واقع الحماية الجزائية للأمن السيبراني دراسة مقارنه الاردن قطر

Real criminal protection for cybersecurity, a comparative study in Jordan and Qatar

إعداد

د. مصعب تركي إبراهيم نصار

Dr. Musab Turki Ibrahim Nassar

أستاذ القانون الجنائي المساعد - كلية الشرطة - دولة قطر

Doi: 10.21608/jinfo.2024.340209

استلام البحث ٨ / ١٢ / ٢٠٢٣

قبول البحث ١٨ / ١٢ / ٢٠٢٣

نصار، مصعب تركي إبراهيم (٢٠٢٤). واقع الحماية الجزائية للأمن السيبراني دراسة مقارنه الاردن قطر. ***المجلة العربية للمعلوماتية وأمن المعلومات***، المؤسسة العربية للتربية والعلوم والآداب ، مصر، ٥(١٤) ، ١٢٩ – ١٥٢.

https://jinfo.journals.ekb.eg

واقع الحماية الجزائية للأمن السيبراني دراسة مقارنه الاردن قطر

المستخلص:

تعد الحماية الجزائية للأمن السيبراني مسألة حيوية في العصر الحديث، حيث يتزايد التهديد السيبراني وتطوره باستمرار. تهدف دراسة مقارنة بين الأردن وقطر إلى فهم وتقييم واقع الحماية الجزائية للأمن السيبراني في هاتين الدولتين ومقارنتهما. في الأردن، تم اتخاذ خطوات هامة في الآونة الأخيرة لتعزيز الحماية الجزائية للأمن السيبراني. تم إقرار قوانين وتشريعات جديدة تتعامل مع جرائم القرصنة والاختراق والتلاعب الإلكتروني. تم تعزيز قدرات الشرطة والجهات القضائية في التعامل مع هذه الجرائم من خلال توفير التدريب والموارد اللازمة. تم إنشاء وحدات خاصة لمكافحة الجرائم السيبرانية وتقديم الدعم الفني للتحقيقات. من جانبها، تعتبر قطر واحدة من الدول الرائدة في مجال الأمن السيبراني في المنطقة. تم تبني قوانين وتشريعات قوية لمكافحة جرائم الإنترنت والقرصنة. تم تنفيذ استراتيجية وطنية للأمن السيبراني تركز على تعزيز التوعية والتعليم وتطوير القدرات التقنية. تم إنشاء هيئات خاصة لمكافحة الجرائم السيبرانية وتعزيز التعاون بين القطاع العام والخاص. على الرغم من التقدم في كلا البلدين، هناك تحديات تواجهها. من بينها نقص الكوادر المتخصصة والتدريب المستمر، وضرورة تحديث التشريعات والقوانين لمواجهة التهديدات المتطورة، وضمان التنسيق والتعاون القوي بين الجهات المختلفة المعنية بالأمن السيبراني. وفي الختام، يتطلب تعزيز الحماية الجزائية للأمن السيبراني في الأردن وقطر التركيز على تعزيز التشريعات والقوانين، وتطوير القدرات التقنية، وتعزيز التوعية والتدريب، وتعزيز التعاون المشترك. يتعين على البلدين الاستفادة من الخبرات المحلية والدولية وتبادل المعرفة والتجارب لبناء نظام قوي للحماية الجزائية للأمن السيبراني.

Abstract:

The field of criminal protection for cybersecurity is crucial in the modern era, as cyber threats continue to increase and evolve. A comparative study between Jordan and Qatar aims to understand and evaluate the current state of criminal protection for cybersecurity in these two countries and compare them .In Jordan, significant steps have been taken recently to enhance criminal protection for cybersecurity. New laws and regulations have been enacted to address crimes such as hacking, intrusion, and electronic manipulation. The capabilities of the police and judicial authorities have been strengthened in dealing

ISSN : 2735-3737 eISSN : 2735-3745

with these crimes through training and providing necessary resources. Special units have been established to combat cybercrimes and provide technical support for investigations.On the other hand, Qatar is considered one of the leading countries in cybersecurity in the region. Strong laws and regulations have been adopted to combat internet crimes and piracy. A national cybersecurity strategy has been implemented, focusing on enhancing awareness, education, and technological capabilities. Special entities have been established to combat cybercrimes and enhance cooperation between the public and private sectors.Despite the progress in both countries, there are challenges to be addressed, including a shortage of specialized personnel and continuous training, the need to update laws and regulations to counter evolving threats, and ensuring strong coordination and cooperation among the various entities involved in cybersecurity.In conclusion, enhancing criminal protection for cybersecurity in Jordan and Qatar requires a focus on strengthening legislation, developing technological capabilities, promoting awareness and training, and enhancing mutual cooperation. Both countries need to benefit from local and international expertise, exchange knowledge and experiences, and build a robust system for criminal protection of cybersecurity.

مقدمة:

تشكل الجرائم الإلكترونية المنظمة العابرة للحدود الوطنية تحد كبيراً للجهات القضائية والأمنية في جميع أنحاء العالم، حيث يتم استخدام التكنولوجيا الحديثة لارتكاب هذه الجرائم والتي تشمل الاحتيال الإلكتروني، التجسس، القرصنة الإلكترونية، الاختراق، التزوير، والكثير من الأنشطة الغير مشروعة، وبسبب تزايد هذه الجرائم واتساع نطاقها، أصبح من الضروري تطوير الأدوات والتقنيات التي تساعد في جمع الأدلة الرقمية اللازمة لتتبع ومعاقبة المتورطين في هذه الجرائم، ومن أجل ذلك، تم ابتكار مفهوم الأدلة الرقمية، والتي تشمل جميع البيانات والمعلومات الإلكترونية التي يمكن استخدامها في إثبات وجود الجريمة وتحديد مرتكبيها.

ISSN : 2735-3737 eISSN : 2735-3745

إن الأهمية الحقيقية للبحث في هذا الموضوع تكمن في تحديد أنجع السبل لتحقيق العدالة ومكافحة هذا الصنف من الجريمة، حيث تمثل الأدلة الرقمية الوسيلة الأساسية لإثبات وتحديد المسئولين عن الجرائم الإلكترونية المنظمة العابرة للحدود الوطنية ومع ذلك، تفرض المحدوديات القانونية والتقنية في جمع وتحليل هذه الأدلة نفسها، مما يتسبب في صعوبة في إثبات الجرائم الإلكترونية المنظمة عبر الحدود الوطنية فمثلاً، يمكن للجناة استخدام تقنيات التشفير والخوادم الوهمية للتمويه والإفلات من قبضة الجهات المختصة بجمع الأدلة الرقمية.

وعليه يقتضي علينا التطرق إلى ماهية الجريمة الالكترونية في الفقرة الأولى، بالإضافة إلى التطرق إلى جهود دولة قطر لمواجهة الجريمة الالكترونية في الفقرة الثانية، وكذا إبراز الإجراءات المتبعة لضبط الأدلة الالكترونية في الفقرة الثالثة.

الفقرة الأولى: ماهية الجرائم الالكترونية:

للتطرق إلى ماهية الجرائم الالكترونية وجب علينا التطرق إلى تعريف الجرائم الالكترونية، ثم بيان أهم خصائص الجريمة الالكترونية.

أولا: تعريف الجريمة الالكترونية:

لم يستقر الفقه على وضع تعريف محدد للجريمة الالكترونية، كون الجرائم المستحدثة تتطور من حين إلى أخر، فهناك من أطلق عليها الجريمة المعلوماتية أو جرائم الحاسوب والكمبيوتر، أو جرائم الانترنت، أو جرائم الشبكة العنكبوتية، أو جرائم تقنية المعلومات.

وقد عرفها جانب من الفقه بأنها ذلك النوع من الجرائم التي تتطلب ألماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعلها[١]، وعرفت أيضا بأنها الجرائم التي يكون فيها الحاسوب وسيلة ارتكاب فعل غير مشروع، أو محل لوقوع الفعل غير المشروع، وذلك بالقيام بعمل أو الامتناع عن أدائه من شأنه الاعتداء على الأموال المادية أو المعنوية، شريطة أن يكون مرتكبها على معرفة بتقنية استخدام الحاسوب والتعامل مع معطياته[٢] .

أما بالنسبة لموقف التشريعات من تعريف الجريمة الالكترونية، فقد عرف المشرع القطري الجريمة الالكترونية بأنها " أي فعل ينطوي على استخدام وسيلة

---

[١] _ د. علي جبار الحسيني، جرائم الحاسوب والانترنت، دار اليازوني للنشر والتوزيع، عمان، الأردن، ط ١، ٢٠٠٩، ص ٣٣.

[٢] _ د. خالد عياد الحلبي، اجراءات التحقيق والتحري في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط١، ٢٠١١، ص ٣١.

ISSN : 2735-3737 eISSN : 2735-3745

تقنية المعلومات أو نظام معلوماتي، أو الشبكة المعلوماتية، بطريقة غير مشروعة بما يخالف القانون" .

وقد حدد المشرع القطري في هذا القانون المصطلحات المرتبطة بالجريمة الالكترونية، حيث عرف المقصود بتقنية المعلومات، وكذا التطرق إلى المقصود بالبيانات والمعلومات الالكترونية، بالإضافة إلى تطرقه إلى تعريف بعض المفاهيم ذات الصلة بالتعريف كالنظام المعلوماتي و الشبكة المعلوماتية ومعالجة المعلومات والموقع الالكتروني وبيانات المرور وكذا المحرر الرسمي الالكتروني[٣].

مع العلم انه هناك دول خلت تشريعاتها من إعطاء تعريف للجريمة الالكترونية على غرار قانون الجريمة الالكترونية الأردني، في قانون الجرائم الالكترونية رقم ٢٧ لسنة ٢٠١٥.

ومن جانبنا نؤيد عدم إدراج التشريعات تعريفا للجريمة الالكترونية، ذلك لأنه لا يوجد تعريف جامع ومانع لهذا النوع من الجرائم، وهذا يرجع إلى تنوع الوسائل التي ترتكب بها هذه الجرائم وسرعة تطورها [٤]، مع الأخذ بعين الاعتبار أن الخوض في التعريفات من مسائل الفقه.

ثانيا: خصائص الجريمة الالكترونية :

تتسم الجرائم الالكترونية ببعض الخصوصيات التي تميزها عن بقية الجرائم الأخرى، ومن أبرزها صعوبة الكشف عن هوية الجاني وسهولة إخفاء أثارها وأدلتها وهوية فاعلها ومن السهل الوقوع فيها، وقد تكون سرعة انتشارها هي السبب الأساسي في صعوبة الكشف عن الجاني أو تدارك أثارها بما يجعل الضرر الناتج عنها صعب التقدير، وفيما يلي إبراز أهم الخصائص التي تتميز بها الجرائم الالكترونية[٥]:

- من السهل ارتكابها، وذلك لاستخدام وسائل ذات طابع تقني.
- من السهل إخفاء معالم الجريمة، وفي ذات الوقت من الصعب ملاحقة مرتكبيها.
- يتطلب ارتكاب هذا النوع من الجرائم قدرا من المعرفة في الأنظمة المعلوماتية.
- السرعة في ارتكاب الجريمة الالكترونية لاعتمادها على الوسائل الحديثة.

---

[٣] راجع المادة الأولى من القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجريمة الالكترونية القطري الجريدة الرسمية رقم ١٥،بتاريخ ٢-١٠-٢٠١٤ .

[٤] مريم عبد اللطيف المسلماني، مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الالكترونية، مجلة القانون والمجتمع، جامعة قطر، كلية الحقوق، المجلد ١٠، العدد ٠٢، لسنة ٢٠٢٢، ص ١٨.

[٥] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت، دراسة مقارنة، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والأنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧، ص ٣١-٣٣ .

ISSN : 2735-3737 eISSN : 2735-3745

_ تؤثر هذه الجريمة على اقتصاد الدول .
_ جريمة تتسم بالغموض نظرا لصعوبة إثباتها والتحقيق فيها على عكس الجرائم التقليدية.
_ عولمة هذه الجرائم التي تؤدي إلى التحرك الدولي نحوى مواجهتها .

الفقرة الثانية: جهود دولة قطر لمواجهة الجريمة الالكترونية:

سعت دولة قطر إلى تكريس نظام قانوني فعال في مجال مكافحة الجريمة الالكترونية خاصة باعتبارها من الجرائم المنظمة العابرة للحدود الوطنية، ونظرا لخطورة هذا النوع من الجرائم وتميزه بجملة من الخصائص كما سبق التطرق إليه، وعليه وفي هذا الإطار سنتطرق إلى جهود دولة قطر على المستوى الوطني، بالإضافة إلى الجهود الدولية .

أولا: الجهود القطرية على المستوى الوطني:

تختلف السلطات الوطنية المختصة في البحث عن الأدلة الرقمية في الجرائم المنظمة العابرة للحدود الوطنية من دولة إلى أخرى، ولكن في العادة تتضمن هذه السلطات الشرطة الإلكترونية: وهي السلطة المسئولة عن جمع وتحليل الأدلة الرقمية في حالات الجرائم المنظمة العابرة للحدود الوطنية والهجمات الإلكترونية.

ويشمل عملها تحديد مصادر الهجمات وتتبع الجرائم المنظمة العابرة للحدود الوطنية وجمع الأدلة الرقمية، النيابات العامة، وهي السلطة المسئولة عن تحليل وتبادل الأدلة الرقمية في إطار التعاون الدولي في مكافحة الجرائم الإلكترونية المنظمة، ويشمل عملها تحليل الأدلة الرقمية المقدمة من الدول الأخرى وتبادل الأدلة الرقمية مع الدول الأخرى، الجهات المتخصصة في مجال الأمن السيبراني: وهي السلطات المسئولة عن تحليل وتبادل الأدلة الرقمية في إطار مكافحة الهجمات السيبرانية وحماية البنية التحتية الحيوية للدولة، ويشمل عملها تحديد وتحليل الأدلة الرقمية وتطوير استراتيجيات الحماية والدفاع السيبراني، بالإضافة إلى الجهات المختصة في مجال الأمن القومي وهي السلطات المسئولة عن جمع وتحليل الأدلة الرقمية المتعلقة بالأمن القومي والدفاع عن الدولة. ويشمل عملها جمع الأدلة الرقمية المتعلقة بالتهديدات الإرهابية والأمن السيبراني والتجسس الإلكتروني.

يجب على هذه السلطات الوطنية المختصة البحث عن الأدلة الرقمية في الجرائم المنظمة العابرة للحدود الوطنية أن تعمل بشكل متكامل وتعاون مع بعضها البعض لضمان حماية الأفراد والمجتمع والدولة بشكل عام.

وعليه وفي هذا الإطار سوف نتطرق إلى النصوص القانونية التي كرسها المشرع القطري في مكافحة هذا النوع من الجرائم، بالإضافة إلى التطرق لمختلف الأجهزة المتخصصة في هذا المجال.

ISSN : 2735-3737 eISSN : 2735-3745

١ _ من ناحية النصوص والأحكام القانونية:

نص قانون العقوبات القطري على جرائم الحاسب الآلي، وأدرجها ضمن الجرائم الواقعة على المال، ونظمها في ١٨ مادة تبدأ بالمادة ٣٧٠ وتنتهي بالمادة ٣٨٧، حيث احتوت على أحكام تتعلق بنظام المعالجة الآلية للبيانات، وفيروس الحاسب الآلي، وبطاقات الدفع الممغنطة [٦]، وتعتبر دولة قطر من أوائل الدول العربية التي وضعت أحكاما في قانون العقوبات تتعلق بالجرائم ذات الصلة بالحاسب الآلي .

وفيما يتعلق بسريان القانون القطري على الجرائم العابرة للحدود، تجدر الإشارة إلى أن المشرع القطري أخذ بمبدأ العالمية، حيث حدد جرائم على سبيل الحصر تخضع لهذا المبدأ، ولم يذكر من بينها الجرائم الالكترونية، حيث نص في المادة ١٧ من قانون العقوبات القطري على أنه "تسري أحكام هذا القانون على كل من وجد في الدولة بعد أن ارتكب في الخارج، بوصفه فاعلا أو شريكا أيا من جرائم الاتجار في المخدرات أو في الأشخاص أو جرائم القرصنة أو الإرهاب الدولي"، وفي هذا الجانب يرى الدكتور بشير سعد أنه من الضروري إدراج الجرائم الالكترونية ضمن الجرائم التي يطبق عليها هذا المبدأ، لكونه يساهم في تفعيل التعاون الدولي لمكافحة هذا النوع من الجرائم [٧].

وبالرجوع إلى قانون الإجراءات الجنائية القطري نجد أن المشرع القطري اهتم بمكافحة هذا النوع من الجرائم من خلال إقراره لجملة من النصوص ذات الصبغة الدولية والتي تسمح بمتابعة مرتكبي هذا النوع من الجرائم من خلال تكريس تعاون الجهات القضائية القطرية، مع الجهات القضائية الدولية وتقديم المساعدة القانونية المتبادلة في المجال الجنائي، حيث نصت المادة ٤٠٧ من القانون رقم ٢٣ لسنة ٢٠٠٤، على أنه " مع عدم الإخلال بأحكام الاتفاقيات الدولية المعمول بها في دولة قطر مع شرط المعاملة بالمثل، تتعاون الجهات القضائية القطرية مع الجهات القضائية الأجنبية و الدولية، وتقدم لها المساعدة القانونية في المجال الجنائي، طبقا لأحكام القانون" [٨].

يتضح من نص المادة السالفة الذكر بأن المشرع القطري أولى اهتماما كبيرا بالتعاون الدولي في مجال مكافحة الجريمة المنظمة من خلال تعاون الأجهزة القضائية التابعة لدولة قطر مع الأجهزة القضائية التابعة لدول أجنبية من خلال تقديم

---

[٦] _ القانون رقم ١١ لسنة ٢٠٠٤، المتضمن قانون العقوبات القطري، الجريدة الرسمية العدد ٧، لسنة ٣٠-٠٥-٢٠٠٤.

[٧] _ مريم عبد اللطيف المسلماني، مرجع سابق، ص٣٠ .

[٨] _ القانون رقم ٢٣ لسنة ٢٠٠٤، المتضمن قانون الإجراءات الجنائية القطري، الجريدة الرسمية العدد ١٢، لسنة ٢٩-٠٨-٢٠٠٤.

ISSN : 2735-3737 eISSN : 2735-3745

المساعدات القانونية المتبادلة، كما نص قانون الإجراءات الجنائية القطري على أحكام تفصيلية في مجال تنظم مسألة التعاون الدولي في مجال مكافحة الجريمة من خلال وضع أحكام تتعلق بتسليم المحكوم عليهم، كما نظم مسألة الإنابة القضائية، بالإضافة إلى نقل المحكوم عليهم المحبوسين من دولة قطر إلى دول أجنبية أو العكس، وهذا ما سنتناوله بالتفصيل في الباب الثاني .

إن الطبيعة الخاصة للجريمة الالكترونية ومع تطورها وأثرها البالغ على الاقتصاد الوطني وكذا متطلبات حماية الخصوصية للأشخاص، ومع الاتفاق الدولي على إلزامية مكافحة هذا النوع من الجرائم دفع المشرع القطري على التماشي مع هذا التطور في مجال التكنولوجيا الرقمية، حيث أصدر المشرع القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية، بهدف مواجهة مختلف الاعتداءات التي يتعرض لها النظام المعلوماتي، بحيث يواكب الوسائل الحديثة التي ترتكب بها هذا النوع الجرائم.

كما تجدر الإشارة بأن هناك عدة دول أصدرت تشريعات خاصة تنظم مسألة مكافحة الجرائم الالكترونية، كالتشريع الإماراتي، والبحريني، والمصري، والأردني، وغيرها مع اختلاف التشريعات في التسميات التي أطلقتها على القانون الذي يجرم الاعتداءات التي تتم على الأنظمة المعلوماتية [٩].

وبالرجوع إلى قانون مكافحة الجرائم الالكترونية القطري، نجد أنه نص على مجوعة من العقوبات لمختلف الجرائم في الباب الثاني منه، حيث نجده في المادة الثانية من الفصل الأول نص على جرائم الاعتداء على أنظمة وبرامج وشبكات المعلومات والمواقع الالكترونية على أنه "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها.

وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة ".

[٩] _ مريم عبد اللطيف المسلماني، مرجع سابق، ص ٣٥.

ISSN : 2735-3737 eISSN : 2735-3745

بالإضافة على تنصيصه على عقوبات أخرى تتعلق بجرائم المحتوى، وكذا جرائم التزوير والاحتيال الالكتروني، وجرائم بطاقات التعامل الالكتروني،وجرائم التعدي على حقوق الملكية الفكرية [١٠].

أما في مجال التعاون الدولي لمكافحة الجرائم الالكترونية، فان المشرع القطري لم يكتفي بالقواعد العامة المنصوص عليها في قانون الإجراءات الجنائية القطري بل أفرد بابا خاصا للتعاون الدولي من أجل مسايرة التوجه الدولي في إطار مكافحة هذا النوع من الجرائم [١١].

٢- من ناحية خصوصية الإجراءات: نتيجة التطور المتسارع والانفتاح العالمي والعولمة، فقد بات العديد من الجرائم يتم ارتكابها من خلال شبكة الانترنيت، ونتيجة التنظيم الالكتروني لهذا النمط من الجرائم فقد أضيفت صفة العقيد، وصعوبة الملحقة لمرتكبي هذه الجرائم، وكان لابد من وجود إطار تشريعي قانوني لمواجهة هذه الجرائم في الوطن العربي.

٢-١. التحقيق في الجرائم الالكترونية:

يعد التحقيق أول مرحلة من مراحل الدعوى الجزائية، وهو عبارة عن إجراءات تتخذها السلطات بالتحقيق من أجل جمع المعلومات والأدلة التي تساعد على التحقيق في الجريمة، وهناك مجموعة من الإجراءات يجب إتباعها في هذا الإطار للحصول على الدليل على وقوع الجريمة، وسنتناول في هذا الجزء التفتيش والخبرة فقط لكونهما أكثر الإجراءات تماسا وأهمية في نطاق الجريمة الالكترونية.

أ. التفتيش: يقصد بالتفتيش البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها و كل ما له علاقة بها أو بفاعلها، والتفتيش في الجرائم الالكترونية أما أن يكون عن المكونات المادية للحاسوب، أو يكون عن المكونات المعنوية مثل البيانات والمعلومات، و يختلف تفتيش الكيانات المادية وتفتيش الكيانات المعنوية كالأتي:

_ **تفتيش المكونات المادية للحاسب الآلي**: إن التفتيش المتعلق بالكيانات المادية في نطاق الجرائم الالكترونية يسهل إجراؤه وتنطبق عليه القواعد التقليدية للتفتيش، إذ لا خلاف على إن الولوج إلى المكونات المادية للحاسوب بحثا عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبيها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هو من الأماكن العامة أو

---

[١٠] _ راجع المواد ٢ إلى ١٣ من القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية القطري .

[١١] _ راجع المادة ٢٣ وما بعدها من القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية القطري .

ISSN : 2735-3737 eISSN : 2735-3745

من الأماكن الخاصة، حيث إن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له حرمة، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها التفتيش وبنفس الإجراءات المقررة قانونا في التشريعات المختلفة، مع مراعاة التمييز بين ما إذا كانت مكونات الحاسوب المراد تفتيشها منعزلة عن غيرها من أجهزة الأخرى، أم أنها متصلة بحاسوب أخر أو بنهاية طرفيه في مكان أخر كمسكن غير المتهم مثلا، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود التي يستلزمها المشرع لتفتيش هذه الأماكن، أما إذا وجد شخص يحمل مكونات الحاسوب المادية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة سواء كانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أم كانت من الأماكن العامة بالتخصيص كالمقاهي و المطاعم و السيارات العامة، فان تفتيشها لا يكون إلا في الحالة التي يجوز فيها تفتيش الأشخاص وبنفس القيود المنصوص عليها في هذا المجال.

_ **التفتيش عن المكونات المعنوية للحاسب الآلي:** أثار تفتيش الكيانات المعنوية خلافا كبيرا في الفقه، فذهب رأي في الفقه إلى جواز تفتيش وضبط البيانات الالكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أي شيء)، فان ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة، بينما ذهب رأي أخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فانه يقترح أصحاب هذا لمواجهة هذا القصور التشريعي بالنص صراحة على جواز تفتيش المكونات المعنوية للكمبيوتر.

أما بالرجوع إلي بعض التشريعات المقارنة وفي هذا المجال فقد تعرض المشرع الأردني لموضوع التفتيش عن الكيانات المعنوية للحاسب الآلي حيث نص على أنه: يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم[١٢].

وإذا ما تصفحنا المواد الخاصة بالتفتيش في قانون مكافحة الجرائم الالكترونية القطري رقم (١٤) لسنة (٢٠١٤) سنجد أن المشرع القطري نص في

---

[١٢] _ مخلد ابراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجريمة الالكترونية، المجلة العربية للنشر العلمي، العدد ٣٧، لسنة ٢٠٢١، ص ٢٨٧ .

ISSN : 2735-3737 eISSN : 2735-3745

المادة (١٤) للنيابة العامة أو من تندبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة ، ويجب أن يكون أمر التفتيش مسببا ومحددا، و يجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة، فإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ ما يلزم بشأنها، إضافة إلى ما نصت عليه المادة (١٥) من ذات القانون بقولها "لا يجوز استعباد أي دليل ناتج عن وسيلة من وسائل تقنية المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الالكترونية أو البيانات والمعلومات الالكترونية بسبب طبيعة ذلك"، لذا يستدل من النص السابق أن المشرع القطري قد أحسن التوجه حين نص صراحة على جواز التفتيش على الكيانات المعنوية للحاسب الآلي، وتلاشى الخلاف الذي من الممكن أن يحصل لو نص على خلاف ذلك[١٣]، وهذا أيضا ما نص عليه المشرع الأردني.

ب. الخبرة: يقوم المحقق الجنائي في مجال الكشف عن غموض الجريمة وفاعلها باتخاذ الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه، ومن ضمن هذه الإجراءات الاستعانة بأهل الخبرة وذلك تحقيقا لمبدأ هام وهو مبدأ التخصص نظرا لكون الخبرة وهي تقدير مادي أو ذهني يبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها وبمعلوماته الخاصة سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أم بجسم الجريمة أم المواد المستعملة في ارتكابها أم أثارها.

إن اختيار الخبير في الجرائم الالكترونية يتوقف على نوع الجريمة المرتكبة ومجال الخبرة المطلوبة وطبيعتها الفنية، فلا يكفي حصول الخبير على درجة علمية معينة، وإنما ينبغي أن تكون لديه خبرة علمية تخصصية وكفاءة فنية عالية في حقل أو أكثر من حقول تقنية المعلومات ونظمها ووسائلها، فقد تكون الجريمة المرتكبة تزوير مستندات أو تلاعبا في البيانات أو الغش أثناء نقل أو بث البيانات أو إطلاق الفيروسات أو قرصنة أو اعتداء على حرمة الحياة الخاصة أو التجسس[١٤]، وقد نص المشرع القطري في المادة (١٨) من قانون مكافحة الجرائم الالكترونية على أنه " للنيابة العامة أن تأمر كل ذي صلة بتسليم الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الالكترونية أو بيانات المرور أو معلومات المحتوى ذات الصلة

[١٣] _ راجع المادتين ١٤ و ١٥ من القانون رقم ١٤ لسنة ٢٠١٤، المتضمن إصدار قانون مكافحة الجرائم الالكترونية القطري، الجريدة الرسمية عدد ١٥، لسنة ٢٠١٤.

[١٤] _ مخلد إبراهيم الزعبي، مرجع سابق، ص ٢٨٨ .

ISSN : 2735-3737 eISSN : 2735-3745

بموضوع الجريمة أو ما يفيد في كشف الحقيقة وللنيابة العامة أن تأمر بالتحفظ على الأجهزة أو الأدوات أو الوسائل المستخدمة في ارتكاب الجريمة"[١٥].

٢-٢. المحاكمة في الجرائم الالكترونية:

تعد السلطة القضائية هي السلطة المختصة للفصل في المنازعات التي قد تنشأ الأفراد، أو بين الأفراد والسلطة، وقد منحت القوانين الوطنية هذه السلطة الاستقلالية في إصدار أحكامها، وفي الوقائع إن إجراءات المحاكمة في الجرائم التقليدية لا تختلف عن إجراءات المحاكمة في الجرائم الالكترونية، مع العلم أن القاضي ينظر في قضايا ليس لديه الخبرة فيها، فعلى سبيل المثال استعان قاضي في باريس بخبيرين أحدهما انجليزي، والثاني أمريكي، إضافة إلى خبير فرنسي لإعداد تقرير حول إمكانية رصد مسار الانترنيت، وتختلف مرحلة المحاكمة عن مرحلة التحقيق، حيث أن السلطة المختصة بالتحقيق هي النيابة العامة، أما السلطة المختصة هي المحاكمة يمثلها قضاة مستقلون، ولتوضيح التحقيق والمحاكمة في الجرائم الالكترونية[١٦]، سنتناول مرحلة المحاكمة في الجرائم الالكترونية من خلال الآتي:

أ. المحكمة المختصة في الجرائم الالكترونية: يختص القضاء القطري في الدعاوي و الطلبات المدنية والجزائية المعروضة عليه، إضافة إلى القواعد القانونية التي تحدد اختصاص كل محكمة في النظر بالدعوى، أما بالرجوع إلى بعض التشريعات المقارنة فقد نص المشرع الأردني على المحاكم النظامية، وجعلها صاحبة الاختصاص بالنظر في الدعاوي المدنية والجزائية، حيث نص المشرع الأردني على أنه "تمارس المحاكم النظامية في المملكة حق القضاء على جميع الأشخاص في جميع المواد المدنية و الجزائية باستثناء المواد التي يفوض فيها حق القضاء إلى محاكم دينية، أو محاكم خاصة بموجب أحكام أي قانون أخر.

ب. إجراءات المحاكمة في الجرائم الإلكترونية :الإحالة هو الإجراء الذي يترتب عنه دخول الدعوى في اختصاص المحكمة، والأصل في المحاكمة أن تكون علنية لضمان الصالح العام، إلا أن القانون أجاز النظر في بعض الدعوى بطريقة سرية لا يحضرها الجمهور، وذلك لاعتبارات المحافظة على النظام العام والآداب، وقد صنف المشرع الأردني الجرائم الإلكترونية إلى جنايات وجنح،واعتقد أن المشرع الأردني قد أصاب في ذلك، لأنه ليس من العدل أن تكون جريمة الدخول إلى موقع مثل جريمة الاستغلال الجنسي للأطفال[١٧]، وأيضا هذا ما نص عليه المشرع القطري في المادة (٤٩) يعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة في ارتكاب جناية أو جنحة

---

[١٥] القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية القطري .

[١٦] مخلد ابراهيم الزعبي، مرجع سابق، ص ٢٨٩ .

[١٧] مخلد إبراهيم الزعبي، مرجع سابق، ص ٢٨٩ .

ISSN : 2735-3737 eISSN : 2735-3745

معاقب عليها بموجب أحكام هذا القانون، بذات العقوبات المقررة للفاعل الأصلي، إضافة إلى المادة (٥٠) يعاقب كل من شرع في ارتكاب جناية أو جنحة معاقبا عليها بموجب أحكام هذا القانون بالحبس مدة لا تجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة التامة[١٨].

إضافة إلى ذلك نصت المادة (١٩) من قانون مكافحة الجرائم الإلكترونية القطري "على الجهة المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على الأجهزة أو الأدوات أو وسائل تقنية المعلومات، أو الأنظمة المعلوماتية أو البيانات أو المعلومات الإلكترونية محل التحفظ، لحين صدور قرار من الجهات القضائية المعنية بشأنها، كما أخذ المشرع السعودي بحجية الدليل الإلكتروني في الإثبات، فقد نص قانون التعاملات الإلكترونية السعودي في المادة (٢) على أن أهداف هذا النظام، هي إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بواسطة سجلات إلكترونية يعول عليها.

٣_ من ناحية الأجهزة المختصة بمكافحة الجرائم الالكترونية:

تتخصص مصالح البحث والتحري وإنفاذ القانون والإجراءات الوطنية بشكل متزايد في إجراء التحقيقات المتعلقة بجرائم الإنترنت والجرائم التي تنطوي على عناصر من الأدلة الرقمية، وتبرز أهمية هذه التخصصات في تيسير عملية جمع وتحليل وتبادل الأدلة الرقمية، وذلك يرجع قبل كل شيء إلى الطبيعة الخاصة لجرائم الإنترنت، التي تواجه صعوبات خاصة فيما يتعلق بضبط الجرائم، وتطبيق القوانين، وجمع وتحليل الأدلة، ومن ثم فإن مستوى المهارات والقدرات التقنية لمصالح البحث والتحري وإنفاذ القانون والإجراءات سيؤثر مباشرة على فعالية إجراءات الوقاية من الجريمة وإجراءات القمع المتخذة لمكافحة جرائم الإنترنت.

ونظراً للدور المتزايد الذي تلعبه الأجهزة الإلكترونية والإنترنت والاتصالات العالمية في الحياة اليومية، أصبح استغلال الأدلة الرقمية مثل الرسائل القصيرة والبريد الإلكتروني وبيانات التصفح على الإنترنت شيئًا مألوفًا في العديد من التحقيقات، ولذلك وفي جميع مستويات مصالح البحث والتحري وإنفاذ القانون (سواء على المستوى المحلي أو الوطني)، تشير المؤشرات إلى وجود حاجة متزايدة للحصول على مهارات أساسية على الأقل للتحقيق في جرائم الإنترنت [١٩].

---

[١٨] _ أنظر المادتين ٤٩ و ٥٠ من القانون رقم ١٤ لسنة ٢٠١٤ .

[١٩] _ Nations Unies, Collecte et partage de preuves électroniques, Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée, 18 août 2015، p 5.

ISSN : 2735-3737 eISSN : 2735-3745

إن العديد من البلدان بحاجة إلى المساعدة التقنية في مجال التحقيق في جرائم الإنترنت، وخاصة فيما يخص تقنيات التحقيق، حيث كشفت دراسة مكتب الجريمة والمخدرات أن ٦٠% من البلدان قد أبلغت أن مصالحها للبحث والتحري تحتاج إلى مساعدة في هذا المجال[٢٠].

بالإضافة إلى ذلك، أظهرت المعلومات المقدمة من في الدراسة أن التحقيقات في جرائم الإنترنت غالبًا ما يتم تحويلها من فروع الشرطة المحلية إلى جهة مسؤولة عن البحث والتحري والتحقيق والمحاكمة على المستوى الوطني، وهذا يشير إلى أن قدرات التحقيق في جرائم الإنترنت يمكن أن تختلف بشكل كبير من مستوى محلي إلى مستوى وطني، وأن بعض البلدان بحاجة إلى مساعدة لتعزيز قدراتها في مجال التحقيق في جرائم الإنترنت[٢١].

وفي هذا الإطار أوجد المشرع القطري مجموعة من الأجهزة والهيئات بهدف متابعة ومكافحة مختلف أنواع الجرائم الالكترونية بالنظر إلى الخصوصية التي تمتاز بها هذا النوع من الجرائم نذكرها على النحو التالي:

٣ _ ١. نيابة الجرائم الالكترونية:

أصدر سعادة النائب العام قراره رقم ٧٢ لسنة ٢٠١٨ م، بشأن إنشاء نيابة الجرائم الالكترونية وتحديد اختصاصاتها، وبموجبه تم إنشاء نيابة الجرائم الالكترونية بتاريخ ٢١-٠٦-٢٠١٨م، حيث تختص بالتحقيق والتصرف في الجرائم التالية [٢٢] :

_ الجرائم التي تقع بالمخالفة لأحكام القانون رقم ٨ لسنة ١٩٧٩ بشأن المطبوعات والنشر، عدا ما كان من اختصاص نيابة أمن الدولة ومكافحة الإرهاب.

_ الجرائم المنصوص عليها في المواد ٢٠٣، ٢٩٣، ٣٣١، ٣٣٢، ٣٣٣ والفصل الخامس المتضمن جرائم الحاسب الآلي من قانون العقوبات القطري رقم ١١ لسنة ٢٠٠٤.

_ الجرائم التي تقع بالمخالفة لأحكام القانون رقم ٣٤ لسنة ٢٠٠٦ المتضمن إصدار قانون الاتصالات والمعدل بالقانون رقم ١٧ لسنة ٢٠١٧.

_ الجرائم التي تقع بالمخالفة لأحكام القانون رقم ١٤ لسنة ٢٠١٤ المتضمن قانون مكافحة الجرائم الالكترونية، عدا ما كان من اختصاص نيابة أمن الدولة ومكافحة الإرهاب .

---

[20] _ Nations Unies, Collecte et partage de preuves électroniques, Op. Cit. P. ٥.

[21] _ Nations Unies, Collecte et partage de preuves électroniques, Op. Cit. P. ٥.

[٢٢]- مريم عبد اللطيف المسلماني، مرجع سابق، ص ٤٣.

ISSN : 2735-3737 eISSN : 2735-3745

_ الجرائم التي تقع بالمخالفة لأحكام القانون رقم ١٦ لسنة ٢٠١٠ المتضمن إصدار قانون المعاملات والتجارة الالكترونية، عدا ما كان من اختصاص نيابة التجارة وشؤون المستهلك .
_ الجرائم التي تقع بالمخالفة لأحكام القانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية.
_ الجرائم المرتبطة ارتباطا لا يقبل التجزئة بالجرائم سالفة البيان.
_ أي مهام أخرى تكلف بها في نطاق الاختصاص .
ويكون اختصاص نيابة الجرائم الالكترونية شاملا جميع أنحاء الدولة .

بالإضافة إلى نيابة التعاون الدولي التي تختص بمجال تسليم المتهمين أو المحكوم عليهم أو الأشياء المتحصلة من الجريمة كما تختص بالنظر في طلبات الإنابة القضائية والتحقيق فيها، بالإضافة إلى النظر في تبادل التنفيذ القضائي، كما تقوم بدراسة مشاريع الاتفاقيات الدولية و مذكرات التفاهم، و هذا في إطار التعاون الدولي المنصوص عليه في القانون رقم ١٤ لسنة ٢٠١٤ المتضمن قانون مكافحة الجرائم الالكترونية.

٣-٢. إدارة مكافحة الجرائم الاقتصادية والالكترونية:

تعد إدارة مكافحة الجرائم الاقتصادية والالكترونية إحدى الوحدات الإدارية بوزارة الداخلية، لها دور بارز في التعاون الدولي لمكافحة الجريمة الالكترونية، من خلال الأحكام الواردة في الباب الرابع من قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الالكترونية، كما تختص إدارة مكافحة الجرائم الاقتصادية والالكترونية في التحقيق بالجرائم وعرضها على النيابة العامة، وكذلك البحث والتحري في المواقع الالكترونية المشبوهة، والبحث والتحري في البلاغات المقدمة من قبل المتضررين، وعلى الصعيد الدولي هناك تعاون بينهما وبين الأنتربول وشركات الأمم (كالسناب شات، والاستغرام) للتصدي للجريمة الالكترونية [٢٣].

٣-٣. إدارة الاتصال للشرطة العربية و الدولية (الانتربول) بوزارة الداخلية:

إدارة الاتصال للشرطة العربية والدولية (الانتربول) تتبع مكتب معالي رئيس مجلس الوزراء وزير الداخلية في الهيكل التنظيمي، وكانت تسمى في السابق شعبة الاتصال والانتربول، تعمل على تنمية علاقات التعاون والتنسيق في مجال مكافحة الإجرام عربيا و دوليا.

وتضم شعبة الاتصال مجلس وزراء الداخلية العرب، والتي تم إنشاؤها بموجب النظام الأساسي للمجلس الذي نص على إنشاء شعبة اتصال في كل دولة

[٢٣] _ مريم عبد اللطيف المسلماني، مرجع سابق، ص ٤٣ – ٤٤

ISSN : 2735-3737 eISSN : 2735-3745

عربية عضو وتضم الإدارة المكتب المركزي الوطني (الانتربول) الذي نشأ بموجب النظام الأساسي للمنظمة حيث ينص على إنشاء مكتب مركزي وطني في كل دولة[٢٤].

ومن الأمثلة العملية لتعاون دولة قطر مع الانتربول في مجال مكافحة الجريمة الالكترونية هو الحكم الصادر عن المحكمة الابتدائية بدولة قطر بتاريخ ٢٠١٨/١٠/٣٠م، حيث تتلخص وقائع الدعوى في أنه وردت معلومات للشرطة الجنائية الدولية (الانتربول) بأن المتهم متواجد بدولة قطر و يقوم بتحميل ورفع مواد إباحية تخص الأطفال وبعد البحث والتحري تبين أن المتهم هو الذي يملكها ويستخدمها، وتمت إدانته بتهمة نشر وتداول مقاطع إباحية خاصة بالأطفال بواسطة تقنية المعلومات [٢٥].

٣-٤. اللجنة الوطنية لأمن المعلومات :

أنشأت اللجنة الوطنية لأمن المعلومات بموجب القرار الأميري رقم (١٩) لسنة ٢٠١٦، برئاسة رئيس مجلس الوزراء ووزير المواصلات والاتصالات، نائبا للرئيس، وتضم في عضويتها ممثل عن كل الجهات التالية : (وزارة الداخلية، وزارة الدفاع، وزارة الخارجية، وزارة التجارة والصناعة، وزارة المالية، وزارة العدل، وزارة المواصلات والاتصالات، النيابة العامة، جهاز أمن الدولة، مصرف قطر المركزي).

ونص القرار أعلاه في المادة (٣) منه على أنه : " تهدف اللجنة إلى تعزيز أمن المعلومات في الدولة بما يحقق خطط التنمية الشاملة في جميع المجالات، وذلك من خلال التوجيه الاستراتيجي للجهود الوطنية اللازمة لتنفيذ الأهداف المحددة في الإستراتيجية الوطنية لأمن المعلومات، وتحقيق التعاون مع الجهات المختصة أو المعنية في هذا المجال ".كما نص القرار بأن اللجنة أن تمارس كافة الاختصاصات والصلاحيات اللازمة لتحقيق أهدافها، وأشار إلى بعض منها على وجه الخصوص، ومن بينها إنشاء قنوات الاتصال مع المؤسسات الدولية والجهات الخارجية المختصة ووضع أطر التعاون معها ومتابعة التطورات والمستجدات في هذا المجال [٢٦].

٣-٥. الوكالة الوطنية للأمن السيبراني:

لقد نصت المادة (٣) من القرار الأميري رقم (١) لسنة ٢٠٢١ بإنشاء الوكالة الوطنية للأمن السيبراني على أن الهدف من إنشاء الوكالة هو المحافظة على

---

[٢]-راجع الموقع الرسمي لوزارة الداخلية لدولة قطر،
https://portal.moi.gov.qa/wps/portal/MOIInternet/departmentcommittees

[٢٥] مريم عبد اللطيف المسلماني، مرجع سابق، ص ٤٥ .

[٢٦] قرار أميري رقم ١٩ لسنة ٢٠١٦، المتضمن إنشاء اللجنة الوطنية لأمن المعلومات، الجريدة الرسمية العدد ٥، لسنة ٢٠١٦-٠٤-٢٧.

ISSN : 2735-3737 eISSN : 2735-3745

الأمن الوطني السيبراني وتنظيمه وتعزيز المصالح الحيوية للدولة وحمايتها في مواجهة تهديدات الفضاء السيبراني وفي سبيل كشف ذلك منحت الوكالة كافة الاختصاصات والصلاحيات، منها إعداد الإستراتيجية الوطنية للأمن السيبراني، وضع وتحديث السياسات المتعلقة بتعزيز الأمن السيبراني، وضع أطر لكيفية إدارة المخاطر السيبرانية، رفع مستوى الوعي بالأمن السيبراني، ولم نجد نصا صريحا خاص بالتعاون الدولي لمكافحة الجريمة الالكترونية إلا أن المادة سالفة الذكر نصت على بنود يستفاد منها اتخاذ الوكالة التعاون الدولي كآلية للمحافظة على الأمن السيبراني حيث منحت الوكالة مكنة إبرام العقود ومذكرات التفاهم مع الجهات المحلية والدولية المعنية بالأمن السيبراني[٢٧]، كما تقوم الوكالة بإعداد التقارير عن الحالة الأمنية السيبرانية محليا وإقليميا ودوليا [٢٨]، كما تضع الوكالة آليات لتبادل المعلومات ذات العلاقة بالأمن السيبراني مع الجهات المحلية والدولية[٢٩] .

ثانيا: الجهود القطرية على المستوى الدولي :

سعت قطر لتجريم الجرائم المنظمة على المستوى الدولي كلك وكان بعقد اتفاقيات ثنائية ومتعددة الأطراف.

١-الاتفاقيات الثنائية:

أبرمت دولة قطر العديد من الاتفاقيات الثنائية مع مختلف الدول في مجال مكافحة الجرائم الالكترونية، نشير إلى بعض منها على النحو التالي:

١-١. في مجال مكافحة الجريمة:

- اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر وحكومة الجمهورية الجزائرية الديمقراطية الشعبية، والتي نصت على أن يتعاون الطرفان في المجال التقني وتبادل المعلومات والخبرات في عدة مجالات من بينها مكافحة الجرائم الالكترونية[٣٠].

- مذكرة تفاهم بشأن مكافحة الجريمة بين حكومة دولة قطر وحكومة جمهورية إيطاليا، والتي تناولت التعاون في مجال منع وكشف وقمع الجريمة ومرتكبيها من

---

[٢٧] أنظر البند ١٨ من المادة ٣، من القرار الأميري رقم ١ لسنة ٢٠٢١، المتضمن إنشاء الوكالة الوطنية للأمن السيبراني،الجريدة الرسمية عدد٣ لسنة ٢٠٢١-٠٣-٢٤.

[٢٨] أنظر البند ٥ من المادة ٣، من القرار الأميري رقم ١ لسنة ٢٠٢١، المتضمن إنشاء الوكالة الوطنية للأمن السيبراني،الجريدة الرسمية عدد٣ لسنة ٢٠٢١-٠٣-٢٤.

[٢٩] أنظر البند ٩ من المادة ٣،المرجع نفسه.

[٣٠] اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر وحكومة الجمهورية الجزائرية الديمقراطية، الجريدة الرسمية عدد ١٥، لسنة ٢٠١٧.

ISSN : 2735-3737 eISSN : 2735-3745

خلال السلطات المختصة في كلا البلدين، وتبادل المعلومات في عدة مجالات من بينها جرائم الحاسوب الآلي و الشبكة المعلوماتية العالمية (الانترنيت)[٣١].

١-٢.في المجال الأمني:

- مذكرة تفاهم للتعاون الأمني بين وزارة الداخلية في دولة قطر وإدارة الشرطة الوطنية بجمهورية كوريا، والتي نصت على يتعاون الطرفان في مجال مكافحة الجريمة بصفة عامة، وحددت على وجه الخصوص بعض الجرائم من بينها جرائم الحاسب الآلي و شبكة المعلومات (الانترنيت) [٣٢].

- مذكرة تفاهم للتعاون الأمني بين حكومة دولة قطر بوزارة الداخلية وحكومة المملكة المتحدة والتي نصت على التعاون في مجال الأمن الالكتروني، وتبادل الخبرات والمعلومات في مجال التحقيقات المعنية بالجرائم الالكترونية[٣٣].

١-٣.في المجال القضائي:

- اتفاقية التعاون القانوني والقضائي بين حكومة دولة قطر وحكومة المملكة المغربية.

١-٤. في مجال الأمن السيبراني:

- خطاب نوايا للتعاون في مجال الأمن السيبراني بين حكومة دولة قطر وحكومة الولايات المتحدة الأمريكية، والذي ينص على التعاون في مجال تبادل المعلومات ومكافحة الجريمة السيبرانية.

مما سبق يتضح لنا بأن دولة قطر أقامت تعاون ثنائي مع مختلف دول العالم في سبيل التعاون الدولي لمكافحة الجرائم الالكترونية، حيث أن إبرام اتفاقيات ثنائية الأطراف في هذا المجال يعطي انطباع بوجود وعي بضرورة التحرك الدولي من أجل التصدي للجريمة الالكترونية[٣٤].

---

[٣١] _ مذكرة تفاهم بشأن مكافحة الجريمة بين حكومة قطر وحكومة جمهورية ايطاليا، الجريدة الرسمية عدد ٩ لسنة ٢٠١٨ .

[٣٢] _ مذكرة تفاهم للتعاون الأمني بين وزارة الداخلية في دولة قطر وادارة الشرطة الوطنية بجمهورية كوريا، الجريدة الرسمية عدد ٧ لسنة ٢٠١١ .

[٣٣] _ مذكرة تفاهم للتعاون في تطوير القدرات الشرطية المتصلة بمنع، وكشف، وتحري الجرائم، وحفظ الأمن بين وزارة الداخلية بدولة قطر وإدارة شرطة العاصمة الكبرى –لندن- ، الميتروبوليتان، الجريدة الرسمية عدد ٨ لسنة ٢٠١٠ .

[٣٤] _ مريم عبد اللطيف المسلماني، مرجع سابق، ص ٥١ .

ISSN : 2735-3737 eISSN : 2735-3745

٢- الاتفاقيات المتعددة الأطراف:

سبق وأن أشرنا بأن هناك خمس اتفاقيات دولية أبرمت في مجال مكافحة الجرائم الالكترونية، ودولة قطر طرفا في إحدى هذه الاتفاقيات وهي الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات حيث وقعت عليها بتاريخ ٢٠١٠/١٢/٢١ م، وصادقت عليها بتاريخ٢٠١٢/١٢/٢٤ م.

وهناك اتفاقيات أخرى أبرمتها دولة قطر لها صلة في موضوع مكافحة الجرائم الالكترونية بشكل غير مباشر كونها جريمة عابرة للحدود، نورد منها على النحو التالي:

٢-١. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية:

انضمت إليها دولة قطر بتاريخ ٢٠٠٨/٠٦/٢٧ م، ونصت على تبادل وتحليل المعلومات عن طبيعة الجريمة المنظمة و التكنولوجيا المستخدمة، وان على كل دولة طرف أن تقوم بتطوير العاملين في أجهزتها في مكافحة الجريمة عبر الوطنية التي ترتكب باستخدام الحواسيب أو شبكات الاتصالات السلكية أو اللاسلكية أو غير ذلك من أشكال التكنولوجيا المستخدمة.

٢-٢. الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية:

وقعت عليها دولة قطر بتاريخ ٢٠١٠/١٢/٢١ م، وصادقت عليها بتاريخ ٢٠١٢/٠٣/٠٥ م، ونصت على تجريم الاستعمال غير المشروع لتقنية المعلومات، كما نصت على أحكام تتعلق بالتعاون القانوني والقضائي والتعاون في مجال التحقيق وتسليم المجرمين.

٢-٣. الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب:

وقعت عليها دولة قطر بتاريخ ٢٠١٠/١٢/٢١ م، وصادقت عليها بتاريخ ٢٠١٢/٠٥/٢٤ م، والهدف منها مكافحة جرائم غسل الأموال وتمويل الإرهاب حيث أشارت إلى تعزيز التعاون العربي والتنسيق المشترك لتبادل المعلومات الالكترونية بما في ذلك التحويل الالكتروني للأموال.

٢-٤. معاهدة الويبو بشأن حق المؤلف لسنة ١٩٩٦ م: أصبحت دولة قطر طرفا فيها منذ ٢٠٠٥/١٠/٠٨ م، وهي إحدى اتفاقيات المنظمة العالمية للملكية الفكرية، وتعتبر هذه المعاهدة اتفاق خاص في إطار اتفاقيات برن وتتناول حماية المصنفات وحقوق مؤلفيها في البيئة الرقمية، وتتضمن المعاهدة موضوعين يتعين حمايتهما بموجب حق المؤلف وهما برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها

ISSN : 2735-3737 eISSN : 2735-3745

ومجموعة البيانات أو المواد الأخرى " قواعد البيانات"، وفي هذا الصدد نشير إلى أن المشرع القطري في قانون مكافحة الجرائم الالكترونية الصادر بالقانون رقم (١٤) لسنة ٢٠١٤ أشار في المادة (١٣) منه على تجريم التعدي على حقوق الملكية الفكرية[٣٥].

خاتمة:

حاولنا من خلال مداخلتنا هذه الوقوف على أهم الصعوبات القانونية للحماية الجزائية للأمن السيبراني ، وقد توصلنا إلى النتائج التالية :

-التحول للعالم الرقمي جعله يصبح قرية صغيرة بفضل شبكات الانترنت فاصبح لا يعترف بالحدود الاقليمية للدول مما سهل ارتكاب أفعال اجرامية عدة عابرة للحدود.

-التوظيف السلبي لمختلف الوسائط الرقمية كان له تبعات خطيرة على الوعي والفكر وعلى الآسرة المجتمعية، مما ابرز نوعا جديدا من الاعمال الجرمية العابرة للحدود عرفت بالجرائم المعلوماتية.

-الجريمة الالكترونية ذات بعد دولي، أي أنها عابرة الحدود، فهي قد تتجاوز الحدود الجغرافية بسبب أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الاحيان تحديات قانونية إدارية فنية، كما ينتج عنه صعوبات سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية و صعوبة اثباتها.

-صعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة، بحيث أن تطبيق القواعد التقليدية على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الاثبات، ومتابعة مرتكبيها.

-جرائم الانترنت صعبة الاكتشاف ، فهي تختلف بعض الشيء عن الجريمة التقليدية، لأن الجاني من الممكن أن يستخدم اسما مستعارا، اضافة الى أنها صعبة الاثبات ، لأنها لا تترك أثرا ماديا، بسبب امكانية حذف الآثار المعلوماتية المستخدمة في ارتكاب الجريمة خلال ثوان.

-مشكلة الاختصاص من المشكلات التي تعرقل الحصول على الدليل في الجريمة المعلوماتية ذلك أن هذه الجرائم التي تثير مسألة الاختصاص على المستوى المحلي و الدولي بسبب التداخل والترابط بين شبكات المعلومات.

[٣٥] _ القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية .

ISSN : 2735-3737 eISSN : 2735-3745

-وقفت القوانين العقابية عاجزة عن التصدي لبعض الجرائم الالكترونية العابرة للحدود للمشكلات الموضوعية و الاجرائية التي تعترضها.

-على الرغم من القصور على مستوى التشريع الوطني، تمكّن القضاء الاردني والقطري خلال السنوات المنصرمة من معالجة الوضع بنجاح ملحوظ عبر النصوص القانونية المتاحة، فلقد قام بتكييف نصوص قانون العقوبات على الافعال الجرمية المستجدة باستعمال الوسائل المعلوماتية، اذ صدرت احكام قضائية عن المحاكمة الجزائية المختصة طبقت النصوص الجزائية على افعال جرمية تمت بوسائل معلوماتية.

توصيات :

للتغلب على هذه الصعوبات القانونية المتعلقة بالجريمة الإلكترونية فإننا نوصي بالآتي:

-مسؤولية مكافحة هذه الجريمة هي مسؤولية كل فرد في المجتمع في الاصل، كون استعمال المسائل الالكترونية هي في متناول الافراد عموما وليست مقتصرة على هيئات او جمعيات بالتخصيص، مما يتوجب توعية وطنية تبدأ من الفرد وصولا الى الجماعة

-تطوير استراتيجية وطنية لمكافحتها وتوثيق التعاون الوطني بين الحكومة والقطاعين الخاص والعام وتأسيس مركز يؤهل المختصين.

-إعادة مراجعة المنظومة القانونية المتعلقة بالجرائم والجنح والجنايات وتكييفها مع مستجدات الواقع التكنولوجي الجديد.

-نهج اجراءات شاملة ومتوازنة للتصدي للجريمة الالكترونية بما فيها مناهج جديدة لجمع البيانات، وتعزيز التعاون الدولي، وإضفاء تناغم على الأحكام الجنائية الوطنية ونهج منع الجريمة.

-يستلزم مزيدا من التعاون بين الدول وأصحاب المصلحة المعنيين، والحاجة إلى إضفاء نوع من التناغم على الأحكام الجنائية التي من شأنها أن تحد أو تقضي بالكامل على السلوك الإجرامي.

-محاولة العمل على توحيد المصطلحات القانونية والفنية في التشريعات السيبرانية للمجتمعات الدولية.

ISSN : 2735-3737 eISSN : 2735-3745

-وضع المنظومة الجزائية التقليدية أمام تحديات كبرى تفرض علينا التعملق والمواكبة لمواجهة خطر محدق يتهدد المجتمعين الوطني والدولي ككل بتكثيف الجهود الدولية والاقليمية لمكافحة هذا النوع من الاجرام.

ISSN : 2735-3737 eISSN : 2735-3745

الهوامش:

علي جبار الحسيني، جرائم الحاسوب والانترنت، دار اليازوني للنشر والتوزيع، عمان، الأردن، ط ١، ٢٠٠٩، ص ٣٣.

خالد عياد الحلبي، اجراءات التحقيق والتحري في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، طَ١، ٢٠١١، ص ٣١.

راجع المادة الأولى من القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجريمة الالكترونية القطري الجريدة الرسمية رقم ١٥،بتاريخ ٢-١٠-٢٠١٤ .

مريم عبد اللطيف المسلماني، مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الالكترونية، مجلة القانون والمجتمع، جامعة قطر، كلية الحقوق، المجلد ١٠، العدد ٠٢، لسنة ٢٠٢٢، ص ١٨.

عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت، دراسة مقارنة، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والأنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧، ص ٣١-٣٣ .

القانون رقم ١١ لسنة ٢٠٠٤، المتضمن قانون العقوبات القطري، الجريدة الرسمية العدد ٧، لسنة ٣٠-٠٥-٢٠٠٤.

القانون رقم ٢٣ لسنة ٢٠٠٤، المتضمن قانون الإجراءات الجنائية القطري، الجريدة الرسمية العدد ١٢، لسنة ٢٩-٠٨-٢٠٠٤.

المواد ٢ إلى ١٣ من القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية القطري .

المادة ٢٣ وما بعدها من القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية القطري .

مخلد ابراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجريمة الالكترونية، المجلة العربية للنشر العلمي، العدد ٣٧، لسنة ٢٠٢١، ص ٢٨٧ .

المادتين ١٤ و ١٥ من القانون رقم ١٤ لسنة ٢٠١٤، المتضمن إصدار قانون مكافحة الجرائم الالكترونية القطري، الجريدة الرسمية عدد ١٥، لسنة ٢٠١٤.

القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية القطري .

قرار أميري رقم ١٩ لسنة ٢٠١٦، المتضمن إنشاء اللجنة الوطنية لأمن المعلومات، الجريدة الرسمية العدد ٥، لسنة ٢٠١٦-٠٤-٢٧.

البند ١٨ من المادة ٣، من القرار الأميري رقم ١ لسنة ٢٠٢١، المتضمن إنشاء الوكالة الوطنية للأمن السيبراني، الجريدة الرسمية عدد٣ لسنة ٢٠٢١-٠٣-٢٤.

ISSN : 2735-3737 eISSN : 2735-3745

البند ٥ من المادة ٣، من القرار الأميري رقم ١ لسنة ٢٠٢١، المتضمن إنشاء الوكالة الوطنية للأمن السيبراني،الجريدة الرسمية عدد٣ لسنة ٢٠٢١-٠٣-٢٤.

اتفاقية للتعاون في مجال مكافحة الجريمة المنظمة بين حكومة دولة قطر وحكومة الجمهورية الجزائرية الديمقراطية، الجريدة الرسمية عدد ١٥، لسنة ٢٠١٧.

مذكرة تفاهم بشأن مكافحة الجريمة بين حكومة قطر وحكومة جمهورية ايطاليا، الجريدة الرسمية عدد ٩ لسنة ٢٠١٨ .

مذكرة تفاهم للتعاون الأمني بين وزارة الداخلية في دولة قطر وادارة الشرطة الوطنية بجمهورية كوريا، الجريدة الرسمية عدد ٧ لسنة ٢٠١١ .

[١]مذكرة تفاهم للتعاون في تطوير القدرات الشرطية المتصلة بمنع، وكشف، وتحري الجرائم، وحفظ الأمن بين وزارة الداخلية بدولة قطر وإدارة شرطة العاصمة الكبرى –لندن، الميتروبوليتان، الجريدة الرسمية عدد ٨ لسنة ٢٠١٠ .

القانون رقم ١٤ لسنة ٢٠١٤، المتضمن قانون مكافحة الجرائم الالكترونية .

Nations Unies, Collecte et partage de preuves électroniques, Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée, 18 août 2015 ،p 5.

ISSN : 2735-3737 eISSN : 2735-3745