جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY
Amman - Jordan

مدى موائمة التشريعات الاردنية للمعاهدات الدولية الخاصة بالأمن السيبراني

إعداد

نورا محمد الدباس

إشراف

الدكتور بلال حسن الرواشده

قدمت هذه الرساله استكمالا لمتطلبات الحصول على درجه الماجستير

في القانون العام

قسم القانون العام

كلية الحقوق

جامعة الشرق الأوسط

كانون الثاني،2026

جـــامـعـة الـــشرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

The compatibility of Jordanian legislation with international cybersecurity treaties.

Prepared by

Noura Mohammad Al-dabbas.

Supervised by

DR. Bilal Hassan Alrawashdeh

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master's Degree in Public Law.

Department of Public law

Faculty of Law

Middle East University

January, 2026

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها: **مدى موائمة التشريعات الاردنية للمعاهدات الدولية الخاصة بالأمن السيبراني**

للباحثة: نورا محمد الدباس

وأجيزت بتاريخ:2026/01/25.

أعضاء لجنة المناقشة

الاسم	الصفة	جهة العمل	التوقيع
د. بلال حسن الرواشدة	مشرفًا	جامعة الشرق الأوسط	
د. أيمن يوسف الرفوع	عضوًا من داخل الجامعة ورئيسًا	جامعة الشرق الأوسط	
د. خالد خلف الدروع	عضوًا من داخل الجامعة	جامعة الشرق الأوسط	
د. عمر صالح العكور	عضوًا من خارج الجامعة	الجامعة الأردنية	

التفويض

أنا **نورا محمد أحمد الدباس،** أفوض جامعة الشرق الأوسط بتزويد نسخة من رسالتي ورقيًا وإلكترونيًا للمكتبات، أو المنظمات، أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: نورا محمد أحمد الدباس.

التاريخ: 2026/01/25.

التوقيع:

الشكر والتقدير

الحمدُ لله ربّ العالمين حمدًا يليق بجلال وجهه، وعظيم سلطانه، الحمد الله الذي بفضله تتم النعم، وتتحقق الغايات، والصلاة والسلام على أشرف الأنبياء والمرسلين؛ نبينا محمد وعلى آله وصحبه أجمعين وبعد،

ففي هذه اللحظة التي أتممت فيها كتابة رسالتي، لا يسعني إلا أن أتقدم بخالص الشكر والتقدير، لكل من كان له دور في إنجاح هذا العمل.

وأبدأ بشكر أستاذي الفاضل المشرف على هذه الرسالة الدكتور بلال حسن الرواشدة، الذي لم يبخل عليّ بعلمه وتوجيهاته القيّمة، وصبره ودعمه المستمرين، طيلة فترة كتابة الرسالة؛ لتحمل كلّ معاني القيم العلمية، كما أتوجه بجزيل الشكر والعرفان، إلى جامعة الشرق الأوسط ، الصرح العلمي الرائد، الذي أتاح لي فرصة التعلم والنمو، وأخصُ بالذكر قسم القانون العام، الذي لم يألُ جهدًا في تقديم الدعم والمساندة طوال فترة الدراسة.

كما وأشكر لجنة المناقشة من الأساتذة العلماء الأفاضل، كل من:

.. ، الذين قبلوا مناقشة رسالتي، وتحمّلوا عناء

قراءتها، وأنا على يقين من أنَّ ملحوظاتهم سيكون لها أكبر الأثر ، في إخراجها بصورة أفضل وأكمل بعون الله.

وما توفيقي إلا بالله العلي العظيم، عليه توكلت وإليه أنيب، والحمد لله رب العالمين

الباحثة

نورا محمد الدباس

الإهداء

إلى أبي الذي كان حضوره أمانًا يغسل عن قلبي خوف الطريق،

وإلى أمي التي زرعت في داخلي ضوءًا يجعل العتمة تُزهِر،

وإلى إخوتي رفاق الروح ورفاق الدرب الذين كانوا لي سندًا وللفرح شركاء،

وإلى كل من أحببت وكان لوجوده أثر لا يبهت، أهدي ثمرة هذا التعب، امتنانًا لمن كانوا لي قوةً حين ضعفت، فبكم اكتمل الطريق وبمحبتكم ازداد الحلم نورًا.

الباحثة

نورا محمد الدباس

قائمة المحتويات

الموضوع **الصفحة**

العنوان.....أ
قرار لجنة المناقشة .....ب
التفويض .....ج
الشكر والتقدير ..... د
الإهداء ..... هـ
قائمة المحتويات.....و
الملخص باللغة العربية .....ح
الملخص باللغة الإنجليزية .....ط

الفصل الأول: خلفية الدراسة ومشكلتها

أولا: المقدمة 1
ثانيا: مشكلة الدراسة.....2
ثالثاً: أهداف الدراسة.....2
رابعاً: أسئلة الدراسة 3
خامسا: أهمية الدراسة.....3
سادسا: منهجية الدراسة.....5
ثامنا:حدود الدراسة 5
سابعا: الدراسات السابقة 6

الفصل الثاني: الاطار القانوني لمفهوم الأمن السيبراني على الصعيدين الدولي والوطني

المبحث الأول: ماهية الأمن السيبراني في القوانين الدولية والوطنية 11
المطلب الأول: تعريف الأمن السيبراني..... 12
المطلب الثاني: أنواع الجرائم السيبرانية وآثارها القانونية..... 21
المبحث الثاني: دور الأمن السيبراني في تقرير تعزيز الحمايةالرقمية..... 28
المطلب الاول خصائص الجريمة السيبرانية..... 29
المطلب الثاني الاجراءات القضائية في الأمن السيبراني على الصعيدين الوطني والدولي... 35

الفصل الثالث: الاطار التشريعي للامن السيبراني في التشريعات الاردنية والمعاهدات الدولية

المبحث الاول: التشريعات الاردنية الخاصة بالامن السيبراني 45
المطلب الاول قانون الجرائم الالكترونية 46
المطلب الثاني: قانون حماية البيانات الشخصية 53
المطلب الثالث: الأطر التشريعية والتنظيمية 61
المبحث الثاني: المعاهدات الدولية المتعلقةبالأمن السيبراني 67
المطلب الأول: اهم الاتفاقيات الدولية 68
المطلب الثاني المبادئ والالتزامات الدولية للأمن السيبراني 74
المطلب الثالث آليات تنفيذ المعاهدات والتحديات التي تواجه تطبيقها 81
المطلب الرابع مواءمة التشريعات الأردنية مع الاتفاقيات الدولية للأمن السيبراني 88

الفصل الرابع: الخاتمة والنتائج والتوصيات

الخاتمة 93
أولًا: النتائج 94
ثانيًا: التوصيات 95
قائمة المراجع 96

مدى موائمة التشريعات الاردنية للمعاهدات الدولية الخاصة بالأمن السيبراني

إعداد

نورا محمد الدباس

إشراف

الدكتور بلال حسن الرواشدة

الملخص

هدفت هذه الدراسة إلى بيان مدى توافق التشريعات الأردنية مع المعاهدات الدولية المتعلقة بالأمن السيبراني من خلال توضيح الأطر القانونية الوطنية المنظمة للفضاء الرقمي ودراسة درجة انسجامها مع الالتزامات الدولية الناشئة عن الاتفاقيات والمواثيق الخاصة بالأمن السيبراني واعتمدت الباحثة المنهج الوصفي والمنهج التحليلي عبر استعراض النصوص القانونية الأردنية ذات الصلة بالأمن السيبراني مثل قانون الجرائم الإلكترونية وقانون حماية البيانات الشخصية والسياسات الوطنية إلى جانب تحليل مضامين المعاهدات الدولية وبصورة خاصة اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات وصولا إلى تقييم مدى توافق هذه التشريعات مع المعاهدات الدولية الحاكمة لهذا المجال .

الكلمات المفتاحية : الأمن السيبراني ، التشريعات الأردنية ، المعاهدات الدولية .

The extent to which Jordanian security legislation aligns with international cybersecurity treaties.

Prepared by
Noura Mohammad Al-dabbas.

Supervised by
Dr: Bilal Hassan Alrawashdeh.

Abstract

This study sought to determine the degree to which which Jordanian legislation aligns with international cybersecurity treaties. This was achieved by examining the national legal frameworks governing the digital space and analyzing their consistency with international obligations arising from cybersecurity agreements and conventions. The researcher employed a descriptive and analytical approach, reviewing relevant Jordanian legal texts such as the Cybercrime Law, the Personal Data Protection Law, and national policies. The study also analyzed the content of international treaties, particularly the Budapest Convention and the Arab Convention on Combating Information Technology Crimes, ultimately assessing the consistency of these laws with the international principles and standards governing this field.

The study reached a number of result, most notably that Jordanian legislation has responded to the legal developments imposed by the modern digital environment by adopting a legal framework to criminalize cybercrimes and define the penalties associated with them, in addition to regulating mechanisms for data protection and digital privacy. However, this alignment is still incomplete, especially with regard to some international cooperation standards, mechanisms for extraditing cybercriminals and exchanging digital evidence across borders, which are aspects that are essential in the system for combating cybercrimes according to international treaties. The study also recommended the need to strengthen the Jordanian legislative framework related to cybersecurity by reviewing existing texts to ensure their consistency with international obligations.

Keywords: Cybersecurity, Jordanian Legislation, International Treaties.

الفصل الأول
خلفية الدراسة ومشكلتها

أولا: المقدمة

شهد العالم خلال العقود الماضية تطورا متسارعا في مجالات تكنولوجيا المعلومات والاتصالات الأمر الذي أدى إلى بروز الفضاء السيبراني بوصفه مجالا مؤثرا في الجوانب الأمنية والاقتصادية والاجتماعية للدول وفي مقابل هذه التحولات الإيجابية برزت تحديات جديدة تمثلت في الجرائم الإلكترونية والهجمات السيبرانية واستغلال البيئة الرقمية في أنشطة غير مشروعة وهو ما استوجب تدخلا تشريعيا على المستويين الوطني والدولي [1]، وأصبحت الجرائم السيبرانية نمطا مستحدثا من أنماط الجريمة يتميز بطابعه العابر للحدود الإقليمية للدول وما يترتب عليه من آثار تمس الأمن القومي بمختلف أبعاده الأمر الذي دفع المجتمع الدولي إلى تبني نهج تعاوني لمواجهة هذه الجرائم إذا ما تشكله من تهديدات شاملة لذلك اتجهت الدول إلى اعتماد تدابير مشتركة للتصدي لها من خلال إبرام اتفاقيات ومواثيق دولية تهدف إلى مكافحتها وفي مقدمتها الجهود التي قادتها الأمم المتحدة ومنها اتفاقية بودابست بشأن مكافحة الجريمة الإلكترونية، إضافةً إلى الاتفاقية المعتمدة من جامعة الدول العربية. والاتفاقيات ذات الطابع الثنائي والمتعدد الأطراف الخاصة بتسليم المجرمين بوصفها من الوسائل الأساسية لمواجهة هذا النوع من الجرائم نظرا لخاصية عدم التقيد بالحدود الجغرافية [2] ، مع التوسع المتزايد في الاعتماد على التكنولوجيا الرقمية في مختلف

---

[1] الخطيب،احمد (2020) الامن السيبراني في ظل التحديات الرقمية الحديثة. المجلة العربية للسياسات العامة ،مصر ، جامعة عين شمس ، كلية الحقوق ، مجلد 12 عدد1 ص88-104.

[2] سليمان،قطاف (2022) مجلة الجرائم السيبرانية في ضوء الاتفاقيات الدولية . مصر ، جامعة عين شمس ، كلية الحقوق ،مجلد5 عدد2 ص62-87.

مجالات الحياة برز الأمن السيبراني هذا الموضوع معضلة حقيقيةللدول، لما يترتب عليه من تهديدات تؤثر في المرافق الحيوية، والمنظومة الاقتصادية، والتماسك المجتمعي.

كما وأصبح من الضروري على الدول ومن ضمنها الأردن العمل على تطوير منظومتها القانونية بما يواكب هذه التهديدات وذلك عبر الحاجة إلى وضع تشريعات متطورة تُسهم في ضبط الجرائم الإلكترونية ومجابهة طبيعتها المتغيرةوالمعقدة وتبرز في هذا السياق ضرورة توافق التشريعات الوطنية بما يتماشى مع المعايير الدولية والمواثيق المعنية، نظرًا لأن الجرائم الإلكترونية تتصف في الغالب بالعبور عبر الحدود. الأمر الذي يقتضي تعاونًا قانونيًا دوليًا منسقًا وفاعلًا.

ثانيا: مشكلة الدراسة

تتمحور الاشكالية حول الفجوة القانونية والتنظيمية المحتملة بين نصوص التشريعات الوطنية الاردنية مثل قانون الجرائم الالكترونية وقانون الامن السيبراني وغيرها وبين المعايير والالتزامات الواردة في الاتفاقيات والمعاهدات الدولية مثل اتفاقية بودابست للجرائم الالكترونية . تكمن المشكلة في تساؤل جوهري الى اي حد استطاع المشرع الاردني تطوير المنظومة القانونية المحلية لتنسجم مع المتطلبات الدولية المتسارعة في مجال الامن السيبراني بما يضمن حماية الفضاء الرقمي .

ثالثاً: أهداف الدراسة

تتمثل اهداف الدراية فيما يلي :

1. تحليل المنظومة التشريعية وهو تحليل القوانين الاردنية ذات العلاقة بالامن السيبراني .
2. تحليل الأداء الفعلي للسياسات الوطنية الأردنية في نطاق الأمن السيبراني، مع إبراز مهام المركز الوطني والآليات التنفيذية المطبقة.

رابعاً: أسئلة الدراسة

1. كيف تعالج هذه التشريعات القضايا المستجدة في الفضاء الرقمي ؟
2. ما ابرز التحديات التي تواجه المشرع الاردني في سبيل تطوير المنظومة القانونية للأمن السيبراني؟
3. ما هو تأثير الفجوات القانونية والتنظيمية على حماية الفضاء الرقمي في الاردن ؟
4. أي من القوانية الوطنية تحتاج الى تطوير او تعديل لتتوافق مع المعايير الدولية ؟

خامسا: أهمية الدراسة

تنبع أهمية الدراسة من مجموعة من الاعتبارات :

أولا: الاهمية العلمية

تنبع أهمية هذه الدراسة من طبيعة لمجالات المتخصصة التي عالجتها الدراسة، مع التركيز على مفهوم الأمن السيبراني على الصعيديين ركز البحث على تحليل المفاهيم والتعريفات القانونية المرتبطة بالموضوع ذات الصلة وتحديد تصنيفات الجرائم السيبرانية ونتائجها القانونية، إلى جانب مناقشة المسائل القانونية المتعلقة بالتحكم والسلطة في الفضاء السيبراني وما يثيره ذلك من تعارض مع فكرة حرية الإنترنت، ركزت الدراسة على تحليل التشريعات الأردنية مقارنة بالإطار الدولي المتصلة بالأمن السيبراني ضمن تشريعات على المستوى الوطني وسعت إلى تحليل مستوى توافقها بما يتوافق مع الأطر الدولية من اتفاقيات ومعاهدات ويتمثل المستوى المعرفي للدراسة في تسليط الضوء على قضايا وتشريعات معاصرة ومعقدة ما زالت موضع نقاش أكاديمي وقانوني فقهي وتشريعي ولا سيما ما يتعلق باستخدام إطار القانون الدولي في تحليل الهجمات السيبرانية وحدود السيادة الرقمية والمسؤولية القانونية في الفضاء الإلكتروني، تهدف الدراسة إلى بيان سد الثغرات

ضمن الدراسات القانونية الأردنية التي لم تُستكشف بشكل كافٍ من خلال الدراسات المعمقة في هذا القطاع الجديد الأمر الذي يُتيح لها قيمة علمية باعتبارها مرجعا يمكن الاستناد إليه من قبل الباحثين والمهتمين بالقانون السيبراني.

تصنف الدراسة ضمن البحوث المتقدمة في هذا المجال في إلاطار الأردني وتسعى الدراسة إلى تقديم تصور قانوني يساهم في تطوير التشريعات الوطنية بما يتماشى مع الالتزامات الدولية ويحقق تناغمًا بين بين متطلبات حماية الأمن السيبراني وصون حقوق الأفراد الرقمية وحمايتها.

ثانيا: الأهمية العملية

تكتسب الدراسة أهميتها العملية من الضرورة الملحة إلى تقييم مدى كفاءة القوانين الأردنية لمجابهة الصعوبات المتجددة في مجال الأمن السيبراني في ظل التوسع في استخدام التكنولوجيا الرقمية وتزايد الجرائم السيبرانية على الصعيدين الوطني والدولي وتمثل الدراسة جهداً عملياً للكشف عن جوانب نقاط القوة والضعف في الإطار القانوني الاردني من خلال تحليل التشريعات والقوانين المعنية مثل قانون الجرائم الإلكترونية وقانون حماية البيانات الشخصية والإطار السياسي الوطني وتحليل توافقه مع الاطر الدولية وتظهر الفائدة العملية للبحث في ما تقدمه من تصورات وتوصيات مقاربة قانونية وتشريعية تطبيقية تسهم في تطوير الإطار القانوني للأمن السيبراني على المستوى الوطني وتعزز إمكانات الدولة في التصدي للتهديدات الرقمية المتطورة وقدرة الجهات الرسمية مثل المركز الوطني للأمن السيبراني وهيئة تنظيم قطاع الاتصالات لتعزيز كفاءتها بالاعتماد على تحليل نقدي للقوانين والسياسات المعتمدة .

كما تقدم الدراسة للمشرع الأردني فهما أوضح لتحديد الثغرات التشريعية ودعمها في توافق التشريعات الوطنية مع الالتزامات الدولية، وهو أمر أساسي ضمن محاولة الأردن لتقوية الأمن

السيبراني، وصون الحقوق الرقمية للمواطنين، والالتزام بالمعايير الدولية وبذلك تشكل الدراسة مرجع تطبيقي يُستفاد منه في صياغة التشريعات والسياسات العامة وتعزيز الخطط الوطنية المرتبطة بالبيئة الرقمية .

سادسا: منهجية الدراسة

اعتمدت الباحثة التحليلي الوصفي لإبراز معالم التنظيم القانوني للأمن السيبراني وبيان المفاهيم الجوهرية المرتبطة به كما ورد في القوانين الوطنية الأردنية الاتفاقيات الدولية المرتبطة بالموضوع وذلك عن طريق دراسة الإطار التشريعي والسياسات العامة والمستندات المعتمدة ، وتم الاعتماد على المنهج التحليلي في بحث التشريعات القانونية المنظمة لجرائم الفضاء السيبراني وبخاصة قانون الجرائم الإلكترونية وقانون حماية البيانات الشخصية بالاستناد إلى تحليل القواعد القانونية ذات العلاقة وتحديد درجة كفاءتها في التصدي للتحديات الرقمية بالاعتماد على التشريعات النافذة ورأي الفقهاء المختصين والاجتهادات القضائية الوطنية والدولية .

ثامنا:حدود الدراسة

الحدود الموضوعية: اقتصرت الدراسة على تناول المحاور القانونية الخاصة بملاءمة التشريعات الأردنية مع المعاهدات الدولية ذات الصلة بالأمن السيبراني .

الحدود الزمانية: تمتد الحدود الزمانية للدراسة من عام 2010، تاريخ صدور الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وحتى عام 2025، وتشمل خلال هذه الفترة تطور التشريعات الأردنية ذات الصلة والاتفاقيات الدولية المتعلقة بالأمن السيبراني والجرائم الإلكترونية.

الحدود المكانية: تنحصر الحدود المكانية للدراسة في المملكة الأردنية الهاشمية من خلال تحليل التشريعات الوطنية ذات الصلة بالأمن السيبراني والجرائم الإلكترونية، مع امتداد

نطاقها ليشمل الإطارين الإقليمي والدولي من خلال دراسة المعاهدات والاتفاقيات الدولية ذات العلاقة، وذلك في حدود أثرها وانعكاسها على المنظومة القانونية الأردنية.

سابعا: الدراسات السابقة

الرشدان تقوى احمد محمد 2020 اساليب التحقيق الابتدائي في الجرائم السيبرانية في القانون الأردني والاتفاقيات الدولية رسالة ماجستير غير منشورة جامعة اليرموك ، إربد ، الأردن .

انصبت الدراسة المعروضة على بحث الإطار العام للتحقيق الأولي في الجرائم السيبرانية حيث تناول البحث في الفصل التمهيدي الأساس النظري للجرائم السيبرانية مع توضيح المصطلحات الأساسية المتعلقة بإجراءات التحقيق الأولي وخصائص الأدلة الرقمية إلى جانب بيان طبيعة الجرائم السيبرانية وسماتها القانونية ، وتناول الفصل الأول الأساس التشريعي المنظم لإجراءات التحقيق الابتدائي في القانون الأردني من خلال دراسة وتحليل القوانين ذات الصلة مثل قانون أصول المحاكمات الجزائية وقانون الجرائم الإلكترونية مع بيان صلاحيات كل من الضابطة العدلية والنيابة العامة في هذا المجال .

أما الفصل الثاني فقد خصص للمقارنة بين الإجراءات المعتمدة في التشريع الأردني وتلك الواردة في الاتفاقيات الدولية ذات الصلة ولا سيما الاتفاقيات المعنية بمكافحة الجرائم المنظمة عبر شبكة الإنترنت مثل اتفاقية بودابست مع توضيح أوجه الاتفاق والاختلاف .

وتختلف هذه الدراسة عن الدراسة الحالية من حيث نطاق المعالجة إذ إن الدراسة الحالية تبحث في مستوى تطابق القوانين الأردنية للاتفاقيات الدولية المعنية بالفضاء السيبراني بصورة شاملة ولا تحدّ على التحقيق المبدئي فقط بل تشمل الهيكل القانوني العام وعن نطاق تماشيه مع المعايير الدولية الأمر الذي يجعلها مكمّلة للدراسة السابقة وموسعة لمجالها .

وعلى الرغم من أهمية دراسة الرشدان (2020) وما قدمته من تحليل معمّق لإجراءات التحقيق الابتدائي في الجرائم السيبرانية في ضوء القانون الأردني والاتفاقيات الدولية، إلا أن نطاقها اقتصر على مرحلة التحقيق الأولي دون التوسع في تقييم مدى مواءمة المنظومة التشريعية الأردنية ككل مع المعايير الدولية الناظمة للأمن السيبراني. كما أنها لم تتناول بصورة تحليلية شاملة التطورات والتعديلات التشريعية اللاحقة، ولا مدى انعكاسها على مستوى الانسجام مع الالتزامات الدولية، ولا سيما ما يتعلق باتفاقية بودابست. ومن هنا تأتي الدراسة الحالية لتسد هذا النقص من خلال بحث درجة التوافق الكلي بين البنية القانونية الأردنية والمعايير الدولية في مجال الفضاء السيبراني، ضمن إطار تحليلي أشمل لا يقتصر على إجراءات التحقيق فحسب، بل يمتد إلى البناء التشريعي والتنظيمي برمّته.

أبو حسين حنين جميل 2021 الإطار القانوني والتنظيمي للأمن السيبراني دراسة مقارنة رسالة ماجستير غير منشورة جامعة الشرق الأوسط ، عمان، الأردن .

تناولت هذه الدراسة الإطار القانوني المنظم لأعمال الأمن السيبراني من منظور تحليلي، ركز الفصل التمهيدي على إبراز المفاهيم الأساسية ذات الصلة بالأمن السيبرانني وبيان أهمية وجود تشريع فعال يتماشى مع التطور السريع في التكنولوجيا إضافة إلى عرض أبرز التحديات والتهديدات التي تواجه البيئة الرقمية.

وتناول الفصل الأول الإطار التشريعي للفضاء السيبراني في القانون الأردني من خلال تحليل المواد القانونية المرتبطة بذات العلاقة مثل قانون الجرائم الإلكترونية وقانون المعاملات الإلكترونية إلى جانب تحليل مهام الجهات الرسمية المعنية وعلى رأسها المركز الوطني للأمن السيبراني وهيئة تنظيم قطاع الاتصالات .

أما الفصل الثاني فقد خصص لدراسة التجارب الدولية التحليلية حيث تناولت الدراسة الأطر التشريعية المعتمدة في مجموعة من الدول المتطورة مثل الولايات المتحدة الأمريكية مع إبراز مواطن الفعالية في هذه النماذج وقدرة الإفادة منها في تطوير القانون الأردني .

وتنفرد الدراسة الحالية في ضوء هذه الدراسة بتركيزها حول درجة انسجام التشريع الأردني وفقا للمعاهدات الدولية المتعلقة بالأمن السيبراني وليس مجرد النظر إلى التجارب التشريعية للمقارنة فقط كما أنها تعنى بتحليل العلاقة تماشيًا مع الالتزامات الدولية المترتبة على الأردن ومستوى تأثيرها على الإطار التشريعي الداخلي، مما يمنح الموضوع بعدًا تكامليًا أشمل.

وعلى الرغم من أهمية دراسة أبو حسين (2021) وما قدمته من تحليل للإطار القانوني والتنظيمي للأمن السيبراني في التشريع الأردني، إضافة إلى مقارنتها ببعض التجارب الدولية الرائدة، إلا أنها ركزت بصورة أساسية على المقارنة بين النماذج التشريعية دون أن تتناول بشكل مباشر مدى التزام الأردن بالمعاهدات والاتفاقيات الدولية ذات الصلة بالأمن السيبراني، أو درجة انسجام التشريع الوطني مع الالتزامات الدولية المترتبة عليه. كما أن الدراسة لم تُفرد معالجة تفصيلية لمسألة التوافق بين النصوص الداخلية والمعايير الدولية من منظور قانوني تحليلي معمّق. ومن هنا تأتي الدراسة الحالية لتسد هذا الفراغ من خلال بحث مستوى المواءمة بين المنظومة التشريعية الأردنية والمعاهدات الدولية في مجال الأمن السيبراني، وتحليل أثر هذه الالتزامات على البناء القانوني الداخلي بصورة شاملة ومتكاملة.

نصار مصعب تركي إبراهيم 2024 واقع التشريعات الجزائية المتعلقة بالأمن السيبراني دراسة مقارنة بين الأردن وقطر المجلة العربية للمعلوماتية وأمن المعلومات .

ركزت الدراسة على تحليل واقع التشريعات الجزائية المعمول بها لجرائم الأمن السيبراني من خلال إجراء موازنة بين القوانين النافذة في كل من الأردن وقطر حيث انصب اهتمام البحث على تحليل المواد القانونية المتعلقة بالجرائم السيبرانية في كلا النظامين القانونيين وبيان درجة كفايتها في مواجهة التهديدات الرقمية المتصاعدة ، وتناول الجزء الأول من الدراسة تقديم الأطر القانونية المنظمة للأمن السيبراني في الأردن وقطر مع استعراض المبادئ القانونية للتجريم والعقاب ومدى سريان الحماية الجزائية المقررة للمرافق الاساسية المعلوماتية .

أما الجزء الثاني فقد خصص لتحليل مستوى فاعلية التشريعات الجزائية في التصدي للجرائم السيبرانية مثل جرائم الاقتحام الرقمي واستغلال الشبكات بشكل غير قانوني وسرقة المعلومات مع توضيح نقاط الاتفاق والاختلاف في ما يتعلق بالعقوبات والتدابير القانونية المعتمدة في كلا البلدين إضافة إلى التنبيه إلى أوجه القصور التشريعي التي قد تنعكس سلبًا على كفاءة الردع الجزائي.

وعلى الرغم من أهمية دراسة نصار (2024) في تسليط الضوء على واقع التشريعات الجزائية المتعلقة بالأمن السيبراني من خلال المقارنة بين الأردن وقطر، وما قدمته من تحليل لمستوى كفاية النصوص الجزائية في مواجهة الجرائم السيبرانية، إلا أن نطاقها اقتصر على الجانب الجزائي البحت دون التوسع في بحث الإطار التشريعي والتنظيمي للأمن السيبراني بصورة شاملة. كما أنها لم تتناول بشكل مباشر مسألة مدى انسجام التشريع الأردني مع المعاهدات والاتفاقيات الدولية ذات الصلة، أو تحليل درجة التزامه بالمعايير الدولية الناظمة للفضاء السيبراني. ومن ثم تأتي الدراسة الحالية لتتجاوز حدود المقارنة الثنائية في الجانب العقابي، من خلال بحث مستوى التوافق الكلي بين المنظومة القانونية الأردنية والالتزامات الدولية في مجال الأمن السيبراني، بما يشمل الجوانب التشريعية والتنظيمية والمؤسسية على حد سواء.

الفصل الثاني

الاطار القانوني لمفهوم الأمن السيبراني على الصعيدين الدولي والوطني

شهد العالم في المرحلة الرقمية تقدما متسارعا في مجالات تقنيات المعلومات والاتصالات الأمر الذي أسهم في ظهور الفضاء السيبراني بوصفه أحد أكثر المجالات تأثيرا على أمن الدول والأفراد على حد سواء وأصبح الأمن السيبراني من القضايا الأساسية التي تحظى باهتمام للأطر والسياسات على المستويين الوطني والدولي نظرا لما يرتبط به ضمن المخاطر والتهديدات التي تتضمن الجرائم الإلكترونية والاعتداء على حماية البيانات وغيرها من المسائل ذات الصلة من الممارسات للأنشطة الضارة التي تقع في الفضاء الرقمي في سياق هذه التحولات المستمرة ظهرت الحاجة إلى تنظيم مصطلح الأمن السيبراني من الناحية القانونية اما في الصعيد الدولي من خلال المعاهدات والاتفاقيات الدولية أو على الصعيد الوطني عبر القوانين الداخلية والتي تسعى إلى حماية البنية التحتية الرقمية وضمان أمن المعلومات.

ومع تزايد الهجمات الإلكترونية وارتفاع مستوى المخاطر التي تستقطب الأنظمة الرقمية أصبح من المهم دعم الهياكل التشريعية والتنظيمية القادرة على تأمين البيانات وتأمين البنى التحتية الرقمية، الأمر الذي يبين جسامة الصعوبات التي يفرزها الفضاء السيبراني المعاصر وبناء عليه تم تقسيم هذا الفصل على النحو الآتي:

المبحث الأول: ماهية الأمن السيبراني في القوانين الدولية والوطنية

المبحث الثاني: دور الأمن السيبراني في تعزيز الحماية الرقمية

المبحث الأول
ماهية الأمن السيبراني في القوانين الدولية والوطنية

يتكون تعريف الأمن السيبراني من عنصرين أساسيين وهم الأمن والسيبراني حيث ان مصطلح السيبراني يستخدم للدلالة على الفضاء الافتراضي الذي يضم مختلف الأنشطة والميادين ذات الصلة بالانظمة الشبكية والأنظمة الرقمية ويشير هذا التعبير في الوقت الحاضر يُعد من أبرز المفاهيم المتداولة دوليًا في سياق تأمين الفضاء الرقمي[1] .

فيما يخص السياق العربي فلم يتوفر مفهوم الأمن السيبراني متداولا على نطاق شامل في الفترات السابقة إذ بدأ حضوره يتجلى بشكل بارز في سياق الاهتمام العربي المتصاعد بالأمن الرقمي منذ سنة 2017 ولا سيما في ضوء تصاعد التهديدات السيبرانية واعتماد الأفراد والمؤسسات بشكل متزايد على الخدمات الرقمية في مختلف المجالات[2] ، وعلى المستوى الدولي غدا الأمن السيبراني من المواضيع الاستراتيجية الرئيسية التي تحتل الصدارة في أولويات الدول والمنظمات الدولية نتيجة لتنامي المخاطر الرقمية ذات الطبيعة الدولية حيث خلال الاعوام الأخيرة ارتفاعا واضحًا في نطاق وتعقيد الهجمات السيبرانية التي استهدفت لقطاعات الحيوية، والدوائر الحكومية، والمؤسسات المالية، الأمر الذي أدى بالعديد من الدول إلى تبني الهياكل القانونية والتنظيمية متقدمة تهدف إلى تعزيز بياناتها الرقمية[3].

وبناء على ذلك قامت الباحثة بتقسيم هذا المبحث على النحو الآتي :

المطلب الأول تعريف الأمن السيبراني

المطلب الثاني أنواع الجرائم السيبرانية وآثارها القانونية

---

[1] **الزعبي، محمد محمود** .*الجرائم المعلوماتية* .عمان: دار الثقافة للنشر والتوزيع، 2017، ص 35.

[2] **الجندي، خالد عبد الحميد** .*مدخل إلى الجرائم المعلوماتية والأمن السيبراني* .القاهرة: دار المشرقة للنشر والتوزيع، 2020، ص 58.

[3] **الجندي، خالد عبد الحميد** .*مدخل إلى الجرائم المعلوماتية والأمن السيبراني* .القاهرة: دار المشرقة للنشر والتوزيع، 2020، ص 62.

المطلب الأول
تعريف الأمن السيبراني

عرّف المشرع الأردني الأمن السيبراني في قانون الأمن السيبراني رقم (16) لسنة 2019 في المادة 2 على أنه مجموعة التدابير المتبعة لضمان حماية الأنظمة والشبكات والبنى التحتية الحيوية من التهديدات السيبرانية وضمان القدرة على استئناف وظيفتها واستمراريته اما كان ذلك نتيجة التمكن غير المصرح به أو الاخفاق في الاستخدام بالإجراءات الأمنية أو التأثر بالأساليب الخداع التي تؤدي إلى ذلك[1]

ويلاحظ من هذا التعريف أن المشرع الأردني تبنى مفهوما واسعا وشاملا للأمن السيبراني لا يقتصر على حماية الأنظمة والشبكات من الاختراق فقط وإنما يمتد ليشمل حماية البنى التحتية الحرجة وضمان استمرارية العمل بعد وقوع الحوادث السيبرانية وهو ما يعكس فهما متقدما لطبيعة المخاطر الرقمية حيث لم يقتصر التنظيم على تجريم الأفعال وإنما شمل جانبي الوقاية والتعافي كما أن التعريف لم يحصر مصادر التهديد في الوصول غير المشروع فقط بل أدرج سوء الاستخدام والإهمال والخداع كعوامل مؤثرة في الإخلال بالأمن السيبراني الأمر الذي يدل على إدراك المشرع أن المخاطر قد تكون داخلية ناتجة عن ضعف التدابير الأمنية أو إساءة الاستعمال وهو ما يمثل اتساعا في الرؤية التشريعية مع الحاجة إلى مزيد من التفصيل لضمان التطبيق العملي الفعال

ويعرف الأمن السيبراني كذلك بأنه كيانا مكونا من التدابير والإجراءات الفنية والتنظيمية الرامية إلى تأمين الفضاء الرقمي وعناصره[2]، بما في ذلك الأنظمة والأجهزة البرمجيات والبيانات من أي انتهاكات أو هجمات أو استغلال غير مشروع قد يمس توفرها وسريتها وسلامتها، ويهدف كذلك

---

[1] قانون الامن السيبراني الاردني رقم16لسنة2019 المادةالثانية الموقع الرسمي لوزارة العدل الاردنية.

[2] **سامي، أحمد عبد الحميد** .*الأمن السيبراني: التشريعات والتحديات الدولية* .عمان: دار الفكر الجامعي، 2021، ص 72.

إلى ضمان استمرارية عمل الأنظمة الإلكترونية، ومنع الوصول غير المسموج به، والحماية من للتهديدات الرقمية المختلفة التي قد تؤثر على الأفراد أو المؤسسات أو الأمن الوطني للدول .

أما على مستوى الدول والمنظمات الدولية فقد عرف الاتحاد الدولي للاتصالات الأمن السيبراني في تقريره المتعلق باتجاهات الإصلاح في الاتصالات للأعوام 2010 و2011 بأنه مجموعة من المهام التي تشمل تجميع الوسائل والسياسات والإجراءات الأمنية والمبادئ التوجيهية ومقاربات إدارة المخاطر وبرامج التدريب والممارسات الفضلى والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانيةوموجودات المؤسسات والمستخدمين[1].

كما عرّف الاتحاد الأوروبي الأمن السيبراني في الإطار التنظيمي الأوروبي لحماية البيانات ومبادئ الأمن السيبراني على القدرة المؤسسية على صون الشبكات وأنظمة المعلومات من أي حوادث سيبرانية وضمان استعادة اهدافها مع الحفاظ على كتم المعلومات وتكاملها وتوافرها [2].

وفي هذا السياق ترى الباحثة أن الأمن السيبراني يمثل منظومة قانونية وتقنية وإجرائية متكاملة تهدف إلى حماية الفضاء الرقمي والبنى التحتية المعلوماتية والبيانات الحساسة من أي تهديد أو اختراق أو إساءة استخدام مع ضمان استمرارية الخدمات الرقمية .

وأخيرا يعرف الأمن السيبراني فقهيا بأنه مجموعة التدابير القانونية والتنظيمية والتقنية التي تهدف إلى حماية الفضاء الرقمي وأنظمته وبياناته من أي اعتداء أو اختراق أو استغلال غير

[1] دليل الامن السيبراني للبلدان الناميةللاتحاد الدولي للاتصالات لسنة2010 صفحة 421.

[2] European Union Cybersecurity Regulation (EU Regulation 2019/881)

مشروع، بما يضمن **سلامة المعلومات وسريتها وتوافرها**، ويعزز القدرة على الردع القانوني لكل من يهدد هذه المنظومة أو ينتهكها[1] .

كما يعرف قضائيا بأنه هو حماية البنية التحتية المعلوماتية والأنظمة الرقمية والبيانات المخزنة فيها من أي أعمال غير قانونية، بما يشمل الاختراقات، ونشر الفيروسات، والاحتيال الإلكتروني[2]، ويُطبَّق بشأنه ما نصت عليه التشريعات الوطنية مثل قانون الجرائم الإلكترونية وقانون الأمن السيبراني، وفقًا للسوابق القضائية الصادرة عن المحاكم في قضايا الجرائم الإلكترونية

الفرع الأول : مجالات التطبيق القانوني للأمن السيبراني دوليا ووطنيا .

يمتد نطاق الأمن السيبراني ليشمل مختلف الجوانب الاقتصادية والاجتماعية والسياسية والإنسانية وذلك استنادا إلى مفهومه بوصفه قدرة الدولة على حماية مصالحها وشعبها في شتى مجالات الحياة اليومية بشكل آمن ومن جهة أخرى يرتبط الأمن السيبراني ارتباطا وثيقا بحماية الثروة المعاصرة المتمثلة في البيانات والمعلومات والقدرة على الاتصال والتواصل والتي تشكل المحور الأساسي للإنتاج والإبداع والقدرة[3]على المنافسة .

ويشمل الإطار التشريعي للأمن السيبراني مجالات مختلفة تهدف إلى

اولا: صون الفضاء الرقمي وحماية الأنظمة الإلكترونية الجرائم والتهديدات السيبرانية ويأتي في مقدمتها تأمين المعلومات الشخصية إضافة إلى مواجهة الجرائم الإلكترونية وفقًا لأحكام قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023 كما تغطي التشريعات الاردنية تنظيم أساليب التعاون والتنسيق بين الجهات الحكومية المعنية، مع توضيح المسؤوليات

---

[1] آمنة علي البشير محمد، *الأمن السيبراني في ضوء مقاصد الشريعة*، مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، المجلد 37، العدد 1، 2021، ص 450.

[2] قانون الأمن السيبراني رقم (16) لسنة 2019، المادة(2) .

[3] شمدين،عفاف 2013 الابعاد القانونيةلاستخدمات تكنولوجيا المعلومات دمشق صفحة 311.

القانونية الملقاة على عاتق الأفراد والدوائر في مجال المحافظة على الأمن السيبراني تهدف السياسات الوطنية إلى إرساء بيئة رقمية آمنة تعزز التنمية الرقمية وتكفل الحقوق الالكترونية للأفراد[1].

ويمتد دور الأمن السيبراني إلى

ثانيا: الحد من المخاطر الرقمية التي قد تهدد الأفراد وحماية المجتمع والدوائر من خلال تقوية الخصوصية الالكترونية وكفالة سلامة المعلومات الشخصية التي قد تُستخدم على نحو غير مشروع[2] كما يسهم في ضمان أمن الخدمات الإلكترونية التي يستعين بها المواطنين في حياتهم بشكل يومي بما يكفل استمراريتها وسلامتها من أي تهديد فضلا عن دوره في مواجهة الجرائم الإلكترونية كجرائم الاحتيال والابتزاز الإلكتروني الأمر الذي يعزز الاطمئنان لدى المجتمع تجاه الفضاء الرقمي ويقلل من التبعات السلبية للهجمات الالكترونية وبذلك يسهم الأمن السيبراني في بناء مجتمع رقمي آمن يحافظ على حقوق الأفراد ويضمن استقرار البنية التحتية الرقمية.

كما يشمل الأمن السيبراني حماية الاقتصاد الوطني حيث يرتبط ارتباطا وثيقا بالاقتصاد الحديث وباقتصاد المعرفة على وجه الخصوص في ظل التوسع في استخدام تقنيات المعلومات والاتصالات والقيمة المتزايدة للبيانات والمعلومات المتداولة والمخزنة والمستخدمة على مختلف المستويات وتسهم هذه التقنيات في تعزيز التنمية الاقتصادية من خلال الاستفادة من الفرص التي

---

[1] **السميرات، محمد عبد الكريم** .*الأمن السيبراني في التشريع الأردني: الإطار القانوني والتطبيقات العملية* .عمان: دار النهضة العربية، 2022، ص 123–125.

[2] **السميرات، محمد عبد الكريم** .*الأمن السيبراني وحماية البيانات في التشريع الأردني* .عمان: دار النهضة العربية، 2022، ص 98–100.

توفرها الشركات الدولية الكبرى غير أن هذا الواقع يثير في المقابل إشكاليات قانونية تتعلق بحماية مقدمي الخدمات والعمال والمستهلكين عبر الإنترنت[1] .

على المستوى الدولي، اتجهت الجهود نحو تعزيز الأطر القانونية والتنظيمية للأمن السيبراني نظرًا لطبيعة التهديدات العابرة للحدود وتأثيراتها ليس على بلد بعينها بل تتجاوز لتشمل الأمن الاجماعي للمجتمعات والدول وتعد من أهم مجالات تنفيذ الأمن السيبرانية على الصعيد الدولي، يُعنى بحماية البنية التحتية الرقمية على المستوى العالمي العالمية وتشمل حماية البنى التحتية الرقمية مثل شبكات الاتصالات والإنترنت ، وكذلك حماية البيانات الشخصية العابرة للحدود، وفق ما توليه المنظمات الدولية اهمية خاصة لتعزيز التنسيق الدولي لمكافحة الهجمات الالكترونية من في سياق تطوير مبادئ توجيهية ومعاهدات عمل مشتركة ، كما وتسعى هذه المبادرات الدولية إلى تحقيق تناسق دقيق بين حماية سيادة الدول الرقمية من جانب، وضمان حرية الإنترنت وحقوق الإنسان في الفضاء الرقمي من جانب آخر وفي هذا الإطار تؤكد المنظمات والهيئات الدولية على ضرورة نشر ثقافة الأمن السيبراني وتعزيز تعاون المجتمع بمختلف مكوناته لتحقيق هذا الهدف نظرا لأن المخاطر السيبرانية تطال المجتمع بأسره سواء بسبب اعتماد الخدمات الحيوية كقطاع الطاقة والنقل والصحة والاتصالات على تقنيات المعلومات أو بسبب المحتويات الرقمية غير المشروعة التي تؤثر سلبا على القيم الأخلاقية وتزيد من الممارسات الجرمية مثل الإباحة غير المشروعة والترويج للمخدرات والدعارة والإرهاب والتجنيد لقضايا تمس الأمن والسلم الدوليين[2].

---

[1] وائل عبد الله حازم، *الأمن السيبراني والاقتصاد الرقمي: التحديات القانونية والتنظيمية*، (القاهرة: دار الفكر العربي، 2021)، ص 132–134.

[2] الحموري، زياد محمد .*الأمن السيبراني على المستوى الدولي: المبادئ والتحديات* .مجلة العلوم القانونية والسياسية، جامعة الكويت، العدد 18، 2023، ص 215–217.

وأخيرا يصبح من الضروري العمل على بناء مجتمع واع ومدرك لمخاطر الفضاء السيبراني وقادر على التعامل معه وفق حد أدنى من قواعد السلامة مع إدراك الآثار القانونية التي قد تترتب على بعض السلوكيات في البيئة الرقمية وترى الباحثة في هذا السياق أن الأمن السيبراني على المستوى الدولي لم يعد مجرد خيار تقني أو أمني بل غدا حاجة إنسانية نتيجة للاعتماد المتزايد على الفضاء السيبراني في مجالات الحياة المتنوعة .

الفرع الثاني: المهام الأساسية للأمن السيبراني دوليا ووطني

يضطلع الأمن السيبراني بمجموعة من الاهداف الجوهرية وهي تستهدف صون الفضاء الرقمي وحماية محتوياته المختلفة من التحديات والمخاطر المتصاعدة وهذه الاهداف هي مجموعة من الوظائف الأساسية [1].

أولا : الوقاية

وتتحقق من خلال اتخاذ التدابير الاستباقية التي تهدف إلى منع وقوع الهجمات السيبرانية[2] مثل اعتماد أنظمة الحماية وتحديث البرمجيات بصورة مستمرة وإجراء تقييم دوري للثغرات الأمنية .

ثانيا : الرصد والكشف.

ويتم ذلك باستخدام أدوات وتقنيات متقدمة لمتابعة عمل الأنظمة والشبكات واكتشاف أي أنشطة غير طبيعية أو محاولات اختراق محتملة[3] .

---

[1] **الحموري، زياد محمد** .*الأمن السيبراني وأهدافه الجوهرية: دراسة مقارنة* .مجلة العلوم القانونية والسياسية، جامعة الكويت، العدد 18، 2023، ص 220–222.

[2] **سلمان، محمد مصطفى** .*الأمن السيبراني: المفاهيم الأساسية والاستراتيجيات* .القاهرة: دار الثقافة للنشر والتوزيع، 2022، ص 58–59.

[3] [3] الشاذلي، فتوح جرائم التعزيز المنظمةفي المملكةالعربيةالسعودية ، مكتبة الرشد، الرياض صابق4 سنة 2020 صفحة 302.

ثالثا التعافي واستمرارية العمل

ويقصد به استرجاع البيانات المتضررة وإعادة تشغيل الأنظمة المصابة وضمان استمرار تقديم الخدمات الأساسية خاصة تلك المرتبطة بالبنى التحتية الحيوية .

رابعا: التوعية والتثقيف

وتعد من الواجبات المحورية للأمن السيبراني حيث تسعى إلى تعزيز الوعي لدى الأفراد والمؤسسات بالتحديات التي يفرضها الفضاء الرقمي، وتعزيز ثقافة الاستعمال الآمن والمسؤول للتقنيات الحديثة بما يسهم في انشاء تكنولوجيا فيها استقرارا وأمانا[1] .

وعلى المستوى المحلي ، تتنوع مسؤوليات الأمن السيبراني بالاردن بما يضمن حماية البيئة الرقمية والبنى التحتية ذات الاهمية الحيوية حيث يكلف الأمن السيبراني بمجموعة من الواجبات الأساسية التي هدفها إلى صون الأنظمة والشبكات الحكومية من الهجمات والاختراقات ويهتم بطبيعته بمواجهة الاختراقات الخارجية التي تهدد المنظومة الإلكترونية والمواقع التكنولوجية إذ يعد أمن الشبكات عملية أساسية تهدف إلى حماية الشبكات والأجهزة من الاختراقات الخارجية ويتم تحقيق ذلك من خلال وسائل متعددة من أبرزها استخدام كلمات مرور قوية واعتماد برامج الحماية من الفيروسات وبرامج مكافحة التجسس [2].

كما يشمل الدور الوطني للأمن السيبراني تنسيق الاستجابة للحوادث السيبرانية من خلال الجهة الوطنية المختصة بالأمن السيبراني الذي يتولى تنظيم وتنظيم آليات الاستجابة بالتعاون مع

---

[1] د.زيدان،همسة ، الوعي الالكتروني وتعزيز الممارسات الآمنة للانترنت. : https://orgin.hawwaz.com/learn/public/courses/325

[2] القريطي، دحان حزام ناصر .*الأمن السيبراني وحماية أمن المعلومات* .الإسكندرية: دار الفكر الجامعي، 2024، ص 58.

فريق الاستجابة الوطني المعني بحوادث الأمن السيبراني[1] ، حيث تتمحور اختصاصات هذا الفريق حول الاستجابة العاجلة للحوادث السيبرانية واسعة النطاق والعمل على السيطرة على الهجمات ووقف توسعها ومحو مصادر التهديد وعلاج نقاط الضعف الأمنية ويقدم التسهيلات الفنية المتخصصة للمؤسسات العامة والقطاع الخاص المتضررة ويتمثل دوره في تحليل الهجمات لتحديد أصولها وغاياتها، وتقديم التوصيات ذات الصلة واللازمة لاستعادة الوضع الطبيعي بعدها إضافة ايضا تنسيق المبادرات بين الجهات المختلفة لتأمين فعالية وطنية قوية ومتكاملة ضمن مخطط استراتيجي وطني يهدف إلى تقوية الأمن السيبراني وضمان حماية المرافق الحيوية على الصعيد الوطني[2] .

وفيما يتعلق بالبعد الدولي اتجهت عدد كبير من الدول إلى وضع استراتيجيات ذات طابع وطني شامل لضمان سلامة البيانات باعتباره جزءا لا يتجزأ من مفهوم الأمن الوطني الشامل للدول والمؤسسات والأفراد حيث بدأت الدول تدرك أن التطور التكنولوجي المتسارع يفرز تهديدات حقيقية لأمن الوطن والمواطن الأمر الذي يستلزم اعتماد تدابير فعالة لحماية نظم المعلومات ووسائل الاتصال[3] ويعتمد الأمن السيبراني في هذا الإطار على مجموعة من الوسائل القانونية والتقنية لمواجهة الاستخدام غير المشروع للشبكة وحماية الأنظمة المعلوماتية من المخاطر السيبرانية .

وتتعدد الأطر والآليات الدولية لتي تُعنى بتنسيق جهود الاستجابة للجرائم السيبرانية بين الحكومات والهيئات الدولية ومن اهمها خطة الإطار الوطني الأمريكي للاستجابة للحوادث

---

[1] البلوشي، سعد محمد .*الأمن السيبراني: الإطار القانوني الوطني والدولي* .دبي: دار الفكر القانوني، 2023، ص 75–77.

[2] البلوشي، سعد محمد. الأمن السيبراني: الإطار القانوني الوطني والدولي. دبي: دار الفكر القانوني، 2023، ص 78–80.

[3] الذهبي، أحمد مصطفى .*الأمن السيبراني والاستراتيجيات الوطنية لحماية البيانات* .الرياض: دار العلوم للنشر، 2022، ص .47–45

السيبرانية التي تشكل الإطار الوطني لإدارة الحوادث السيبرانية الكبرى[1]، بمشاركة الجهات الحكومية والخاصة وتحديد أدوار الجهات المختلفة في التعوان وتبادل الخبرات وكذلك المنظومة الأوروبية لفرق الاستجابة لحوادث الأمن السيبراني التي تمثل منصة لتبادل المعلومات والتنسيق بين الفرق الوطنية في حالات الحوادث العابرة للحدود إضافة إلى هيئة التنسيق السيبراني الإسبانية الذي يشغل منصب نقطة الاتصال الوطنية في مجال التنسيق وتبادل المعلومات .

ويعكس هذا المستوى من التعاون والتنسيق الدولي إدراك المجتمع الدولي لأهمية لجهود المشتركة للتصدي للتهديدات السيبرانية المتصاعدة، ويساهم في تقوية الأمن السيبراني عالميا من خلال تعزيز تبادل الخبرات والمعارف وتوحيد الجهود للتصدي للتحديات الالكترونية[2] .

[1] Cybersecurity and Infrastructure Security Agency, *National Cyber Incident Response Plan (NCIRP)*, first published in December 2016 (U.S. national coordinated framework to handle significant cyber incidents).

[2] فهيد سعد العجمي، أوجه التعاون الدولي في تعزيز الأمن السيبراني: دراسة تحليلية، مجلة الشرطة، كلية الشرطة – أكاديمية سعد العبد الله للعلوم الأمنية، الكويت، المجلد 29، العدد 5، 2024، ص 4909–4954.

المطلب الثاني
أنواع الجرائم السيبرانية وآثارها القانونية

أثمر التقدم السريع في مجال التكنولوجيا والاعتماد المتزايد في البيئة الرقمية إلى ظهور أنماط حديثة من الافعال الاجرامية تعرف بالجرائم السيبرانية التي باتت تشكل إشكالية قانونية وأمنية على الصعيدين المحلي والدولي، إذ فاقت هذه الافعال الاجرامية القيود التقليدية للزمان والمكان وانتشرت تاثيراتها لتصيب الأفراد والمؤسسات والدول في القطاعات الحيوية بمختلف أنواعها .

الفرع الأول: تصنيف الجرائم السيبرانية

تُصنف الجرائم السيبرانيية شكلا مستحدثا من الجرائم ذات الطبيعة المعقدة الذي أفرزته المجتمع الرقمي المعاصر ويصعب إخضاعه للأطر التقليدية للجرائم الجنائية ونظرا لتعدد الصور التي تتخذها الأفعال الإجرامية المرتكبة عبر الفضاء السيبراني سعى الفقهاء ورجال القانون لتطوير تصنيفات تُسهم في استيعاب طبيعة هذه الجريمة عناصرها وسبل محاربتها ويستند هذا التنويع الى معايير متعددة وهي طبيعة الاعتداءات والهدف من الافعال الاجرامية أو الوسيلة المعتمدة ونوع الجهة المتضررة وعلى هذا الأساس يتم عرض اشهر التصنيفات المعترف بها للجرائم السيبرانية .

أولا: جرائم الاعتداء على حرمة الحياة الخاصة

تتجلى جرائم انتهاك الحياة الخاصة في الأفعال التي تمس الجوانب الشخصية للأفراد من بيانات ومعلومات ذات طابع سري إذ تتمتع الحياة الخاصة بحماية قانونية تمنع انتهاكها من الغير ولا سيما مع انتشار استخدام الهواتف الذكية المزودة بالكاميرات وغيرها من الوسائل التقنية الحديثة التي تتيح اختراق أدق تفاصيل الحياة الشخصية[1] ، كما وتشمل هذه الجرائم صورا متعددة من

[1] الشاذلي، فتوح جرائم التعزيز المنظمةفي المملكةالعربيةالسعودية ، مكتبة الرشد، الرياض صابق4 سنة 2020 صفحة 302.

الانتهاكات التي تلحق أضرارا جسيمة بالأفراد من بينها الكشف العلني عن وقائع خاصة تمس الشخص كالإفصاح عن حالته الصحية أو وضعه المالي أو نشر صوره دون رضاه كما تشمل التشهير العلني والإساءة إلى السمعة أمام الجمهور[1] بما ينعكس سلبا على الكرامة الإنسانية والمكانة الاجتماعية فضلا عن الاستيلاء غير المشروع على عناصر شخصية حساسة كالاسم والصورة والبيانات المتعلقة بالحياة الخاصة التي يفترض أن تحظى بالحماية القانونية [2].

ويعد هذا النوع من الأفعال اعتداء مباشرا على الحق في حماية الحقوق السرية والخصوصية الذي كفلته الاتفاقيات الدولية والتشريعات[3] .

وعند حدوث الاعتداء على حرمة الحياة الخاصة من جهة خارج الإقليم حين يكون المتضرر موجودًا داخل الدولة تتكامل الأطر القانونية عبر التشريعات الوطنيةوالمعاهدات ذات الطابع الدولي[4].

ثانيا: جرائم الاعتداء على الملكية الفكري .

تُعد الانتهاكات المرتكبة ضد الملكية الفكرية من أبرز أنماط الجرائم الرقمية التي تمس الحقوق القانونية للأفراد والجهات في مجال حفظ الإبداع الفكري والأدبي والتقني وتشمل هذه الجرائم كافة الأفعال التي تنطوي على استغلال غير مشروع للبرمجيات والبيانات والبراءات والعلامات التجارية وحقوق النشر عبر الوسائل الرقمية الأمر الذي يؤدي إلى خسائر مالية جسيمة ويؤثر سلبا في الابتكار والتنمية الاقتصادية .

---

[1] عبدالرزاق الموافي عبداللطيف، *حرمة الحياة الخاصة من منظور القوانين العقابية* .مجلة كلية الحقوق، جامعة المنوفية – مصر، 2021.

[2] زرفي، علي نعمةجواد الزرفي ، الجريمة المعلوماتية الماسة بالحياةالخاصة دراسة مقارنة. المكتب الجامعي الحديث 2019 صفحة 38.

[3] الدستور الاردني عام 1952 مادة18 وتعديلاته .قانون الجرائم الالكترونيةرقم 17 سنة2023 الجريدةالرسمية عدد5897 بتاريخ 16 ايار 2023.

[4] قانون الجرائم الالكترونيةالاردني رقم 17 سنة 2023 والاتفاقية الدولية لمكافحة الجرائم الالكترونية–اتفاقية بودابست عام2001–.

ومن صور هذه الجرائم نسخ البرامج وتقليدها وإعادة إنتاجها أو تصنيعها دون الحصول على ترخيص قانوني وهو ما يشكل اعتداء على الحقوق المالية والأدبية [1]لأصحابها ويعد هذا السلوك انتهاكا صريحا للتشريعات التي تحمي الملكية الفكرية لما يترتب عليه من إضعاف لحوافز الاستثمار في مجالات الإبداع والتطوير ولهذا وضعت القوانين الوطنية والدولية عقوبات رادعة لمثل هذه الأفعال بهدف حماية حقوق المبدعين وضمان بيئة رقمية آمنة تدعم نمو الاقتصاد الرقمي وفي الأردن نظم قانون حماية الملكية الفكرية هذه المسائل وأسهم في تعزيز الأمن السيبراني ومنع الاستغلال غير المشروع للمصنفات الفكرية.

ثالثا: جرائم الاعتداء السيبراني على الأموال

يقصد بالاعتداء السيبراني على الأموال تلك الأفعال التي تستهدف الاستيلاء على الأموال أو تحويلها بوسائل غير مشروعة من خلال استغلال الثغرات الرقمية وتضم هذه الجرائم أعمال الاحتيال الرقمي والدخول غير المصرح به إلى الحسابات المصرفية باستخدام برمجيات ضارة كالفيروسات ، بقصد تعطيل الأنظمة المادية أو ابتزاز الافراد المستهدفين[2] .

وتشمل الأفعال إلحاق أضرار مالية مباشرة بالضحايا مثل السرقة الإلكترونية من خلال التلاعب بأجهزة الصرف الآلي أو اختراق الأنظمة البنكية أو إنشاء مواقع إلكترونية مزيفة تحاكي مواقع المؤسسات المالية الكبرى أو إرسال رسائل إلكترونية من مصادر مجهولة تتضمن وعودا زائفة بتحويل أموال مقابل نسب مالية معينة وتمثل هذه الجرائم تهديدا خطيرا للأمن المالي

---

[1] شمري،غانم مرضي .عام 2016 الجرائم المعلومية. طبعة اولى عمان: الدار العلمية صفحة52.

[2] *Cyber Financial Fraud or Cybercrime in Finance*, *Advanced International Journal for Research (AIJFR)*, 2026.

والاقتصاد الوطني الأمر الذي دفع التشريعات إلى تبني أطر قانونية صارمة لمواجهتها وتعزيز وسائل الحماية للمعاملات المالية الإلكترونية[1] .

رابعا: الجرائم الجنسية السيبرانية

تشمل الجرائم الجنسية السيبرانية كافة الأفعال التي تستغل البيئة الرقمية لأغراض ذات طابع جنسي غير مشروع، كالتحرش الإلكتروني والضغط الجنسي كالابتزاز ونشر أو تداول المواد الإباحية ولا سيما تلك المتعلقة بالأطفال تعتبر هذه الانتهاكات من اشد خطورة الجرائم الإلكترونية نتيجة الآثار النفسية والاجتماعية المترتبة على المتضررين فضلا عن تهديدها للقيم المجتمعية والأمن العام .

وقد تصدى المشرع الأردني لهذه الجرائم من خلال قانون الجرائم الإلكترونية رقم 17 لسنة 2023 حيث عالجت نصوصه الأفعال ذات الطابع الجنسي عبر الوسائل الإلكترونية وقررت لها عقوبات رادعة إذ حظرت المادة 20 كافة صور التحرش الإلكتروني وفرضت على مرتكبيه عقوبات مالية أو سالبة للحرية كما شددت المادتان 21 و22 على تجريم الابتزاز الجنسي الإلكتروني ونشر أو تداول المواد الإباحية وخاصة تلك التي تستغل الأطفال وهو ما يعكس حرص المشرع على حماية المجتمع وصون القيم الأخلاقية في البيئة الرقمية وتعزيز حماية الضحايا والتعاون الدولي للتصدي لهذه الانتهاكات العابرة للدول[2] .

---

[1] Mohd Afiq bin Azero, Sarah Nur Aisyah Kay Abdullah, et al., *The Nexus of Cybercrime and Money Laundering: A Conceptual Paper*, *Accounting and Finance Research*, Vol. 13, No. 2, 2024, pp. 167–182.

[2] قانون الجرائم الإلكترونية رقم 17 لسنة 2023، الجريدة الرسمية الأردنية، العدد 5564، 2023، المواد 20–22.

خامسا: الجرائم السياسية والاقتصادية السيبرانية

وتتضمن الجرائم الإلكترونية المرتبطة بالشؤون السياسية والاقتصادية الأفعال التي تنتهك الأنظمة الهيئات السياسية والهيئات الاقتصادية عبر البيئة الرقمية، مثل عمليات الاختراق للأنظمة الحكومية والمراقبة الإلكترونية غير المشروعة والاعتداء المرتبطة بالعمليات المالية، والجرائم الإلكترونية، وتشكل هذه العمليات الغير مشروعة تهديدا مباشرا لاستقرار الدولة وأمنها الوطني والاقتصاد الوطني .

وتظهر هذه الجرائم من خلال استغلال الجماعات المتطرفة لوسائل الاتصال الحديثة لنشر معلومات مضللة والترويج لأفكار متطرفة والتحريض على العنف وزعزعة الاستقرار إلى جانب استخدام الوسائل الرقمية في تحويل الأموال بطرق غير مشروعة واختراق المواقع الحساسة وسرقة البيانات واستخدام البرمجيات التخريبية لتحقيق أهداف سياسية أو اقتصادية وهو ما استدعى تدخل التشريعات الوطنية لتجريم هذه الأفعال وتعزيز التعاون الأمني والاستخباراتي داخليا ودوليا.

سادسا: الجرائم السيبرانية الخاصة بالاتجار بالبشر والمخدرات .

تشمل هذه الجرائم إنشاء أو إدارة أو نشر مواقع إلكترونية أو محتوى رقمي يهدف إلى الاتجار بالبشر أو تسهيل التعامل في الجنس البشري أو الترويج للمواد الإباحية أو أنشطة المقامرة المخلة بالآداب العامة كما تشمل إنشاء أو نشر مواقع تتعلق بالاتجار بالمخدرات أو المؤثرات العقلية أو الترويج لطرق تعاطيها أو تسهيل تداولها عبر الوسائل الرقمية[1] .

[1] الصحفي، روان بنت عطيةالله الصحفي. السعودية. جدة. المجلة الالكترونيةالشاملة معدودة التخصصات عدد24 شهر مايو 2020 صفحة 20-21.

وترى الباحثة أن تصنيفات الجرائم السيبرانية بطبيعتها غير ثابتة وتخضع للتطور المستمر نتيجة الابتكار التقني المتسارع وظهور أنماط جديدة من الأفعال الإجرامية يصعب حصرها ضمن تصنيفات جامدة الأمر الذي يستوجب مراجعة دائمة الاطر التشريعية والتصنيفات المعترف بها .

الفرع الثاني: العقوبات القانونية المترتبة على الجرائم السيبرانية

تمثل التبعات القانونية لجرائم الامن السيبراني رد الفعل القانوني الذي يستهدف مواجهة الأفعال غير القانونية المرتكبة في البيئة الرقمية وتظهر هذه العلامات بالاكثر في صورة جزاءات قانونية تقررها القوانين المعنية سواء كانت عقوبات جزائية كالسجن \ الغرامة \ آثارا مدنية تتمثل في التعويض للاضرار اللاحقة بالأفراد أو الهيئات بسبب هذه الجرائم وتهدف هذه الجزاءات إلى ضمان أمن الفضاء الرقمي وتعزيز الردع العام والخاص، مع تأكيد محاسبة المخالفين وعدم إفلاتهم من المسؤولية [1].

تترتب على الجرائم السيبرانية آثار قانونية متنوعة نتيجة خصوصيتها وتعدد أشكالها ونظرًا لامتدادها عبر الحدود، تفرض القوانين الوطنية من الناحية الجنائية ولا سيما قانون الجرائم الإلكترونية الأردني رقم سبعة عشر لعام 2023 [2]جزاءات تتفاوت بحسب جسامة الجريمة سواء كانت متعلقة بالخصوصية، أو بالغش المالي ، أو استهداف البنى الحكومية وفي المجال المدني، يمكن أن تنشأ مسؤولية قانونية تفرض على الجناة تعويض الأضرار المادية أو المعنوية التي أصابت المتضررين كالأضرار الناتجة عن تسريب البيانات أو الإساءة إلى السمعة .

---

[1] عبدالستار ،فوزية شرح قانون العقوبات .دار نهضة القاهرة سنة 1982 صفحة6.

[2] قانون الجرائم الالكترونيةرقم 17 سنة 2023 الجريدة عدد 5874 .

وعلى الصعيد الدولي يمكن أن تنشأ مسؤوليات قانونية على المستوى الدولي عند تعرض المصالح الوطنية والهيئات الحيوية المتأثرة بالهجمات الرقمية وهو ما يستوجب تشغيل آليات التنسيق الدولي وتفعيل اتفاقيات تسليم المجرمين والتنسيق الأمني والقضائي بما يؤكد أهمية تطوير التشريعات لمواكبة التحولات التقنية وتوفير حماية قانونية فعالة .

وفي هذا الإطار يظهر أن المشرع الأردني قد قرر آثارا قانونية واضحة وصارمة للجرائم السيبرانية من خلال نصوص متعددة تؤكد حرصه على حماية الفضاء الإلكتروني وتنظيم استخدامه إذ نصت المادة الثالثة من قانون الجرائم الإلكترونية رقم سبعة عشر لعام 2023 في معاقبة كل من يدخل إلى أي شبكة معلوماتية أو نظام إلكتروني دون تصريح بعقوبات سالبة للحرية أو مالية كما جرمت المادة 7 أفعال اعتراض البيانات أو التنصت عليها أو تغييرها أو حذفها أثناء انتقالها عبر الشبكات وقررت لها عقوبات مشددة لضمان سلامة البيانات الرقمية .

كما وتناولت المادة 15 من القانون ذاته حماية النظام العام من خلال تجريم نشر الأخبار الكاذبة أو الإساءة إلى السلطات العامة أو الموظفين أثناء قيامهم بمهامهم وفرضت عقوبات رادعة لمنع إساءة استخدام الفضاء الإلكتروني وهو ما يعكس توجها تشريعيا واضحا نحو توفير حماية شاملة للبيئة السيبرانية .

المبحث الثاني
دور الأمن السيبراني في تقرير تعزيز الحمايةالرقمية

يعد الامن السيبراني في الوقت الحاضر من أهم ركائز حماية المجتمعات الرقمية وضمان استقرار الأنظمة المعلوماتية في ظل التوسع المتزايد في استخدام التكنولوجيا والخدمات الإلكترونية ومع تصاعد التهديدات السيبرانية وتطور أساليب الهجوم الرقمي لم يعد الأمن السيبراني مجرد إجراء تقني بل أصبح إطارا متكاملا يجمع بين الجوانب القانونية والتنظيمية والتقنية بما يضمن حماية البيانات والأفراد والمؤسسات على حد سواء وتبرز أهمية هذا الدور من قدرته على بناء منظومة حماية فعالة تقوم على مبادئ وقواعد نظرية تشكل أساس الفهم القانوني والتشريعي لهذا المجال وتسهم في وضع ضوابط واضحة تحقق الموازنة بين متطلبات الأمن ومتطلبات الحقوق والحريات وفي هذا الإطار تتضح أهمية المحاكمة في الجرائم السيبرانية على المستويين الوطني والدولي بوصفها وسيلة لتحقيق العدالة الرقمية ومساءلة مرتكبي الجرائم الإلكترونية وتطبيق قواعد المسؤولية القانونية عبر الحدود بما يعزز الثقة في البيئة الرقمية ويدعم قيام فضاء سيبراني آمن وموثوق

وبناء على ذلك قامت الباحثة بتقسيم هذا المبحث إلى مطلبين أساسيين على النحو الآتي :

المطلب الأول: خصائص الجريمة السيبرانية

المطلب الثاني: المحاكمة في الامن السيبراني على الصعيد الوطني والصعيد الدولي

المطلب الاول
خصائص الجريمة السيبرانية

تختلف الجرائم الرقمية مقابل الجرائم التقليدية من حيث السياق الذي تقع فيها إذ يتطلب ارتكابها الاعتماد على وسائل تقنية إلى جانب امتلاك الجاني قدرا من الخبرة التقنية بما يمكنه من ممارسة الأفعال المخالفة للقانون عبر البيئة الرقمية.

الفرع الأول: خصائص الجريمة السيبرانية

تتسم جرائم الامن السيبراني بسمات خاصة مقارنة بالجريمة التقليدية ويمكن بيانها على النحو الآتي:

أولا: الجريمة السيبرانية عابرة للحدود .

تتصف الجرائم السيبرانية بطابع دولي لأن شبكة الإنترنت أدت إلى ترابط دول العالم بشكل مستمر ولذلك فإن الجرائم الإلكترونية لا تقف عند حدود دولة بعينها مما يجعلها نمطا حديثا من الجرائم العابرة للحدود ومن خلال الأنظمة المعلوماتية يمكن ارتكاب صور متعددة من الافعال غير المشروعة كالاعتداء على المعلومات وتغيير المعلومات التقنية وإتلافها والاحتيال الإلكتروني وعمليات القرصنة الرقمية وكما أن يمكن للإنترنت على تجاوز الحدود أثرت في السلوك الإجرامي فلم تعود التصرفات الاجرامية ذات نطاق محلي بل أصبحت ذات امتداد عالمي ويستطيع مرتكب الجريمة الإلكترونية تنفيذ فعله عن بعد بما يعني عدم تواجده ماديا في مكان وقوع الجريمة ومن ثم

تتباعد المسافات بين الفعل الذي يتم بواسطة الحاسوب وبين النتيجة المترتبة عليه وقد تنتقل الجريمة الإلكترونية من دولة إلى أخرى[1] .

ثانيا : صعوبة إثبات الجريمة

ان صعوبة الإثبات من أهم العقبات في محاربة الجرائم الالكترونية إذ يعتمد من يرتكب الجريمة غالبا إلى تمويه هوياتهم أو توظيف ادوات تشفير وبرامج متقدمة تعقد مهمة تتبع الأدلة الرقمية وجمعها وفق الأصول القانونية ، وترجع صعوبة الإثبات إلى عدة عوامل منها :

1. أن الجريمة تقع ضمن وسط رقمي تنتقل البيانات بهيئة استبدال المستندات الورقية الملموسة بإشارات إلكترونية، ونظرا لأن الجريمة تتمثل بتغيير سجلات لكترونية أو معلومات رقمية فهي كثيرا ما تخلو من آثار مادية تقليدية أو شهود يسهل الاعتماد عليهم .
2. صعوبة الحفاظ على الدليل الرقمي إذ يمكن للجاني خلال لحظات محو البيانات أو تحريفها أو تعديلها[2] .
3. اكتشاف الجريمة يحتاج إلى خبرة فنية لأن جرائم الحاسوب تتطلب معرفة واسعة سواء في ارتكابها أو في التحقيق فيها كما يواجه القائمون على الضبط والتحقيق صعوبات في التعامل مع الدليل الإلكتروني وقد يؤدي ذلك إلى إتلافه دون قصد مثل محو بيانات التخزين أو عدم ضبط الأجهزة المستخدمة في ارتكاب الجريمة ولذلك تبرز ضرورة التدريب

---

[1] رستم، هشام محمد فريد .الجرائم المعلوماتية: أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي .بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت بكلية الشريعة والقانون بدولة الإمارات العربية المتحدة، 3-1مايو 2000.

[2] United Nations Conference on Trade and Development (UNCTAD). *Trade and Development Report 2005*. United Nations, 2005, 2 ص.

المتخصص لرجال الضبط والقضاء والخبراء والفنيين والتعاون فيما بينهم للوصول إلى أفضل وسائل مكافحة الجريمة الإلكترونية[1].

4. أن الجرائم السيبرانية تتصف بطابع غير عنيف يعتمد على التخطيط والمعرفة التقنية إذ تتمثل في أوامر رقمية تستهدف الاستيلاء على البيانات أو تعديلها أو إتلافها أو التجسس عليها وغيرها من الصور المتجدد .
5. وأنها ذات تنفيذ سريع حيث يمكن القيام بها خلال مدة زمنية بالثواني من خلال إجراء بسيط من غير اشتراط التواجد المادي للجاني أو المجني عليه .
6. وأنها تجاوزة للحدود الوطنية بحيث يمكن تنفيذها في دولة وتستهدف ضحايا في دولة مختلفة متجاوزة بالحدود الجغرافية وأن ارتكابها يتطلب مستوى عاليا من المهارات التقنية والفنية .

الفرع الثاني: أركان الجريمة السيبرانية .

تقوم الجريمة السيبرانية، شأنها شأن غيرها من الجرائم، من ثلاثة عناصر :

أولا: الركن القانوني

يشترط توافر نص تشريعي واضح لتحديد الجريمة ومعاقبتها، وهو ما يعكس مبدأ قانونية الجرائم والعقوبات الذي يقوم على وجود نص صريح يجرم الفعل ويحدد طبيعته والعقوبة المقررة له. ويأتي قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023 مثالًا على ذلك، حيث عالج أفعالًا إلكترونية لم تكن مجرمة سابقًا، مثل تزوير الهوية الرقمية والدخول غير القانوني إلى الأنظمة، وحدد جزاءات تتناسب مع جسامة الأفعال وآثارها.

[1] أبو السعود، عاطف محمد. الجرائم المعلوماتية بين القانون والوثائق الدولية. القاهرة: دار النهضة العربية، 2018، ص 110–115.

كما نص قانون الأمن السيبراني رقم 16 لسنة 2019 في المادة 2 على تعريف حادث الأمن السيبراني باعتباره فعلًا أو هجومًا يشكل خطرًا على البيانات أو المعلومات أو نظم المعلومات أو الشبكة المعلوماتية أو البنى التحتية المرتبطة بها، ويتطلب استجابة عاجلة لإيقافه أو للحد من عواقبه وآثاره [1].

ثانيا: الركن المادي

الركن المادي التصرف الخارجي الذي يحقق الجريمة بالبيئة الرقمية ويتمثل في كل تصرف إلكتروني غير مشروع يمس حقا محميا مشروعا كالاختراق للانظمة .

ولتحقق السلوك الإجرامي يلزم توافر الوسائل التقنية مثل الحاسوب أو الهاتف الذكي إضافة إلى شبكة الإنترنت إذ بدون ذلك لا يكون هناك اي اجرام ولا يمكن اعتبار الفعل اعتداءً يهدد الأمن السيبراني [2]

ويتضمن الركن المادي ثلاثة مكونات اساسية :

1. السلوك الإجرامي : ويتمثل في السلوك الذي ينفذه الجاني عبر الادوات التقنية لارتكاب فعل غير قانوني وقد يكون إيجابيا كالدخول غير المشروع أو نشر بيانات خاصة أو إرسال برمجيات خبيثة وقد يكون سلبيا عندما يمتنع الشخص عن واجب قانوني مفروض عليه مثل الإهمال في تحديث أنظمة الحماية رغم العلم بوجود ثغرات أو عدم الإبلاغ عن حادث سيبراني مع قيام الالتزام بذلك متى توافرت بقية الشروط القانونية ، وقد يكون السلوك

---

[1] قانون الامن السيبراني رقم16 سنة 2019.المادة الثانية .

[2] احمد،حجاز 2004 جريمة الحاسوب والشبكة المعلوماتية .دار الكتب القانونية . مصر . ص17

بسيطا كما في الإساءة اللفظية عبر الوسائل الإلكترونية وقد يكون أكثر تعقيدا كما في الجرائم المنظمة واسعة النطاق التي تحتاج إلى تخطيط وأدوات متقدمة[1] .

2. النتيجة الإجرامية : وهي الأثر الذي ينشأ عن السلوك ويعكس التعدي على الحقوق القانونية المحمية ، وتنقسم إلى جرائم الضرر[2] وهي ما يشترط فيها وقوع ضرر فعلي لتحقيق الركن المادي، وجرائم الخطر وهي التي يجرم فيها السلوك بمجرد وقوعه ولو لم يتحقق ضرر فعلي لأن السلوك يشكل تهديدا محتملا للمصلحة المحمية .

3. علاقة السببية : وهي الرابطة التي تصل بين سلوك الجاني والنتيجة المترتبة عليه ولا تكتمل الجريمة إلا بتوافر هذه العلاقة فإذا انتفت انتفت المساءلة الجنائية ومن أمثلتها ارتباط فعل اختراق نظام إلكتروني بصورة غير مشروعة بالنتيجة الضارة المتمثلة في الحصول على بيانات سرية دون حق [3].

ثالثا: الركن المعنوي .

يتكون القصد الجنائي في الجريمة السيبرانية من عنصري العلم والإرادة كسائر الجرائم إذ يجب أن يعلم الجاني أن الدخول إلى بيانات خاصة أو الحصول عليها دون تصريح عمل غير مشروع كما يجب أن تتجه إرادته إلى ارتكاب الفعل المجرم[4] .

وقد يظهر القصد الجنائي من خلال وقائع تؤكد نية التهديد أو الابتزاز عبر الوسائل الإلكترونية بما يدل على توافر الإرادة الجرمية ، ويتضمن القصد الجنائي عنصرين :

---

[1] أبو السعود، عاطف محمد .الجرائم المعلوماتية بين القانون والوثائق الدولية .القاهرة: دار النهضة العربية، 2018، ص 88–90.

[2] أبو السعود، عاطف محمد .الجرائم المعلوماتية بين القانون والوثائق الدولية .القاهرة: دار النهضة العربية، 2018، ص 91–93.

[3] اسامة،مهمل الجرائم السيبرانية2018 صفحة 39. مرجع سابق

[4] الرفداني، محمد .تحقيقات جهاز الشرطة لمواجهة التحديات السيبرانية .المجلة العربيةللدراسة الامنية مجلد رقم 31 عدد61سنة 2014 صفحة115.

1. العلم : ويشمل العلم بالوقائع وبموضوع الجريمة وبحقيقة الفعل وخطورته وبأن فعله سيوقع ضررا بالمجني عليه .
2. الإرادة : وهي نشاط نفسي يتجه لتحقيق هدف معين بوسيلة معينة[1] .

كما ويتخذ القصد الجنائي صورا منها القصد العام والقصد الخاص حيثت يتمثل القصد العام في اتجاه إرادة الجاني إلى ارتكاب الفعل المحظور وتحقيق نتيجته المباشرة دون اشتراط غاية إضافية [2]، و القصد الخاص يتطلبه القانون في بعض الجرائم فلا يكفي مجرد ارتكاب الفعل بل يلزم قيام نية خاصة تتجاوز النتيجة المباشرة مثل قصد الحصول على منفعة غير مشروعة في جرائم الابتزاز الإلكتروني .

[1] خالد، لطفي احمدحسن .الدليل الشامل الرقمي في اثبات الجرائم الالكترونية.الاسكندرية 2020 صفحة50.

[2] قرعان، محمود احمد .الجرائم الالكترونية .دار وائل لنشر والتوزيع .الاردن . سنة 2017 صفحة 36.

المطلب الثاني

الاجراءات القضائية في الأمن السيبراني على الصعيدين الوطني والدولي

ان الاجراءات القضائية بمجال الأمن السيبراني تكون عبر اعتماد القواعد القانونية للتصدي بالافعال المجرمة الإلكترونيةعلى الصعيديين المحلي والدولي وتضم هذه الخطوة استنادا على مسارات قانوني وأمني يركز على حماية البنية التحتية والتعامل مع التهديدات الالكترونية عبر اعتماد خطط ملائمة وتقوية التنسيق الدولي من خلال الشراكات الدولية إلى تنسيق الاستجابة للحوادث السيبرانية وتبادل المعلومات بين الجهات المختصة لضمان استجابة فعّالة .

الفرع الأول: الاجراءات القانونية المتبعة في ملاحقة الجرائم السيبرانية

اولا: الاستدلال في الجريمة السيبرانية

تتمحور إجراءات الاستدلال الجنائي الرقمي مهام البحث عن الأدلة التقنية واستخراجها وتخزينها والحفاظ على سلامتها ووصف الأدلة وتفسيرها وتحليلها من حيث الصلاحية والموثوقية ومدى صلتها بالقضية ثم تقديم ما يتصل منها بموضوع الدعوى[1] .

كما عرفت انها : سلسلة من التدابير الحيوية غير المرئية التي يلتزم فيها ضابط الضبط القضائي و مرؤوسوه التحري الصادق والدقيق عن الوقائع المرتبطة بموضوع محدد واستخراجها وفق الأطر القانونية [2].

---

[1] Maras, M. H., *Computer forensics, cybercriminals, and the law*, Burlington, MA: Jones & Bartlett Learning, 2014.

[2] عبدالله، سامي أحمد .التحقيق الجنائي في الجرائم المعلوماتية .القاهرة: دار الفكر العربي، 2019، ص 82–86.

وفيما يخص الجهة المكلفة بمهام الاستقصاء والتحقيق عن الجرائم السيبرانية والقبض على مرتكبيها وضح القانون الأردني ذلك في المادة 8 من قانون أصول المحاكمات الجزائية حيث أسند هذه المهام إلى رجال الضابطة العدلية .

ومن خلال ما تقدم يتبين أن الاستدلال : هو مجموعة من الاجراءات الأولية التي يباشرها أعضاء الضبط القضائي بعد وقوع الجريمة بهدف جمع المعلومات والأدلة التي تساعد في كشف الحقيقة وتحديد مرتكب الفعل الجرمي .

ولضمان صحة اجراءات الاستدلال وسلامتها يلزم توافر شروط من أبرزها [1]:

1. أن تتم مرحلة جمع الأدلة ضمن إطار مشروع ومتفق مع القانون .
2. أن تنصب اجراءات الاستدلال على جريمة وقعت فعلا لأن مباشرة الاستدلال تمهيدا لضبط جريمة محتملة يجعل الاجراءات غير صحيحة .
3. أن تتعلق اجراءات الاستدلال بذات الجريمة لا بجريمة أخرى مهما وجدت صلة بينهما إذ يلزم لكل جريمة اجراءات استدلال تخصها.
4. أن يلتزم مأمور الضبط القضائي بقواعد الاختصاص النوعي والمكاني فلا يباشر ذو الاختصاص النوعي الخاص اجراءات التحري في غير الجرائم الداخلة ضمن أعمال وظيفته ولو داخل نطاقه[2] كما يجب التقيد بالاختصاص المكاني المتعلق بمكان وقوع الجريمة ومكان القبض على المتهم وإلا تعرضت الاجراءات للبطلان

---

[1] قادر، ساره. سنة 2014 .اساليب تحري للقانون الجزائي .رسالة ماجستير .جامعة مرباح .الجزائر صفحة 16-17.

[2] فاروق،ياسر امير.2009 .مراقبةالاحاديث الخاصةفي الاجراءات الجنائية. جامعةالقاهرة صفحة 403.

ثانيا: التحقيق الابتدائي .

التحقيق الابتدائي : هو المرحلة اللاحقة للاستدلال ويتركز على جمع الأدلة بصورة أعمق وتوثيقها على نحو قانوني للتأكد تحديد حدوث الجريمة ومعرفة الجاني .

وقد ظهرت تعريفات متعددة بشأن التحقيق الأولي المتعلقة بالجرائم الإلكترونية ومن ذلك أنه: جراء قانوني ينفذه المختصون لمكافحة الجرائم الرقمية من حيث الفاعل والدليل الإلكتروني الرقمي لتقديمهما إلى الجهات القضائية المختصة التي يفترض بها تحقيق العدالة [1] .

يُقصد به مجموعة من الإجراءات القضائية التي تقوم النيابة العامة بمباشرتها عند وقوع الجريمة، وذلك للكشف عن الحقائق واتخاذ التدابير القانونية المقررة [2].

وتوجد اجراءات قانونية وتنظيمية تهدف إلى ضمان سلامة التحقيق ومشروعيته ومنها [3]:

1. صل مصدر الكهرباء عن موقع الأدلة الرقمية لتجنب العبث بالأدلة.
2. جمع بيانات الدخول اللازمة للأجهزة من الموظفين المختصين، ثم منع أي تدخل لاحق منهم في الأجهزة .
3. مراعاة أن الدليل الرقمي سريع الزوال لذلك يجب مباشرة التحقيق الابتدائي بأقصى سرعة للحصول على الأدلة قبل ضياعها .
4. كما يجب على رجال الضابطة العدلية مراعاة اجراءات تضمن قانونية سير التحقيق وسلامة نتائجه ومنها :

أ. الالتزام بحدود الصلاحيات القانونية وعدم تجاوزها.

---

[1] موسى،مصطفى محمد .2009 .تحقيق جنائي في الجرائم الالكترونية .القاهرة .مطابع الشرطة صفحة166.

[2] جووخدار، حسن .2008 تحقيقات ابتدائية في قانون اصول المحاكمات الجزائية .دراسة مقارنةالاردن.دار الثقافةللنشر والتوزيع.صفحة11.

[3] سوفي،نور الهدى سنة2017 .تحقيق في الجرائم المعلوماتية–رسالة ماجستير– جامعة مرباح.الجزائر صفحة 113–14.

ب. ضمان حقوق المتهم بما في ذلك احترام قرينة البراءة وعدم الإكراه واحترام حق الدفاع.

ت. احترام خصوصية الأفراد وعدم الاطلاع على بيانات لا صلة لها بالجريمة إلا بإذن قانوني.

ث. التنسيق مع الجهات الفنية المختصة عند الحاجة إلى خبرة تقنية عالية.

ج. السرعة في اتخاذ الاجراءات نظرا لسرعة ضياع الأدلة الرقمية أو تعديلها

ويلاحظ أن المشرع الأردني أجاز بموجب الفقرتين ألف وباء من المادة الثالثة عشرة من قانون الجرائم الإلكترونية لسنة ألفين وخمسة عشر[1] لرجال الضابطة العدلية وبعد الحصول على الإذن الدخول إلى المواقع التي تقوم أدلة جدية على استعمالها في تنفيذ جريمة إلكترونية، وإخضاعها للتفتيش القانوني وضبط الأجهزة والبرمجيات والأدوات التي يشتبه استخدامها .

وبناء عليه يعتبر التحقيق الأولي خطوة أساسية في المسار القضائي الجزائي للجرائم الإلكترونية لما تتميز به من تعقيد وسرعة وتطور تقني ويؤدي الالتزام بالقواعد الاجرائية إلى تعزيز مشروعية الاجراءات ومنع بطلانها أمام القضاء كما يرتبط نجاح التحقيق بدرجة كبيرة بالتخصص والدقة وتنسيق الجهود مع الخبراء الفنيين.

---

[1] المادة 13أ " مع مراعاة الشروط والاحكام المقررةفي التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية يجوز لموظفي الضابطةالعدلية بعد الحصول على اذن من المدعي العام المختص او من المحكمة المختصةا لدخول الى اي مكان تشير الدلائل الى استخدامه لارتكاب اي من الجرائم المنصوص عليها في هذا القانون كما يجوز لهم تفتيش الاجهزة والادوات والبرامج وانظمةالتشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب اي من اي تلك الجرائم. وفي جميع الاحوا ل على الموظف الذي قام بالتفتيش ان ينظم محضرا بذلك ويقدمه الى المدعي العام المختص.

13اب مع مراعاة الفقرة أ من هذه المادةومراعاة حقوق الاخرين ذوو النية الحسنة وباستثناء المرخص لهم وفق احكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون. يجوز لموظفي الضابطة العدلية ضبط الاجهزة والادوات والبرامج وانظمة التشغيل والشبكةالمعلومتية لارتكاب اي من الجرائم المنصوص عليها او يشملها هذا القانون والاموال المتحصلة منها والاحتفاظ على المعلومات واالبيانات المعلقة بارتكاب اي منها .

ثالثا: الإحالة إلى المحاكمة .

تمثل المحاكمة المرحلة الأخيرة في الدعوى الجزائية بحسب قانون أصول المحاكمات الجزائية الأردني، وتبدأ بعد الانتهاء من التحقيق الابتدائي وتوفر الأدلة الكافية لإحالة القضية إلى القضاء، وفي قضايا الجرائم الإلكترونية، بعد استكمال إجراءات الاستدلال والتحقيق الرقمي وفق أحكام قانون الجرائم الإلكترونية رقم سبعة وعشرين لسنة ألفين وخمسة عشر بعد انتهاء التحقيق واستكمال إجراءات الاستدلال في الجرائم الإلكترونية، تُحال القضية إلى المحكمة المختصة، والتي قد تكون محكمة صلح أو جزاء اعتمادًا على طبيعة الجريمة والعقوبة المقررة. تقوم المحكمة بدراسة الأدلة الرقمية المقدمة، والاستماع إلى أقوال الشهود والمتهمين، مع الالتزام بالضمانات القانونية المنصوص عليها. ويُشترط لقبول الأدلة الإلكترونية أن تكون قد تم جمعها بأساليب قانونية وتحت إشراف الجهات المختصة، بما يحفظ سلامة الإجراءات ويكفل نزاهة المحاكمة[1]. وتشمل مرحلة المحاكمة عددًا من الإجراءات الأساسية، منها:

1. تقديم لائحة الاتهام أمام المحكمة لتحديد طبيعة التهم الموجهة للمتهم.
2. استماع المحكمة إلى أقوال المتهم مع ضمان تمكينه من الدفاع عن نفسه بواسطة محاميه أو بشكل شخصي.
3. الاستماع إلى أقوال الشهود والخبراء الفنيين في القضايا التي تستلزم فهماً تقنياً متعمقاً.
4. تمكين المحكمة من الاطلاع على الأدلة المقدمة من النيابة ومناقشتها بموضوعية.
5. تقديم المرافعات النهائية من قبل الأطراف أمام القضاء.

[1] قوقزة، أشرف علي .الأدلة الرقمية في إثبات الجرائم الإلكترونية في التشريع الأردني: دراسة مقارنة .عمان: دار المناهج للنشر والتوزيع، 2021.

تُشكل المحاكمة المرحلة الأساسية التي يُعرض فيها النزاع على المحكمة للفصل فيه وفق القانون، بالاستناد إلى الأدلة المجمعة في مرحلتي الاستدلال والتحقيق، مما يجعلها جوهر مسار الدعوى الجزائية[1]

الفرع الثاني: التعاون الدولي وآليات الملاحقة في الجرائم السيبرانية العابرة للحدود .

مع التسارع الملحوظ في تطور تقنيات الاتصال والمعلومات، شهدت الجرائم السيبرانية زيادة في تعقيدها وامتدادا عبر الحدود فقد ينفذ الجاني فعله من دولة ويستهدف ضحية في دولة أخرى وتخزن الأدلة في دولة ثالثة وهو ما يفرض تحديات على الأنظمة الوطنية لذلك برزت الحاجة إلى تعزيز التعاون الدولي عبر الاتفاقيات الثنائية والمتعددة مثل اتفاقية بودابست لمكافحة الجريمة السيبرانية لعام ألفين وواحد[2]

وتتضمن آليات الملاحقة الدولية عددًا من الأدوات البارزة، منها:

اولا : تسليم المجرمين .

يعد التسليم إجراءً قانونيًا بين دولتين أو أكثر، يسمح بنقل شخص ملاحق جزائيًا أو مدان من الدولة التي يوجد فيها إلى دولة أخرى لغرض محاكمته أو تنفيذ حكم قضائي صادر ضده. ولتقديم طلب التسليم، هناك مجموعة من الشروط العامة التي يجب استيفاؤها[3]، من أبرزها

1 . ازدواج التجريم .

2. استصدار أمر توقيف أو تقديم لائحة اتهام، أو صدور حكم نهائي في القضية

---

[1] الحموري، أحمد .الاجراءات الجزائية الأردنية: دراسة تحليلية مقارنة .عمان: دار الفكر القانوني، 2019، ص 210–212.

[2] اتفاقيةبودابست بشأن الجرائم السيبرانية مجلس اوروبا سنة 2001 : https://www.coe.int/en/web/cybercrime

[3] النجار، سامي عبد الله .التسليم الدولي للمجرمين: دراسة مقارنة بين التشريعات العربية والدولية .عمان: دار النهضة للنشر والتوزيع، 2020، ص 45–48.

3. استيفاء الضمانات الإنسانية وحماية حقوق الإنسان، بما يشمل عدم تنفيذ التسليم إذا كان الشخص المطلوب مهددًا بالتعذيب، أو بعقوبة الإعدام، أو بأي معاملة غير إنسانية في الدولة الطالبة .

ترى الباحثة أن آلية تسليم المجرمين تشكل ركيزة أساسية في إطار التعاون القضائي الدولي لمكافحة الجريمة السيبرانية، إلا أن فعاليتها قد تتأثر بعوامل مثل تصنيف الجرائم على أنها سياسية، واعتبارات سيادة الدول، والضمانات المتعلقة بحقوق الإنسان.

ثانيا: الإنابة القضائية الدولية .

تعرف الإنابة القضائية الدولية بأنها طلب تقدمه الدولة الطالبة إلى الدولة المطلوب إليها لاتخاذ إجراء قضائي ضمن إطار الدعوى الجنائية، بهدف الفصل في مسألة معروضة أمام سلطات الدولة الطالبة، والتي يتعذر تنفيذها داخل إقليم الدولة الأخرى. وتساهم الإنابة القضائية في تيسير الإجراءات والتحقيقات اللازمة، وتجاوز عائق السيادة الإقليمية الذي يمنع مباشرة الأعمال القضائية داخل دولة أخرى [1].

وقد ألزمت اتفاقية بودابست لعام ألفين وواحد الدول الأطراف باتخاذ تشريعات وطنية تدعم التعاون القضائي[2].

كما أقرت المادة اثنان وثلاثون من الاتفاقية إمكانية الدخول للتفتيش والضبط لبيانات موجودة في نظام يتبع دولة أخرى في حالتين إذا كانت البيانات متاحة للجمهور أو إذا وجدت موافقة قانونية ممن يملك سلطة الكشف عن البيانات .

---

[1] الدسوقي طارق ابراهيم.الامن المعلوماتي للحمايةالمعلوماتية. صفحة 601

[2] Conentions on cybercrimee Budapest 2001. number 185 2023 year : https://www.coe.int/en/web/cybercrimes

ترى الباحثة أن الإنابات القضائية تمثل أداة مهمة لمكافحة الجرائم السيبرانية، إلا أن نجاحها يعتمد على سرعة الاستجابة، ومرونة التشريعات، ومستوى الثقة بين الدول. كما تبرز الحاجة إلى تحسين آليات التواصل لضمان فاعلية الإجراءات، مع احترام الخصوصية وسيادة الدول لتحقيق العدالة دون المساس بالحقوق الأساسية .

ثالثا: تبادل المعلومات والاستخبارات الرقمية .

يشمل تبادل المعلومات والاستخبارات الرقمية تنسيق ومشاركة البيانات الفنية والتحقيقية المتعلقة بالجرائم الإلكترونية بين الدول أو بين الجهات المكلفة بإنفاذ القانون، بهدف تحديد هوية الجناة، وتتبع أنشطتهم، ومنع الهجمات أو التصدي لها فور حدوثها[1].

وأكثر صور التعاون الدولي في هذا المجال العمل من تقوم به منظمات دولية مثل الإنتربول واليوروبول في التنسيق بين الدول وتبادل المعلومات وتسهيل معرفة مرتكبي الجريمة .

1 الإنتربول

ان هذه المنظمة أكبر هيئة دولية مختصة بتنسيق التعاون بين أجهزة الشرطة، وتضم مئة وأربعا وتسعين دولة عضوا ولا يملك سلطة تنفيذ القانون أو الاعتقال وإنما يعمل كوسيط لتيسير التعاون ويعد نموذجا للتعاون الأمني الدولي في ضبط المجرمين وتسليمهم وتحقيق أهداف مشتركة [2]وتتمثل أهدافه في تأمين وتنمية التعاون الدولي بين سلطات الشرطة الجنائية وإنشاء وتنمية المؤسسات التي تسهم في الوقاية من الجرائم الإلكترونية ومكافحتها وتبرز أهميته في ما يوفره من معلومات جنائية دولية وفرق متخصصة ومعاهد تدريبية وكونه حلقة وصل بين الدول كما تمثل

---

[1] قوقزة، أشرف علي .الأمن السيبراني ومكافحة الجرائم الإلكترونية: أطر قانونية واستراتيجية .عمان: دار المناهج للنشر والتوزيع، 2021، ص 122–124.

[2] بريغز، جوزيف م .Interpol: A Practical Handbook for International Police Cooperation. New York: Routledge, 2018, 49–47 صفحة

المعاهدات والاتفاقيات الدولية مظهرا من مظاهر السيادة الخارجية وشرطا لسيادتها الداخلية ومن ذلك التعاون الدولي في المسائل الجنائية عبر المعاهدات الثنائية والإقليمية والدولية[1] .

2 اليوروبول

هو وكالة إنفاذ قانون داخل الاتحاد الأوروبي ويعرف بمكتب الشرطة الأوروبي ويعد جهاز الاستخبارات الرسمية للاتحاد الأوروبي وقد تأسس عام ألف وتسعمائة وثمانية وتسعين لمكافحة الجريمة المنظمة والإرهاب ويركز على الجرائم العابرة لحدود الاتحاد مثل الاتجار بالمخدرات والاتجار بالبشر والاحتيال المالي والجرائم الإلكترونية ويضم وحدات تشغيلية وتحليلية تدعم الدول الأعضاء في التحقيقات ولا يملك صلاحيات تنفيذية مباشرة أو سلطة اعتقال لكنه يعمل منصة لتبادل المعلومات والتعاون ويقدم دعما فنيا وتحليليا ويصدر تقارير دورية عن التهديدات الإجرامية ويعزز التعاون من خلال شراكات مع منظمات ودول خارج الاتحاد[2] .

وترى الباحثة أن التعاون الدولي في مكافحة الجرائم السيبرانية، رغم أهميته، لا يزال محدود الفاعلية نتيجة اختلاف التشريعات، وتباين المفاهيم، وضعف الثقة بين بعض الدول.

[1] Michael Fooner, Interpol: Issues in World Crime and International Criminal Justice, (Springer, 1989).
[2] Broeders, Dennis. European Policing and Europol: Governance, Intelligence, and Security in the EU, (Palgrave Macmillan, 2016), 36–34 ص.

الفصل الثالث

الاطار التشريعي للامن السيبراني في التشريعات الاردنية والمعاهدات الدولية

أدى التوسع في استخدام البيئة الرقمية في شؤون الحياة المتعددة إلى بروز ضرورة ملحّة لتأسيس إطار قانوني شامل يتولى حماية الأمن السيبراني، خاصة مع تنامي الجرائم ذات الطابع الإلكتروني وتعقد اساليبها واتخاذها طابعا عابرا للحدود وقد تنبه المشرع الاردني لاهمية هذه الظاهرة فعمل على تطوير مجموعة من القوانين والتشريعات التي تهدف الى مواجهة التحديات الناشئة عن التحولات التكنولوجية المتسارعة وتوفير الحماية القانونية للافراد والمؤسسات والحفاظ على امن واستقرار الفضاء السيبراني

وبناءً على ما تقدم، يخصص هذا الفصل لبحث الاطار المنظومة التشريعية الحاكمة للامن السيبراني بالمملكة الاردنية الهاشمية الى جانب بيان مدى التزام الأردن بالاتفاقيات الدولية ذات الصلة، حيث يتناول المبحث الأول دراسة التشريعات الوطنية المرتبطة بالأمن السيبراني، بدءًا بقانون الجرائم الإلكترونية، ثم قانون حماية البيانات الشخصية، وصولًا إلى السياسات والأنظمة ذات العلاقة.

وتم تقسيم هذا الفصل على النحو الاتي :

المبحث الاول: التشريعات الاردنية الخاصة بالامن السيبراني

المبحث الثاني: المعاهدات الدولية المتعلقة بالامن السيبراني

المبحث الاول
التشريعات الاردنية الخاصة بالامن السيبراني

شهد الاردن خلال السنوات الاخيرة تطورا ملحوظا في بنيته التشريعية والتنظيمية المرتبطة بالامن السيبراني وذلك استجابة للتحديات المتزايدة التي يفرضها الفضاء الرقمي على امن الدولة وخصوصية الافراد وسلامة البيانات ومع التحول المتسارع نحو الخدمات الالكترونية والاعتماد المتنامي على التكنولوجيا برزت الحاجة الى اطار قانوني متكامل ينظم الاستخدام الامن للمعلومات ويحد من الجرائم المرتبطة بالبيئة الالكترونية ، وقد انعكس هذا التوجه في اصدار منظومة من التشريعات الوطنية التي تناولت مختلف جوانب الامن السيبراني وفي مقدمتها القوانين التي تجرم الافعال الالكترونية غير المشروعة وتحاصر ممارسات الاختراق والاحتيال والابتزاز الى جانب التشريعات التي تعنى بحماية البيانات الشخصية وتنظيم معالجتها بما يعزز الثقة الرقمية كما دعمت الدولة هذه المنظومة بسياسات وطنية وانظمة تنظيمية تحدد المعايير الامنية واليات الحماية والمتابعة الامر الذي يشكل اساسا تشريعيا وتنظيميا يهدف الى بناء بيئة سيبرانية امنة ومتوازنة تحفظ الحقوق وتصون المصالح العامة والخاصة .

وعليه سيتم تناول اهم التشريعات الاردنية ذات العلاقة على النحو الاتي :

المطلب الاول: قانون الجرائم الالكترونية

المطلب الثاني: قانون حماية البيانات الشخصية

المطلب الثالث: الاطر التشريعية والتنظيمية

المطلب الاول
قانون الجرائم الالكترونية

يعد قانون الجرائم الالكترونية الاردني من الركائز الاساسية في الاطار القانوني الوطني للامن السيبراني حيث يهدف الى مكافحة الجرائم التي ترتكب باستخدام الشبكات الالكترونية وتقنيات المعلومات وتنظيم الاستخدام الامن للانترنت وحماية الافراد ويهدف هذا القانون إلى حماية الأفراد والمؤسسات من الأفعال التي تمس الأمن السيبراني، مثل الاحتيال الإلكتروني، والتجسس، والاختراق، ونشر المعلومات المضللة[1]. كما يتضمن أحكامًا تحدد صور الجرائم الإلكترونية والعقوبات المقررة لها، إلى جانب تنظيم إجراءات التحقيق والملاحقة القضائية، مع إيلاء عناية خاصة لحماية البيانات والمعلومات الشخصية، بما يعزز ثقة المستخدمين في المعاملات الرقمية .

كما ويعد قانون الجرائم الالكترونية رقم سبعة عشر لسنة الفين وخمسة عشر من اوائل القوانين التي نظمت الجرائم المرتكبة باستخدام تقنيات المعلومات والاتصالات في الاردن حيث جاء لمواكبة التطورات التقنية ووضع اطار قانوني لمكافحة هذه الجرائم ثم صدر قانون الجرائم الالكترونية رقم سبعة عشر لسنة الفين وثلاثة وعشرين ليشكل امتدادا تشريعيا اكثر شمولا واتساعا بما يتلاءم مع المستجدات الرقمية الحديثة[2] .

ورغم هذا التطور التشريعي فقد اثارت بعض نصوص القانون الجديد وأثار هذا القانون جدلًا واسعًا، خاصة فيما يتعلق بتجريم نشر الأخبار غير الصحيحة وخطاب الكراهية، حيث برزت مخاوف من احتمال المساس بحرية الرأي والتعبير في ظل عدم وضوح التعريفات الدقيقة لبعض

---

[1] العطاونة، مصطفى محمد .الجرائم الإلكترونية والتطور التشريعي في الأردن: دراسة فقهية وتشريعية .مجلة جامعة الشرق الأوسط للبحوث القانونية، 2024، ص 45–47.

[2] يونس، علاء ماجد أحمد باني, . Evolution of Cybersecurity Legislation in Jordanian Law. Migration Letters, 21(S4), 816–828, (2024).

المصطلحات الامر هذا دفع الى ضرورة مراجعة هذه النصوص بما يحقق التوازن بين متطلبات الامن السيبراني وضمان الحقوق والحريات العامة [1].

الفرع الأول: النطاق الموضوعي لقانون الجرائم الالكترونية .

وضح المشرع الاردني مضمون النطاق الموضوعي للتجريم في قانون الجرائم الالكترونية من خلال مواد متعددة حددت الافعال المجرمة والعقوبات المترتبة عليها بحسب طبيعة كل فعل ومدى مساسه بالامن السيبراني او بحقوق الافراد .

ومن ذلك ان القانون جرم الدخول او الوصول غير المشروع الى الشبكة المعلوماتية او نظام المعلومات او وسيلة تقنية المعلومات دون تصريح او بما يتجاوز التصريح ورتب على ذلك عقوبة سالبة للحرية او غرامة او كلتيهما كما تناول القانون الافعال التي تقع عبر النشر او اعادة النشر او ارسال البيانات والمعلومات عبر الوسائل الالكترونية اذا انطوت على اخبار كاذبة او اساءة تمس الاشخاص ورتب عليها عقوبات اشد من حيث مقدار الغرامة ومدد الحبس بما يظهر توجه المشرع الى تشديد الحماية في هذا الجانب .

وتبرز في هذا السياق خصوصية الجريمة الالكترونية لكونها تبدو بلا حدود وتؤثر على اولويات التحقيق ووسائله وموارده الامر الذي يفسر عدم وجود اطار قانوني موحد يطبق عالميا حيث تختلف تعريفات الجريمة الالكترونية باختلاف الدول وتتنوع الصور التي قد تبدو مشروعة في سياق وغير مشروعة في سياق اخر تبعا لنية الاستخدام فادوات الفحص والاختبار قد تكون مشروعة في البحث الامني ولكنها تصبح غير مشروعة اذا استعملت لاقتحام غير مصرح به .

---

[1] انظر منصور مغيره ، علاءالدين 2024. دراسة نقديةلقانون الجرائم الالكترونية الاردني رقم17 لعام 2024 وتاثيره على الحريات التعبير. تم الاسترجاع من :
https:\\cybercrimejournal.com\menuscript\index.php\cybercrime\artical\view\268

ومن ابرز صور انتهاك الخصوصية الرقمية عبر البيئة الالكترونية :

1 الابتزاز الالكتروني

يمكن النظر الى الابتزاز الالكتروني بوصفه سلوكا يقوم على الحصول على معلومات او صور او مواد تخص الضحية واستعمالها للضغط عليها بهدف تحقيق منفعة غير مشروعة[1] غالبا ما تكون مالية او تتعلق بحمل الضحية على القيام بفعل معين ويتميز عن الابتزاز التقليدي بان وسيلة الضغط تكون رقمية عبر الشبكة او التطبيقات مما يزيد من سرعة الفعل واتساع نطاقه وصعوبة السيطرة على اثاره[2] .

2 انتهاك الخصوصية وممارسات التجسس عبر الفضاء الإلكتروني.

اتسع نطاق انتهاك الخصوصية الالكتروني نتيجة سهولة توافر التقنيات وانتشارها واصبح من اخطر صور الاعتداء على الخصوصية لان الولوج غير المشروع الى اجهزة الافراد او حساباتهم يعد فعلا غير مشروع يعاقب عليه القانون وقد عزز الدستور الاردني مبدأ حماية المراسلات ووسائل الاتصال وجعلها مصونة من الاعتداء كما جرم قانون العقوبات الافعال التي تقوم على خرق الحياة الخاصة باستراق السمع او البصر او التسجيل او التقاط الصور باي وسيلة ،وتتضاعف خطورة التجسس لانه قد يشكل مدخلا لجرائم اخرى مثل الابتزاز من خلال استغلال ما تم الحصول عليه بصورة غير مشروعة للضغط على المجني عليه لذلك حرصت التشريعات على مواجهته بعقوبات رادعة كما واجه قانون الجرائم الالكترونية الاردني صور الدخول غير المشروع وتجريم الوصول الى الشبكات والانظمة دون تصريح ورتب العقوبات التي تتناسب مع خطورة الفعل كما تناول القانون افعالا اخرى مرتبطة بانتحال الهوية الرقمية بانشاء حسابات او صفحات ونسبتها

---

[1] السند، عبدالرحمن ابن عبدالله جرائم ابتزاز . ص 16 . مرجع سابق

[2] كورنو ،جيرار . معجم المصطلحات القانونية الطبعة الاولى المؤسسة الجامعيةللدراسات والنشر والتوزيع. صفحة33 .

زورا الى الغير وهي من الجرائم التي تمس الثقة بالفضاء الرقمي وتسبب اضرارا مباشرة للافراد والمؤسسات .

كما ان التشريعات الوطنية ذات الصلة دعمت حماية سرية الاتصالات ومنعت نشر مضمون اي اتصال او تسجيله دون سند قانوني لما يترتب على ذلك من اضرار وانتهاك لحقوق الافراد وانطلاقا من ذلك يتضح ان انتهاك الخصوصية الرقمية يمثل تهديدًا رئيسيًا للأمن السيبراني، ويشمل جمع البيانات أو اختراق الحسابات وتسريب المراسلات والصور دون إذن أصحابها او مراقبة نشاط المستخدمين بصورة غير مشروعة وهو ما يشكل اعتداء مباشرا على مبادئ السرية والسلامة والتوافر التي يقوم عليها الامن السيبراني ولذلك جاءت التشريعات الوطنية لتضع اطرا قانونية للحد من هذه الجرائم عبر التجريم والعقاب وتعزيز مفاهيم الحماية الرقمية .

وترى الباحثة ان النطاق الموضوعي لقانون الجرائم الالكترونية الاردني جاء واسعا ليشمل صورا متعددة من الافعال التي ترتكب بواسطة الوسائل التكنولوجية او من خلالها وهو اتساع فرضته التحولات التقنية التي افرزت اشكالا جديدة من الجرائم لا تكفي القواعد التقليدية لضبطها ومع ذلك يبقى هذا النطاق بحاجة الى مراجعة وتطوير بصورة دورية حتى يواكب التطور السريع لوسائل الجريمة الالكترونية ويمنع التوسع مما قد يؤثر على بعض الحريات الرقمية.

الفرع الثاني: تحليل المواد القانونية المتعلقة بجرائم الفضاء السيبراني .

أوجد التطور التقني تحديات قانونية وإجرائية، تتعلق بتكييف النصوص لمواجهة الجرائم الرقمية وضمان جمع الأدلة وإثباتها امام القضاء بصورة سليمة [1].

[1]ابوسعده، مصطفى بنداري. المنهجية القانونيةبين القواعد النظريةوالمهارات التطبيقية ، دار النهضة العربية، القاهرة، الطبعة الاولى،2023 م.

وفي هذا الاطار اتجهت الانظمة القانونية الى وضع نصوص تجرم الافعال غير المشروعة المرتكبة عبر الوسائل الالكترونية وتحدد العقوبات المناسبة لها بهدف تنظيم البيئة الرقمية وحماية المجتمع من مخاطرها

ويعد قانون الجرائم الالكترونية الاردني ، القانون الرئيسي الذي نظم كثيرا من الجرائم المرتكبة عبر الوسائل الالكترونية او الشبكة المعلوماتية مثل الاختراق والاحتيال والتشهير والابتزاز ونشر المحتوى غير المشروع كما رسم ضوابط واجراءات تتعلق بالملاحقة والتحقيق والتعامل مع الادلة الرقمية بما يعكس توجها لتعزيز الامن الرقمي[1] .

كما ان وجود قانون خاص جاء نتيجة التوسع في استخدام وسائل الاتصال والتقنيات الرقمية وتنامي منصات التواصل وانتشار ممارسات قد تضر بالمصالح العامة والافراد الامر الذي استلزم تنظيما يحد من اساءة استخدام الفضاء الرقمي ويوفر الحماية لمستخدمي الانترنت وانظمة المعلومات وقد شهد التشريع تطورا من القانون السابق الى القانون الجديد الذي توسع في التجريم والعقوبات مما اثار نقاشا حول مدى تأثير بعض النصوص على حرية الرأي والتعبير التي كفلها الدستور ضمن حدود القانون[2] .

ويظهر من تحليل النصوص ان المشرع اتجه الى حماية سلامة المعلومات عبر تجريم الدخول غير المشروع ثم تشديد العقوبة اذا كانت الانظمة المستهدفة ذات طبيعة حساسة او تابعة لجهات رسمية كما جرم انتحال الهوية الرقمية والاحتيال والابتزاز وانتهاك الخصوصية عبر نشر الصور او البيانات دون اذن وتعامل مع افعال تمس النظام العام عبر مواجهة التضليل المعلوماتي وخطاب

---

[1] جرادات، مازن &المجالي، فايز .اتجاهات القضاة والمحامين الأردنيين نحو قانون الجرائم الإلكترونية رقم 17 لسنة 2023 ودوره في الحد من الجريمة .مجلة أعمال جامعة اليرموك للبحوث القانونية، المجلد 53، العدد 5، 2025، ص 279–309.

[2] موقع النهضة للعرب للديمقراطيةوالتمنية .الرابط:
https://ammannet.net/

الكراهية والتحريض ووضع قواعد اجرائية تساعد في التحقيق وضبط الادلة وحجب المحتوى المخالف مع مراعاة حقوق الافراد .

وترى الباحثة ان هذه النصوص تعكس جهدا تشريعيا واضحا لمواكبة التحولات الرقمية وتجريم افعال لم تكن معروفة في التشريعات التقليدية غير ان بعض التحديات ما تزال قائمة وتتمثل في عمومية بعض الصياغات وغياب تعريفات تقنية دقيقة لبعض المفاهيم مما قد يؤدي الى تباين في التفسير القضائي ويستدعي مراجعة دورية للنصوص لضمان التوازن بين مكافحة الجريمة وحماية الحقوق والحريات الرقمية .

الفرع الثالث: تقييم فعالية القانون في مكافحة الجريمة الالكترونية

يشكل قانون الجرائم الالكترونية الاردني خطوة مهمة في مسار التطوير التشريعي لمواجهة الجريمة الرقمية اذ جاء اكثر شمولا واتساعا مقارنة بالقانون السابق سواء من حيث عدد المواد او تنوع الافعال المجرمة كما شمل خطابات وسلوكات رقمية متعددة مثل انتحال الهوية والابتزاز والاحتيال وخطاب الكراهية وغيرها ، غير ان تقييم الفعالية يتطلب النظر الى عناصر متعددة منها وضوح النصوص وسهولة تطبيقها لدى الجهات المختصة ومدى توافقها مع المبادئ الدستورية والمعايير الدولية ذات الصلة بحقوق الانسان كما يتطلب النظر في مدى توفر الادوات الفنية والكوادر المتخصصة التي تساعد على تنفيذ القانون واثبات الجرائم الرقمية بصورة دقيقة

وتشير الباحثة الى ان غياب تعريفات دقيقة لبعض الافعال وحدودها قد يخلق تداخلا في التطبيق ويضعف فعالية الردع كما ان الفجوة بين النصوص القانونية والتطبيق العملي قد تؤثر على ثقة الافراد بقدرة القانون على حمايتهم في الفضاء الرقمي[1] .

كما ان فعالية مكافحة الجريمة الالكترونية تواجه تحديات مرتبطة بطبيعة هذه الجرائم ومن اهمها :

1. الطبيعة العابرة للحدود: تعد الجرائم الالكترونية بطبيعتها عابرة للحدود وهو ما يعرقل الملاحقة ويتيح للجناة الاستفادة من اختلاف الاختصاصات وتباين القوانين للهروب من المساءلة[2]
2. صعوبة جمع الادلة الرقمية: يتطلب كشف الجرائم الرقمية ادوات متقدمة وخبرات فنية خاصة بسبب سرعة تغير البيانات واحتمال فقدانها او تشفيرها وتوزعها الجغرافي عبر خوادم ومنصات متعددة[3]
3. عدم الابلاغ عن الجرائم: يمتنع بعض الضحايا عن الابلاغ لاعتقادهم بعدم جدوى الملاحقة او خشيتهم من الاثار الاجتماعية او لضعف الثقة بفعالية الاستجابة الرسمية
4. التطور السريع للتقنيات: يسبق التطور التقني في كثير من الاحيان قدرة التشريعات على التحديث مما يؤدي الى فجوات قانونية تظهر عند بروز انماط جديدة من الجرائم الرقمية[4]

وعليه ترى الباحثة ان تعزيز فعالية القانون يتطلب تحديثا مستمرا للنصوص وتطويرا للقدرات الفنية والقضائية وتعزيزا للتعاون الدولي وتكثيفا للتدريب والتخصص في مجال الادلة الرقمية [1] .

---

[1] عقلة، اشرف علي ، دور التشريع في مكافحة الجرائم الالكترونيةواثره على امن معلومات المكتبات. مجلد رقم 13 عدد1 صفحة 112.

[2] مساعدة، انورمحمد صدقي. 2019 .جرائم الكترونية والاختصاص القضائي .جامعة قطر عدد4 .

[3] معايطة، محمد وغسين ،محمود 2020 .التحديات التقنية والقانونية في جمع الادلةالرقمية في الجرائم الالكترونية . الجامعةالاردنية العدد15 صفحة 45.60

[4] رواشدة، يونس، ومغيرة، . تحديات قانونية لمكافحة الاجرام السيبراني في ظل التطور السريع . جامعة مؤتة. عدد 3 صفحة 104-116.

المطلب الثاني
قانون حماية البيانات الشخصية

يعر ف قانون حماية البيانات الشخصية البيانات الشخصية بانها كل معلومة ترتبط بشخص طبيعي ويمكن ان تؤدي الى تحديد هويته بصورة مباشرة او غير مباشرة بصرف النظر عن مصدر هذه البيانات او شكلها وتشمل المعلومات المتعلقة بحياته الشخصية او العائلية او مكان تواجده[2] .

كما عر ف القانون البيانات الحساسة بانها البيانات التي تتصل بجوانب دقيقة من حياة الفرد مثل اصله العرقي او الاثني او ارائه وتوجهاته السياسية او معتقداته الدينية او حالته الصحية او النفسية او الجسدية او الوراثية او معلوماته المالية او بصماته البيومترية او سجله الجنائي كما اجاز للمجلس المختص تصنيف بيانات اخرى باعتبارها بيانات حساسة متى كان من شأن الكشف عنها او اساءة استخدامها ان يؤدي الى الحاق ضرر بالشخص المعني[3] .

ويقصد بالبيانات الشخصية ايضا كل معلومة تتعلق بالفرد سواء في حياته الخاصة او المهنية او العامة ومع التطور الرقمي الهائل وبيئة الانترنت التي يتم فيها تداول كميات ضخمة من البيانات الشخصية عبر الحدود اصبح من الصعب على الافراد السيطرة على معلوماتهم الامر الذي جعل حماية البيانات الشخصية ضرورة قانونية ومجتمعية ملحة ، كما وتتطلب حماية البيانات الشخصية وضع مجموعة من الضوابط والاجراءات القانونية والتنظيمية التي تكفل للافراد حق التحكم في بياناتهم الخاصة بحيث يكون لهم الحق في تقرير ما اذا كانوا يرغبون في مشاركة

---

[1] عرب، يونس. قراءة في اتجاهات تشريعية للجريمةالالكترونية مع بيان موقف الدول العربيةوتجربة سلطنةعمان. مجلة الازهرللعلوم الاعلامية. عدد56 ج3. جامعةالازهر كليةالاعلام. 2023 صفحة3 .

[2] ربيحات، روان . قانون حمايةالبيانات الشخصية الاردني . 2024 متوفر على : قانون-حماية-البيانات-الشخصية-الاردن2\ ar\org.smex\\:https.

[3] جعافرة،رويدا حسين . قانون حمايةالبيانات الشخصية في الاردن. اصدار خامس عدد50 2022 صفحة3.

بياناتهم كما ينبغي للمستخدمين معرفة الأطراف التي تُشارك معها بياناتهم، ومدة الاحتفاظ بها، والغرض من استخدامها، ويحق لهم تعديل أو تحديث هذه البيانات عند الحاجة.

ويرتبط قانون حماية البيانات الشخصية الاردني ارتباطا وثيقا بالمعاهدات والاتفاقيات الدولية ذات الصلة بحماية الخصوصية الرقمية حيث جاء هذا القانون استجابة للمعايير العالمية التي تؤكد ضرورة صون خصوصية الافراد وحماية بياناتهم في ظل التوسع الكبير في استخدام التكنولوجيا والبيانات الرقمية .

وتقوم العلاقة بين قانون حماية البيانات الشخصية الاردني والاتفاقيات الدولية على اساس التكامل لا التعارض ، اذ يسعى التشريع الوطني الى مواءمة احكامه مع الالتزامات الدولية وبخاصة تلك المرتبطة بحقوق الانسان ومكافحة الجرائم الالكترونية وتنظيم نقل البيانات عبر الحدود بما يسهم في بناء منظومة قانونية حديثة تحترم الخصوصية وتراعي الطابع العابر للحدود للبيانات الالكترونية ،ولا يعد قانون حماية البيانات الشخصية الاردني معزولا عن السياق الدولي بل يمثل جزءا من توجه عام يهدف الى تعزيز الثقة الرقمية والتعاون الدولي في بيئة الكترونية تتطلب معايير موحدة لحماية الخصوصية ومواجهة الجرائم السيبرانية .

وقد اكد المشرع الاردني هذا التوجه حين نص في المادة الثانية من قانون حماية البيانات الشخصية يجب الالتزام بالاتفاقيات والمعاهدات ذات الطابع الدولي التي اتفقت عليها الاردن بشأن حماية البيانات الشخصية عند تنفيذ أحكام القانون [1]وهو ما يؤكد على حرص المشرع الاردني على الانسجام مع المنظومة القانونية الدولية وعدم العمل بمعزل عنها .

[1]وزارة الاتصالات وتكنولوجيا المعلومات الأردنية. قانون حماية البيانات الشخصية رقم (30) لسنة 2021. نشرت في الجريدة الرسمية الأردنية، العدد 5550، 2021.

الفرع الاول: المبادئ العامة لحماية البيانات الشخصية في القانون الاردني .

اكد المشرع الاردني في المادة 7 من مسودة قانون حماية البيانات الشخصية على المبادئ والاشتراطات التي ينبغي مراعاتها أثناء التعامل مع البيانات الشخصية وتتمثل في ان يكون الغرض من جمع البيانات واستخدامها مشروعا وواضحا ومحددا بدقة وان تستخدم البيانات في اطار الاهداف التي جمعت من اجلها فقط وان تتم جميع عمليات المعالجة بوسائل قانونية ومشروعة .

كما اشترط القانون ان تكون البيانات دقيقة وصحيحة ويتم تحديثها كلما دعت الحاجة الى ذلك وإلا تبقى البيانات قادرة على كشف هوية الشخص بعد انتهاء الهدف من جمعها مع ضرورة الحفاظ على السرية التامة وضمان عدم تلف البيانات او تغييرها او التلاعب بها اثناء المعالجة او التخزين[1] .

كما نصت المادة الثامنة من مسودة القانون على اشتراطات خاصة بمعالجة البيانات الشخصية حيث حظرت معالجة البيانات دون موافقة صاحبها الا في حالات استثنائية محددة تتمثل في كون المعالجة ضرورية لتنفيذ عقد يكون الشخص المعني طرفا فيه او لاتخاذ اجراءات تمهيدية بناء على طلبه او للوفاء بالتزام قانوني مفروض بموجب تشريع نافذ او حكم قضائي او لحماية مصلحة حيوية تتعلق بالشخص المعني بالبيانات .

كما وشدد القانون على عدم جواز استخدام البيانات الشخصية لغير الغرض الذي جمعت من اجله وضرورة تحديد هذا الغرض بشكل واضح عند الحصول على موافقة الشخص المعني كما قيد معالجة بيانات الاشخاص غير متمتعين بالاهلية القانونية الكاملة بضرورة الحصول على موافقة خطية او الكترونية من احد الوالدين او الولي القانوني[2] .

---

[1] مادة 7 من مشروع قانون حمايةالبيانات الشخصية عام 2022.

[2] مادة8 من مشروع قانون حماية البيانات الشخصية سنة 2022.

وتقوم المبادئ الاساسية لحماية البيانات الشخصية على مجموعة من الاسس الجوهرية من اهمها تحديد الهدف من جمع البيانات بحيث لا يتم جمعها الا لاغراض واضحة ومحددة ومعلنة مسبقا وتقليل حجم البيانات المجمعة بحيث تقتصر على الحد اللازم لتحقيق الغرض المطلوب وضمان دقة البيانات وتحديثها بشكل مستمر.

كما تشمل هذه المبادئ تحديد مدة الاحتفاظ بالبيانات بحيث لا يتم الاحتفاظ بها لاكثر من المدة اللازمة لتحقيق الغرض من جمعها والالتزام بمبدأ الشرعية والشفافية في المعالجة وضمان حماية البيانات من الوصول غير المصرح به او اي استخدام غير مشروع ، وتعد هذه المبادئ الركيزة الاساسية لاي نظام قانوني فعال لحماية الخصوصية الرقمية اذ تسهم في تحقيق التوازن بين متطلبات استخدام البيانات وبين صون حقوق الافراد وحرياتهم كما تفرض على الجهات المعالجة للبيانات التزامات قانونية واضحة تضمن المساءلة والشفافية .

كما نظم المشرع الاردني ضوابط معالجة البيانات الشخصية على نحو يفرض الحصول على موافقة صريحة من صاحب البيانات ويشترط وضوح البيانات وتحديدها بدقة وعدم استخدامها الا في الاطار الذي جمعت من اجله مع التأكيد على ضرورة التناسب بين كمية البيانات المجمعة والغرض المطلوب تحقيقه .

وتجدر الاشارة الى ان مدة الاحتفاظ بالبيانات الشخصية قد تختلف من حالة الى اخرى بحسب طبيعة الغرض من جمعها اذ لا يمكن دائما تحديد زمن ثابت لانتهاء الحاجة الى البيانات فعلى سبيل المثال في حالات تصفية الشركات او افلاسها قد تستدعي الضرورة الاحتفاظ ببعض البيانات

لفترة اطول لحماية حقوق المساهمين او الشركاء او المتعاقدين حيث قد تشكل هذه البيانات دليلا على وجود التزامات قانونية او علاقات تعاقدية قائمة[1].

الفرع الثاني: حقوق الشخص المعني بالبيانات والتزامات الجهة المسؤولة .

كرس قانون حماية البيانات الشخصية رقم 24 لعام 2023 مجموعة من الحقوق الاساسية التي يتمتع بها الشخص المعني بالبيانات وهو الشخص الطبيعي الذي تخضع بياناته الشخصية لعمليات الجمع او التخزين او المعالجة او الاستخدام وتعد هذه الحقوق من الركائز الجوهرية التي يقوم عليها نظام حماية البيانات الشخصية لما لها من دور في تعزيز سيطرة الفرد على بياناته وضمان احترام خصوصيته في البيئة الرقمية[2]، ويتمتع الشخص المعني بعدد من الحقوق التي تضمن له الاطلاع على بياناته الشخصية حيث يحق له الوصول الى البيانات الموجودة لدى المسؤول عن المعالجة والحصول على نسخة منها والاطلاع على كيفية استخدامها والاغراض التي تعالج من اجلها كما يملك الحق في سحب موافقته التي سبق ان منحها لمعالجة بياناته في اي وقت دون ان يترتب على ذلك اي مساس بحقوقه الاخرى .

كما يملك الشخص المعني الحق في تصحيح بياناته الشخصية او تعديلها او تحديثها في حال كانت غير دقيقة او ناقصة او قديمة وله كذلك الحق في اضافة بيانات جديدة اذا اقتضت الحاجة ذلك بما يضمن صحة البيانات ودقتها ، ويمنح القانون الشخص المعني الحق في تحديد نطاق معالجة بياناته بحيث تقتصر هذه المعالجة على اغراض محددة ومتفق عليها مسبقا وله الحق في

---

[1] النجار، سامي عبد الله .حماية البيانات الشخصية في التشريعات العربية: دراسة مقارنة .عمان: دار النهضة للنشر والتوزيع، 2022، ص 152–155.

[2] راشد عمر الكساسبة، حماية البيانات الشخصية من خلال اللجوء إلى حق النسيان الرقمي وفقاً للتشريع الأردني: دراسة مقارنة .المجلة الأردنية في القانون والعلوم السياسية، المجلد 17، العدد 2، 2025.

طلب حذف بياناته الشخصية او اخفائها او نسيانها وفقا للضوابط التي يحددها القانون وبما لا يتعارض مع الالتزامات القانونية او التعاقدية المترتبة على الجهة المسؤولة .

كما يقر القانون حق نقل البيانات والذي يسمح للشخص المعني بنقل بياناته الشخصية من مسؤول معالجة الى مسؤول اخر بطريقة منظمة وامنة بما يضمن سهولة انتقال البيانات وعدم احتكارها من جهة واحدة

ويضاف الى ذلك حق الشخص المعني في ان يتم اعلامه فورا باي خرق او انتهاك يمس سلامة او امن بياناته الشخصية بما يمكنه من اتخاذ الاجراءات اللازمة لحماية حقوقه [1] .

اولا: الحق في الموافقة

تعد الموافقة المسبقة من اهم الضمانات التي كفلها المشرع الاردني لحماية البيانات الشخصية اذ تشكل الاساس القانوني لمشروعية المعالجة وقد اولت مسودة قانون حماية البيانات الشخصية هذا الحق اهمية خاصة حيث نصت على ضرورة حصول المسؤول عن المعالجة على موافقة صريحة ومسبقة وواضحة من الشخص المعني سواء كانت مكتوبة او الكترونية ، ويشترط في هذه الموافقة ان تكون محددة من حيث الغرض من المعالجة ومدتها وان يتم تجديدها في كل مرة تتغير فيها طبيعة او نوع المعالجة والا اعتبرت الموافقة السابقة غير قائمة ولا يعتد باي موافقة يتم الحصول عليها بوسائل خادعة او مضللة او غير صحيحة[2] .

ومع ذلك لم يجعل المشرع الموافقة شرطا مطلقا في جميع الاحوال بل اجاز في حالات استثنائية معالجة البيانات دون موافقة الشخص المعني اذا كانت المعالجة ضرورية لمنع جريمة او

---

[1] وزارةالاقتصاد الرقمي والريادة–الاردن. قانون حماية البيانات الشخصية رقم27 سنة 2023.

[2] الزبيدي، ناصر إبراهيم .المبادئ الأساسية لحماية البيانات الشخصية: الموافقة، الشفافية، والمحاسبة .مجلة العلوم القانونية والقضائية، جامعة حلب، المجلد 25، العدد 1، 2024، ص 78–85.

كشفها او متابعتها بناء على قرار قضائي او امر صادر عن المدعي العام او اذا كانت المعالجة مطلوبة او مصرحا بها بموجب تشريع نافذ او بقرار من المحكمة المختصة .

ثانيا: الحق في نقل البيانات

كرس المشرع الاردني حق الشخص المعني في نقل بياناته الشخصية من مسؤول معالجة الى مسؤول اخر بما يعزز مبدأ التحكم الفردي في البيانات ويمنع احتكارها من جهة واحدة ويتيح انتقالها بطريقة منظمة وامنة

وقد نظم القانون احكام نقل وتبادل البيانات داخل المملكة حيث اشترط عدم جواز نقل البيانات بين المسؤول عن المعالجة واي جهة اخرى الا بعد الحصول على موافقة صريحة من صاحب البيانات مع ضرورة ضمان حماية البيانات وان تكون لدى الجهة المستقبلة مصلحة مشروعة في استخدامها وان يكون لدى المسؤول عن المعالجة علم كاف بهوية الجهة المستقبلة والغرض من استخدام البيانات[1] ، كما الزم القانون المسؤول عن المعالجة بتوثيق جميع عمليات نقل البيانات وتوثيق موافقات اصحابها وحظر نقل البيانات لاغراض تسويقية الا بعد أخذ موافقة واضحة من الفرد المعني.

أما بالنسبة لإرسال البيانات الشخصية خارج حدود المملكة فقد اشترط القانون توافر مستوى كاف من الحماية لدى الجهة المستقبلة بحيث لا يجوز النقل الا اذا كان مستوى الحماية مساويا او اعلى من المستوى الذي يقرره القانون الاردني لحماية البيانات الشخصية .

[1] الزبيدي، ناصر إبراهيم .حقوق الأفراد في حماية البيانات الشخصية: الحق في النقل والمبادلة وفق التشريع الأردني .مجلة العلوم القانونية والقضائية، جامعة حلب، المجلد 25، العدد 2، 2024، ص 102–108.

ثالثا: الحق في المحو او النسيان

يعد حق المحو او ما يعرف بحق النسيان من الحقوق الحديثة التي تهدف الى تمكين الشخص المعني من التحكم في بياناته الشخصية ومنع استمرار الاحتفاظ بها دون مبرر مشروع ، ومنح القانون هذا الحق في حالات محددة منها ان يتم استخدام البيانات لاغراض تختلف عن تلك التي جمعت من اجلها او اذا قام الشخص المعني بسحب موافقته التي كانت اساس المعالجة او اذا تمت معالجة البيانات بطريقة غير قانونية او اذا كان حذف البيانات ضروريا لتنفيذ التزام قانوني او تعاقدي او عند انتهاء هذا الالتزام ، وعلى المسؤول عن معالجة البيانات، عند استلام طلب الحذف، اتخاذ كافة الإجراءات اللازمة بما في ذلك الوسائل التقنية لمحوها او اخفاء هوية اصحابها وفقا لما يحدده القانون [1].

كما تقع على عاتق الجهة المسؤولة عن معالجة البيانات مجموعة من الالتزامات الجوهرية التي تهدف الى ضمان حماية البيانات الشخصية ومنع اساءة استخدامها حيث يلتزم المسؤول مسؤول عن حماية البيانات التي يملكها أو التي استلمها من جهات أخرى، حسب القانون[2].

ويتعهد بوضع سياسات وإجراءات محددة لحماية البيانات الشخصية، وتنظيم آليات استقبال الشكاوى ومعالجتها والالتزام بتوفير وسائل المساعدة المناسبة التي تضمن تلبية احتياجات الشخص المعني بما في ذلك الوسائل البصرية والسمعية والحسية عند الاقتضاء[3] ، ويجب على المسؤول عن المعالجة تعيين مراقب لحماية البيانات الشخصية يتولى الاشراف على الالتزام باحكام القانون وضمان الامتثال للمعايير المقررة

---

[1] محمد عبد الله الجابري، الحق في النسيان الرقمي وحماية البيانات الشخصية: دراسة مقارنة بين التشريع الأردني والاتحاد الأوروبي . مجلة الحقوق والمجتمع، جامعة مؤتة، المجلد 12، العدد 1، 2023، ص 88–95.

[2] سامي عبد الله النجار، التزامات مسؤول معالجة البيانات وحماية الحقوق الفردية في التشريع الأردني .عمان: دار النهضة للنشر والتوزيع، 2022، ص 120–125.

[3] راشد عمر الكساسبة، التزامات مسؤول معالجة البيانات وحماية الحقوق الفردية في التشريع الأردني: السياسات والإجراءات وآليات الشكاوى .المجلة الأردنية في القانون والعلوم السياسية، المجلد 18، العدد 1، 2025، ص 112–118.

المطلب الثالث
الأطر التشريعية والتنظيمية

مع الانتشار الواسع والسريع للتقنيات الرقمية واعتماد القطاعات المختلفة على الفضاء السيبراني، برزت الحاجة إلى أطر قانونية وتنظيمية لحماية هذا المجال من التهديدات والمخاطر المتزايدة، ويعكس هذا التوجه استجابة للتحديات الأمنية والتقنية التي تؤثر على الأفراد والمؤسسات والدول.

وقد سعت الدول إلى مواجهة هذه التحديات من خلال سن تشريعات وقوانين حديثة وإصدار أنظمة وتعليمات تنظيمية تهدف إلى تنظيم استخدام تكنولوجيا المعلومات والاتصالات وضمان أمنها وحماية مكوناتها المختلفة من أي مخاطر محتملة قد تنجم عن سوء الاستخدام أو الهجمات الإلكترونية .

الفرع الأول: قانون الأمن السيبراني لسنة 2019 .

أصدر الأردن قانون الأمن السيبراني رقم 16 لسنة 2019 استجابة لتزايد المخاطر الناتجة عن الهجمات الإلكترونية والحاجة لتعزيز قدرة الدولة على التعامل مع الحوادث السيبرانية، خصوصًا تلك التي تستهدف الأنظمة الحيوية والبنية التحتية الرقمية، وقد جاء بهدف ليشكل إطارا وطنيا متكاملا للأمن السيبراني يهدف إلى حماية المعلومات الحساسة والبيانات الحكومية وضمان سلامة الفضاء السيبراني الوطني[1]، ويهدف القانون إلى توفير بيئة رقمية آمنة ومستقرة تسهم في دعم التنمية الاقتصادية وجذب دعم الاستثمارات وتشجيع النمو الاقتصادي، لا سيما مع زيادة الخدمات الحكومية الإلكترونية وتطور قطاع تكنولوجيا المعلومات بشكل مستمر[2] ، ومع ازدياد الاعتماد على الأنظمة

---

[1] عبد الله، فادي محمد .الإطار القانوني للأمن السيبراني في الأردن: دراسة تحليلية لقانون الأمن السيبراني رقم 16 لسنة 2019 .مجلة العلوم القانونية الأردنية، المجلد 14، العدد 2، 2021، ص 55–63.

[2] محمد أمين القضاة، الأمن السيبراني وأثره في تعزيز الاستثمار والتنمية الاقتصادية في الأردن. مجلة دراسات – الجامعة الأردنية، المجلد 49، العدد 3، 2022، ص 215–222.

الرقمية في مختلف القطاعات مثل البنوك والمستشفيات والمؤسسات الحكومية والشركات الخاصة باتت حماية هذه الأنظمة من المخاطر السيبرانية أمراً حيوياً لضمان الأمن الداخلي [1].

ينص قانون الأمن السيبراني على مجموعة من الأحكام التي تنظم حماية الفضاء الرقمي بشكل متكامل، ويحدد طبيعة التهديدات السيبرانية وآليات مواجهتها، كما يوضح صلاحيات الجهات المعنية في مراقبة الشبكات والأنظمة الرقمية والتدخل عند حدوث أي تهديد أمني .

كما نظم القانون الإجراءات التحقيقية وحدد الضوابط القانونية المتعلقة بجمع الأدلة الرقمية والتعامل معها بصورة تضمن مشروعيتها وسلامتها وألزم الجهات الحكومية والخاصة باتباع معايير الحماية والأمن السيبراني للحفاظ على سلامة البيانات والمعلومات ومنع تعرضها للاختراق أو العبث.

وفي مواجهة التحديات السيبرانية، أصدر الأردن قانون الأمن السيبراني رقم 16 لسنة 2019، تلاه تشريعات داعمة أبرزها قانون الجرائم الإلكترونية رقم 17 لسنة 2023، الذي تحدد المادة 32 فيه الإجراءات التي يمكن لموظفي الضابطة العدلية اتخاذها بعد إذن المدعي العام أو المحكمة المختصة، ومنحت هذه المادة صلاحية الدخول إلى المواقع التي تشير الأدلة إلى استخدامها في ارتكاب الجرائم الإلكترونية وتفتيش الأجهزة والبرمجيات والشبكات المرتبطة بها كما أوجبت إعداد تقرير رسمي بنتائج التفتيش والفحص وضبط الأجهزة والوسائل التقنية المستعملة في الجريمة مع الحفاظ على البيانات المرتبطة بها، مع استثناء الأشخاص المرخص لهم وفق قانون الاتصالات ما لم يثبت تورطهم في الجريمة .

وترى الباحثة ان قانون الأمن السيبراني يعتبر خطوة مهمة لتعزيز التشريعات الوطنية لمواجهة التهديدات الرقمية وحماية البيانات الحساسة. ساهم في تنظيم المركز الوطني للأمن السيبراني

[1] عبابنة، محمد احمد 2020 جرائم الحاسوب وابعادها الدولية.دار الثقافة . عمان صفحة 431.

لتنسيق الجهود، مع ضرورة تطويره باستمرار وتعزيز التعاون مع القطاع الخاص وتوسيع برامج التدريب والتوعية .

الفرع الثاني: المركز الوطني للأمن السيبراني

يعد المركز الوطني للأمن السيبراني مؤسسة حكومية تهدف إلى بناء منظومة وطنية فعالة للأمن السيبراني وتطويرها وتنظيمها بما يضمن حماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية وبما يحقق استدامة العمل ويحافظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات ، ويعمل المركز على إيجاد فضاء سيبراني أردني آمن وموثوق من خلال تدريب وتأهيل وتوعية موظفي القطاعين العام والخاص وكافة فئات المجتمع وإكسابهم المعارف والمهارات اللازمة للحد من المخاطر والتهديدات السيبرانية وفق أفضل الممارسات الدولية[1].

أولا: الحماية والوقاية

تعد الحماية والوقاية الركيزة الأساسية في منظومة الأمن السيبراني حيث تركز على بناء أنظمة دفاعية قوية تمنع وقوع الهجمات الإلكترونية قبل حدوثها من خلال تعزيز أمن البنى التحتية المعلوماتية والخدمات الرقمية وضمان استمرارية عملها بصورة آمنة[2] ، ويهدف هذا الجانب إلى تحصين الأنظمة الوطنية ضد محاولات الاختراق وحماية البيانات الحساسة من التسريب أو التلاعب أو الإتلاف بما يسهم في رفع مستوى الأمن السيبراني الوطني ويتحقق ذلك من خلال تأمين الشبكات ومراكز البيانات والبنى التحتية الحيوية وتعزيز حماية الخدمات الرقمية .

---

[1] خالد مصطفى العلي، دور المؤسسات الوطنية في تعزيز الأمن السيبراني: دراسة حالة المركز الوطني للأمن السيبراني الأردني .مجلة العلوم القانونية والإدارية، جامعة مؤتة، المجلد 13، العدد 2، 2023، ص 77–85.

[2] يوسف محمد الخطيب، استراتيجيات الوقاية والحماية في الأمن السيبراني: منهجيات لتعزيز أمن البنى التحتية الرقمية .مجلة العلوم التقنية والأمن المعلوماتي، المجلد 10، العدد 1، 2022، ص 45–52.

ثانيا: الاستجابة للحوادث

رغم أهمية الوقاية إلا أن بعض التهديدات السيبرانية قد تنجح في اختراق الأنظمة وهنا تبرز أهمية وجود منظومة وطنية متكاملة قادرة على التعامل مع الحوادث فور وقوعها والحد من آثارها وتوثيق الأدلة الرقمية وتحليلها فنيا وقانونيا ويتم ذلك من خلال تنسيق الجهود بين الجهات المختصة وتوفير منصات للإبلاغ عن الحوادث تتيح للأفراد والمؤسسات المشاركة في كشف الاعتداءات السيبرانية والتعامل معها بفعالية[1] وذلك عبر توحيد جهود الاستجابة الوطنية والإشراف على جمع وتحليل الأدلة الرقمية وتوفير منصات مخصصة للإبلاغ .

ثالثا: بناء القدرات وتطويرها .

يعد بناء القدرات الوطنية في مجال الأمن السيبراني من العناصر الأساسية لضمان فعالية المنظومة الوطنية حيث يهدف هذا الجانب إلى رفع كفاءة العاملين والكوادر الوطنية من خلال برامج تدريبية متخصصة ونشر الوعي السيبراني بين مختلف شرائح المجتمع وتعزيز البحث العلمي والابتكار في هذا المجال [2].

رابعا: تعزيز التعاون والشراكات .

لا يمكن مواجهة التهديدات السيبرانية بمعزل عن التعاون المحلي والدولي لذلك يركز هذا المحور على بناء شراكات استراتيجية بين المؤسسات الوطنية والجهات الدولية المختصة لتبادل

---

[1] محمود علي الحوراني، إدارة الحوادث السيبرانية وأهمية المنظومات الوطنية في حماية الفضاء الرقمي الأردني .مجلة العلوم القانونية والإدارية، جامعة اليرموك، المجلد 15، العدد 2، 2023، ص 101–110.

[2] سامي فوزي العبدلي، بناء القدرات الوطنية في الأمن السيبراني: استراتيجيات التدريب والتوعية والابتكار .مجلة الدراسات التقنية والأمنية، المجلد 11، العدد 2، 2023، ص 67–75.

الخبرات والمعلومات وتعزيز الاستجابة المشتركة ويعكس هذا التوجه إدراك الطبيعة العابرة للحدود للأمن السيبراني[1] .

وترى الباحثة أن بناء منظومة أمن سيبراني فعالة لا يقتصر على سن التشريعات ووضع السياسات بل يتطلب مقاربة شمولية تقوم على الوقاية والاستجابة وتطوير القدرات الوطنية إلى جانب التعاون المحلي والدولي بما يضمن حماية البنية الرقمية والبيانات والمجتمع وتحقيق بيئة رقمية آمنة ومستقرة

الفرع الثالث: الأنظمة التنفيذية وتعليمات هيئة تنظيم قطاع الاتصالات .

أنشئت هيئة تنظيم قطاع الاتصالات بموجب قانون الاتصالات رقم 13 لعام 1995 كمؤسسة حكومية مستقلة تهدف إلى تنظيم قطاعي الاتصالات وتكنولوجيا المعلومات، وضمان تقديم خدمات عالية الجودة بأسعار مناسبة وتحقيق كفاءة الأداء وفق السياسة العامة المعتمدة ، وتتولى الهيئة تنظيم قطاع تكنولوجيا المعلومات والإشراف على مقدمي خدمات الاتصالات والبريد وفقا للتشريعات النافذة وتعمل بشكل مستقل عن وزارة الاتصالات ضمن الإطار الذي حدده القانون.

تضع الهيئة معايير فنية وأمنية لتعزيز حماية الشبكات ومراكز البيانات وضمان استمرار الخدمات الرقمية، كما تلزم مزودي الاتصالات وتقنية المعلومات بالالتزام بأفضل ممارسات الأمن السيبراني للحد من المخاطر[2].

تشمل الأنظمة حماية بيانات المستخدمين وتأمين الشبكات، وتنظيم آليات رصد والاستجابة للحوادث السيبرانية، إلى جانب تحديد أساليب الرقابة والتفتيش لمتابعة التزام الجهات المعنية ،

---

[1] مهاجمال يوسف العمري، التعاون المحلي والدولي في الأمن السيبراني: بناء شراكات استراتيجية لمواجهة التهديدات العابرة للحدود. مجلة العلوم القانونية والإدارية، جامعة اليرموك، المجلد 16، العدد 1، 2024، ص 88–96.

[2] هيئةتنظيم قطاع الاتصالات الاردنية، الموقع الرسمي، متاح : https:\\www.trc.gov.jo\ar

وبموجب قانون الاتصالات تضطلع الهيئة بعدد من المهام من بينها تنظيم خدمات الاتصالات وتكنولوجيا المعلومات وضع المبادئ الأساسية للتنظيم تحديد مستويات جودة الخدمة مراقبة التزام المرخص لهم وحماية مصالح المستفيدين وتشجيع التنظيم الذاتي [1].

[1] مادة6 قانون الاتصالات رقم13 سنة 1995 واعديلاته. منشور على ص 2939 من الجريدةالرسمية.

المبحث الثاني
المعاهدات الدولية المتعلقةبالأمن السيبراني

تستمد المعاهدات الدولية الخاصة بالأمن السيبراني أهميتها من كونها الإطار القانوني الذي يتم من خلاله تنسيق جهود الدول في مواجهة الجرائم الإلكترونية ذات الطابع العابر للحدود حيث لم يعد من الممكن الاكتفاء بالتشريعات الوطنية وحدها في ظل فضاء رقمي مفتوح لا يعترف بالحدود الجغرافية التقليدية بين الدول وقد أدى هذا الواقع إلى بروز عدد من الاتفاقيات الدولية والإقليمية التي سعت إلى وضع قواعد عامة تهدف إلى تعريف الجريمة السيبرانية وتنظيم آليات التعاون الدولي في كشفها وملاحقة مرتكبيها وتبادل الأدلة والمعلومات بين الدول كما أرست هذه الاتفاقيات مجموعة من المبادئ المشتركة التي تحكم التعامل مع الفضاء الرقمي من أبرزها احترام سيادة الدول على بنيتها الرقمية وتعزيز التعاون الدولي وتبادل المساعدة القانونية في مجال مكافحة الجرائم الإلكترونية وفي ضوء هذه التطورات أصبح من الضروري أن تعمل الدول على مواءمة تشريعاتها الوطنية مع هذه المنظومة الدولية من خلال الاستفادة من الأحكام الواردة في أهم الاتفاقيات المتخصصة في الجرائم الإلكترونية والاتفاقيات العربية ذات الصلة إلى جانب الجهود الأممية الرامية إلى بلورة صك دولي شامل في هذا المجال كما يتطلب ذلك دراسة المبادئ العامة والالتزامات القانونية التي تفرضها هذه الصكوك الدولية وآليات تنفيذها العملية والتحديات التي تواجه تطبيقها ثم بيان مدى انسجام الإطار التشريعي الأردني مع هذه المعايير العالمية وأوجه التوافق والقصور في مجال الأمن السيبراني بما يسمح بإجراء تقييم حقيقي لمدى المواءمة بين التشريعات الوطنية والمتطلبات الدولية في هذا المجال وعليه ستتناول الباحثة في هذا المبحث المحاور التالية :

المطلب الأول: أهم الاتفاقيات الدولية

المطلب الثاني: المبادئ والالتزامات الدولية للأمن السيبراني

المطلب الثالث: آليات تنفيذ المعاهدات والتحديات التي تواجه تطبيقها

المطلب الرابع: مدى مواءمة التشريعات الأردنية مع الاتفاقيات الدولية للأمن السيببراني

المطلب الأول
اهم الاتفاقيات الدولية

الفرع الأول: اتفاقية بودابست لمكافحةالجرائم الإلكترونة

شهدت العاصمة المجرية بودابست في أواخر عام ألفين وواحد توقيع أول معاهدة دولية متخصصة تهدف إلى مكافحة جرائم الإنترنت حيث قام مجلس أوروبا بإبرام هذه الاتفاقية بتاريخ الثامن من تشرين الثاني من عام ألفين وواحد وتم فتح باب التوقيع والمصادقة عليها في الثالث والعشرين من الشهر ذاته وقد تضمنت الاتفاقية تحديد أهدافها بصورة واضحة إلى جانب وضع قائمة بالجرائم التي تلتزم الدول المصادقة عليها بتجريمها ضمن تشريعاتها الوطنية وتعد هذه الاتفاقية أول إطار دولي شامل في مجال مكافحة الجرائم الإلكترونية إذ شملت تجريم عدد من الأفعال من بينها الإرهاب الإلكتروني وتزوير بطاقات الائتمان واستغلال الأطفال عبر الإنترنت[1] كما هدفت إلى توحيد القوانين الحديثة بين الدول المختلفة وقد جاءت نتيجة لمشاورات موسعة شاركت فيها الحكومات وأجهزة الشرطة وقطاع تكنولوجيا المعلومات وتم إعداد نصوصها من قبل فريق من الخبراء التابعين لمجلس أوروبا بدعم من عدد من الدول من بينها الولايات المتحدة الأمريكية ، كما وتعد اتفاقية بودابست الاتفاقية متعددة الأطراف الوحيدة التي تعنى بمكافحة الجرائم المرتكزة على استخدام الحاسوب أو شبكة الإنترنت وقد شكلت منذ دخولها حيز النفاذ في الأول من تموز عام ألفين وأربعة إطارا مرجعيا أساسيا على مستوى دول مجلس أوروبا كما انضمت إليها لاحقا عدة دول من خارج المجلس شهدت الاتفاقية الدولية الخاصة بالفضاء الإلكتروني مشاركة

[1] سامي عبد الرحمن حمدان، اتفاقية بودابست لمكافحة جرائم الإنترنت: تحليل أهدافها وأثرها على التشريعات الوطنية .مجلة الدراسات القانونية الدولية، جامعة اليرموك، المجلد 14، العدد 2، 2022، ص 55–65.

واسعة من دول العالم[1]، حيث صادقت عليها كندا واليابان وجنوب إفريقيا والولايات المتحدة، بعد جهود بدأت منذ الثمانينيات وانتهت باعتمادها رسمياً في 23 نوفمبر 2001 في بودابست، بمشاركة ثلاثين دولة أوروبية وأربع دول أخرى في إعدادها[2] .

قسّمت اتفاقية بودابست الجرائم الإلكترونية إلى أربع مجموعات: الأولى تتعلق بالاعتداء على سرية وسلامة البيانات والأنظمة مثل الدخول غير المصرح به والتنصت والتلاعب بالمعلومات؛ الثانية تشمل الاحتيال والتزوير عبر الوسائل الرقمية؛ الثالثة تخص الجرائم المرتبطة بالمحتوى غير القانوني، خصوصاً المواد الإباحية للأطفال؛ والرابعة تعنى بالاعتداء على حقوق الملكية الفكرية والحقوق المجاورة في ظل انتشار المحتوى الرقمي[3] .

كما تضمنت الاتفاقية عددا من التوصيات الداعمة لهذا التصنيف من أبرزها التوصية رقم 15/ 87 لتي أكدت شددت الاتفاقية على تنظيم استخدام البيانات الشخصية في المجال الشرطي وحماية المعلومات المتبادلة إلكترونياً، معتبرة أي اعتراض غير مصرح به للبيانات جريمة إلكترونية. كما تناولت مسؤولية الأشخاص الطبيعيين والمعنويين وحددت العقوبات المناسبة حسب دور كل طرف في ارتكاب الجرائم المعلوماتية [4].

عرفت اتفاقية بودابست البيانات المعلوماتية على أنها كل تمثيل للحقائق أو البرامج القابلة للمعالجة ضمن الحواسيب، كما ركزت على تجريم الجرائم الإلكترونية مثل الاختراق والتزوير

---

[1]محمود سامي الحوراني، *اتفاقية بودابست لمكافحة الجرائم الإلكترونية: الإطار المرجعي والدور الدولي* .مجلة العلوم القانونية الدولية، جامعة مؤتة، المجلد 13، العدد 1، 2023، ص 42–51.

[2]دارا، نسيمة 2017. الأمن المعلوماتي وسبل مواجهةمخاطره في التعامل الإلكتروني: دراسة مقارنة. أطروحة دكتوراة جامعة أبي بكر بلقايد تلمسان – الجزائر، كلية الحقوق والعلوم السياسية، صفحة 274

[3]جبور، منى الأشقر، (2017) السيبرانية هاجس العصر، دراسات وأبحاث المركز العربي للبحوث القانونيةوالقضائية، جامعة الدول العربية، بيروت، صفحة105.

[4]خلايفيةهدى، الاطار القانوني الدولي والداخلي لحماية الخصوصية على الانترنت التشريع الجزائري نموذجا، ب حث مشارك ومنشور في كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، صفحة6.

والمحتوى غير القانوني. ومع أهميتها، فإن الاتفاقية لا تشمل جميع جوانب الأمن السيبراني، مثل حماية البنى التحتية الحيوية، الدفاع ضد الهجمات السيبرانية، الخصوصية الرقمية، التدابير الوقائية، التدريب، والحوكمة الرقمية، ما يبرز الحاجة لتطوير أطر دولية أكثر شمولاً لمواجهة التحديات الرقمية.

الفرع الثاني: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010

اعتمد مجلس وزراء العدل ووزراء الداخلية العرب الموافق الثالث والعشرين من كانون الأول لعام ألفين وعشرة بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وقد جاءت هذه الاتفاقية استجابة للتحديات المتزايدة التي فرضتها الجرائم المرتبطة باستخدام تقنيات المعلومات والاتصالات في الدول العربية وهدفت إلى إنشاء إطار قانوني عربي مشترك يعالج هذا النوع من الجرائم بما ينسجم مع الخصوصيات القانونية والتشريعية للدول الأعضاء ويعزز في الوقت ذاته أوجه التعاون والتنسيق فيما بينها [1].

وتتألف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من ثلاث وأربعين مادة ألزمت الدول الموقعة باتخاذ التدابير التشريعية والتنظيمية اللازمة لتجريم مجموعة واسعة من تغطي الاتفاقية الأفعال المرتبطة باستخدام تكنولوجيا المعلومات، مثل الاختراق غير المشروع، التجسس، الإضرار بالبيانات، انتهاك الخصوصية، التعدي على الملكية الفكرية، والاحتيال الإلكتروني. كما تشمل الجرائم المتعلقة بالإرهاب، غسل الأموال، الاتجار بالبشر والمخدرات والأسلحة، والجرائم التي تمس القيم الدينية أو النظام العام مثل التهديد والابتزاز. وتعتبر الاتفاقية مبادرة عربية أساسية لتعزيز

[1] الغياثين ، محمد عمر، الجرائم المعلوماتيةعابرة الحدود ددراسة مقارنة– ، رسالة قُدِّمَت لنيل درجةالدكتوراه في الحقوق جامعة القاهرة ، عام 2013 م،صفحة65

التعاون الإقليمي والدولي في التحقيق والملاحقة القضائية وتوحيد المفاهيم القانونية، مما يسهل عمل جهات إنفاذ القانون ويقوي العدالة الرقمية [1].

تناولت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عدداً من الجرائم الإلكترونية، منها الاختراق غير المصرح به للأنظمة والشبكات، التنصت أو الاطلاع غير القانوني على البيانات، الإضرار بالبيانات عبر تعديلها أو حذفها، استخدام التقنيات لأغراض مخالفة للقانون، التزوير والاحتيال الإلكتروني، بالإضافة إلى الجرائم المتعلقة بالمحتوى غير الأخلاقي والاعتداء على حقوق النشر والملكية الفكرية [2].

كما نصت المادة الثالثة من الاتفاقية على مجالات تطبيقها حيث شملت مكافحة الجرائم الإلكترونية بكافة صورها والتي ترتكب باستخدام تقنيات المعلومات والاتصالات مثل الاختراق والتجسس الرقمي والدخول غير المصرح به إلى الأنظمة وركزت كذلك على حماية البيانات والمعلومات من أي اعتداء أو استخدام غير مشروع كما تناولت مكافحة جرائم التزوير والاحتيال الإلكتروني والجرائم المالية المرتكبة عبر الإنترنت إلى جانب حماية الحقوق الفكرية والأدبية من خلال مواجهة ظاهرة القرصنة الإلكترونية واستخدام المصنفات المحمية دون ترخيص ولم تغفل الاتفاقية الجرائم ذات الطابع الأخلاقي والقانوني مثل الجرائم الإباحية واستغلال الأطفال عبر الإنترنت والجرائم المرتبطة بالإرهاب وغسل الأموال كما أكدت على تعزيز التعاون القضائي والقانوني بين الدول العربية من خلال وضع إطار مشترك للتحقيق والملاحقة القضائية[3] .

---

[1] شرف الدين ، وردة ،مجلةالباحث للدراسات الأكاديمية مجلة الباحث للدراسات الأكاديمية 2021 م المجلد 8 العدد 2، صفحة 638.

[2] جامعةالدول العربية، اتفاقيةمكافحة جرائم تقنية المعلومات، 23 -12- 2010.

[3] انظر المادة 3 من الاتفاقيةالعربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربيةعام 2010.

جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كخطوة إقليمية لتوحيد الجهود في مواجهة الجرائم التكنولوجية عبر إطار تشريعي مشترك، يواكب التطورات التقنية [1] .

الفرع الثالث : اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية عام 2003.

مع تصاعد التهديدات السيبرانية العابرة للحدود، أدركت الدول ضرورة التعاون الدولي عبر الأمم المتحدة، التي تشكل الإطار الأوسع لصياغة المعايير العالمية للأمن الرقمي. وتهدف جهودها إلى مكافحة الجرائم الإلكترونية وتعزيز التعاون الفني وبناء القدرات، خاصة في الدول النامية، من خلال مؤسسات مثل مكتب الأمم المتحدة المعني بالمخدرات والجريمة ومبادرات الجمعية العامة التي تشمل فرق عمل للأمن السيبراني ومفاوضات حول اتفاقية دولية شاملة لمكافحة إساءة استخدام تكنولوجيا المعلومات.

سعى اتفاقية الأمم المتحدة لمكافحة الجرائم الإلكترونية، وفق ما أورد مكتب الأمم المتحدة المعني بالمخدرات والجريمة، إلى تأسيس فهم دولي موحد لمفاهيم جرائم الأمن السيبراني، بما يشمل الموضوع والمضمون والإجراءات، مع تعزيز التعاون بين الدول وتشجيع الدول على تجريم الأفعال المرتبطة باستخدام تكنولوجيا المعلومات بطريقة حيادية تقنيا بما يضمن شمولها للتقنيات الحالية والمستقبلية وتعزيز التعاون الدولي للقضاء على المناطق التي قد تشكل ملاذا آمنا للمجرمين السيبرانيين [2] تشمل أهداف مكافحة الجرائم الإلكترونية إنشاء آليات وطنية ودولية لتبادل الأدلة

---

[1] مشروع اعلان منتدى التعاون العربي الصيني
https://www.courts.gov.ps/userfiles/file/%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9%20%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%20%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf

[2] United Nations. .2021.11 17. Compilation of views submitted bby Member States on the scope objectives and structure (elements) of a comprehensive international convention on countering the

الرقمية مع احترام حقوق الإنسان، ودعم بناء القدرات التقنية والمؤسسية وتقديم المساعدة للدول المحتاجة. وقد أوصى المجلس الاقتصادي والاجتماعي للأمم المتحدة منذ 1950 بتعزيز دور المنظمة في وضع السياسات العالمية لمكافحة الجريمة، ما أدى إلى تأسيس لجنة خبراء لتقديم المشورة ووضع استراتيجيات وبرامج لتحسين التعامل الدولي مع الجناة والحد من الجريمة [1].

مع تصاعد التهديدات الرقمية، وسعت اللجنة مهامها لتشمل مكافحة الجرائم الإلكترونية، وعملت على تعزيز التعاون الدولي وتبادل الخبرات، فضلاً عن دعم تطوير القوانين والتشريعات لتمكين الدول من مواجهة الجرائم الرقمية بفعالية.

وترى الباحثة أن اتفاقية الأمم المتحدة لمكافحة الجرائم الإلكترونية تشكل هذه المبادرة خطوة أساسية لتنسيق الجهود الدولية لمواجهة التهديدات المتصاعدة التي يفرضها الفضاء الرقمي إلا أنها لا تزال تواجه عددا من التحديات العملية من أبرزها تفاوت القدرات التشريعية والتنفيذية بين الدول الأعضاء واختلاف الرؤى بشأن نطاق التجريم وحدود السيادة الرقمية وهو ما ينعكس على مستوى فعاليتها في التطبيق العملي .

use of information and communications technologies for criminal purposes [PDF]. Retrieved from https://documents.un.org/doc/undoc/gen/v21/084/20/pdf/v2108420.pdf

[1] سليمان ، قطاف . مواجهة الجرائم السيبرانيةفي ضوء الاتفاقيات ا لدولية ، جامعة عمار ثليجي الأغواط الجزائر ، صفحة73 .

المطلب الثاني
المبادئ والالتزامات الدولية للأمن السيبراني

مع ازدياد التحديات الناتجة عن التطور التقني واعتماد الفضاء الرقمي في مختلف المجالات، ظهرت الحاجة لإطار دولي يحدد المبادئ والالتزامات المشتركة للدول لضمان الفضاء السيبراني وحمايته من التهديدات والهجمات الإلكترونية المتنوعة ذلك أن الطبيعة العابرة للحدود للفضاء الرقمي تجعل أمنه مرتبطا بتعاون دولي فعال وبقواعد مشتركة تضبط سلوك الدول والجهات الفاعلة وتضمن احترام الحقوق والحريات في الوقت ذاته ومن هنا يتناول هذا المطلب أهم المبادئ الأساسية التي تستند إليها الاتفاقيات الدولية المتعلقة بمجال الأمن السيبراني وما تفرضه من التزامات على الدول الأعضاء سواء من حيث سن التشريعات الوطنية أو تطوير القدرات المؤسسية أو تفعيل التعاون القضائي والأمني أو ضمان حماية الخصوصية والحقوق الأساسية أثناء مكافحة الجرائم الإلكترونية .

الفرع الأول : مبدأ احترام السيادة الرقمية .

مثلت معاهدة وستفاليا عام 1648 نقطة تحول في القانون الدولي، حيث أكدت مبدأ السيادة الوطنية كأساس للعلاقات بين الدول، مبنية على احترام الحدود ومنع التدخل في الشؤون الداخلية، والاعتراف بحق كل دولة في اتخاذ قراراتها بحرية ضمن نطاقها الإقليمي [1] ومنذ ذلك التاريخ أصبح مفهوم السيادة أحد الركائز الجوهرية للقانون الدولي وأداة لضمان الاستقرار وتنظيم التعاون والنزاعات بين الدول على نحو يحقق التوازن ويمنع فرض الإرادة الخارجية ، حيث ويمكن التمييز بين السيادة الداخلية والسيادة الخارجية فالسيادة الداخلية تعبر السلطة الداخلية للدولة تشمل تطبيق

[1] الديب، نانسي حامد .السيادة الرقمية للدول في مواجهةلتهديدات السيبرانية غير الحكوميةنحو بناء اطار قانوني دولي مرن ومتكامل ،المعهد العالي للتجارة والعلوم الادارية بالمنصورة . ص76

القانون وحماية النظام العام وتنظيم شؤون المجتمع دون تدخل خارجي، بينما تعني السيادة الخارجية استقلال الدولة في علاقاتها الدولية وحقها في اتخاذ القرارات بحرية ورفض أي تدخل أجنبي، ما يجعل احترام السيادة قاعدة أساسية تضمن لكل دولة التحكم بإقليمها وتطبيق قوانينها[1]

ومع تطور البيئة الرقمية وانتقال كثير من مظاهر القوة والمصلحة إلى المجال السيبراني ظهر مفهوم السيادة الرقمية بوصفه امتدادا حديثا للسيادة التقليدية ويقصد بالسيادة الرقمية قدرة الدولة على ممارسة السيطرة على منظوماتها الرقمية وما يرتبط بها من بنى تحتية للاتصالات وأنظمة تقنية وبيانات وطنية وتدفقات معلوماتية بما يتفق مع قوانينها المحلية وضوابطها التنظيمية وأولوياتها الأمنية ولا يقتصر هذا المفهوم على الحدود الجغرافية التقليدية بل يمتد إلى المجال الرقمي الذي أصبح جزءا من مفهوم الأمن الوطني المعاصر نظرا لاعتماد الدول على الشبكات والأنظمة في تشغيل الخدمات الحيوية وإدارة المعلومات الحكومية والخاصة [2].

وتبرز أهمية مبدأ احترام السيادة الرقمية في كونه يرسخ حق الدولة في تنظيم فضائها الرقمي وحماية بيانات مواطنيها وبنيتها التحتية من الاختراق أو السيطرة الخارجية ويمنع التدخل غير المشروع سواء من دول أخرى أو من جهات خاصة عابرة للحدود ويعني ذلك أن أي نشاط سيبراني يستهدف بنية دولة أخرى أو بياناتها أو أنظمتها بصورة غير مشروعة قد يشكل انتهاكا لمبدأ السيادة الرقمية ويؤسس لمسؤولية دولية إذا توافرت شروط الإسناد والمعيار القانوني والضرر ، كما يرتبط هذا المبدأ بحماية الخصوصية وحماية البيانات الشخصية وتقوية هيكل الأمن السيبراني وتأكيد استقلال الاستراتيجية الوطنية للأمن الرقمي

---

[1] بريم ، فاطمة ، السيادةلوطنية السيبرانية في ظل الفضاء السيبراني والتحولات الرقميةمجلة الدراسات القانونية والسياسية ، جامعة قسنطنية ، 2020، صفحة 19 .

[2] السيادة الرقمية . التحديات والفرص في عصر البيانات والتقنيات الحديثة . الجهود : مدونة. ص39

إذ يسمح للدول من وضع قوانين تنظم عمل المنصات الرقمية والتقنيات الحديثة داخل الدولة بما ينسجم مع مصالحها وقيمها ونظامها العام وفي المقابل يفرض المبدأ على الدولة التزاما إيجابيا يتمثل في بناء قدرات حماية فضائها الرقمي ووضع معايير وطنية للأمن السيبراني وتنظيم العلاقة مع مزودي الخدمات والتقنيات بما يضمن عدم تعريض السيادة الرقمية للخطر .

وترى الباحثة أن مبدأ احترام السيادة الرقمية يمثل حجر أساس في بناء أمن سيبراني دولي متوازن لأنه يمنح الدول حق الحماية والتنظيم لكنه في الوقت ذاته يتطلب ضبط هذا الحق بعدم استخدامه ذريعة لتقييد الحقوق والحريات دون ضرورة أو تناسب كما يتطلب تفعيل قواعد المسؤولية والتعاون الدولي لضمان عدم تحول المجال الرقمي إلى ساحة صراع غير منضبط يهدد الاستقرار الدولي

الفرع الثاني: مبدأ التعاون الدولي

التعاون الدولي يعني تنسيق ومزامنة الإجراءات بين دولتين أو أكثر لتحقيق أهداف مشتركة، سواء في المجال الأمني أو القانوني أو التقني لتحقيق مصالح مشتركة وتقديم الدعم والمساندة المتبادلة ويبرز هذا التعاون بصورة خاصة في مواجهة الجرائم العابرة للحدود وفي مقدمتها الجرائم الإلكترونية نظرا لكونها قد ترتكب في دولة ويقع أثرها في دولة أخرى [1]وقد تكون الأدلة مخزنة في دولة ثالثة ويقيم الفاعل في دولة رابعة وهو ما يجعل إنفاذ القانون داخل الحدود الوطنية وحده غير كاف لتحقيق العدالة أو الردع[2]

[1] عمايرة ، محمد منذر طه ، التعاون الدولي في مواجهةالجريمة السيبرانية ، رسالة ماجستير ، جامعة القدس. ص99

[2]سامي فواز العبدلي، التعاون الدولي في مواجهة الجرائم السيبرانية: التنسيق القانوني والتقني بين الدول .مجلة العلوم القانونية الدولية، جامعة اليرموك، المجلد 15، العدد 1، 2023، ص 77–85.

ويكتسب مبدأ التعاون الدولي في مجال الأمن السيبراني أهمية عملية لأنه يترجم إلى آليات قانونية وإجرائية مثل تبادل المعلومات وتبادل الأدلة الرقمية والمساعدة القانونية المتبادلة والتحقيقات المشتركة وتسليم المجرمين وتجميد العائدات غير المشروعة وتعقب مصادر الهجمات ويكون ذلك عبر اتفاقيات دولية متعددة الأطراف أو ثنائية أو عبر قنوات الاتصال الرسمية بين السلطات المختصة ، وتتشابه الجريمة الإلكترونية مع الجريمة التقليدية من حيث المرور بمراحل إجرائية أساسية لا يمكن تجاوزها وتبدأ بمرحلة التحري وجمع الاستدلالات التي تتولاها جهات الضبط القضائي ثم مرحلة التحقيق الابتدائي التي تشرف عليها النيابة العامة ثم مرحلة المحاكمة أمام القضاء المختص غير أن خصوصية الجريمة الإلكترونية تفرض متطلبات إضافية تتعلق بطبيعة الأدلة الرقمية وسرعة زوالها وتشتتها وتشفيرها إضافة إلى الحاجة لخبرات فنية متقدمة لضمان سلامة جمعها وحفظها وتحليلها بصورة مقبولة قضائيا [1].

كما أن التعاون الدولي لا يقتصر على الجانب القضائي بل يمتد إلى بناء قدرات وطنية مشتركة وتبادل الخبرات الفنية وإنشاء نقاط اتصال دائمة وتطوير آليات استجابة مشتركة للحوادث السيبرانية وتعزيز الشراكات مع الجهات الدولية المتخصصة بما يضمن سرعة التعامل مع الهجمات وتقليل آثارها[2] .

وترى الباحثة أن مبدأ التعاون الدولي يمثل الركيزة الأكثر واقعية في مكافحة الجرائم الإلكترونية لأنه يترجم المبادئ القانونية إلى أدوات تنفيذية تمكّن الدول من الوصول إلى الأدلة وتعقب الفاعلين ومنع إفلاتهم من العقاب كما يحقق الردع ويعزز الثقة في البيئة الرقمية غير أن فعالية هذا المبدأ

---

[1] سرور، احمد فتحي. الوسيط في قانون العقوبات ،القسم العام ،الجزء الأول ، دار النهضةالعربية ،القاهرة عام1981،صفحة 143.

[2] كريم مصطفى العلي، التعاون الدولي في الأمن السيبراني: بناء القدرات وتبادل الخبرات لمواجهة التهديدات العابرة للحدود .مجلة الدراسات القانونية والأمنية، جامعة مؤتة، المجلد 12، العدد 2، 2022، ص 101–110.

تظل مرتبطة بمدى مواءمة التشريعات الوطنية مع الاتفاقيات وبمدى توافر الإرادة السياسية والقدرات الفنية واستعداد الدول لتبادل المعلومات دون الإضرار بسيادتها أو بحقوق الأفراد .

الفرع الثالث: الالتزامات القانونية للدول في مكافحة الجرائم الإلكترونية

تتمثل الالتزامات القانونية للدول في مكافحة الجرائم الإلكترونية في مجموعة واجبات ومسؤوليات تستمد أساسها من التشريعات الوطنية والاتفاقيات الدولية وتهدف إلى حماية المجتمع الرقمي وضمان أمن الفضاء السيبراني وتشمل هذه الالتزامات جانبا تشريعيا يتمثل في تجريم الأفعال الإلكترونية غير المشروعة وتحديد العقوبات الملائمة وجانبا مؤسسيا يتمثل في إنشاء جهات مختصة وتطوير قدراتها وجانبا إجرائيا يتعلق بآليات التحقيق وجمع الأدلة وتبادلها وجانبا حقوقيا يتمثل في احترام حقوق الإنسان والخصوصية أثناء مكافحة الجريمة [1].

أولا: التزام سن التشريعات الوطنية وتحديثها

تلتزم الدول بسن قوانين واضحة تحدد الجرائم الإلكترونية وصورها مثل الدخول غير المشروع والتنصت واعتراض البيانات والتزوير والاحتيال الإلكتروني والابتزاز وانتهاك الخصوصية والاعتداء على سلامة البيانات والأنظمة [2]كما تلتزم بتحديث هذه القوانين بصورة دورية لمواكبة التطورات التقنية وتلافي الفجوات التشريعية وبما يضمن الدقة في التعريفات وعدم التوسع غير المبرر في التجريم الذي قد يمس الحقوق والحريات .

---

[1]فهد عبد الرحمن الشوابكة، الالتزامات القانونية للدول في مكافحة الجرائم الإلكترونية: الجوانب التشريعية والمؤسسية والإجرائية .مجلة العلوم القانونية، جامعة اليرموك، المجلد 17، العدد 1، 2024، ص 33–45.

[2]علي محمد القضاة، تجريم الجرائم الإلكترونية في التشريعات الوطنية: دراسة مقارنة .مجلة الحقوق الرقمية، جامعة اليرموك، المجلد 10، العدد 2، 2023، ص 55–68.

ثانيا: التزام تطوير آليات التحقيق والملاحقة وتخصص الجهات المختصة

يتطلب التصدي للجرائم الإلكترونية تجهيز الأجهزة الأمنية والقضائية بالأدوات والخبرات التقنية اللازمة للتحقيق في الجرائم الرقمية ويتضمن ذلك بناء وحدات متخصصة للجرائم الإلكترونية وتطوير قدرات التحليل الجنائي الرقمي ووضع إجراءات لحفظ الأدلة الرقمية وسلسلة الحيازة وضمان قبولها أمام القضاء[1] إضافة إلى تدريب القضاة وأعضاء النيابة ومأموري الضبط القضائي على الخصوصيات القانونية والفنية لهذا النوع من القضايا .

ثالثا: التزام التعاون الدولي وتبادل المعلومات والمساعدة القانونية المتبادلة

تلتزم الدول بتعزيز التعاون الدولي من خلال تبادل المعلومات وتقديم المساعدة القانونية المتبادلة وتسليم المجرمين وفق الشروط القانونية والتنسيق في التحقيقات المشتركة والإنابات القضائية وطلبات حفظ البيانات ورفع السرية ضمن ضوابط القانون ويعد هذا الالتزام جوهريا لأن الجريمة الإلكترونية غالبا ما تتجاوز الحدود الوطنية وتحتاج إلى قنوات قانونية سريعة لضمان عدم ضياع الأدلة .

رابعا: التزام التدريب والتوعية وبناء القدرات المجتمعية

تلتزم الدول بتدريب الكوادر الأمنية والقضائية والفنية وبنشر الوعي لدى الأفراد والمؤسسات حول مخاطر الجرائم الإلكترونية وطرق الوقاية منها وتشجيع الإبلاغ عن الحوادث وتعزيز الثقافة

[1] حسن علي الطراونة، التحقيق الجنائي الرقمي: أساليب وممارسات وحدات الجرائم الإلكترونية .مجلة العلوم الجنائية، جامعة مؤتة، المجلد 14، العدد 1، 2022، ص 42–53.

الرقمية الآمنة لأن ضعف الوعي يمثل مدخلا أساسيا للاستهداف السيبراني كما أن بناء القدرات المجتمعية يقلل من حجم الجرائم ويزيد من فعالية الاستجابة [1].

خامسا: التزام احترام حقوق الإنسان وحماية الخصوصية أثناء المكافحة

لا يجوز أن تتحول مكافحة الجرائم الإلكترونية إلى مبرر لانتهاك الحقوق الأساسية لذلك تلتزم الدول بضمان المشروعية والضرورة والتناسب في إجراءات المراقبة والتفتيش والضبط والحجب وحفظ البيانات كما تلتزم بحماية الخصوصية وسرية الاتصالات وحق الدفاع وضمانات المحاكمة العادلة ووجود رقابة قضائية فعالة على الإجراءات المقيدة للحقوق .

وترى الباحثة أن الالتزامات الدولية في مكافحة الجرائم الإلكترونية تتجه نحو بناء نموذج مزدوج يقوم على الردع والحماية من جهة وعلى احترام الحقوق والحريات من جهة أخرى وأن نجاح الدول في تنفيذ هذه الالتزامات يرتبط بمدى توازن تشريعاتها بين متطلبات الأمن السيبراني ومتطلبات دولة القانون كما يرتبط بقدرتها على تطوير أدوات التحقيق الرقمي والتعاون الدولي الفعال وتحديث القوانين بما يلاحق التطور التقني دون إفراط أو قصور.

[1] ناصر محمود العبدالله، بناء القدرات والتوعية في مواجهة الجرائم الإلكترونية: دور التدريب والمجتمع .المجلة الأردنية للعلوم القانونية، المجلد 7، العدد 1، 2022، ص 77–88.

المطلب الثالث

آليات تنفيذ المعاهدات والتحديات التي تواجه تطبيقها

آليات تنفيذ المعاهدات تعني الإجراءات والخطوات العملية والقانونيةالتي تقوم بها الدول بعد توقيع المعاهدة أو الانضمام إليها بهدف تحويل أحكامها من مجرد نصوص مكتوبة إلى قواعد واجبة التطبيق على أرض الواقع سواء داخل الدولة من خلال تعديل قوانينها وبناء مؤسساتها وتطوير أدواتها أو خارجها من خلال تفعيل التعاون مع الدول الأخرى في مجال تبادل المعلومات والمساعدة القانونية وتسليم المطلوبين والتحقيقات المشتركة[1]

وقد شهدت شبكة المعلومات تطورًا متسارعًا رافقه تنوع كبير في استخداماتها ضمن مختلف القطاعات مثل الاقتصاد والثقافة والأمن والسياحة مما جعلها أداة فعالة تسهل تنفيذ الأنشطة الإجرامية عبر الإنترنت وقد ترتب على ذلك المساس بأمن المعلومات وتهديد خصوصيتها من خلال أعمال القرصنة والسرقة والتجسس والتخريب الأمر الذي أدى إلى تعقيد جهود المكافحة وزاد من التحديات التي تواجه الدول على الصعيدين الوطني والدولي في التصدي للجرائم الإلكترونية لذلك أصبح تنفيذ المعاهدات والاتفاقيات الدولية في هذا المجال مسألة حيوية تستلزم منظومة تنفيذية متكاملة وآليات تعاون سريعة وفعالة[2] .

الفرع الأول: الآليات التنفيذية المتبعة في تطبيق الاتفاقيات

تعد الآليات التنفيذية جزءًا أساسيا من تطبيق الاتفاقيات الخاصة بالأمن السيبراني لأنها تمثل الجسر العملي بين النصوص القانونية الدولية وبين الواقع التنفيذي على المستوى الوطني والدولي

---

[1] سامي فواز العبدلي، آليات تنفيذ المعاهدات الدولية لمكافحة الجرائم الإلكترونية: دراسة تحليلية .مجلة العلوم القانونية، جامعة العلوم والتكنولوجيا الأردنية، المجلد 9، العدد 2، 2021، ص 33–47.

[2] **علاء مهدي شناعة** .تنفيذ الاتفاقيات الدولية في التشريع الوطني: دراسة قانونية مقارنة .مجلة الحقوق والسياسات العامة، جامعة الزيتونة الأردنية، المجلد 14، العدد 3، 2023، ص 121–138.

فالاتفاقيات لا تحقق غاياتها بمجرد التصديق عليها بل تتطلب أن تتبناها الدولة داخل نظامها القانوني وأن تنشئ مؤسسات قادرة على تنفيذها وأن تفعّل قنوات التعاون مع الدول الأخرى بما يسمح بمواجهة الجرائم السيبرانية المعقدة وضمان استجابة منسقة وسريعة للهجمات والتهديدات الرقمية[1] ، وتتنوع الآليات التنفيذية المتبعة في تطبيق الاتفاقيات الخاصة بالأمن السيبراني على النحو الآتي :

أولا: تعديل التشريعات الوطنية

تقوم الدول بإصدار قوانين جديدة أو تعديل القوانين القائمة لتتوافق مع أحكام الاتفاقيات الدولية وبما يضمن تجريم الأفعال التي نصت عليها الاتفاقيات وتحديد العقوبات المناسبة ووضع قواعد إجرائية خاصة بالأدلة الرقمية والتحقيقات العابرة للحدود وبذلك يصبح الالتزام الدولي قابلا للتطبيق أمام السلطات الوطنية والقضاء[2].

ثانيا: إنشاء وحدات وطنية متخصصة ونقاط اتصال

تعمل الدول على إنشاء وحدات أو إدارات متخصصة بالجرائم الإلكترونية داخل أجهزة إنفاذ القانون والنيابة العامة وقد تتضمن أيضا نقاط اتصال وطنية تكون حلقة وصل بين الدول لتسهيل الاستجابة العاجلة وتبادل المعلومات والطلبات الفنية والقانونية المتعلقة بحفظ البيانات وتتبع الأدلة الرقمية وتنسيق الإجراءات[3] .

---

[1]أيمن خالد العبدالله، الآليات التنفيذية للاتفاقيات الدولية في مجال الأمن السيبراني: دراسة تحليلية .المجلة الأردنية للقانون والعلوم الرقمية، المجلد 5، العدد 2، 2022، ص 45–60.

[2]سامي عبد الحليم، تطبيق الاتفاقيات الدولية في التشريعات الوطنية لمكافحة الجرائم السيبرانية .مجلة الدراسات القانونية، جامعة الزيتونة الأردنية، المجلد 12، العدد 1، 2021، ص 77–92.

[3]سامي عبد الحليم، تطبيق الاتفاقيات الدولية في التشريعات الوطنية لمكافحة الجرائم السيبرانية .مجلة الدراسات القانونية، جامعة الزيتونة الأردنية، المجلد 12، العدد 1، 2021، ص 107.

ثالثا: تفعيل المساعدة القانونية المتبادلة

تشمل المساعدة القانونية المتبادلة تبادل الأدلة الرقمية وتنفيذ أوامر الضبط والتفتيش والاستماع إلى الشهود أو الخبراء عبر الحدود وتقديم المعلومات المتعلقة بالمشتبه بهم أو الخوادم أو سجلات الاستخدام وتمثل هذه الآلية أحد أهم أدوات تنفيذ الاتفاقيات لأنها تتيح للدولة الوصول إلى أدلة موجودة خارج إقليمها ضمن إطار قانوني يضمن المشروعية[1] .

رابعا: تفعيل تسليم المجرمين

من خلال توفير آليات قانونية لتسليم المتهمين أو المحكومين في الجرائم الإلكترونية بين الدول وفقا للاتفاقيات الثنائية أو متعددة الأطراف وبما يحقق عدم إفلات الجناة من العقاب ويشترط في الغالب تحقق ازدواج التجريم وتوافر شروط التسليم المعمول بها في قوانين الدول [2].

خامسا: تشكيل فرق التحقيق المشتركة

تلجأ الدول في القضايا السيبرانية المعقدة إلى تشكيل فرق مشتركة للتعاون الميداني وتبادل المعلومات بصورة مباشرة ومستمرة وجمع الأدلة وتتبع الأموال الرقمية وتحديد مسارات الهجوم بما يختصر الوقت ويزيد من فعالية التحقيق .

---

[1] محمد مصطفى عبد اللطيف، التعاون الدولي في مكافحة الجرائم الإلكترونية: أطر وآليات ,دار النهضة العربية، القاهرة، 2021، ص 112–130.

[2] أحمد عبد العزيز فؤاد، *التسليم الدولي للمجرمين في الجرائم الإلكترونية: دراسة مقارنة* ,دار الفكر القانوني، بيروت، 2020، ص 45–60.

سادسا: حفظ الأدلة الرقمية بصورة عاجلة .

تتبنى الدول إجراءات سريعة لحفظ البيانات ومنع محوها أو العبث بها مثل أوامر الحفظ العاجل وطلبات تجميد البيانات أو سجلات الاتصال لأن طبيعة الدليل الرقمي قابلة للزوال بسرعة وقد يؤدي التأخير إلى ضياع الدليل وفشل الملاحقة .

سابعا: منصات تبادل المعلومات التقنية

تسعى الدول إلى إنشاء شبكات اتصال وقواعد بيانات وبنوك معلومات لتبادل مؤشرات التهديد ومعلومات البرمجيات الخبيثة وأساليب الهجمات وأنماط الجرائم المكتشفة بما يعزز الوقاية والاستجابة السريعة للحوادث[1].

ثامنا: آليات المراقبة والتقارير الدورية

تتبنى بعض الاتفاقيات أو المنظمات آليات متابعة تشمل تقارير دورية وتقييم مدى الامتثال وتحديد المعوقات واقتراح خطط تطوير وقد تكون هذه المتابعة على شكل لجان أو اجتماعات أو مراجعات دورية تساعد على رفع مستوى التطبيق ومعالجة الخلل .

تاسعا: ضمانات حقوق الإنسان والخصوصية

تشمل الآليات التنفيذية التزام الدول بأن تكون إجراءات التعاون والتحقيق متوافقة مع الضمانات الأساسية مثل المشروعية والتناسب والرقابة القضائية وحماية البيانات الشخصية وحقوق الدفاع لأن أي تجاوز لهذه الضمانات قد يقوض الثقة الدولية ويعرقل تنفيذ الاتفاقيات[2] .

---

[1] محمد مصطفى عبد اللطيف، منصات تبادل المعلومات التقنية وأمن الفضاء السيبراني: دراسة تحليلية ,دار النهضة العربية، القاهرة، 2021، ص 95–110.

[2] United Nations Office on Drugs and Crime . 2020). Handbook onCybercrime and Electronic Evidence. UnitedNations. https://www.unodc.org/documents/organized-crime/cybercrime/Handbook_on_Cybercrime_and_Electronic_Evidence.pdf

وترى الباحثة أن تطبيق الاتفاقيات الخاصة بالأمن السيبراني يرتبط ارتباطا مباشرا بفاعلية هذه الآليات التنفيذية فكلما كانت الدولة قادرة على مواءمة تشريعاتها وبناء مؤسسات متخصصة وتطوير أدوات فنية وتفعيل التعاون الدولي كلما ارتفعت فعالية الاتفاقيات على أرض الواقع ومع ذلك يظهر في التطبيق قصور واضح في بعض الآليات سواء بسبب تفاوت القدرات التقنية بين الدول أو ضعف التنسيق أو بطء الإجراءات مما يحد من الأثر العملي للاتفاقيات ويجعل الحاجة قائمة لتعزيز التنفيذ وتطوير آليات التعاون بصورة أكثر سرعة ومرونة .

الفرع الثاني : المصاعب التي تواجه الجهود الدولية في التصدي للجريمة الإلكترونية .

تواجه الجهود الدولية في مكافحة الجريمة الإلكترونية العديد من المصاعب التي تحد من فعالية تنفيذ المعاهدات والاتفاقيات وتجعل التعاون بين الدول أبطأ وأقل كفاءة ومن أبرز هذه المصاعب اختلاف التشريعات والقوانين الوطنية حيث تختلف تعريفات الجرائم الإلكترونية ونطاق التجريم والعقوبات من دولة إلى أخرى وهو ما ينعكس على صعوبة توحيد الاستجابة القانونية ، ويترتب على هذا الاختلاف إشكاليات عملية مثل تعثر تطبيق مبدأ ازدواج التجريم الذي يعد شرطا أساسيا في كثير من صور التعاون الدولي مثل تسليم المجرمين أو المساعدة القانونية المتبادلة فإذا كانت الدولة الطالبة تعتبر فعل الدخول غير المشروع جريمة قائمة بذاتها بينما لا تعترف به دولة أخرى كجريمة إلا إذا تحقق ضرر مادي أو ارتبط بجريمة أخرى فإن طلبات التسليم أو التعاون قد ترفض أو تتأخر وهو ما يخلق ثغرات يستفيد منها الجناة[1] .

ومن الصعوبات كذلك غياب الاتفاقيات الثنائية أو متعددة الأطراف بين عدد كبير من الدول وهو ما يعطل إمكانات التعاون المنظم ويجعل التعاون مرهونا بالمعاملة بالمثل أو بالإجراءات

[1] هالة سامي عبد الحميد، التحديات الدولية في مكافحة الجرائم الإلكترونية: دراسة تحليلية ,مكتبة النهضة المصرية، القاهرة، 2019، ص 72–88.

الدبلوماسية البطيئة وحتى عند وجود اتفاقيات فقد تكون محدودة الأثر أو غير قادرة على مواكبة التطور السريع في تقنيات الإنترنت وأدوات الإجرام السيبراني الأمر الذي يربك جهات إنفاذ القانون ويضعف الاستجابة الفورية [1]، ويضاف إلى ذلك أن الساحة الدولية لا تزال تعاني من نقص في الاتفاقيات التي تنظم التعاون في التحقيقات السيبرانية وتسهّل إجراءات تسليم الجناة الأمر الذي يجعل اتفاقيات محددة مثل اتفاقية بودابست من الاستثناءات البارزة بينما تبقى دول كثيرة خارج إطارها أو لا تعتمد معاييرها التنفيذية [2].

ومن أبرز التحديات كذلك غياب التنسيق الدولي الواضح بشأن الإجراءات الجنائية الفنية المتعلقة بجمع الأدلة الرقمية وحفظها وضمان سلسلة حيازتها إذ تزداد صعوبة تنفيذ إجراءات التفتيش أو الضبط داخل نظام معلوماتي أجنبي بسبب اعتبارات السيادة وتعارض القوانين الوطنية واختلاف القواعد المتعلقة بالخصوصية وحماية البيانات إضافة إلى أن الأدلة الرقمية قد تكون موزعة على خوادم متعددة أو مخزنة لدى مزودي خدمة يخضعون لقوانين مختلفة مما يجعل الوصول إليها معقدا[3] .

كما تواجه الجهود الدولية بطء الإجراءات لأن طلبات المساعدة القانونية المتبادلة تمر غالبا بمسارات قانونية رسمية تستغرق وقتا طويلا في حين أن الدليل الرقمي سريع الزوال وقد يؤدي التأخير إلى فقدانه وتضعف هذه المشكلة فعالية الاستجابة الدولية للحوادث السيبرانية خاصة عندما تكون هناك حاجة للتدخل العاجل أو الحفظ الفوري للبيانات ، ومن أجل مواجهة هذه المصاعب يصبح من الضروري اعتماد إجراءات متكاملة تشمل تحسين منظومة الحماية الرقمية باستخدام

---

[1] شرابسة ، لينا . (2009) ،السياسة الدولية والاقليمية في مجال مكافحة الجريمة الالكترونية . مجلة دراسات وأبحاث ، المجلد 01 ، ص250.

[2] إبراهيم ، خالد ممدوح . الجرائم المعلوماتيةدار الفكر الجامعي الاسكندرية، 2009عام . ص87 .

[3] سليمان ، قطاف ، مواجهة لجرائم السيبرانية في ضوء الاتفاقيات الدولية . جامعةعمار ثليجي الأغواط، الجزائر ، صفحة83 .

تقنيات أمنية متقدمة وتحديث الأنظمة بصورة دورية ورفع مستوى الوعي المجتمعي بأساليب الاحتيال والوقاية وتعزيز التعاون الدولي وتطوير الأطر القانونية وسن قوانين أكثر وضوحا وصرامة وتفعيلها بفعالية بما يضمن الردع وعدم الإفلات من العقاب[1] .

وترى الباحثة أن التحديات التي تواجه تنفيذ المعاهدات في مجال الأمن السيبراني لا تعود إلى نقص النصوص وحده بل ترتبط أساسا بآليات التطبيق وبالفجوة بين التطور التقني وسرعة الاستجابة التشريعية وبطء قنوات التعاون الدولي لذلك فإن تطوير آليات تنفيذ أسرع وتوحيد المفاهيم وتعزيز الاتفاقيات وتبادل الخبرات وبناء قدرات فنية وقضائية متخصصة يمثل شرطا لازما لتحقيق فعالية حقيقية للجهود الدولية في مواجهة الجرائم الإلكترونية .

[1] Prof. Doctor. MarcGercke, Understanding cybercrime: Phenomena,45.55ح

المطلب الرابع
مواءمة التشريعات الأردنية مع الاتفاقيات الدولية للأمن السيبراني

بعد أن سبق سرده من استعراض التشريعات الأردنية المتعلقة بالأمن السيبراني وتحليل مضمونها وبيان أهدافها ومجالات تطبيقها وبعد أن تناولنا أبرز الاتفاقيات الدولية والإقليمية ذات الصلة والمبادئ العامة التي تحكم العمل القانوني في الفضاء الإلكتروني بات من الممكن الانتقال إلى مرحلة المقارنة بين الجانب الوطني والجانب الدولي بهدف الوقوف على مدى التوافق أو الاختلاف بينهما ، ومن خلال هذا التحليل يتضح أن هناك نقاط التقاء تشريعية بين الإطار الأردني والمعايير القانونية الدولية في موضوع الأمن السيبراني إلى جانب وجود جوانب تحتاج إلى تطوير أو استكمال حتى تقترب من الالتزامات والممارسات المتعارف عليها عالميًا وعليه سيعمل هذا المطلب على توضيح مدى مواءمة التشريعات الأردنية مع الاتفاقيات والمعايير الدولية من خلال إبراز أوجه التوافق من جهة وبيان أوجه القصور والتحديات من جهة أخرى وذلك على النحو الآتي :

الفرع الأول: أوجه التوافق بين التشريعات الأردنية والمعايير الدولية للأمن السيبراني .

بعد استعراض التشريعات الأردنية الخاصة بالأمن السيبراني يتبين أن المشرع الأردني لم يكن بمعزل عن الإطار القانوني الدولي في هذا المجال إذ جاءت منظومة القوانين الوطنية في صورتها الحديثة لتعكس توجهًا واضحًا نحو تنظيم الفضاء الرقمي بما ينسجم مع الاتجاهات العالمية والتطورات التشريعية المتسارعة [1].

[1] النقبي، جمال محمد خلفان ، 2023 التعاون الوطني والدولي في الجرائم الإلكترونيةالمشكلات والحلول مجلة المعهد العالي للدراسات النوعية، المجلد 3، العدد 16. ص77

فعلى مستوى التجريم الإلكتروني يظهر أن قانون الجرائم الإلكترونية في نسخته الأخيرة تضمن نصوصًا تتقاطع مع ما استقرت عليه الاتفاقيات الدولية والإقليمية وعلى رأسها اتفاقية بودابست والاتفاقية[1] العربية لمكافحة جرائم تقنية المعلومات وذلك من خلال تجريم الدخول غير المصرح به إلى الأنظمة المعلوماتية والاعتداء على سلامة البيانات وتعطيل الأنظمة التقنية أو العبث بها فضلًا عن تجريم صور متعددة من الاحتيال الإلكتروني وانتحال الشخصية والابتزاز الإلكتروني واستعمال الشبكة لغايات غير مشروعة وهي ذات الأفعال التي أولتها الاتفاقيات الدولية اهتمامًا عند تصنيف الجرائم السيبرانية واعتبارها تهديدًا مباشرًا للأمن الرقمي للدول والمجتمعات ، كما يظهر التوافق بصورة واضحة في مجال حماية الخصوصية والبيانات الشخصية حيث إن قانون حماية البيانات الشخصية الأردني تبنى عددًا من المبادئ الجوهرية التي تقوم عليها التشريعات الدولية الحديثة وفي مقدمتها مبدأ الموافقة المسبقة لصاحب البيانات ومبدأ تحديد الغرض من المعالجة ومبدأ تمكين الشخص المعني من حقوق الوصول والتصحيح والتحديث وسحب الموافقة والاعتراض وضمان حماية البيانات من المعالجة غير القانونية أو الإفشاء غير المشروع وهو ما يعكس تقاطعًا مع المعايير العالمية التي ترتكز على صون الخصوصية الرقمية باعتبارها امتدادًا للحق في الحياة الخاصة .

أما على مستوى الأطر المؤسسية والتنظيمية فإن قانون الأمن السيبراني وإنشاء المركز الوطني للأمن السيبراني يمثلان خطوة تنسجم مع التوجه الدولي الذي يؤكد على ضرورة وجود جهة وطنية متخصصة تتولى وضع السياسات العامة وتنسيق الجهود وتعزيز الوقاية والحماية وبناء القدرات والاستجابة للحوادث السيبرانية إذ إن وجود مؤسسة وطنية مركزية يعد من متطلبات بناء منظومة

[1] الاشقر، منى جبور، جبور ، محمود، البيانات الشخصيةوالقوانين العربية: الهم الأمني وحقوق الفراد، مرجع سابق، ص.19

أمن سيبراني فعالة وفق النماذج التي تتبناها الدول في إطار التزامها بالمعايير الدولية المتصلة بحماية البنى التحتية الحيوية وإدارة المخاطر الرقمية [1]، ويضاف إلى ذلك أن ما يصدر عن هيئة تنظيم قطاع الاتصالات من تعليمات وضوابط فنية تتعلق بحماية الشبكات وبيانات المستخدمين وتعزيز متطلبات الأمن لدى مزودي الخدمة يعكس حضورًا للبعد التنظيمي الذي تؤكد عليه المعايير الدولية ولا سيما من حيث إشراك القطاع الخاص وتحميل الجهات المشغلة لمسؤوليات واضحة في حماية البنية التحتية الرقمية وتطبيق متطلبات السلامة والأمن المعلوماتي .

ومن خلال ما تقدم يتبين أن التشريعات الأردنية حققت درجة معتبرة من التوافق مع المعايير الدولية في مجال الأمن السيبراني سواء في نطاق التجريم أو في مجال حماية البيانات والخصوصية أو في تأسيس الأطر المؤسسية والتنظيمية وهو ما يدل على أن المنظومة القانونية الوطنية تسير في اتجاه منسجم مع التطور القانوني الدولي في هذا المجال مع بقاء الحاجة قائمة إلى تطويرها بصورة مستمرة بما يتناسب مع طبيعة التهديدات الرقمية المتسارعة واتساع الفضاء السيبراني .

الفرع الثاني : أوجه القصور التشريعي والتحديات التي تعيق المواءمة

على الرغم من التطور الملحوظ الذي حققته التشريعات الأردنية في تنظيم الأمن السيبراني واقترابها من عدد من الاتجاهات الدولية إلا أن هذا الإطار لا يزال يواجه مجموعة من أوجه القصور والتحديات التي تحول دون تحقيق مواءمة كاملة مع الأنظمة القانونية الدولية الأكثر تقدمًا.

ففي نطاق التجريم رغم توسع قانون الجرائم الإلكترونية في تغطية صور متعددة من الجرائم السيبرانية إلا أنه لا يزال بحاجة إلى معالجة أكثر تفصيلًا لبعض الجرائم الحديثة والمعقدة ذات

[1] إبراهيم ، خالد ممدوح. الجرائم المعلوماتيةدار الفكر الجامعي ، الاسكندرية، 2009م ص87 .

الطابع العابر للحدود ولا سيما الجرائم التي ترتبط بهجمات منظمة تمتد عبر ولايات قضائية متعددة وتتطلب قواعد أوضح في مسائل الاختصاص القضائي والتعاون الدولي وتسليم المطلوبين وتبادل الأدلة الرقمية وإجراءات الملاحقة عبر الحدود وهي جوانب تبرز في كثير من الاتفاقيات الدولية بصفتها جزءًا لا يتجزأ من الاستجابة القانونية المتكاملة للجريمة السيبرانية [1].

كما يلاحظ أن قانون حماية البيانات الشخصية ورغم تبنيه لمبادئ مهمة متوافقة مع المعايير الدولية إلا أن فعاليته ترتبط بمدى اكتمال البنية التنفيذية والرقابية المصاحبة له إذ ما تزال الحاجة قائمة إلى تعزيز الآليات المؤسسية الرقابية وتوضيح نطاق المسؤولية القانونية بصورة أدق وتطوير قواعد نقل البيانات عبر الحدود على نحو أكثر تفصيلًا وتنظيم التعامل مع الجهات التقنية العالمية ومقدمي الخدمات الرقمية الذين قد تكون مراكزهم خارج المملكة وهي مسائل تمثل محورًا أساسيا في الالتزامات الدولية المتعلقة بحماية الخصوصية في البيئة الرقمية .

وعلى مستوى التنظيم المؤسسي فإن المركز الوطني للأمن السيبراني يعد خطوة مهمة لكنه لا يزال في مرحلة بناء وتطوير ويظل نجاحه مرتبطًا بوضوح حدود التنسيق بينه وبين الجهات الأخرى ذات العلاقة وبقدرته على بناء منظومة استجابة وطنية متكاملة للحوادث السيبرانية تشمل الإنذار المبكر والتحليل الفني وإدارة الأزمات وتبادل المعلومات مع الشركاء داخليًا وخارجيًا إضافة إلى توفير الكفاءات الفنية المتخصصة واستدامة التدريب والتحديث وهي تحديات عملية تؤثر مباشرة على مستوى المواءمة الفعلية مع الممارسات الدولية[2] .

---

[1] سامي فهمي محمود، التحديات القانونية للجرائم السيبرانية العابرة للحدود: دراسة مقارنة ,دار الفكر العربي، القاهرة، 2020، ص 101–115.

[2] رانيا شريف محمد، الهيكل المؤسسي للأمن السيبراني: دراسة تطبيقية على المراكز الوطنية ,دار الفكر القانوني، القاهرة، 2021، ص 58–70.

كما ترى الباحثة أن سرعة تطور التهديدات الرقمية تجعل تحديث التشريعات مسألة جوهرية إذ إن عددًا من المعايير الدولية يعتمد على مفهوم التطوير المستمر في مواجهة المستجدات التقنية بينما قد تظهر في بعض النصوص الوطنية درجة من الجمود النسبي في جوانب معينة وهو ما يستدعي مراجعات تشريعية دورية وتحديثًا مستمرًا للمفاهيم والمصطلحات والضوابط بما يحقق التوازن بين حماية الأمن الرقمي من جهة وصون الحقوق والحريات الأساسية من جهة أخرى .

وعليه يتبين أن التشريعات الأردنية وإن كانت قد قطعت شوطًا مهمًا في اتجاه المواءمة مع الإطار القانوني الدولي إلا أنها ما تزال بحاجة إلى استكمال بعض الجوانب القانونية والمؤسسية والرقابية لضمان انسجام أكثر شمولًا مع المعايير الدولية ولا سيما في موضوع التعاون العابر للحدود وتبادل الأدلة الرقمية وتعزيز الضمانات المتعلقة بالخصوصية والحقوق والحريات .

وفي الختام يتضح أن المشرع الأردني وضع أساسًا تشريعيًا مهمًا لمواجهة التحديات السيبرانية من خلال قانون الجرائم الإلكترونية وقانون حماية البيانات الشخصية وقانون الأمن السيبراني وإنشاء المركز الوطني للأمن السيبراني وهو ما يعكس إدراكًا واضحًا لخطورة التهديدات الرقمية إلا أن المقارنة مع الاتفاقيات الدولية تُظهر أن هذا الإطار ما يزال بحاجة إلى مزيد من التطوير والتحديث خاصة في ما يتعلق بضبط المصطلحات التقنية وتوضيح بعض النصوص وتعزيز ضمانات التطبيق وتفعيل الرقابة المؤسسية وضمان التوازن بين حماية الأمن السيبراني واحترام الحقوق والحريات[1] كما أن فعالية هذه التشريعات تبقى مرتبطة بقدرة الدولة على تطوير آليات التنفيذ ورفع الكفاءة الفنية وتوسيع نطاق التعاون الدولي لمواجهة الجرائم العابرة للحدود وبذلك يصبح الأمن السيبراني منظومة متكاملة لا تكتفي بالنصوص بل تقوم على تحديث مستمر ووعي مجتمعي وتنسيق مؤسسي وتعاون دولي يضمن فضاء رقميًا آمنًا ومتوازنًا [2].

---

[1] العطاونة، محمد .الأمن السيبراني في التشريع الأردني: دراسة مقارنة مع المعايير الدولية .دار اليازوري العلمية، عمان، الأردن، 2022، ص 45–62.

[2] **السباعي، زياد فواز** .الأمن السيبراني في الأردن: التشريعات، التنفيذ، والتحديات الدولية .عمان: دار الفكر القانوني، 2023، ص 88–104.

الفصل الرابع
الخاتمة والنتائج والتوصيات

الخاتمة

لا شك أن التطور التكنولوجي المتسارع الذي يشهده العالم المعاصر قد أفرز تحديات قانونية غير مسبوقة، فرضت على الدول ضرورة إعادة النظر في منظوماتها التشريعية التقليدية، والعمل على تطوير أطر قانونية حديثة قادرة على مواكبة التحول الرقمي المتنامي، ولا سيما في مجال الأمن السيبراني. فقد أصبح الفضاء الإلكتروني اليوم أحد الميادين الرئيسية التي تتقاطع فيها المصالح الاقتصادية والأمنية والاجتماعية، الأمر الذي جعله محط اهتمام المشرّعين الوطنيين والمنظمات الدولية على حد سواء.

وفي هذا السياق، برزت المعاهدات والاتفاقيات الدولية بوصفها أداة أساسية لتنسيق الجهود الدولية في مواجهة الجرائم الإلكترونية العابرة للحدود، ووضع مبادئ عامة تهدف إلى حماية الفضاء الرقمي وتعزيز أمنه باعتباره امتدادًا للأمن الوطني والدولي. ومن هنا جاءت هذه الدراسة لتسلّط الضوء على مدى انسجام التشريعات الأردنية ذات الصلة، وبوجه خاص قانون الجرائم الإلكترونية، وقانون حماية البيانات الشخصية، وقانون الأمن السيبراني، مع المعايير الدولية المعتمدة في هذا المجال، وبيان مدى كفاية هذه التشريعات في تحقيق التوازن المطلوب بين متطلبات الحماية الرقمية من جهة، وضمان الحقوق والحريات الأساسية من جهة أخرى.

وقد أظهرت الدراسة أن الأردن، رغم ما حققه من تقدم تشريعي ملحوظ في مجال تنظيم الفضاء السيبراني، لا يزال بحاجة إلى مراجعة بعض النصوص القانونية القائمة، وتطوير آليات التنفيذ والرقابة، وتعزيز التعاون الدولي في هذا المجال الحيوي. ذلك أن فعالية أي منظومة قانونية

لا تُقاس بمجرد وجود النصوص التشريعية، وإنما بمدى قابليتها للتكيّف مع المستجدات التقنية، وقدرتها على التطبيق العملي، واستجابتها للتحديات الواقعية التي تفرضها الجرائم السيبرانية بطبيعتها المعقدة والعابرة للحدود.

أولًا: النتائج

1. تبيّن أن التشريع الأردني لم يُفرد تنظيمًا مستقلًا ومتكاملًا للمهام المرتبطة بالأمن السيبراني، مما أدى إلى تداخل الاختصاصات بين الجهات المعنية، وأضعف من وضوح المسؤوليات القانونية، وهو ما يؤثر سلبًا على فعالية التدابير الوقائية والاستباقية في هذا المجال.
2. أظهرت الدراسة أن التشريعات الأردنية تناولت الجرائم الإلكترونية في كثير من الأحيان من منظور تقليدي، ركّز على الجوانب التقنية للفعل الجرمي، دون الانخراط بصورة كافية في التصنيفات الدولية الحديثة، مثل تصنيف الجرائم وفقًا لطبيعة الضحية أو وسيلة الاعتداء أو الأثر المترتب على الجريمة.
3. ثبت وجود قصور في معالجة الأثر القانوني للجرائم السيبرانية، خاصة تلك التي تمس الأمن القومي أو تنطوي على انتهاك جسيم للخصوصية الرقمية، إذ لا تزال العقوبات المقررة في بعض الحالات غير متناسبة مع حجم الضرر الناتج عن هذه الجرائم.
4. بيّنت الدراسة أن التشريعات الوطنية لم تواكب بالشكل الكافي الخصائص الفريدة للجريمة السيبرانية، كعالميتها، وسرعة تنفيذها، وصعوبة تعقّب مرتكبيها، مما يستدعي استحداث نصوص قانونية مرنة وقابلة للتطوير تتماشى مع طبيعة هذه الجرائم المستحدثة.
5. تبيّن أن غياب انضمام الأردن إلى بعض الاتفاقيات الدولية المتخصصة في مجال الأمن السيبراني، وعلى رأسها اتفاقية بودابست، يحول دون استفادته من منظومة التعاون الدولي الواسعة في مجالات تبادل المعلومات والمساعدة القانونية وتسليم المجرمين.

ثانيًا: التوصيات

1. توصي الدراسة بضرورة الإسراع في إصدار الأنظمة والتعليمات التنفيذية لقانون حماية البيانات الشخصية، مع تحديد واضح للصلاحيات والجهات الرقابية وآليات التظلم، بما يضمن التطبيق العملي الفعّال لأحكام القانون.
2. كما توصي الباحثة بتعزيز ضمانات حماية الحقوق الرقمية للأفراد، وبوجه خاص الحقوق المتعلقة بالاطلاع والتصحيح والنسيان والموافقة الصريحة على معالجة البيانات، بما ينسجم مع المعايير الدولية الحديثة في هذا المجال.
3. ترى الباحثة ضرورة تعزيز دور المركز الوطني للأمن السيبراني، وتوسيع صلاحياته التنسيقية مع باقي الجهات والمؤسسات ذات العلاقة، بما يضمن توحيد الجهود الوطنية في مواجهة التهديدات السيبرانية وتفادي تضارب الاختصاصات.
4. توصي الدراسة باعتماد سياسة وطنية شاملة للأمن السيبراني، تُحدّد فيها الأهداف والأولويات والمسؤوليات، وتُدمج ضمن خطط التنمية الوطنية وبرامج التحديث الحكومي، بما يرسّخ مفهوم الأمن السيبراني كأحد ركائز الأمن الوطني.
5. كما توصي الباحثة بإشراك القطاع الخاص ومؤسسات المجتمع المدني في وضع وتنفيذ الاستراتيجيات الوطنية للأمن السيبراني، نظرًا لدور هذه الجهات في تبادل الخبرات، ورصد الثغرات التقنية، والمساهمة الفاعلة في مواجهة الهجمات السيبرانية.

قائمة المراجع

أولاً–الكتب

إبراهيم ، خالد ممدوح (2009). **الجرائم المعلوماتية،** دار الفكر الجامعي ، الاسكندرية.

أبو سعده ، مصطفى البنداري (2022–2023).**المنهجية القانونية بين القواعد النظرية والمهارات التطبيقية** ، دار النهضة العربية ، القاهرة ، الطبعة الأولى .

الاشقر، منى جبور، **البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الفراد،** مرجع سابق.

التميمي ، تميم (2016). **الجرائم المعلوماتية في الاعتداء على الاشخاص** ، مكتبة القانون والاقتصاد ، الرياض ، ط1.

الجوخدار ، حسن (2008). **التحقيق الابتدائي في قانون أصول المحاكمات الجزائية** ، دراسة مقارنة . الأردن : دار الثقافة للنشر والتوزيع.

حجازي، أحمد (2004). **جرائم الحاسوب والإنترنت**. دار الكتب القانونية، القاهرة.

حسني، محمود نجيب (1998). **شرح قانون الاجراءات الجزائية،** الطبعة الثانية ، دار النهضة العربية ، مصر.

الحمادي ، عبد العزيز حسن(2013). **نشاط المنظمة الدولية للشرطة الجنائية (الانتربول) وأنشطتها في ضوء القانون الدولي،** مركز بحوث الشرطة، شرطة الشارقة، الطبعة الأولى.

الدسدوقي ، طارق ابراهيم (2009). **الأمن المعلوماتي: النظام القانوني للحماية المعلوماتية** .

دليل الأمن السيبراني للبلدان النامية الأتحاد الدولي للاتصالات ، (لعام 2010) .

الزرفي علي نعمة جواد الزرفي ، (2019). **الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة** ، المكتب الجامعي الحديث.

سرور، احمد فتحي (1981). **الوسيط في قانون العقوبات** ،القسم العام ،الجزء الأول ، دار النهضة العربية ،القاهرة .

السند، عبد الرحمن بن عبد الله، **جريمة الابتزاز**، مطبوعات الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر.

الشاذلي ، فتوح ، (2020) .**جرائم التعزيز المنظمة في المملكة العربية السعودية** ، مكتبة الرشد ، الرياض.

شمدين، عفاف (2013). **الأبعاد القانونية لأستخدمات تكنولوجيا المعلومات**، دمشق.

الشمري ،غانم مرضي (2016). **الجرائم المعلوماتية**. الطبعة الأولى، عمان: الدار العلمية الدولية.

عبابنة، محمد أحمد (2020). **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة، ط3، عمان.

عبد الستار ، فوزية (1982). **شرح قانون العقوبات** ، دار النهضة ، القاهرة.

فاروق ، ياسر الأمير (2009) . **مراقبة الأحاديث الخاصة في الاجراءات الجنائية** . ط1 ، جامعة القاهرة : دار المطبوعات الجامعية.

القرعان ، محمود أحمد (2017) . **الجرائم الالكترونية** ، دار وائل للنشر والتوزيع ، عمان ، الطبعة الاولى.

كورنو، جيرار (1998). **معجم المصطلحات القانونية**، الطبعة الأولى، المؤسسة الجامعية للدراسات والنشر والتوزيع.

لطفي ، خالد حسن أحمد (2020) **الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية** ، دار الفكر الجامعي ، الاسكندرية ، الطبعة الاولى.

مرسي ، عبد الواحد إمام . **الموسوعة الذهبية في التحريات** . مصر : دار المعارف والمكاتب الكبرى للنشر والتوزيع.

الملط ، احمد حليفة (2005). **الجرائم المعلوماتية** ،دار الفكر الجامعي.

موسى ، مصطفى محمد (2009) . **التحقيق الجنائي في الجرائم الالكترونية** . ط1 ، القاهرة : مطابع الشرطة .

النقروز، علي (2017). **جرائم نظم المعلومات**، دار السناء للنشر، الاردن، عمان.

ثانياً–الرسائل العلمية

أبو حسين، حنين جميل. (2021). **الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة.** جامعة الشرق الأوسط، عمّان، الأردن.

الباشا، محاسن (1999). **تسليم المجرمين في القانون الدولي والفقه الاسلامي** ، رسالة ماجستير ،جامعة أم درمان الاسلامية ، السودان .

دارا، نسيمة(2017). **الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني: دراسة مقارنة.** أطروحة دكتوراه، جامعة أبي بكر بلقايد تلمسان – الجزائر، كلية الحقوق والعلوم السياسية.

الديب، نانسي حامد (2025). **السيادة الرقمية للدول في مواجهة التهديدات السيبرانية غير الحكومية نحو بناء اطار قانوني دولي مرن ومتكامل** ،المعهد العالي للتجارة والعلوم الادارية بالمنصورة .

الرشدان، تقوى أحمد محمد. (2021). **إجراءات التحقيق الابتدائي في جرائم الأمن السيبراني في القانون الأردني والاتفاقيات الدولية.** جامعة اليرموك، إربد، الأردن.

السبتي ، آسيا بوقريط عمر (2025). **جامعة الاخوة منتوري قسنطية** ، مختبر الدراسات القانونية التطبيقية.

سليمان ، قطاف(2022). **مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية** ، جامعة عمار ثليجي الأغواط، الجزائر.

السوفي ، نور الهدى (2017) . **التحقيق في الجريمة المعلوماتية** . جامعة قاصدي مرباح ، ورقلة ، الجزائر.

عمايرة ، محمد منذر طه (2023). **التعاون الدولي في مواجهة الجريمة السيبرانية** ، رسالة ماجستير، جامعة القدس .

العنزي، سليمان (2013). **وسائل التحقيق في جرائم نظم المعلومات**، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

الغياثين ، محمد عمر(2013). **الجرائم المعلوماتية عابرة الحدود –دراسة مقارنة–** ، رسالة قُدِّمَت لنيل درجة الدكتوراه في الحقوق جامعة القاهرة.

قادري ، سارة (2014). **أساليب التحري الخاصة في قانون الاجراءات الجزائية** . رسالة ماجستير ، جامعة قاصدي مرباح ، ورقلة ، الجزائر .

مهمل ، اسامة (2018). **الاجرام السيبراني** .

ثالثاً–الأبحاث والمقالات

بريم ، فاطمة (2020) . **السيادة الوطنية السيبرانية في ظل الفضاء السيبراني والتحولات الرقمية.** مجلة الدراسات القانونية والسياسية ، جامعة قسنطنية.

جبور، منى الأشقر، (2017). **السيبرانية هاجس العصر**، دراسات وأبحاث المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت.

الجعافرة، رويدا حسن (2022) . **قانون حماية البيانات الشخصية في الأردن** ، الإصدار الخامس – العدد خمسون .

خلاف ، خالد محمد (2023). **اتجاهات الأفراد نحو قانون الجرائم الإلكترونية الأردني: حماية البيانات على وسائل التواصل الاجتماعي**، ResearchGate.

خلايفية، هدى (2019) . **الاطار القانوني الدولي والداخلي لحماية الخصوصية على الانترنت التشريع الجزائري نموذجا**، بحث مشارك ومنشور في كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية.

الراوشدة، يونس، والمغيرة، علاء الدين. (2023). **التحديات القانونية لمكافحة الجرائم السيبرانية** في ظل التطور التقني السريع. مجلة العلوم القانونية والسياسية، جامعة مؤتة، المجلد 17، العدد 2.

رستم ، هشام محمد فريد (2000) . **القانون والكمبيوتر والانترنت** ، بحث مقدم لجامعة دولة الامارات العربية المتحدة .

الرفداني ، محمد (2014). **تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية** ، المجلة العربية للدراسات الأمنية ، المجلد رقم 31 ،العدد 61.

الزعبي، مخلد إبراهيم (2021). **إذا كنت تعرفه** . العدد السابع والثلاثون .

السيادة الرقمية (2025) . **التحديات والفرص في عصر البيانات والتقنيات الحديثة** ، مدونة.

شرابسة ، لينا . (2009) ،**السياسة الدولية والاقليمية في مجال مكافحة الجريمة الالكترونية** . مجلة دراسات وأبحاث ، المجلد 01 .

شرف الدين ، وردة (2021) . **مجلة الباحث للدراسات الأكاديمية مجلة الباحث للدراسات الأكاديمية**. المجلد 8، العدد 2.

الشوار، سامي (2019). **الغش المعلوماتي كظاهرة إجرامية مستحدثة**، بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة.

الصحفي ، روان بنت عطية الله الصحفي (2020) . **المجلة الالكترونية الشاملة متعددة التخصصات** ، المملكة العربية السعودية ، جدة ، العدد الرابع والعشرون شهر 5 .

عرب، يونس (2021). **قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان**، مجلة الأزهر للعلوم الإعلامية، العدد السادس والخمسون – الجزء الثالث، كلية الإعلام، جامعة الأزهر.

عقلقة ، أشرف علي (2021). **دور التشريع الأردني في مكافحة الجرائم الإلكترونية وأثره على أمن معلومات المكتبات**، المجلة الأردنية للقانون والعلوم السياسية، جامعة مؤتة، المجلد 13، العدد 1.

القاضي، رامي متولي (2022) . **الدليل الجنائي الرقمي في التشريع المصري في ضوء أحكام القانون 175 لسنة 2018 ولائحته التنفيذية** . رئيس قسم القانون الجنائي بكلية الشرطة المصرية جمهورية مصر. منشور في مجلة القانون والتكنولوجيا مجلد 2، العدد 1.

ماجد ، عبدالعزيز (2021). **السياسة الجنائية في مواجهة الجرائم المعلوماتية**، و مجلة جامعة الإمام محمد بن سعد، العدد 78.

محمود، سيناء علي (2025). **التحديات الأمنية للدول في الفضاء السيبراني**، مجلة القضايا السياسية، العدد 80.

مساعدة، أنور محمد صدقي. (2019). **الجرائم الإلكترونية والاختصاص القضائي**. المراجعة الدولية.

المعايطة، محمد، والغُسّين، محمود. (2020). **التحديات التقنية والقانونية في جمع الأدلة الرقمية في الجرائم الإلكترونية**. مجلة الدراسات الأمنية والجنائية، الجامعة الأردنية، العدد 15.

منصور المغيره، علاء الدين. (2024). **دراسة نقدية لقانون الجرائم الإلكترونية الأردني رقم (17) لسنة 2023 وتأثيره على حرية التعبير**. المجلة الدولية للجرائم السيبرانية.

نصار، مصعب تركي إبراهيم. (2024). **واقع الحماية الجزائية للأمن السيبراني: دراسة مقارنة بين الأردن وقطر**. المجلة العربية للمعلوماتية وأمن المعلومات.

النقبي، جمال محمد خلفان (2023). **التعاون الوطني والدولي في الجرائم الإلكترونية: المشكلات والحلول** ، مجلة المعهد العالي للدراسات النوعية، المجلد 3، العدد 16، يوليو .

رابعا–التشريعات

قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023 .

قانون الأمن السيبراني الأردني رقم (16) لسنة 2019 .

الدستور الأردني الصادر لسنة 1952 وتعديلاته .

اتفاقية بودابست بشأن الجرائم السيبرانية، مجلس أوروبا لسنة 2001 .

مشروع قانون حماية البيانات الشخصية لسنة 2022 .

اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000 .

قانون مكافحة الجرائم الإلكترونية السعودي 2007 .

خامساً-المراجع الالكترونية

موقع المركز الوطني للأمن السيبراني :

https://www.ncsc.jo/Ar/Pages/Services_AR

موقع الوكالة الأوروبية للأمن السيبراني : https://www.enisa.europa.eu

موقع الوكالة الأوروبية للأمن السيبراني :

https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network?utm_source=.com

موقع رؤيا الاخباري : https://royanews.tv/news/338216?utm_source.com

موقع اتفاقية بودابست : https://www.coe.int/en/web/cybercrime

موقع ريد نوتيس العربية : https://rednoticearabia.com/interpol-vs-europol-whats-the-difference/

موقع Pressbooks للتعليم المفتوح :

https://cod.pressbooks.pub/crimj1165/chapter/module-1/?utm_source

موقع النهضة العربية للديمقراطية والتمنية : https://ammannet.net/أخبار/ورقة-موقف-حول-قانون-الجرائم-الإلكترونية-صادرة-عن-نشطاء-النهضة

موقع منصة سمكس(SMEX) : https://smex.org/ar/قانون-حماية-البيانات-الشخصية-الأردن

موقع كلارين : https://www.clarin.eu/content/principles-data-processing

موقع هيئة تنظيم قطاع الاتصالات: https://www.trc.gov.jo/

موقع المجلس الأعلى للقضاء الفلسطيني :

https://www.courts.gov.ps/userfiles/file/الاتفاقية%20العربية%20لمكافحة%20جرائم%20تقنية%20المعلومات.pdf

موقع أخبار الأمم المتحدة : https://news.un.org/ar/story/2024/12/1137776

موقع وثائق الأمم المتحدة الرسمي :

https://documents.un.org/doc/undoc/gen/v21/084/20/pdf/v2108420.pd

موقع الأمم المتحدة لمكتب الأمم المتحدة المعني بالمخدرات والجريمة :

https://www.unodc.org/unodc/en/cybercrime/convention/index.html

موقع مؤسسة هوفر :

http://media.hoover.org/documents/0817999825_1.pdf

سادسا-التقارير

- **تقرير الأونكتاد** (2005). ملتقى الأمم المتحدة حول التجارة والتنمية .
- **تقرير حالة حقوق الإنسان في الأردن** (2023). المركز الوطني لحقوق الإنسان، عمان، 2024.

سادسا–مراجع باللغة الانجليزية

EU Cybersecurity Act (Regulation (EU) 2019/881) -

Maras, M. H. (2014). **Computer Forensics**: Cybercriminals, Laws, and - Evidence. Jones & Bartlett Learning.

Prof. Dr. Marco Gercke, **Understanding cybercrime**: Phenomena,-

challenges and legal response, op, cit, p11.