النتيجة: نظام مكافحة الإرهاب أوسع في حالات الإرهاب السيبراني، بينما يُعتبر نظام الجرائم المعلوماتية مكملًا له في حالة غياب النية الإرهابية.

٢. من حيث العقوبات الأصلية:

أ. نظام مكافحة الإرهاب وتمويله:

- يُقرّ عقوبات مغلّظة قد تصل إلى الإعدام أو السجن المؤبد، خاصة إذا اقترنت الجريمة بوقوع وفيات أو تهديد المنشآت السيادية، أو إن كانت عبر منظمات إرهابية عابرة للحدود.

ب. نظام مكافحة الجرائم المعلوماتية:

- تتراوح العقوبات بين السجن من سنة إلى عشر سنوات، وغرامات مالية تصل إلى خمسة ملايين ريال، وفقًا لجسامة الفعل وطبيعته (مثل الاختراق، أو إنتاج مواد تحضّ على الإرهاب، أو المساس بالأمن العام).

النتيجة: نظام الإرهاب أشد من حيث العقوبات، ويُفترض تطبيقه إذا ثبت القصد الإرهابي، فيما يُطبق نظام الجرائم المعلوماتية على الجرائم التقنية غير المرتبطة بالإرهاب.

٣. من حيث ظروف التشديد:

- **نظام الإرهاب:** يُشدد العقوبة في حالات ارتكاب الجريمة من خلال شبكة معلوماتية، أو إذا تم تمويلها بوسائل رقمية، أو إذا كان الفاعل جزءًا من تنظيم إرهابي.
- **نظام الجرائم المعلوماتية:** يُشدد العقوبة إذا ارتُكبت الجريمة من خلال جهة منظمة، أو استُخدمت في إطار الابتزاز، أو المساس بالأمن، أو الإساءة للهيئات الحكومية.

النتيجة: كلا النظامين يُقرّ ظروفًا مشددة، إلا أن نظام مكافحة الإرهاب يتعامل مع هذه الظروف كأسباب للانتقال إلى العقوبة الأشد تلقائيًا.

٤. من حيث العقوبات التبعية:

- **نظام الإرهاب:** يُجيز مصادرة الأدوات، حجب المواقع، إغلاق المنصات، شطب التراخيص، والمنع من السفر أو ممارسة النشاط.
- **نظام الجرائم المعلوماتية:** يُقرّ المصادرة، وحجب المحتوى، ومنع النشاط التقني، لكن بدرجة أقل من حيث القوة التنفيذية، وتُمارس غالبًا من قبل الجهات التنفيذية أو القضائية الإدارية.

النتيجة: العقوبات التبعية في نظام الإرهاب أشمل وأوسع نطاقًا، نظرًا لطبيعة الجريمة المرتبطة بالأمن القومي.

٥. من حيث الشروع والمساهمة:

- **نظام الإرهاب:** يُعاقب على الشروع بذات العقوبة أو أقل، ويُعاقب المحرض والمساعد والوسيط بشكل متساوٍ مع الفاعل الأصلي إن ثبت القصد الإرهابي المشترك.
- **نظام الجرائم المعلوماتية:** يُعاقب على المساهمة والشروع بالعقوبات المخففة نسبيًا، مع مراعاة جسامة الفعل وعدم اشتراط القصد الخاص.

النتيجة: نظام الإرهاب أشد في تقدير العقوبة على الشروع والمساهمة، ويُعامل كل متدخل باعتباره جزءًا من المنظومة الإرهابية.

ومما سبق يمكن القول إن نظام مكافحة الإرهاب وتمويله هو الأداة القانونية الأساسية لمكافحة الإرهاب السيبراني، خاصة عند اقتران الأفعال التقنية بالقصد الإجرامي الخاص، بينما يشكّل نظام الجرائم المعلوماتية سندًا تكميليًا للتعامل مع الجرائم الإلكترونية ذات الطابع الجنائي العام غير المرتبط بالأمن الوطني.

المطلب الثاني

إجراءات الضبط الجنائي والإشكاليات العملية في إنفاذ القانون في جرائم الإرهاب السيبراني

تُعد الإجراءات الجنائية حجر الأساس في تمكين الدولة من ضبط الجرائم والتحقيق فيها وملاحقة مرتكبيها، ولا سيما في الجرائم ذات الطبيعة المعقدة مثل الإرهاب السيبراني، الذي يتطلب قدرًا عاليًا من التنسيق التقني والقانوني. وقد أدرك النظام السعودي خطورة هذه الجرائم مبكرًا، فعمل على تطوير بيئة تشريعية ومؤسسية تُعزز من

(ISSN: 2537 - 0758)

فاعلية الضبط الجنائي، مع اعتماد وسائل خاصة تتلاءم مع الطابع الرقمي للجريمة. وبالرغم من الجهود المبذولة، لا تزال هناك تحديات عملية تتعلق بإثبات الجريمة، وتقدير القصد الجنائي، ومشكلات التكييف، وتحديد الاختصاص، مما يفرض ضرورة دراسة معمقة لهذه الإجراءات واستجلاء مواطن القوة والقصور فيها.

ويمكن تقسيم هذا المطلب إلى الفرعين التاليين:

الفرع الأول: الجهات المؤسسية المختصة بمكافحة الإرهاب السيبراني.

الفرع الثاني: الإجراءات الجنائية الخاصة بضبط جرائم الإرهاب السيبراني والإشكاليات العملية في إنفاذ القانون.

الفرع الأول

الجهات المؤسسية المختصة بمكافحة الإرهاب السيبراني

تتعدد الجهات الحكومية في المملكة العربية السعودية التي تتولى مهام مكافحة جريمة الإرهاب السيبراني، نظرًا لتعدد أبعاده الأمنية والتقنية والتشريعية. وتُعد هذه الجهات جزءًا من منظومة وطنية متكاملة تهدف إلى حماية الأمن السيبراني من المخاطر ذات الطابع الإرهابي، عبر أدوار متنوعة تشمل المراقبة والضبط والتشريع والتحليل الفني. ويعكس هذا التنوع المؤسسي إدراك المملكة لأهمية التنسيق بين المؤسسات ذات العلاقة لضمان فاعلية المواجهة. **وسوف يتم بيان أبرز هذه الجهات وتحليل مهامها النظامية على النحو التالي:**

أولاً: دور رئاسة أمن الدولة في حماية الأمن السيبراني:

تعد رئاسة أمن الدولة من أبرز الجهات الأمنية المختصة التي تتولى حماية الأمن الوطني في المملكة العربية السعودية، حيث تشمل مهامها مواجهة جميع أنواع التهديدات الأمنية بما فيها التهديدات السيبرانية. تضطلع رئاسة أمن الدولة بدور رئيس في تحديد الاستراتيجيات الأمنية السيبرانية، وتنسيق الجهود بين القطاعات الأمنية المختلفة بهدف التصدي للهجمات الإلكترونية والإرهاب السيبراني على وجه الخصوص[١٣١].

---

[١٣١] المنصة الوطنية للخدمات الحكومية، الأمن السيبراني في المملكة العربية السعودية، متاح على https://my.gov.sa/en/wps/portal/snp/content/cybersecurity تاريخ الإطلاع ١٤٤٦/٩/١١هـ الساعة ٩ مساءا.

وفي سبيل تحقيق الأمن السيبراني الشامل، تعمل رئاسة أمن الدولة على توفير منظومة أمنية متكاملة ومتطورة تعتمد على التكنولوجيا الحديثة في رصد التهديدات وتحليلها، ومن ثم وضع الآليات والخطط الاستباقية للحد من المخاطر الإلكترونية. كما تسعى إلى تعزيز التعاون الأمني بين المؤسسات الحكومية لتعزيز القدرة على التصدي لهذه الهجمات بفاعلية وسرعة استجابة عالية.

وتسهم رئاسة أمن الدولة بشكل مستمر في التوعية الأمنية من خلال حملات إعلامية وتثقيفية واسعة النطاق، تستهدف كافة شرائح المجتمع، وذلك بهدف رفع مستوى الوعي العام بأهمية الأمن السيبراني، وتزويد المواطنين بالمعرفة اللازمة لتجنب الوقوع ضحايا للجرائم الإلكترونية، مما يؤدي إلى تقليل الأضرار المحتملة وتعزيز الأمن الوطني السعودي بشكل عام[١٣٢].

ولا يقتصر دور رئاسة أمن الدولة على الجانب الوقائي فقط، بل تعمل رئاسة أمن الدولة من خلال وحداتها التقنية والاستخباراتية المتخصصة على مراقبة التهديدات السيبرانية ذات الطابع الإرهابي، سواء تلك التي تستهدف البنية التحتية أو التي تُدار من داخل المملكة أو خارجها. وتشمل جهودها التنسيق مع الهيئة الوطنية للأمن السيبراني، ووزارة الداخلية، والنيابة العامة لضمان شمولية الاستجابة الأمنية والتحقيقات. وتُسهم الرئاسة في إدارة البلاغات الإلكترونية والتحقيق في الهجمات التي تُصنف ضمن التهديدات الوطنية الخطيرة، بالإضافة إلى تنفيذ عمليات أمنية مشتركة لضبط الخلايا الإرهابية الإلكترونية، ومواجهة التهديدات الاستباقية في ضوء المعلومات الاستخباراتية.

ومما سبق يرى الباحث أن رئاسة أمن الدولة السعودية تعد من المؤسسات الأمنية المحورية في مواجهة الإرهاب السيبراني، وأن دورها في تعزيز الإجراءات الوقائية والتنسيق بين الجهات الأمنية المختلفة يمثل ركيزة أساسية من ركائز الأمن الوطني في المملكة، كما أنها تُعد حجر الزاوية في تنسيق الجهود الاستخباراتية والأمنية لمكافحة الإرهاب السيبراني، من خلال ما تملكه من صلاحيات وموارد متقدمة.

ثانيًا: دور وزارة الداخلية السعودية في مكافحة الإرهاب السيبراني:

تؤدي وزارة الداخلية السعودية دورًا بارزًا وأساسيًا في منظومة الأمن الوطني للمملكة، لا سيما في مواجهة الجرائم والإرهاب السيبراني، وذلك من خلال تنفيذ مهامها الأمنية

[١٣٢] هيئة الاتصالات والفضاء والتقنية، التقرير السنوي، الرياض، ٢٠٢٢، ص ١١٤

(ISSN: 2537 - 0758)

الواسعة التي تشمل الوقاية والاستجابة للهجمات الإلكترونية. إذ تقوم الوزارة بتنسيق الجهود الأمنية الوطنية لمكافحة الإرهاب السيبراني، عبر متابعة ورصد التهديدات التي قد تؤثر على أمن المعلومات أو تستهدف البنى التحتية الوطنية، والعمل على اتخاذ الإجراءات الأمنية اللازمة لصدّ تلك الهجمات أو التقليل من آثارها(١٣٣).

وتستند الوزارة في جهودها إلى نظام مكافحة جرائم المعلوماتية السعودي، الذي يوفر لها إطارًا قانونيًا واضحًا للتعامل مع التهديدات الإرهابية السيبرانية، ويحدد العقوبات والإجراءات الجزائية التي يجب تطبيقها على مرتكبي هذه الجرائم، وهو ما يعزز من قدرة الوزارة على حماية الأمن السيبراني، ويزيد من فعالية الإجراءات الأمنية والقانونية التي تتخذها ضد الإرهابيين الإلكترونيين.

وتعمل وزارة الداخلية أيضًا على تعزيز البنية التحتية الأمنية التقنية التي تساعد في التصدي للجرائم الإلكترونية من خلال تطوير القدرات التقنية لكوادر الوزارة، وتحديث أدوات الرصد والتحليل والبرامج الأمنية المستخدمة في الكشف المبكر عن محاولات الاختراق أو الهجوم الإلكتروني. وتأتي هذه الإجراءات في إطار استراتيجية الوزارة لمواكبة التطور التقني في مجال الجرائم الإلكترونية والإرهاب السيبراني(١٣٤) .

ويدل ذلك على إن وزارة الداخلية السعودية تضطلع بدور جوهري يجمع بين الوقاية التقنية، والتدخل الأمني، والتأطير القانوني في مواجهة الجرائم السيبرانية الإرهابية.

كما تولي وزارة الداخلية السعودية اهتمامًا خاصًا بالتوعية الأمنية والمجتمعية من مخاطر الإرهاب السيبراني، عبر تنفيذ حملات تثقيفية تهدف إلى رفع مستوى الوعي العام بين المواطنين والمقيمين، وتعريفهم بأهمية الحفاظ على أمنهم الرقمي، وتوضيح السبل والإجراءات الواجب اتخاذها لتجنب الوقوع ضحية لهذه الجرائم، مما يقلل من احتمالات تعرضهم لتهديدات إلكترونية خطيرة(١٣٥) .

---

(١٣٣) صالح بن علي، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، ٢٠١٩م، ص ٢٨.

(١٣٤) هيئة الاتصالات والفضاء والتقنية، التقرير السنوي لهيئة الاتصالات والفضاء والتقنية، الرياض، ٢٠٢٢، ص ٤١.

(١٣٥) وزارة الداخلية: وزارة الداخلية بالتعاون مع الهيئة الوطنية للأمن السيبراني تنظم جلسات توعوية في مجال الأمن السيبراني، ١٤٤٤هـ، متاح على:https://tinyurl.com/yrd4pm8s تاريخ الإطلاع ١٤٤٦/٩/١١هـ الساعة ٩ مساءا.

ومن أجل تعزيز الاستجابة السريعة للتهديدات الإرهابية الإلكترونية، تعتمد وزارة الداخلية على التعاون والتنسيق مع مختلف الجهات الأمنية المختصة في المملكة، بما فيها الهيئة الوطنية للأمن السيبراني، مما يسهم في سرعة تبادل المعلومات والاستجابة للحوادث السيبرانية بشكل فعال، ويؤدي إلى توفير حماية أكبر للمؤسسات الوطنية والبنية التحتية الحساسة من الهجمات الإرهابية السيبرانية.

ومما سبق يرى الباحث أن وزارة الداخلية السعودية تتخذ إجراءات مدروسة ومنظمة في مجال مكافحة الإرهاب السيبراني، وتتميز بفاعلية استراتيجيتها الوقائية والقانونية، التي تساهم بشكل واضح في تعزيز الأمن الوطني السيبراني. كما يوصي الباحث بأهمية مواصلة الوزارة جهودها لتطوير الأدوات التقنية والتنسيق المستمر مع مختلف الجهات ذات العلاقة لتعزيز القدرات الأمنية ضد التهديدات السيبرانية المتزايدة.

ثالثـاً: دور الهيئـة الوطنيـة للأمـن السـيبراني السـعودية في تعزيـز الإجراءات الوقائية:

تُعد الهيئة الوطنية للأمن السيبراني الجهة التنظيمية العليا المسؤولة عن صياغة السياسات الوطنية للأمن السيبراني، والإشراف على تنفيذ الضوابط واللوائح التي تضمن الحماية الرقمية للمملكة. وقد أنيط بها بموجب "الاستراتيجية الوطنية للأمن السيبراني" مسؤوليات تشمل الوقاية من الهجمات السيبرانية، والاستجابة لها، وتقييم الجاهزية الوطنية.

وتقوم الهيئة بإصدار الضوابط الأساسية للأمن السيبراني التي تُطبق على كافة الجهات الحكومية والقطاعات الحيوية، كما تتولى تنسيق الجهود الوطنية للتصدي للتهديدات السيبرانية، وتقديم الدعم الفني في حالات الطوارئ الإلكترونية. وتُعد الهيئة مرجعًا فنيًا رئيسيًا في تصميم البنية المؤسسية الدفاعية ضد الهجمات الإرهابية الإلكترونية، وتُشارك أيضًا في بناء القدرات وتطوير الكفاءات الوطنية في المجال السيبراني[١٣٦].

حيث قامت الهيئة بمعالجة أكثر من ١٥٠٠ خطر سيبراني، وإغلاق أكثر من ١٤٠٠ من هذه المخاطر، بنسبة إغلاق وصلت إلى ٩٦%، ما يعكس كفاءة الهيئة في

[١٣٦] الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، المملكة العربية السعودية، ٢٠١٨م، ص ١٩.

(ISSN: 2537 - 0758)

إدارة ومواجهة التحديات الأمنية الرقمية، كما نظمت ست حملات توعوية وأكثر من ١٥٠٠ نشاط توعية لتعزيز الوعي بالأمن السيبراني بين موظفي القطاعات الحيوية، ما أسهم في رفع كفاءة الاستجابة والمواجهة للتهديدات السيبرانية المحتملة(١٣٧).

ومما سبق يمكن للباحث القول إن الهيئة تمثل الجهة الفنية الأولى في المملكة المسؤولة عن إنتاج المعرفة الوقائية، وتعميمها عبر أدوات إرشادية وتشريعية وتوعوية فعالة، كما أنها تمثل حجر الزاوية في تأمين الفضاء السيبراني السعودي، من خلال المبادرات التوعوية والإجراءات العملية في إدارة المخاطر.

رابعاً: دور وزارة الاتصالات وتقنية المعلومات السعودية في تطوير البنية التحتية التقنية للأمن السيبراني:

تساهم وزارة الاتصالات وتقنية المعلومات السعودية بشكل فعّال في تطوير البنية التحتية الرقمية، حيث نفذت عددًا من المشاريع والبرامج الرامية إلى فحص أمن شبكات الاتصالات، وإدارة الأزمات التقنية في حالات الطوارئ، وذلك ضمن استراتيجية وطنية تهدف إلى رفع جاهزية القطاع التقني في مواجهة الحوادث السيبرانية الحرجة(١٣٨).

وقد أعلنت الوزارة عن إطلاق "مركز الابتكار الرقمي" المتخصص في تقنيات الأمن السيبراني، ومبادرة "برنامج التقييم الوطني للأمن السيبراني للجهات الحكومية"، إلى جانب شراكات دولية لتعزيز أمن شبكات الاتصالات والمعلومات في المملكة. كما قامت بتدريب وتأهيل الكوادر الفنية، وتحديث البنية التحتية للاتصالات في القطاعين العام والخاص، بما يضمن المرونة الرقمية والقدرة على الصمود أمام الهجمات الإرهابية الإلكترونية.

وفي ضوء ذلك، يرى الباحث أن وزارة الاتصالات تُعدّ ركيزة أساسية في دعم البُعد الفني لمنظومة الأمن السيبراني، حيث تساهم في بناء قاعدة رقمية وطنية قادرة على الاستجابة الفورية لأي تهديد إرهابي يستهدف الفضاء الإلكتروني السعودي.

خامساً: دور النيابة العامة في ملاحقة الجرائم الإرهابية السيبرانية:

تُعد النيابة العامة في المملكة أحد أعمدة إنفاذ القانون، وتضطلع بدور رئيس في التحقيق في الجرائم السيبرانية ذات الطابع الإرهابي، وفقًا لنظام الإجراءات الجزائية

(١٣٧) هيئة الاتصالات والفضاء والتقنية، مرجع سابق، ص ١١٤

(١٣٨) هيئة الاتصالات والفضاء والتقنية، التقرير السنوي، الرياض، ٢٠٢٢، ص ٤٠.

ونظام مكافحة الجرائم المعلوماتية. وقد تم تدريب عدد من منسوبي النيابة على تقنيات التحقيق الرقمي، وتطوير وحدات متخصصة لتحليل البلاغات الإلكترونية. كما تُشارك النيابة في لجان تنسيقية مع الجهات الفنية لضمان سلامة الإجراءات وشرعية الأدلة[١٣٩].

في واقعة افتراضية، تَقدَّم أحد المواطنين ببلاغ إلى النيابة العامة عن نشاط مشبوه في أحد المواقع الإلكترونية التي تُروّج لأفكار متطرفة، وتستخدم برمجيات لتشفير المحادثات وجمع تبرعات عبر العملات الرقمية. قامت وحدة التحقيق الرقمي في النيابة العامة بتحليل البيانات الواردة من البلاغ بالتعاون مع هيئة الأمن السيبراني، ونجحت في تعقب مصدر الموقع وتحديد هوية القائم عليه، باستخدام تقنيات تتبع الشبكات المظلمة وتحليل سجلات الدخول. وبناء على نتائج التحقيق، تم إحالة المتهم إلى المحكمة الجزائية المتخصصة، مع تقديم تقرير فني مفصل يربط بين السلوك الرقمي والنية الإرهابية[١٤٠].

وفي ضوء ذلك، يرى الباحث أن هذا النموذج يُجسد الأدوار التخصصية المتقدمة التي تضطلع بها النيابة العامة، ويعكس تكامل التحقيقات الفنية مع الإجراءات النظامية، بما يعزز من كفاءة الدولة في ملاحقة مرتكبي الجرائم السيبرانية ذات البُعد الإرهابي في وقت مبكر، ويُرسّخ مفهوم الوقاية عبر الأدلة الرقمية.

- **التكامل بين وزارة الداخلية، وهيئة الاتصالات، والنيابة العامة:**

يلعب هذا التكامل دورًا أساسيًا في إنفاذ القانون ضد الإرهاب السيبراني، حيث تتشارك وزارة الداخلية، وهيئة الاتصالات والفضاء والتقنية، والنيابة العامة في أدوار تكاملية تُغطي سلسلة الإجراءات النظامية من الرصد إلى التحقيق ثم المحاكمة.

---

[١٣٩] زكي شناق، الوجيز في نظام الإجراءات الجزائية السعودي، الشقري للنشر، جدة، ط٢، ١٤٤١هـ، ص ٢١١.

[١٤٠] لجأ الباحث إلى المثال الافتراضي نظرًا لصعوبة الحصول على وقائع جنائية حقيقية مرتبطة بجرائم الإرهاب السيبراني في المملكة العربية السعودية، وذلك لما تتسم به هذه القضايا من خصوصية عالية، ولقصر تداولها ضمن نطاق المحكمة الجزائية المتخصصة والجهات الأمنية المعنية فقط، وعدم توفرها للنشر العام أو البحث الأكاديمي المفتوح .

(ISSN: 2537 - 0758)

حيث تتولى وزارة الداخلية عبر قطاعاتها الأمنية مسؤولية تنفيذ عمليات الضبط والقبض، فيما تقوم هيئة الاتصالات بوضع السياسات التنظيمية للقطاع التقني وضمان التزام الشركات بها، وتوفر الدعم الفني للجهات الضبطية. أما النيابة العامة، فهي المعنية بتقدير ملاءمة الدليل الرقمي، وتوجيه الاتهام، ومباشرة الدعوى العامة أمام المحكمة المختصة، وتُعد جهة رقابية على مشروعية الإجراءات الجنائية في هذا السياق(١٤١).

وفي واقعة افتراضية، رصدت وحدة المراقبة الفنية التابعة لهيئة الاتصالات نشاطًا مريبًا على خادم إلكتروني خارجي يستهدف منصات وطنية برسائل إلكترونية تتضمن برامج تجسس خبيثة. تم إحالة البلاغ إلى وزارة الداخلية، التي نفذت عملية ضبط أمني عاجل، بالتنسيق مع النيابة العامة التي أصدرت أمر قبض فوري، ثم تابعت الإجراءات حتى الإحالة إلى المحكمة المختصة(١٤٢).

وفي ضوء ذلك، يرى الباحث أن التنسيق الفعّال بين هذه الجهات يسهم في تعزيز الكفاءة النظامية، ويُقلل من التداخل أو التباطؤ الإجرائي، خاصة في قضايا تتطلب استجابة سريعة ودقيقة كالجرائم السيبرانية الإرهابية.

سادساً: مساهمة الجامعات السعودية ومراكز البحوث في مواجهة الإرهاب السيبراني:

تلعب الجامعات السعودية ومراكز البحوث دورًا بارزًا في تعزيز الأمن السيبراني من خلال التركيز على البحث العلمي والتطوير التقني في هذا المجال. حيث تقوم بالتعاون

(١٤١) وزارة الداخليةhttps://www.moi.gov.sa: تاريخ الإطلاع ١٤٤٦/١٠/١هـ، الساعة ٩ مساءً.
النيابة العامةhttps://www.pp.gov.sa: تاريخ الإطلاع ١٤٤٦/١٠/١هـ، الساعة ٩ مساءً.
هيئة الاتصالات والفضاء والتقنيةhttps://www.cst.gov.sa: تاريخ الإطلاع ١٤٤٦/١٠/١هـ، الساعة ٩ مساءً.

(١٤٢) لجأ الباحث إلى المثال الافتراضي نظرًا لصعوبة الحصول على وقائع جنائية حقيقية مرتبطة بجرائم الإرهاب السيبراني في المملكة العربية السعودية، وذلك لما تتسم به هذه القضايا من خصوصية عالية، ولقصر تداولها ضمن نطاق المحكمة الجزائية المتخصصة والجهات الأمنية المعنية فقط، وعدم توفرها للنشر العام أو البحث الأكاديمي المفتوح.

مع هيئة الاتصالات والفضاء والتقنية بدعم البحوث العلمية المبتكرة التي تهدف إلى التصدي للتهديدات السيبرانية[١٤٣].

ومن أمثلة ذلك دور جامعة نايف العربية للعلوم الأمنية، باعتبارها الجهاز العلمي لمجلس وزراء الداخلية العرب، والتي تلعب دورًا محوريًا في مواجهة الإرهاب السيبراني من خلال عدة محاور رئيسية:

١. **التعليم والتدريب المتخصص:** تقدم الجامعة برامج أكاديمية متقدمة، مثل ماجستير العلوم في الجرائم السيبرانية والتحقيق الجنائي، بهدف تأهيل الكوادر الأمنية بمهارات متقدمة في مجال الأمن السيبراني والتحقيقات الرقمية.
٢. **البحث العلمي والنشر:** من خلال دار جامعة نايف للنشر، تصدر الجامعة دراسات وتقارير متخصصة في مجال الجرائم السيبرانية، مثل[١٤٤]:
   - "الإرهاب السيبراني في المنطقتين الإفريقية والعربية: تقرير استقصائي من ورشة عمل جامعة نايف ومركز الأمم المتحدة لمكافحة الإرهاب"، والذي يقدم تحليلاً شاملاً للتهديدات السيبرانية في هذه المناطق.
٣. **ورش العمل والمؤتمرات:** تنظم الجامعة ورش عمل وملتقيات علمية لتعزيز القدرات في مجال التحليل الجنائي الرقمي ومكافحة الهجمات السيبرانية.
٤. **التعاون الدولي:** تسعى الجامعة لتعزيز التعاون مع المنظمات الدولية في مجالات مكافحة الإرهاب السيبراني، مما يساهم في تبادل الخبرات وتطوير استراتيجيات فعّالة لمواجهة هذه التهديدات.

هذه الجهود المتكاملة تعكس التزام الجامعة بتعزيز الأمن السيبراني ومكافحة الإرهاب الرقمي على المستويين الإقليمي والدولي.

ومما سبق يمكن للباحث القول إن مساهمة الجامعات السعودية أصبحت تمثل إحدى ركائز الأمن الوقائي، من خلال إعداد جيل مؤهل قادر على مجابهة تحديات الإرهاب السيبراني بأساليب علمية وتقنية متطورة.

---

[١٤٣] صالح بن علي، مرجع سابق، ص ٤١.

[١٤٤] جامعة نايف العربية للعلوم الأمنية، الجرائم السيبرانية، متاح على:
https://nup.nauss.edu.sa/index.php/sr/catalog/category/Cybercrimes?utm_source=chatgpt.com

(ISSN: 2537 - 0758)

الفرع الثاني
الإجراءات الجنائية الخاصة بضبط جرائم الإرهاب السيبراني

نظرًا لطبيعة الإرهاب السيبراني المعقدة، فإن ضبط هذا النوع من الجرائم يتطلب إجراءات جنائية دقيقة تستند إلى مزيج من القواعد النظامية والمعايير التقنية الحديثة. وتمثل مرحلة الضبط الجنائي نقطة انطلاق مهمة في سلسلة العدالة الجزائية، حيث تُبنى عليها صحة الأدلة الرقمية وشرعية التتبع الإجرامي.

وتزداد أهمية هذه الإجراءات مع تصاعد التحديات المرتبطة بجمع الأدلة الرقمية، وتفتيش الأجهزة والمواقع الإلكترونية، والحفاظ على حجيتها أمام المحاكم. لذا، يتعين على الجهات المختصة الالتزام بضوابط دقيقة تحفظ توازنًا بين حماية الحقوق والحريات، وتحقيق الأمن العام، **وسأوضح ذلك من خلال العناصر التالية:**

أولًا: الضبط والتفتيش في الجريمة السيبرانية وفق نظام الإجراءات الجزائية:

يشكل ضبط الجريمة السيبرانية المرحلة الأولية والحيوية في سياق الإجراءات الجنائية لملاحقة مرتكبي جرائم الإرهاب السيبراني، إذ ترتبط هذه المرحلة بآليات جمع الأدلة الرقمية، والتحفظ على البيانات، وضبط الأدوات التقنية المستخدمة في الجريمة، وهي مرحلة شديدة الحساسية نظرًا للطبيعة المتغيرة والقابلة للتلاعب للأدلة الإلكترونية.

وقد أرسى نظام الإجراءات الجزائية السعودي[١٤٥] مجموعة من القواعد الدقيقة لضمان مشروعية الضبط، ومن ذلك ما نصت عليه المادة (٢٤) التي عرّفت رجال الضبط الجنائي بأنهم الأشخاص المكلفون بالبحث عن الجرائم ومرتكبيها وجمع المعلومات اللازمة لذلك، كما بينت المادة (٢٦) الجهات المكلفة فعليًا بأعمال الضبط، ومنها: أعضاء النيابة العامة، ومديرو الشرطة، ومسؤولو مكافحة الجرائم المعلوماتية، وهو ما يُعد سندًا نظاميًا لمشروعية إجراء الضبط في القضايا السيبرانية.

---

[١٤٥] نظام الإجراءات الجزائية، الصادر بالمرسوم الملكي رقم (م/٢) بتاريخ ١٤٣٥/١/٢٢هـ، والمنشور في جريدة أم القرى بتاريخ ١٤٣٥/٢/٣هـ، المملكة العربية السعودية.

ويبدأ إجراء الضبط عادة بتلقي بلاغ رسمي، أو بناء على رصد تقني صادر عن جهة معنية[١٤٦]، مثل الهيئة الوطنية للأمن السيبراني، ليُحال إلى جهات الضبط الجنائي المختصة، كإدارات مكافحة الجرائم الإلكترونية، بشرط أن يتم ذلك من قِبل مأمور ضبط مختص ومخول قانونًا. وقد شددت المادة (٢) من النظام على أن القبض والتفتيش يجب ألا يتم إلا وفق الحالات المنصوص عليها نظامًا، كما أكدت على منع إيذاء المقبوض عليه جسديًا أو معنويًا، أو تعريضه لمعاملة مهينة للكرامة، وهي ضمانات أساسية في الجرائم السيبرانية التي قد تتسم بطول مدة الضبط الفني والتحقيق التقني.

أما فيما يخص دخول أماكن الجريمة، ومنها الأجهزة الإلكترونية أو المنصات الرقمية، فقد اشترطت المادة (٤١) أن يكون تفتيش المسكن أو ما في حكمه بموجب إذن كتابي من النيابة العامة، ما لم تكن هناك حالة تلبس. وينسحب ذلك على التفتيش الإلكتروني، بوصفه وسيلة للوصول إلى أدلة الجريمة، لا سيما في حالات تتبع مصادر الهجوم السيبراني أو أدوات تنفيذ الجريمة الرقمية[١٤٧].

وتُعد المادة (٣٣) ذات أهمية خاصة في هذا السياق، حيث أوجبت تحرير محاضر الضبط ووصف المضبوطات بدقة، بما يشمل الأجهزة والبرمجيات والبيانات الرقمية، مع توثيق الإجراءات الفنية التي تم اتخاذها لضمان سلامة الأدلة، ويُعد هذا المحضر من المستندات الرئيسة المعول عليها لاحقًا في مرحلة التحقيق والمحاكمة[١٤٨].

وقد تبنّى النظام مبدأ التدرج في الإجراءات، حيث نصت المادة (٢٧) على وجوب الإبلاغ الفوري من رجل الضبط الجنائي للنيابة العامة عند علمه بجريمة، وهو ما يسمح للنيابة بمتابعة مشروعية إجراءات الضبط، وإصدار الأوامر اللازمة، لا سيما في الجرائم التي تتطلب إذنًا خاصًا كالتفتيش الرقمي أو اعتراض البيانات[١٤٩].

ومما سبق يمكن للباحث القول إن مرحلة الضبط في الجرائم السيبرانية الإرهابية تتطلب فهمًا تقنيًا متقدمًا، مع التزام صارم بضوابط النظام الإجرائي، لا سيما ما يتعلق

---

[١٤٦] زكي محمد شناق، الوجيز في نظام الإجراءات الجزائية السعودي، الشقري للنشر، جدة، ط٢، ١٤٤١هـ، ص ١٢٣.

[١٤٧] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٤١.

[١٤٨] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٣٣.

[١٤٩] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٢٧.

(ISSN: 2537 - 0758)

بسلامة الأدلة وشرعية الوسائل المستخدمة في التحفظ عليها، وهو ما يوجب التعاون الوثيق بين الأجهزة الأمنية والتقنية والنيابة العامة، لتحقيق التوازن بين الفعالية الأمنية والضمانات القانونية.

ثانياً: تفتيش الأدلة الرقمية في جرائم الإرهاب السيبراني:

يشكل التفتيش الرقمي للأدلة مرحلة محورية في الإجراءات الجنائية الخاصة بضبط جريمة الإرهاب السيبراني، نظرًا لارتباطها الوثيق بالحصول على الأدلة الإلكترونية المخزنة في أجهزة أو مواقع أو شبكات رقمية، والتي غالبًا ما تكون عرضة للإخفاء أو الإتلاف أو النقل اللحظي. وقد نظم نظام الإجراءات الجزائية السعودي أحكام التفتيش بدقة، مؤكدًا ضرورة احترام الحقوق الدستورية للفرد الواردة بالنظام الأساسي للحكم[١٥٠]، ومراعاة ضوابط المشروعية الإجرائية.

ويبدأ التفتيش عادة بعد مرحلة الضبط المبدئي، حين تتوفر قرائن جدية على أن الدليل الرقمي موجود في مسكن أو جهاز أو حساب إلكتروني مرتبط بالمشتبه فيه. وقد نصت المادة الثانية والأربعون من النظام على أنه "لا يجوز لرجل الضبط الجنائي الدخول إلى أي مكان مسكون أو تفتيشه إلا في الأحوال المنصوص عليها نظامًا، وبأمر مسبب من هيئة التحقيق والادعاء العام"، مما يجعل إذن التفتيش شرطًا جوهريًا ما لم توجد حالة تلبس.

وتُعد الأجهزة الرقمية أو الحواسيب أو الحسابات السحابية جزءًا من "الأشياء الخاصة بالجريمة" التي يجوز تفتيشها وفق المادة السادسة والأربعين، شريطة أن يكون الغرض منها جمع معلومات عن الجريمة محل التحقيق. وإذا ظهرت أثناء التفتيش جرائم أخرى، يجوز ضبط أدلتها عرضًا. أما إذا تعلق الأمر بتفتيش أشخاص أو متعلقات شخصية، فيجب أن يتم ذلك ضمن شروط المادة الثالثة والأربعين، وبالأخص إذا كانت المتهمة امرأة، وجب أن يُندب للتفتيش امرأة[١٥١].

---

[١٥٠] النظام الأساسي للحكم، الصادر بالأمر الملكي رقم (أ/٩٠) بتاريخ ١٤١٢/٨/٢٧هـ، والمنشور في جريدة أم القرى، السنة ٦٩، العدد ٣٣٩٧، بتاريخ الجمعة ١ رمضان ١٤١٢هـ الموافق ٦ مارس ١٩٩٢م، مكة المكرمة، المملكة العربية السعودية.

[١٥١] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٤٦.

أما تفتيش المساكن، فقد قيدته المادة الرابعة والأربعون بجوازه في حال التلبس فقط، إذا توفرت أمارات قوية على وجود ما يفيد في كشف الحقيقة داخل المسكن. كما تنص المادة الخامسة والأربعون على أنه إذا قامت قرائن ضد شخص حاضر أثناء التفتيش، جاز تفتيشه أيضًا. وتشدد المادة الخامسة والخمسون على عدم جواز تفتيش غير المتهم أو مسكن غير مسكنه، إلا بقرائن قوية على إفادة التفتيش للتحقيق[١٥٢].

وقد اهتم النظام بضمان توثيق الإجراءات، فأوجبت المادة الثامنة والأربعون تدوين محضر مفصل يشتمل على بيانات من أجرى التفتيش، وتاريخ وساعة التفتيش، ووصف الموجودات المضبوطة، مع توقيع الحاضرين. ويجب وفق المادة السابعة والأربعون أن يتم التفتيش بحضور صاحب المسكن أو من ينيبه، أو شاهدين حال تعذر ذلك[١٥٣].

كما أن الرسائل الرقمية، والمكالمات المشفّرة، والبريد الإلكتروني، تخضع لحماية النظام بموجب المادة السادسة والخمسين، فلا يجوز مراقبتها أو الاطلاع عليها إلا بإذن مسبب ولمدة محددة من الجهة المختصة، بينما تمنح المادة السابعة والخمسون للنائب العام دون غيره صلاحية الإذن بمراقبة لمدة محددة لهذه الوسائل متى كان لذلك فائدة في إظهار الحقيقة[١٥٤].

وقد نصت المادة الخمسون على أن يُحرز كل ما يُضبط في التفتيش في حرز محكم مع ذكر بيانات الضبط، وتُحفظ في أماكن خاصة تابعة لجهة الضبط، وتخضع لرقابة النيابة العامة. كما أوجبت المادة الحادية والستون على كل من اطلع على مضبوطات أثناء التفتيش أن يحافظ على سريتها، وألا ينتفع بها بأي طريقة[١٥٥].

ومما سبق يمكن للباحث القول إن تفتيش الأدلة الرقمية في جريمة الإرهاب السيبراني يخضع لضوابط صارمة تضمن موازنة دقيقة بين مصلحة التحقيق الجنائي من جهة، وحقوق الأفراد الرقمية من جهة أخرى، وهو ما يعكس احترافية النظام السعودي في مواكبة تطورات الجريمة الإلكترونية وتقنين آليات مكافحتها.

---

[١٥٢] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٤٤.

[١٥٣] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٤١.

[١٥٤] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مواد ٤٧، ٤٨..

[١٥٥] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٥٠.

(ISSN: 2537 - 0758)

أما عن الوسائل الفنية المعتمدة في التفتيش الإلكتروني:

يفرض الواقع السيبراني استخدام أدوات تقنية متقدمة لتنفيذ التفتيش، مثل برمجيات تحليل الأدلة الرقمية، وأنظمة استعادة البيانات، وأجهزة التصوير الجنائي الرقمي (Forensic Imaging)، وينبغي أن يكون مأمور الضبط ملمًّا بهذه الوسائل أو يعمل ضمن فريق متخصص يشرف على العملية، حتى لا تُمس الأدلة أو تتعرض للتلف أو التلاعب.

كما يجب أن يتم التفتيش في بيئة محكمة، وتحت إشراف جهة قضائية أو أمنية مختصة، مع مراعاة السجلات الإلكترونية وحقوق أطراف ثالثة قد تكون بياناتهم مخزنة بالجهاز محل التفتيش. وينبغي اعتماد تقارير فنية مؤيدة من خبراء معتمدين، لتدعيم مشروعية النتائج[١٥٦].

وبالنسبة للتوثيق الإجرائي لمخرجات التفتيش:

يشترط النظام تحرير محضر تفتيش مفصل يشمل توقيت البدء والانتهاء، وصف دقيق للمعلومات المضبوطة، حالة الجهاز، الإجراءات الفنية المستخدمة، وأسماء المنفذين. وقد أكدت المادة (٦٩) على ضرورة تسليم نسخة من المحضر إلى المتهم أو من يمثله، لضمان الشفافية وحفظ الحقوق. ويُستخدم هذا المحضر لاحقًا كأساس في التحقيقات، وهو ما يستوجب صياغته وفق الأصول الفنية والنظامية[١٥٧].

ومما سبق يمكن للباحث القول إن تفتيش الأجهزة الإلكترونية في الجرائم السيبرانية يخضع لضوابط صارمة لحماية الخصوصية وضمان العدالة، ويُعد ركيزة إجرائية أساسية تتطلب توافر الإذن القانوني، والمهنية الفنية، والتوثيق النظامي الدقيق.

ثالثًا: آليات جمع الأدلة الرقمية واعتمادها قضائيا:

تُعد مرحلة جمع الأدلة الرقمية من أدق مراحل التحقيق في جرائم الإرهاب السيبراني، لما تتسم به هذه الأدلة من طبيعة غير تقليدية، وسهولة إتلافها أو تعديلها أو فقدانها إذا لم تُجمع وفق ضوابط علمية دقيقة. وقد أكد الفقه النظامي السعودي على أن حجية الأدلة الرقمية لا تنشأ من طبيعتها، وإنما من طريقة جمعها وحفظها وتقديمها وفقًا لقواعد الإثبات والإجراءات الجزائية.

---

[١٥٦] زكي شناق، مرجع سابق، ص ٣٥٦

[١٥٧] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٦٩.

ويُشترط في الأدلة الرقمية أن تُجمع من قبل جهات مختصة مثل فرق الاستجابة للحوادث السيبرانية، أو إدارة الأدلة الرقمية بالأجهزة الأمنية، باستخدام أدوات وبرامج تضمن الحفاظ على البصمة الرقمية (Digital Hash)، مما يتيح إثبات سلامة الملفات وصحة مصدرها عند الطعن عليها لاحقًا[١٥٨].

وتُحفظ هذه الأدلة في وحدات تخزين محمية (Forensic Images) مع تسجيل كافة العمليات التقنية التي أجريت عليها في سجل خاص يُرفق بالتقرير الفني النهائي. كما يجب إرفاق توقيع إلكتروني معتمد على التقرير، وإحالة الأدلة إلى النيابة العامة مختومة بختم فني يضمن تمام الحماية[١٥٩].

كما ألزمت المادة (٤٦) من نظام الإجراءات الجزائية بأن يقتصر التفتيش على الأدلة المتعلقة بالجريمة محل التحقيق، وفي حال تم العثور على أدوات أو بيانات تمثل جريمة أخرى، يجب ضبطها وتوثيقها في محضر مستقل. وأكدت المادة (٤٨) على ضرورة تحرير محضر مفصل يشمل توقيت التفتيش، وهوية المنفذين، ووصف الموجودات المضبوطة، والإجراءات التقنية المستخدمة[١٦٠].

ويُراعى عند تحليل الأجهزة والأنظمة الإلكترونية الاستعانة بخبراء مختصين معتمدين لدى الجهات القضائية أو الأمنية، على أن تُوثق النتائج بتقارير فنية رسمية ترفق بمحاضر الضبط لتأكيد حجية الدليل الرقمي، وتهيئته للعرض أمام المحكمة المختصة[١٦١].

ويرى الباحث أن بناء قضية ناجحة في جريمة إرهاب سيبراني مرهون بكفاءة الأدلة الرقمية وجودة تقرير الخبير، وهو ما يفرض ضرورة وجود معايير وطنية موحدة لجمع وتحليل هذه الأدلة، وتوفير معامل جنائية رقمية معتمدة.

---

[١٥٨] عبد العزيز غرم الله، جرائم الإنترنت وعقوباتها، دار الكتاب الجامعي، الرياض، ١٤٣٨هـ، ص٢٣٩

[١٥٩] زكي شناق، الوجيز في نظام الإجراءات الجزائية السعودي، الشقري للنشر، جدة، ط٢، ١٤٤١هـ، ص ١٣٤.

[١٦٠] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مواد ٤٩، ٤٨.

[١٦١] السيد شريف، مرجع سابق، ص ١٩٢.

(ISSN: 2537 - 0758)

رابعاً: التوثيق الإجرائي لمخرجات التفتيش:

يشترط النظام أن يتم توثيق نتائج التفتيش تفصيلًا في محضر رسمي يُعد جزءًا أساسيًا من ملف القضية. ويجب أن يشمل هذا المحضر معلومات دقيقة حول توقيت بدء التفتيش وانتهائه، وهوية منفذيه، ونص الإذن النظامي، ووصف دقيق للمعلومات الرقمية أو الأجهزة المضبوطة، وحالة الجهاز قبل وأثناء التفتيش، والأدوات المستخدمة، والإجراءات التقنية التي تم اتباعها[١٦٢].

وقد نصت المادة (٤٨) من نظام الإجراءات الجزائية على أن يتضمن محضر التفتيش: اسم من أجرى التفتيش، وتوقيعه، وتاريخ وساعة التفتيش، ونص الإذن، ووصف الموجودات، وكافة الإجراءات المتخذة. كما أوجبت المادة (٤٩) إثبات ما إذا كانت هناك أوراق مختومة أو مغلقة، مع منع فضها إلا بإذن من المحقق المختص. وأكدت المادة (٥٠) على وجوب تحريز المضبوطات بإغلاق محكم وتوثيقها بالسجلات الأمنية[١٦٣].

أما المادة (٥٩) فقد أوجبت إبلاغ المتهم أو الشخص المرسلة إليه الرسائل البريدية أو الإلكترونية المضبوطة بمضمونها، أو تسليمه صورة منها، ما لم يكن في ذلك ضرر على التحقيق. كما شددت المادة (٦١) على سرية المعلومات المضبوطة، ومنعت استخدامها أو إفشاءها إلا بإذن نظامي[١٦٤].

خامساً: آليات جمع الأدلة الرقمية واعتمادها قضائياً:

تُعد الأدلة الرقمية أحد أهم وسائل الإثبات في جرائم الإرهاب السيبراني، لما لها من قدرة على الكشف عن هوية الفاعل، وأسلوب الجريمة، وأدوات التنفيذ، بل وأحيانًا النية الإجرامية ذاتها من خلال المراسلات الرقمية أو آثار التصفح أو البرمجيات المستخدمة. غير أن جمع هذه الأدلة يتطلب تقنيات متقدمة، وإجراءات محددة تراعي المشروعية والموثوقية، ويخضع ذلك لمجموعة من الضوابط الفنية والقانونية في النظام السعودي.

وتبدأ مرحلة جمع الأدلة الرقمية فور ضبط الجهاز الإلكتروني أو الوسيط محل الجريمة، حيث يتعين على مأمور الضبط أو الخبير الفني المختص تنفيذ ما يُعرف بـ

---

[١٦٢] السيد الشريف، مرجع سابق، ص ١٩٣.

[١٦٣] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مواد ٤٨، ٤٩، ٥٠.

[١٦٤] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مواد ٥٩، ٦١.

"التصوير الجنائي الرقمي"، وهو إجراء يضمن الحصول على نسخة طبق الأصل من محتويات الجهاز دون التأثير على البيانات الأصلية، بما يحافظ على القيمة الإثباتية للمحتوى الرقمي. ويجب أن يتم هذا الإجراء في بيئة معزولة، مع توثيق كافة الخطوات بسجلات فنية، وذكر توقيت كل عملية، ونوع البرامج المستخدمة[١٦٥].

وقد نص نظام الإجراءات الجزائية في مادته السادسة والأربعين على أن التفتيش لا يجوز إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع المعلومات عنها، أو التحقيق في شأنها، مما يضفي على جمع الأدلة الرقمية طابعًا قانونيًا مقيدًا، ويمنع التجاوز في الاطلاع على بيانات لا علاقة لها بالجريمة. كما أوجبت المادة الخمسون أن تحفظ الأدلة في حرز مغلق، وتُسجّل في سجل خاص، مما يكفل عدم العبث بها وضمان سلامتها حتى عرضها على المحكمة[١٦٦].

ولكي تُعتمد الأدلة الرقمية أمام القضاء، يجب أن يتوافر فيها شرط المشروعية، وسلامة المصدر، وتقرير فني صادر من جهة معتمدة يوضح الإجراءات المتبعة وأثرها على الدليل، وهو ما تلتزم به الجهات المختصة، مثل الهيئة الوطنية للأمن السيبراني، والنيابة العامة. وقد أوضح المنشاوي أن الدليل الرقمي لا يكتسب قوته القانونية إلا بوجود محضر فني يتضمن الخطوات التقنية التي أُجريت عليه منذ لحظة الضبط وحتى عرضه على جهة التحقيق.

ومما سبق يمكن للباحث القول إن جمع الأدلة الرقمية في الجرائم السيبرانية لا يُعد إجراءً تقنيًا فحسب، بل هو عمل قضائي ذو طبيعة مزدوجة، يوجب احترام الضمانات الإجرائية، والتقيد بالمعايير الفنية الدقيقة، بما يكفل قبولها أمام المحكمة واعتمادها كحجة معتبرة لإثبات الجريمة.

سادساً: الإشكاليات العملية في ضبط الجريمة السيبرانية وإثباتها أمام القضاء

رغم التطور الكبير الذي أحرزته المملكة في المجال السيبراني، ما زالت هناك إشكاليات عملية تعيق ضبط جرائم الإرهاب السيبراني وإثباتها قضائيًا، وذلك بالنظر إلى

---

[١٦٥] محمد أحمد المنشاوي، النظام الجزائي الخاص "جرائم التعزير المنظمة"، دار الكتاب الجامعي، الرياض، ١٤٤٤هـ، ص ٢٣٨

[١٦٦] نظام الإجراءات الجزائية، المرسوم الملكي رقم (م/٢) ١٤٣٥هـ، مادة ٤٦.

(ISSN: 2537 - 0758)

الطبيعة التقنية البالغة التعقيد لهذه الجرائم، وتنوع الوسائل المستخدمة فيها، وامتدادها عبر الحدود الدولية. وتظهر هذه الإشكالات على عدة مستويات قانونية وفنية ومؤسساتية، **ويمكن تفصيل أبرزها فيما يلي:**

١. صعوبة تحديد مكان ارتكاب الجريمة السيبرانية: تُعد مشكلة تحديد الموقع الجغرافي للجريمة إحدى أبرز العقبات، إذ لا ترتبط الجريمة السيبرانية بمكان محدد بل تقع في فضاء افتراضي، وقد تُدار من خارج المملكة، أو من خلال خوادم لا تخضع للولاية القانونية السعودية، مما يصعب معه تحديد الجهة المختصة بالضبط أو التحقيق. كما أن الجناة يستخدمون أدوات لإخفاء الهوية الرقمية مثل الشبكات الخاصة الافتراضية (VPN) وخوادم البروكسي، مما يُعقّد من مسألة التتبع والتحقق من هوية الفاعل.

٢. التحديات المتعلقة بحجية الأدلة الرقمية: إن جمع الأدلة الرقمية يمر بمراحل فنية دقيقة، تشمل المصادرة والفحص والحفظ، ويُعد أي خلل في هذه المراحل مدعاة لبطلان الدليل أو التشكيك في صحته. وقد نص نظام الإجراءات الجزائية على جملة من الضمانات، من أبرزها ما ورد في المادة (٤٧) التي تُوجب حضور صاحب المسكن أو من ينوب عنه أثناء التفتيش، والمادة (٤٨) التي تُلزم بتحرير محضر تفتيش دقيق يصف الموجودات والإجراءات المتبعة. إلا أن هذه الضمانات قد لا تتواءم كليًا مع طبيعة التفتيش الإلكتروني، لا سيما في البيئات السحابية أو في الحالات التي لا يكون فيها محل الجريمة ماديًا أو معلومًا.

٣. محدودية التأهيل الفني للقائمين بالضبط والتحقيق: يتطلب التعامل مع الجريمة السيبرانية خبرة متقدمة في تحليل البيانات الرقمية، وفهم آليات الشبكات والبرمجيات. إلا أن الواقع العملي يُظهر وجود نقص في عدد الكوادر المؤهلة، ما يؤثر سلبًا على كفاءة التحقيق وسلامة عرض الأدلة أمام المحكمة. وقد بيّن فهد الطريسي أن غياب التأهيل التقني لدى بعض القائمين بالإجراء يؤدي إلى إشكالات في فهم الأدلة الرقمية أو إثباتها بشكل مقنع[١٦٧].

---

[١٦٧] فهد نايف الطريسي، الإجراءات الجزائية في المملكة العربية السعودية، دار الكتاب الجامعي، الرياض، ٢٠١٩م، ص ٣٠٧.

٤. ضعف البيئة التشريعية المتخصصة في الأدلة الرقمية: لا يزال الاعتماد قائمًا على اجتهاد القضاء في تقدير حجية الدليل الرقمي دون وجود دليل إجرائي وطني شامل ينظم جمع الأدلة السيبرانية وتقديمها أمام المحكمة. كما أن تعدد الأنظمة ذات العلاقة، كـ نظام مكافحة الإرهاب، ونظام مكافحة الجرائم المعلوماتية، ونظام الإجراءات الجزائية، قد يؤدي إلى تضارب في التفسير أو اختلاف في التطبيق القضائي.
٥. تأخر التعاون الدولي في تسليم الأدلة الرقمية: نظرًا للطبيعة العابرة للحدود في الجرائم السيبرانية، فإن الأدلة قد تكون مخزنة في خوادم أجنبية تخضع لقوانين دولة أخرى. وقد تواجه المملكة صعوبات في الحصول على هذه الأدلة نتيجة رفض بعض الشركات العالمية التعاون، أو اشتراطها صدور أوامر قضائية من جهات غير سعودية، مما يؤدي إلى ضياع الوقت وفوات فرصة التحفظ على الأدلة قبل إتلافها أو تعديلها[١٦٨].

ومما سبق يمكن للباحث القول إن ضبط جريمة الإرهاب السيبراني وإثباتها يواجه تحديات متشابكة تتعلق بالتقنيات الحديثة، ومرونة بيئة الجريمة، وضعف التعاون الدولي، ومحدودية التشريع المحلي، الأمر الذي يتطلب بناء منظومة قضائية رقمية متكاملة، تبدأ بتأهيل القضاة والمحققين، وتنتهي بإصدار دليل إجرائي خاص بالأدلة الرقمية في الجرائم السيبرانية.

خاتمة الدراسة:

في ضوء ما سبق، يتضح أن جريمة الإرهاب السيبراني تُعد من أبرز التحديات الجنائية الحديثة التي فرضت نفسها على الساحة القانونية والأمنية، لما تنطوي عليه من تعقيدات فنية، وتداخلات تنظيمية، وتحديات إجرائية غير مسبوقة. فقد كشفت هذه الدراسة، من خلال تناولها الموضوعي والإجرائي لجريمة الإرهاب السيبراني في النظام السعودي، عن مدى تطور البنية النظامية الوطنية في التصدي لهذا النمط من الجرائم، وسعيها إلى تحقيق التوازن بين مقتضيات الحماية الأمنية وضمانات العدالة الإجرائية.

ففي **المبحث الأول**، تم تحليل البنية المفاهيمية للجريمة من حيث أنماطها وتقسيماتها الفنية، وتبيّن أن الإرهاب السيبراني يشمل طيفًا واسعًا من الأفعال التي

[١٦٨] محمد المنشاوي، مرجع سابق، ص٢٦١.

(ISSN: 2537 - 0758)

تستهدف المساس بالأمن الوطني من خلال الفضاء الرقمي، وتختلف جوهريًا عن صور الإرهاب التقليدي. كما أبرزت الدراسة الدور الفاعل للسياسات السعودية في التصدي لتلك الجرائم، من خلال تبني استراتيجيات وطنية متكاملة، تعكس وعي الدولة بخطورة التهديدات الرقمية، وحرصها على تطوير منظومتها الوقائية والتشريعية.

أما **المبحث الثاني**، فقد تضمن تحليلًا دقيقًا للجوانب النظامية والإجرائية الخاصة بجريمة الإرهاب السيبراني، بدءًا من التكييف القانوني لأركان الجريمة، وصولًا إلى العقوبات الأصلية والتبعية المرتبطة بها، ومقارنة تلك العقوبات بين نظام مكافحة الإرهاب ونظام الجرائم المعلوماتية. كما تناولت الدراسة إجراءات الضبط الجنائي، وأبرزت الجهود المؤسسية لجهات مكافحة الإرهاب السيبراني، مع الوقوف على الإشكاليات الفنية والقانونية التي تعترض سبيل إنفاذ القانون، وعلى رأسها مشكلات الإثبات، وتحديات التعاون الدولي، وضعف التأهيل التقني لبعض الكوادر.

وتبيّن من خلال الدراسة أن المملكة العربية السعودية قد قطعت شوطًا مهمًا في بناء منظومة قانونية ومؤسسية فاعلة لمكافحة الإرهاب السيبراني، إلا أن الطابع المتجدد والمعقد لهذه الجريمة يستوجب تعزيز البنية التشريعية بنصوص إجرائية متخصصة، وتطوير القدرات الفنية للأجهزة الضبطية والقضائية، واعتماد أدلة إجرائية رقمية موحدة، لضمان فعالية المواجهة القانونية، وصيانة الحقوق الدستورية.

ومما سبق يمكن للباحث القول إن معالجة جريمة الإرهاب السيبراني لا يمكن أن تُختزل في أداة واحدة أو جهة بعينها، بل تتطلب تكاملًا تشريعيًا، وتعاونًا مؤسسيًا، وتأهيلًا متخصصًا، يستند إلى وعي استراتيجي بمخاطر الفضاء الرقمي، ويهدف إلى تحصين الأمن الوطني، وتعزيز سيادة القانون في البيئة السيبرانية.

أولًا: نتائج الدراسة:

بالنسبة الأركان القانونية المميزة لجريمة الإرهاب السيبراني في النظام السعودي، وكيف تختلف عن الجرائم التقليدية؟

١. تبيّن أن جريمة الإرهاب السيبراني تتميّز بوجود ركن مفترض تقني يتمثل في ضرورة ارتكاب الجريمة عبر وسيط إلكتروني، مما يميزها عن الجرائم الإرهابية التقليدية.
٢. يتكوّن الركن المادي للجريمة من أفعال تقنية كالدخول غير المشروع، التخريب الرقمي، أو تعطيل البنى التحتية الحيوية، وكلها مشمولة ضمن النصوص النظامية في نظام مكافحة الإرهاب وتمويله.

٣. يتطلب الركن المعنوي لهذه الجريمة توفر قصدين: عام يتمثل في العلم والإرادة، وخاص يتجلى في نية الإضرار بالأمن الوطني أو تهديد النظام العام.
٤. يرتبط الركن الشرعي للجريمة بتكامل نصوص نظام مكافحة الإرهاب وتمويله مع نظام مكافحة الجرائم المعلوماتية، ما يوفر أساسًا قانونيًا مزدوجًا.
٥. تبيّن أن الجريمة السيبرانية الإرهابية تستلزم أدوات إثبات غير تقليدية، أبرزها الأدلة الرقمية، مما يفرض تحديات خاصة على التطبيق القضائي.

بالنسبة لمدى كفاية العقوبات النظامية المقررة لمواجهة جريمة الإرهاب السيبراني في ظل طبيعتها المركبة والمتجددة؟

٦. أظهرت الدراسة أن العقوبات الواردة في نظام مكافحة الإرهاب وتمويله تتسم بالصرامة، حيث تصل إلى السجن المؤبد أو الإعدام في بعض الحالات المشددة.
٧. بالمقابل، تتسم العقوبات الواردة في نظام مكافحة الجرائم المعلوماتية بكونها أقل صرامة نسبيًا، ما يفتح إشكالية في التكييف النظامي عند تداخل الأنظمة.
٨. يتضح أن نظام مكافحة الإرهاب عالج صور الشروع والمساهمة وظروف التشديد والتخفيف بمستوى عالٍ من الدقة، بما يتلاءم مع طبيعة الجريمة.
٩. تضمنت العقوبات التبعية تدابير مهمة مثل المصادرة، وحجب المواقع، ونشر الأحكام، وهي تدابير ضرورية لتجفيف منابع الخطر.
١٠. رغم شمولية العقوبات، إلا أن التطبيق القضائي ما زال يواجه تحديات تتعلق بربط الفعل الرقمي بالقصد الإرهابي، ما يستدعي أدوات إثبات تقنية متطورة.

بالنسبة للجهات والمؤسسات الوطنية المختصة بمكافحة الإرهاب السيبراني، وما حدود أدوارها؟

١١. تبيّن أن وزارة الداخلية تمثل الجهة الأمنية الرئيسة في مواجهة الإرهاب السيبراني، من خلال قدراتها على الرصد والتدخل، والتنسيق مع باقي الجهات.
١٢. تؤدي رئاسة أمن الدولة دورًا استخباراتيًا محوريًا في تتبع الشبكات الإرهابية الإلكترونية، وتحليل التهديدات عالية الخطورة.
١٣. تُعد الهيئة الوطنية للأمن السيبراني الجهة التنظيمية الأعلى المختصة بوضع السياسات والمعايير الوقائية الفنية على مستوى المملكة.
١٤. تلعب وزارة الاتصالات وتقنية المعلومات دورًا داعمًا في تطوير البنية التحتية التقنية القادرة على مقاومة الهجمات الإرهابية الرقمية.

(ISSN: 2537 - 0758)

١٥.تتولى النيابة العامة مهام التحقيق والملاحقة في الجرائم السيبرانية الإرهابية، وفق ضوابط دقيقة لضمان حجية الأدلة.

بالنسبة لأبرز الإجراءات الجنائية الخاصة بضبط جريمة الإرهاب السيبراني، وما الإشكاليات التي تعيق إنفاذ القانون فيها؟

١٦.أظهرت الدراسة أن نظام الإجراءات الجزائية يُحدد تفصيلًا ضوابط التفتيش الإلكتروني، خاصة المواد من (٤١) إلى (٦١)، لضمان حماية الحقوق الرقمية.

١٧.يتطلب ضبط الجريمة السيبرانية إجراءات فنية عالية، تشمل التصوير الجنائي الرقمي وتحليل الأدلة الرقمية، وهي أدوات غير متوفرة دائمًا لجميع الجهات.

١٨.من أبرز الإشكالات العملية عدم وضوح نطاق السلطة في الجرائم العابرة للحدود، مما يصعّب من الإجراءات القانونية داخل المملكة.

١٩.تبيّن وجود قصور تشريعي في تنظيم وسائل الإثبات الرقمية، حيث لا يوجد دليل إجرائي وطني موحد يحكم هذه الأدلة.

٢٠.تواجه جهات الضبط صعوبة في الحفاظ على سلامة الأدلة الرقمية من الطعن، بسبب نقص التدريب، وتأخر التعاون الدولي مع مزودي الخدمة العالميين.

ثانياً: توصيات الدراسة:

١. تعديل النصوص النظامية المتعلقة بجريمة الإرهاب السيبراني لتحديدها صراحة وتفصيل أركانها.

* **آلية التنفيذ:** تشكيل لجنة مشتركة من هيئة الخبراء، والنيابة العامة، والهيئة الوطنية للأمن السيبراني، لصياغة تعديلات على نظام مكافحة الإرهاب وتمويله، تُدرج فيها الجريمة بصيغة دقيقة تتضمن الركن المفترض والبيئة التقنية الخاصة بها.

٢. استحداث لائحة تنفيذية خاصة بالإرهاب السيبراني ضمن نظام مكافحة الجرائم المعلوماتية.

* **آلية التنفيذ:** إصدار لائحة من مجلس الوزراء تتضمن آليات التفتيش الرقمي، ومعايير الإثبات، وآليات الحجب والمنع، بما يتناسب مع خصوصية الجريمة السيبرانية الإرهابية.

٣. إصدار تنظيم خاص بالمسؤولية الجنائية للمنصات الرقمية في حال التورط أو الإهمال.

* **آلية التنفيذ:** إصدار تنظيم من هيئة الاتصالات يحدد مسؤوليات شركات التقنية المحلية والعالمية، ويُلزمها بالتعاون مع السلطات السعودية.

٤. إنشاء وحدة مستقلة في النيابة العامة متخصصة في التحقيق في جرائم الإرهاب السيبراني.

* **آلية التنفيذ:** إصدار أمر تنظيمي من النائب العام بإنشاء وحدة متخصصة مزودة بكفاءات تقنية وقانونية، مع تفعيل التعاون مع مركز الأمن السيبراني.

٥. ربط كافة المؤسسات المعنية بالأمن السيبراني بمنصة موحدة لتبادل المعلومات ذات الحساسية الأمنية العالية.

* **آلية التنفيذ:** تدشين نظام إلكتروني موحد تحت إشراف رئاسة أمن الدولة، يربط بين الهيئة الوطنية للأمن السيبراني، والنيابة العامة، ووزارة الداخلية، لتسريع التبليغ والاستجابة.

٦. تكثيف برامج التدريب الجنائي الرقمي للقضاة وأعضاء النيابة وضباط الضبط الجنائي.

* **آلية التنفيذ:** توقيع شراكات تدريبية بين وزارة العدل وجامعة نايف، لتنظيم برامج تخصصية حول أدلة الجرائم السيبرانية ومواجهة الإرهاب الإلكتروني.

٧. وضع معايير قانونية واضحة لتقدير العقوبات في جرائم الإرهاب السيبراني.

* **آلية التنفيذ:** اعتماد دليل قضائي استرشادي من المحكمة العليا يتضمن ظروف التشديد والتخفيف، والمساهمة والشروع في الجريمة.

٨. دعم مراكز الأبحاث والجامعات لإعداد دراسات تحليلية دورية عن التهديدات السيبرانية الإرهابية.

* **آلية التنفيذ:** تخصيص ميزانيات دعم من وزارة الداخلية ومركز دعم القرار لمراكز الأبحاث في الجامعات السعودية لتحليل البيانات وتقديم سيناريوهات استباقية.

٩. وضع ميثاق وطني للتعاون الدولي في قضايا الإرهاب السيبراني، يشمل تبادل الأدلة والبيانات الرقمية.

* **آلية التنفيذ:** توقيع مذكرات تفاهم ثنائية ومتعددة الأطراف مع الدول الصديقة والمنظمات الدولية، بإشراف وزارة الخارجية وهيئة الأمن السيبراني.

١٠. تعزيز الوعي القانوني المجتمعي بخطورة الإرهاب السيبراني من خلال الحملات التوعوية والإعلامية.

* **آلية التنفيذ:** إطلاق حملات وطنية عبر هيئة الأمن السيبراني بالشراكة مع وزارة التعليم ووسائل الإعلام، تشرح سبل التبليغ والوقاية والمساءلة القانونية.

(ISSN: 2537 - 0758)

قائمة المراجع

(أ) قواميس ومعاجم:

١) آبادي محمد بن يعقوب الفيروز، القاموس المحيط، مؤسسة الرسالة، بيروت، ط٢، ١٩٨٧م

٢) حارث سليمان الفاروقي، المعجم القانوني، مكتبة لبنان، بيروت، ط٥، ٢٠١٣م.

٣) محمد بن مكرم ابن منظور، لسان العرب، دار الكتب العلمية، بيروت، ط٢، ١٤٣٠هـ.

(ب) الكتب العامة:

١) السيد محمد شريف، الوجيز في شرح نظام الإجراءات الجزائية السعودي، ط٣، دار الإجادة للنشر والتوزيع، الرياض، ١٤٤٣هـ.

٢) زكي محمد شناق، الوجيز في نظام الإجراءات الجزائية السعودي، الشقري للنشر، جدة، ط٢، ١٤٤٤هـ.

٣) شريف نصر أحمد، القانون الجزائي السعودي "القسم الخاص الجرائم التعزيرية المنظمة"، مكتبة المتنبي، الدمام، ٢٠٢٤م.

٤) عبد القادر عودة، التشريع الجنائي الإسلامي مقارنًا بالقانون الوضعي، دار الكاتب العربي، بيروت، ج١، ٢٠١٣م.

٥) عبد الله الفقيه، الجريمة في الفقه الجنائي، دار النهضة العربية، القاهرة، الطبعة الثانية، ٢٠١٥م.

٦) عبد المجيد الحفناوي، أصول التشريع في المملكة العربية السعودية، دار الكتب، القاهرة، ط٢، ٢٠١٥م.

٧) فهد نايف الطريسي، الإجراءات الجزائية في المملكة العربية السعودية، دار الكتاب الجامعي، الرياض، ٢٠١٩م.

٨) كمال محمد عواد، الوسيط في النظام الجنائي السعودي، دار الإجادة للنشر والتوزيع، الرياض، ٢٠٢٠م.

٩) محمد المنشاوي، شرح نظام الإجراءات الجزائية السعودي الجديد، دار الإجادة للنشر، الرياض، ١٤٣٦هـ.

١٠) محمد حميد المزمومي، الوسيط في شرح نظام الإجراءات الجزائية السعودي، ط٤، مركز النشر العلمي، جامعة الملك عبدالعزيز، الرياض، ١٤٤٤هـ.

١١) محمد عبد الله المرزوقي، السلطة التنظيمية في المملكة العربية السعودية، دار العبيكان، الرياض، ١٤٢٥هـ.

١٢) محمود طه جلال، أصول التجريم والعقاب في السياسة الجنائية المعاصرة: دراسة مقارنة، كلية الحقوق، جامعة عين شمس، ١٤٢٥هـ.

(ج) الكتب المتخصصة:

١) جبور علي الأشقر، السيبرانية هاجس العصر، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٦م.

٢) شمان ناجي الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٦م.

٣) عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية– نمط جديد وتحديات مختلفة، ط٢، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، ٢٠١٤م.

٤) عبد العزيز بن غرم الله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي، دار الكتاب الجامعي للنشر والتوزيع، الرياض، ١٤٣٨هـ.

٥) محمد المنشاوي، النظام الجزائي الخاص– جرائم التعزير المنظمة، دار الكتاب الجامعي للنشر، الرياض، ١٤٤٤هـ.

٦) محمد مجاهد، تضارب المصالح: عقبات تشكيل تحالف عسكري ضد داعش، اتجاهات الأحداث، مركز المستقبل للأبحاث والدراسات، العدد ٨، أبوظبي، ٢٠١٥م.

٧) مها حمد القريني، واقع الجرائم المعلوماتية في المملكة العربية السعودية، الدار العالمية لتقنية المعلوماتية، القاهرة، ٢٠٢١م.

(د) الرسائل الجامعية:

١) سعد بن حمد القحطاني، السياسة الجنائية السعودية في مكافحة جرائم تقنية المعلومات، رسالة دكتوراه، قسم العدالة الجنائية، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٢٠م.

٢) محمد بن سعيد، التهديدات السيبرانية على الأنظمة الأمنية في المملكة العربية السعودية: دراسة تطبيقية، رسالة دكتوراه، جامعة الملك عبد العزيز، الرياض، ٢٠٢٢م.

٣) محمد صالح السبيعي، تأثير الجرائم السيبرانية على المؤسسات المالية في المملكة العربية السعودية، رسالة ماجستير، جامعة الملك سعود، الرياض، ٢٠٢١م.

(هـ) أبحاث علمية منشورة

١) أحمد عبد الله الجميلي، "الآثار الاقتصادية للجرائم السيبرانية على القطاع المالي في المملكة العربية السعودية"، مجلة الاقتصاد الرقمي، مج١، ع٢، دار الفكر الاقتصادي، الرياض، ٢٠٢٢م.

٢) أحمد عبيس الفتلاوي، "الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، الجزائر، ٢٠١٧م.

٣) أماني بهجت، "أمن المعلومات"، المركز الإقليمي للدراسات، العدد ١٩، القاهرة، ٢٠١٥م.

(ISSN: 2537 - 0758)

٤) حازم الجمل، "الحماية الجنائية للأمن السيبراني في المملكة العربية السعودية"، مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية، العدد ١٦٣٧، ٢٠٢٢م.
٥) سحر جمال زهران، "الجوانب القانونية الدولية لجريمة الإرهاب الإلكتروني"، مجلة السياسة والاقتصاد، مج٥، ع٤، ٢٠١٩م.
٦) سعيد بن زعل الخريصي، "جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية في مواجهتها"، مجلة جامعة الأندلس للعلوم الإنسانية والاجتماعية، العدد ٧٣، المجلد ١٠، ٢٠٢٣م.
٧) سهل بن زعل الخريصي، "جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية"، مجلة أبحاث العلوم الإنسانية والاجتماعية، الجامعة الإسلامية بالمدينة المنورة، العدد ٧٣، ٢٠٢٣م.
٨) غادة الطريف، "السياسة الاجتماعية ومكافحة الجرائم الإلكترونية في المجتمع السعودي"، دار جامعة نايف للنشر، الرياض، ٢٠٢٠م.
٩) فهد السويلم، "أثر الجرائم السيبرانية على المنشآت الحيوية في المملكة العربية السعودية"، مجلة الدراسات الاقتصادية السعودية، ع١٢، دار النشر السعودية، الرياض، ٢٠٢١م.
١٠) محمد مجاهد، "تضارب المصالح: عقبات تشكيل تحالف عسكري ضد داعش"، مجلة مركز المستقبل للأبحاث والدراسات المتقدمة، ع٨، أبوظبي، ٢٠١٥م.
١١) ناصر عبد الله الشمري، "أثر الجرائم السيبرانية على القطاع الخاص في المملكة العربية السعودية: دراسة تحليلية"، مجلة البحوث التجارية، ع١٥، دار العلوم للنشر، الرياض، ٢٠٢٠م.
١٢) هشام بشير، "الإرهاب الإلكتروني في ظل الثورة التكنولوجية وتطبيقاتها في العالم العربي"، مجلة آفاق سياسية، العدد السادس، يونيو ٢٠١٤م.
١٣) ميليسيا هاثاواي، فهد السويلم، "المملكة العربية السعودية: لمحة عن الجاهزية السيبرانية"، معهد بوتوماك للدراسات السياسية، فرجينيا، ٢٠١٧م.
١٤) عبد الرزاق المرجان وآخرون، "الأساليب والاتجاهات الحديثة للجرائم السيبرانية والوقاية منها"، دار جامعة نايف للنشر، الرياض، ٢٠٢٥م.
١٥) حمد المنشاوي وآخرون، "الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية"، دار جامعة نايف للنشر، الرياض، ٢٠٢٤م.

(و) الأنظمة والتشريعات:

١) الاتفاقية العربية لمكافحة الجرائم السيبرانية، جامعة الدول العربية، القاهرة، ٢٠١٠م.
٢) الاستراتيجية الوطنية للأمن السيبراني، قرار مجلس الوزراء رقم (٥٧٢)، بتاريخ ١٢ شوال ١٤٣٩هـ، هيئة الخبراء بمجلس الوزراء، الرياض، ١٤٣٩هـ.

٣) الأمر الملكي رقم (٦٨٠١)، بتاريخ ١١ صفر ١٤٣٩هـ، هيئة الخبراء بمجلس الوزراء، الرياض، ١٤٣٩هـ.
٤) النظام الأساسي للحكم، الصادر بالأمر الملكي رقم (أ/٩٠) بتاريخ ١٤١٢/٨/٢٧هـ، والمنشور في جريدة أم القرى، السنة ٦٩، العدد ٣٣٩٧، بتاريخ الجمعة ١ رمضان ١٤١٢هـ الموافق ٦ مارس ١٩٩٢م، مكة المكرمة، المملكة العربية السعودية.
٥) نظام الإجراءات الجزائية، الصادر بالمرسوم الملكي رقم (م/٢) بتاريخ ١٤٣٥/١/٢٢هـ، والمنشور في جريدة أم القرى بتاريخ ١٤٣٥/٢/٣هـ، المملكة العربية السعودية.
٦) نظام مكافحة الإرهاب وتمويله، المرسوم الملكي رقم (م/٢١) بتاريخ ١٤٣٩/٢/١٢هـ، قرار مجلس الوزراء رقم (٩٢) بتاريخ ١٤٣٩/٢/١١هـ، جريدة أم القرى، العدد ٤٦٩٥، ٢١ صفر ١٤٣٩هـ، الموافق ١٠ نوفمبر ٢٠١٧م.
٧) نظام مكافحة الجرائم المعلوماتية، المرسوم الملكي رقم (م/١٧) بتاريخ ١٤٢٨/٣/٨هـ، قرار مجلس الوزراء رقم (٧٩) بتاريخ ١٤٢٨/٣/٧هـ، جريدة أم القرى، السنة ٨٣، العدد ٤١٤٤، ٢٥ ربيع الأول ١٤٢٨هـ، الموافق ١٣ أبريل ٢٠٠٧م.

(ز) **التقارير الرسمية**:

١) الهيئة الوطنية للأمن السيبراني، "الاستراتيجية الوطنية للأمن السيبراني"، الرياض، ٢٠٢٠.
٢) الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، الرياض، ٢٠١٨م.
٣) الهيئة الوطنية للأمن السيبراني، تقرير البرنامج الوطني للتوعية بالأمن السيبراني، الرياض، ٢٠٢٢م.
٤) الهيئة الوطنية للأمن السيبراني، تقرير المركز الوطني الإرشادي للأمن السيبراني، الرياض، ٢٠٢٠م.
٥) الهيئة الوطنية للأمن السيبراني، وثيقة شراكة القطاعين العام والخاص في الأمن السيبراني، الرياض، ٢٠٢٢م.
٦) الهيئة الوطنية للأمن السيبراني، وثيقة ضوابط الأمن السيبراني الأساسية، الرياض، ١٤٤٠هـ.
٧) جامعة الملك سعود، التقرير السنوي لوحدة الأمن السيبراني، جامعة الملك سعود، الرياض، ٢٠٢١م.
٨) رئاسة أمن الدولة، "الأمن السيبراني ومكافحة الإرهاب"، الرياض، ٢٠٢١.
٩) مركز الجرائم السيبرانية والأدلة الرقمية، الإرهاب السيبراني في المنطقتين الإفريقية والعربية: تقرير استقصائي من ورشة عمل جامعة نايف ومركز الأمم المتحدة لمكافحة الإرهاب، دار جامعة نايف للنشر، الرياض، ٢٠٢٤م.

(ISSN: 2537 - 0758)

١٠) مركز الجرائم السيبرانية والأدلة الرقمية، الملتقى الأول لاستخدامات الذكاء الاصطناعي في المجالات الأمنية: تقرير الملتقى، دار جامعة نايف للنشر، الرياض، ٢٠٢٣م.
١١) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، الجريمة السيبرانية والإيقاع الإجرامي التقليدي بالضحايا، دراسة شاملة، مسودة فبراير، جنيف، ٢٠١٩م.
١٢) هيئة الاتصالات والفضاء والتقنية، التقرير السنوي لهيئة الاتصالات والفضاء والتقنية، الرياض، ٢٠٢٢م.
١٣) وزارة الخارجية السعودية، تقرير المملكة حول التعاون الدولي في مجال الأمن السيبراني، الرياض، ٢٠٢١م.
١٤) وزارة الداخلية، "تقرير الحماية من الجرائم المعلوماتية"، الرياض، ٢٠٢٢.

(ج) المواقع الالكترونية:

١. المنصة الوطنية للخدمات الحكومية، الأمن اليسبراني في المملكة العربية السعودي متاح على https://my.gov.sa/en/wps/portal/snp/content/cybersecurity **تاريخ الإطلاع ١٤٤٦/٩/١١هـ الساعة ٩ مساءا.**
٢. جامعة نايف العربية للعلوم الأمنية، الجرائم السيبرانية، متاح على: https://nup.nauss.edu.sa/index.php/sr/catalog/category/Cybercrimes?utm_source=chatgpt.com
٣. وزارة الداخلية: وزارة الداخلية بالتعاون مع الهيئة الوطنية للأمن السيبراني تنظم جلسات توعوية في مجال الأمن السيبراني، ١٤٤٤هـ، متاح على:https://tinyurl.com/yrd4pm8s تاريخ الإطلاع ١٤٤٦/٩/١١هـ الساعة ٩ مساءا.
٤. وكالة الأنباء السعودية. ٢٠١٩. "وزير الطاقة: الهجوم الإرهابي على معملي بقيق وخريص أدى إلى توقف ٥.٧ مليون برميل يوميًا" وكالة الأنباء السعودية(SPA)، ١٤ سبتمبر. تم الاسترجاع في [١٤٤٦/٩/١٢هـ الساعة ٩ مساءاً] من https://www.spa.gov.sa/1969112.
٥. ويكيبيديا.2020 United States federal government data breach. (2020) . تم الاسترجاع في (١٤٤٦/٩/١٢هـ الساعة ٩ مساءً] من https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach