Innovations Journal of Humanities and Social Studies (IJHSS): Vol 4, No 1, 2026

DOI: https://doi.org/10.61856/krp0q603

Scientific Events Gate

Innovations Journal of Humanities and Social Studies

IJHSS

https://eventsgate.org/ijhss

e-ISSN: 2976-3312

القصـــــــور التشـــــريعي في قوانين مكافحـــــــة الجريمـــــــة السيبرانية: دراسة قانونية مقارنة بين السودان والمعايير الدولية دولة قطر نموذجـاً

قريب الله محمد الباز السنهوري

جامعة السودان المفتوحة-السودان

g_albaz@yahoo.com

الملخص: تناولت الدراســة العلاقة بين الأمن الســيبراني والإطار القانوني المنظم له، مع تحليل الآثار القانونية والاجتماعية والاقتصــادية الناتجة عن التهديدات الســيبرانية المتزايدة. في وجود التحول الرقمي واكتشــاف الفجوات التشــريعية التي ترفع معدلات الجريمة السيبرانية، فقد أصبح الأمن السيبراني قضية محورية تتطلب استجابة قانونية فعّالة للتصدي للتهديدات التي تستهدف الأنظمة الرقمية والبنية التحتية المعلوماتية.سلطت هذه الدراسة الضوء على قدرة التشريعات السودانية، خاصة قانون الجرائم المعلوماتية لســنة 2007 و2018، على مواجهة هذه التحديات، مع الاســتناد إلى اللائحة العامة لحماية البيانات General Data Protection Regulation (GDPR) (European Parliament and Council: 2016) نموذج دولي متقدم في حماية البيانات والخصوصية. كما اختارت الدراسة دولة قطر كنموذج عربي معاصر في التشريع السيبراني، وبيّنت المقارنة بين النموذجين وحجم الفجوات التشــريعية وضــرورة تحديث المنظومة القانونية لتواكب التطورات التقنية والحقوقية.اعتمدت الدراسة المنهج الوصفي التحليلي في تقييم النصوص القانونية، وتعرفت من خلاله على القصور والفجوات التشــريعية التي تســاهم في تزايد الجريمة الســيبرانية، مما يســتدعي مراجعة القوانين الحالية، وتعزيز التعاون الدولي، وتطوير التدريب القانوني المتخصص لتحقيق منظومة قانونية فعالة لحماية أمن المعلومات وحقوق الأفراد في البيئة الرقمية.

الكلمات المفتاحية: الأمن السيبراني- الجريمة السيبرانية- الفجوات التشريعية - المعايير الدولية- التشريعات السيبرانية

Legislative Gaps in Cybercrime Laws: A Comparative Analytical Study between Sudan and International Standards (Qatar as a Model)

GARIBALLA MOHAMMED ELBAZ ALSANHORY

Open University of Sudan – Sudan

g_albaz@yahoo.com

Received 25\|07\|2025 - Accepted 22\|09\|2025 Available online 15\|01\|2026

Abstract: This study examines the relationship between cybersecurity and its governing legal framework, analyzing the legal, social, and economic impacts resulting from the growing cyber threats in the context of digital transformation and the discovery of legislative gaps that contribute to the rise in cybercrime rates. Cybersecurity has become a central issue requiring an effective legal response to counter threats targeting digital systems and information infrastructure. The study highlights the capacity of Sudanese legislation—particularly the Cybercrimes Acts of 2007 and 2018—to address these challenges. It also draws upon the General Data Protection Regulation (GDPR) as an advanced international model for data protection and privacy. Additionally, the State of Qatar was selected as a contemporary Arab example of cyber legislation, allowing for a comparative analysis between the two models and the identification of legislative gaps and the urgent need to update the legal framework in line with technological and human rights developments. The study adopts a descriptive-analytical methodology to evaluate legal texts and identify legislative shortcomings and gaps that contribute to the rise of cybercrime. It concludes with a call to review current laws, enhance international cooperation, and develop specialized legal training in order to establish an effective legal system that safeguards information security and individual rights in the digital environment.

DOI: https://doi.org/10.61856/krp0q603

Keywords: Legislative gaps – cybercrime - international standards – cybersecurity - cyber legislations.

المقدمة:

لقد حُظي مفهوم الأمن بمكانة عالية في التشريعات السماوية والوضعية على حد سواء، إذ لا يتحقق الاستقرار المجتمعي والسياسي إلا بتوفره. وقد أشار القرآن الكريم إلى هذا المعنى في قوله تعالى: (الَّذِي أَطْعَمَهُم مِّن جُوعٍ وَآمَنَهُم مِّنْ خَوْفٍ). (قريش، الآية4). في إشارة إلى أن الأمن نعمة عظيمة وركيزة أساسية لاستقرار حياة الأفراد والمجتمعات، ومع تطور العصر وظهور التهديدات الرقمية، بات من الضروري توسعة مفهوم الأمن ليشمل المجال السيبراني، باعتباره بعدًا حديثًا لحماية الكيانات الفردية والمؤسساتية من المخاطر المرتبطة باستخدام التكنولوجيا. من هنا، تنبع أهمية هذا البحث في دراسة الجوانب القانونية والاجتماعية والاقتصادية المرتبطة بالأمن السيبراني، وتسليط الضوء على واقع التشريعات الوطنية وإمكانية تطويرها بما يواكب المتغيرات التقنية المتسارعة.

وفي ظل التحول الرقمي الراهن، أصبح الأمن السيبراني من القضايا الجوهرية التي تشكل تهديدًا حقيقيًا على الأنظمة الرقمية والبنية التحتية المعلوماتية في مختلف المجالات. تتسارع التهديدات الإلكترونية بشكل غير مسبوق، مما يستدعي استجابة شاملة ومعقدة تتجاوز الجوانب التقنية إلى التأثيرات القانونية والاجتماعية والاقتصادية التي تترتب عليها.

قطعاً هذا التحول المستمر في المشهد السيبراني يتطلب إعادة النظر في الأطر القانونية الدولية والمحلية، وتحديثها لتواكب التطور التكنولوجي المتسارع.

تهدف هذه الدراسة إلى تحليل العلاقة المعقدة بين الأمن السيبراني والإطار القانوني المنظم له، مع تسليط الضوء على الآثار القانونية والاجتماعية والاقتصادية التي تنجم عن تزايد التهديدات السيبرانية. وتقييم مدى قدرة التشريعات السودانية على التصدي لهذه التحديات المتزايدة. ومقارنتها بالمعايير الدولية، لتحديد مدى فعاليتها في حماية الأمن السيبراني وحفظ الحقوق الرقمية. اعتماداً على المنهج الوصفي والمقارن.

مشكلة البحث:

تتمثل مشكلة البحث في وجود فجوات تشريعية في القانون السوداني تعيق فاعلية مكافحته للجريمة السيبرانية في ظل التهديدات الرقمية المتزايدة، مما يستدعي تقييم مدى توافق هذه التشريعات مع المعايير الدولية، بهدف تحديد أوجه القصور واقتراح سبل المعالجة. ومن ذلك تمت صياغة المشكلة في السؤال المحوري التالي:

مدى كفاية نصوص التشريع السوداني والتشريع القطري في مكافحة الجريمة السيبرانية ويتفرع عنه الأسئلة التالية :

ما مدى حجم النقص التشريعي - إن وجد - في التشريع السوداني والقطري في مجال الجريمة السيبرانية ؟

ما مدى تأثير النقص التشريعي في القانونين المذكورين في مكافحة الجريمة السيبرانية؟

ما السبيل لمعالجة النقص التشريعي المشار إليه؟

وما مدى توافقها مع المعايير الدولية ذات الصلة؟

وذلك وفق صياغة أهداف محددة في هذه الدراسة .

أهداف الدراسة:

1. التعريف بالأمن السيبراني وتحليل أهميته في ظل الاعتماد المتزايد على التكنولوجيا الرقمية.
2. تقييم التشريعات المرتبطة بالأمن السيبراني، خاصة قانون مكافحة جرائم المعلومات الصادر في العام 2007 والمعدل 2018، ومدى فاعليتها في مواجهة التهديدات الحديثة.
3. تحليل الآثار القانونية والاجتماعية والاقتصادية الناتجة عن تطور التهديدات السيبرانية وتأثيرها على الأفراد والمؤسسات والدول.
4. اقتراح حلول وتعزيز الأطر القانونية لمواكبة التهديدات السيبرانية، بما يشمل تحديث التشريعات، وتعزيز التعاون الدولي، وبناء القدرات المؤسسية.

منهجية الدراسة (Methodology)

اتبعت الدراسة المناهج التالية: -

1. المنهج الوصفي التحليلي، حيث تم تحليل النصوص القانونية السودانية المتعلقة بالجرائم السيبرانية. واستند البحث أيضًا إلى مراجعة الأدبيات الأكاديمية والتقارير الصادرة عن منظمات دولية وإقليمية.
2. المنهج المقارن، تمت مقارنة النصوص السودانية بالتشريعات الدولية. أهمها اللائحة العامة لحماية البيانات (GDPR) التي أصدرها الاتحاد الأوروبي عام 2016 إطارًا قانونيًا شاملاً لحماية البيانات الشخصية للأفراد، تقضي بفرض مجموعة من الالتزامات القانونية على الجهات التي تعالج البيانات كضرورة الحصول على موافقة صريحة من الأفراد وتمكينهم من ممارسة حقوقهم في الوصول إلى بياناتهم الشخصية وتصحيحها وحذفها ونقلها أو التعديل عليها وإلزام المؤسسات بالإبلاغ عن أي خروقات في مدة أقصاها 72 ساعة من اكتشافها للاختراق ، وفي حال عدم الاستجابة تفرض غرامات مالية ضخمة تصل إلى

DOI: https://doi.org/10.61856/krp0q603

4% من إجمالي الإيرادات السنوية أو 20 مليون يورو، أيهما أكبر، في حال عدم الامتثال (European Parliament and Council: 2016). كما يركز قانون مكافحة جرائم تقنية المعلومات في السودان (2018) المعدل (2020) على مكافحة الجرائم الإلكترونية ذات الطابع العدواني، والاختراقات غير المصرح بها للأنظمة المعلوماتية، والقرصنة، والاحتيال الإلكتروني وغيرها، دون أن يقدم إطارًا قانونيًا متكاملًا وهذا ما لاحظته الدراسة من ضمن الفجوات التشريعية لحماية البيانات الشخصية وبمعنى آخر لم يحدد حقوقًا واضحة للأفراد بخصوص بياناتهم (قانون مكافحة جرائم المعلومات السوداني، 2018). كما يفتقر هذا القانون إلى آليات إلزامية للإبلاغ عن خروقات البيانات ضمن إطار زمني محدد، ويتركز اهتمامه على العقوبات الجنائية مثل السجن والغرامات المالية ضد مرتكبي الجرائم الإلكترونية.

أما التشريعات القطرية، في قانونها الموسوم بمكافحة جرائم تقنية المعلومات القطري (2014) الجرائم الإلكترونية ويُجرّم بشكل واضح عمليات القرصنة والاختراقات غير المصرح بها للأنظمة والمعلومات، ويشدد على حماية البنية التحتية الرقمية والأمن السيبراني الوطني (قانون مكافحة جرائم تقنية المعلومات القطري، 2014). مع ذلك، لا يتضمن القانون القطري أحكامًا مفصلة ومباشرة بشأن حماية البيانات الشخصية أو حقوق الأفراد المتعلقة بمعالجتها، وهو بذلك يقترب من النهج السوداني في التركيز على مكافحة الجرائم التقنية أكثر من حماية البيانات الشخصية بمعايير مماثلة لـ(GDPR)

بناءً عليه، يمكن أن نخلص للتمييز بين منهجين تشريعيين: الأول يتمثل في GDPR، الذي يعزز حقوق الأفراد في البيانات ويضع قواعد واضحة للمعالجة والإبلاغ والجزاءات، والنهج الثاني الذي يتجسد في التشريعات السودانية والقطرية، حيث يُعطى تركيز أكبر لمكافحة الجرائم الإلكترونية والقرصنة مع غياب نسبي لإطار حماية البيانات الشخصية المتكامل. هذا الاختلاف يعكس مراحل التطور التشريعي في الدول العربية مقارنةً بالمعايير الأوروبية المتقدمة، وينبئ عن آفاقًا جديدة لزيادة التطور التشريعي في حماية البيانات.

أهمية الدراسة:

أولًا: الأهمية العلمية: تساهم الدراسة في إثراء المعرفة القانونية حول الأمن السيبراني من خلال تحليل الفجوات التشريعية في في اطار قانون مكافحة الجريمة السيبرانية في السودان، ومقارنتها بالمعايير الدولية، مما يُمكّن من تطوير نظرية قانونية حديثة تستجيب للتحديات الرقمية، ويعزز الجهود البحثية في مجال الجريمة السيبرانية.

ثانيًا: الأهمية العملية: يوفر البحث إطارًا عمليًا لصناع القرار والمشرعين لتحديث التشريعات الوطنية، ويسهم في بناء منظومة قانونية فعالة لمكافحة الجرائم السيبرانية، كما يدعم تطوير السياسات الوطنية لحماية البيانات وتعزيز التعاون الدولي في هذا المجال.

الدراسات السابقة:

تناولت الدراسة الأولى قوانين الأمن السيبراني في الهند، مركزةً على الآثار الدستورية والفجوات التشريعية، وأبرزت أوجه القصور في البنية التشريعية لمواجهة التهديدات السيبرانية. (Aziz, 2024).

أم الدراسة الثانية ركزت الدراسة على التحديات التي تواجه القضاء في تنفيذ قوانين الأمن السيبراني في باكستان، مع الإشارة إلى مشكلتي غموض المصطلحات وتعارض القوانين، مما يعرقل تطبيق العدالة الناجعة في قضايا الجريمة الإلكترونية . .(Khan, H., Shabbir, S. S., Ali, A., & Qureshi, A. N. 2024).

المبحث الأول: مفهوم الجريمة وأهمية الأمن السيبراني

الجريمة في اللغة بمعنى الذنب أو الإثم، وتُستخدم للدلالة على كل فعل يؤدي إلى الإخلال بالنظام العام أو انتهاك حقوق الأفراد . أما من الناحية الاصطلاحية، فهي كل فعل أو امتناع يحرّمه القانون ويُعاقب عليه لكونه يُهدد أمن المجتمع أو مصالحه الأساسية. في التشريع السوداني، نص القانون الجنائي السوداني لسنة 1991 على تعريف الجريمة في المادة الثالثة الفقه (7) كالآتي: تشمل كل فعل معاقب عليه بموجب أحكام هذا القانون أو أي قانون آخر. وتُعرف ايضاً على أنها كل فعل أو ترك يُعاقب عليه القانون، وجاء ذلك ضمنيًا في قانون الجرائم كما بين قانون العقوبات لسنة 1991. كما نص قانون مكافحة جرائم المعلومات 2007 وتعديلاته على صور متعددة من الجرائم الإلكترونية (Sudanese Criminal Law and Punishments Act, 1991) مثل الدخول غير المشروع، والتشهير عبر الوسائط الرقمية، والاعتداء على نظم المعلومات (قانون جرائم المعلوماتية السوداني، 2007 – معدل 2020).

أما في التشريع القطري، فقد نص قانون العقوبات على أن الجريمة هي كل فعل يُرتب عليه القانون جزاء جنائيًا، وقد أضاف قانون مكافحة الجرائم الإلكترونية لسنة 2014 تفاصيل دقيقة حول الأفعال المجرّمة إلكترونيًا، مثل الاعتداء على البيانات والمواقع الإلكترونية، وإنشاء منصات تروّج لأنشطة غير مشروعة (Qatari Cybercrime Prevention Law, 2014)

من منظور الشريعة الإسلامية، تُعرف الجريمة بأنها كل فعل محرّم شرعًا يستوجب حدًا أو قصاصًا أو تعزيرًا، وتصنّف إلى جرائم حدود، وجرائم قصاص ودية، وجرائم تعزيرية، وذلك وفقًا لنوع الجناية وأثرها على الفرد والمجتمع (Al-Zuhaili, 1998).

أما مكافحة الجريمة، فهي تمثل مجموعة من الإجراءات الوقائية والعلاجية التي تتخذها الدولة وأجهزتها المختصة لمنع ارتكاب الجرائم أو الحد منها وملاحقة مرتكبيها. لغويًا، تعني المكافحة المجابهة والمقاومة (Al-Mu’jam Al-Waseet, 2004) ، واصطلاحًا تشير إلى السياسات المتكاملة التي تتضمن التشريع، والضبط، والتحقيق، والعقاب، والوقاية المجتمعية .

DOI: https://doi.org/10.61856/krp0q603

في القانون السوداني، تُترجم مكافحة الجريمة من خلال منظومة القوانين الجنائية والإجرائية، إضافة إلى التشريعات الخاصة مثل قانون الأمن الوطني وقانون جرائم المعلوماتية، التي تتيح للجهات المختصة أدوات التحقيق والتتبع.
وفي القانون القطري، تتجلى مكافحة الجريمة بشكل واضح في القوانين الحديثة التي تواكب التطورات التكنولوجية وتفرض عقوبات رادعة، مع إقرار نصوص خاصة بالتعاون الدولي وتبادل المعلومات لمواجهة الجرائم العابرة للحدود .
وفي الشريعة الإسلامية، فإن مكافحة الجريمة تعتمد على مبدأ الردع من خلال العقوبات المشروعة، إلى جانب الوقاية الأخلاقية والتربوية، وتوفير سبل العدل الاجتماعي (الشاطبي، الموافقات؛ ابن القيم، إعلام الموقعين).
وعليه، فإن الجريمة السيبرانية تمثل امتدادًا نوعيًا للجريمة التقليدية، لكنها تختلف عنها في الوسيط والمجال، إذ تُرتكب باستخدام الوسائل التقنية في بيئة رقمية معقدة وعابرة للحدود. وهذا ما يجعل مكافحتها تتطلب مقاربة تشريعية خاصة، تتسم بالمرونة والحداثة، وتُراعي الخصوصية الفنية لهذه الجرائم، وهو ما تسعى هذه الدراسة إلى تحليله وتقويمه في السياق.

التشريعات السيبرانية:

لغةً: التشريع يعني عملية سن القوانين وتنظيمها رسميًا، أما السيبرانية فترمز إلى الفضاء الرقمي أو البيئة الإلكترونية التي تُطبق فيها هذه القوانين، وتشمل جميع الأنشطة المتعلقة بالإنترنت والشبكات الرقمية.(Kshetri, 2017) .
اصطلاحًا: التشريعات السيبرانية هي القوانين واللوائح التي تنظم استخدام الفضاء الرقمي وتعالج الجرائم والمخاطر المرتبطة به، مثل قوانين حماية البيانات، مكافحة الجرائم الإلكترونية، وضوابط التعاملات الرقمية (Brenner, S. W. 2010).
المفهوم الإجرائي للجريمة: في ضوء هذه الدراسة، يُقصد بالجريمة – إجرائيًا – كل سلوك مادي أو رقمي، يتمثل في فعل أو امتناع عن فعل، يُعد مخالفًا لنص قانوني صريح، ويترتب عليه جزاء جنائي، سواء وُقع على الأشخاص أو الممتلكات أو نظم المعلومات، في البيئة الواقعية أو الرقمية، ويُخضع مرتكبه للمساءلة أمام الجهات العدلية المختصة.
ويمتد هذا المفهوم ليشمل الجرائم السيبرانية التي تُرتكب باستخدام الوسائط التكنولوجية الحديثة، مثل أنظمة المعلومات، وشبكات الاتصال، والمنصات الرقمية، وفق ما نصت عليه التشريعات الوطنية كقانون جرائم المعلوماتية السوداني (2020/2007)، والتشريعات الحديثة في الدول المقارنة كقانون الجرائم الإلكترونية القطري 2014.

التصنيف المفاهيمي للجرائم الرقمية:

الجريمة الإلكترونية، المعلوماتية، والسيبرانية، ظهرت أنماط جديدة من الجرائم التي تختلف في طبيعتها وأدواتها وأهدافها عن الجرائم التقليدية. وهو مانتج عنه مفاهيم متعددة مثل الجريمة الإلكترونية، والجريمة المعلوماتية، والجريمة السيبرانية. وعلى الرغم من التقاطع الظاهري بين هذه المصطلحات، فإن كل منها يحمل دلالة خاصة تتعلق بطبيعة الجريمة ومجال ارتكابها والوسائل المستخدمة فيها.
تُعرف الجريمة الإلكترونية (Electronic Crime) بأنها كل فعل غير مشروع يُرتكب باستخدام جهاز إلكتروني، سواء كان متصلاً بالإنترنت أو لا. فهي ترتبط أساسًا باستخدام الوسائل الإلكترونية كأداة لارتكاب الجريمة، وقد تشمل أفعالاً مثل إدخال فيروسات عبر أجهزة تخزين خارجية أو استخدام هاتف ذكي في تنفيذ أعمال احتيالية ومثاله (شخص يستخدم USB يحتوي على فيروس لتخريب بيانات جهاز كمبيوتر في شركة).
أما الجريمة المعلوماتية (Information Crime)، فتتعلق بالمحتوى ذاته، أي بالمعلومات والبيانات، وتتمحور حول سرقتها أو تعديلها أو تدميرها. وغالبًا ما تكون هذه الجرائم موجهة إلى قواعد البيانات أو نظم المعلومات الحساسة، مثل تلك الموجودة في المؤسسات الحكومية أو المالية. وتتميز هذه الجرائم بأنها قد تُرتكب دون الحاجة إلى الاتصال بالإنترنت، إذ يكفي الوصول إلى المعلومة المخزنة على وسائط إلكترونية لتنفيذ الجريمة. مثاله (موظف يسرق قاعدة بيانات العملاء من نظام الشركة ويبيعها لشركة منافسة).
وفي المقابل، تشير الجريمة السيبرانية (Cyber Crime) إلى أي نشاط إجرامي يتم عبر الإنترنت أو من خلال الفضاء السيبراني، وهي أشمل وأوسع من النوعين السابقين. وتشمل هذه الفئة أنشطة مثل اختراق المواقع الإلكترونية، وهجمات حجب الخدمة (DDoS)، والتصيد الإلكتروني (Phishing)، وكل ما يتم من خلال الشبكات الرقمية، مما يجعلها تتطلب أدوات متقدمة وتقنيات اتصال عن بُعد مثال (هاكر يخترق موقع بنك إلكتروني ويسرق بيانات البطاقات البنكية للعملاء).
إن التمييز بين هذه الأنواع الثلاثة، بخلاف الجريمة العامة، لا يأتي من باب التصنيف الأكاديمي فحسب، بل يُعد ضروريًا لفهم طبيعة كل نوع، وتحديد الجهات المسؤولة عن مكافحته، ووضع الأطر القانونية المناسبة له. فبينما تُعالج الجريمة الإلكترونية في سياق أمني تقني، قد تتطلب الجريمة المعلوماتية مقاربة قانونية متخصصة بحماية البيانات، في حين تُواجه الجريمة السيبرانية بتقنيات الدفاع السيبراني والاستراتيجيات الأمنية الرقمية المعقدة.
ومن خلال ذلك، سيتم تحليل هذه المفاهيم بشكل أعمق، مع استعراض أبرز الأمثلة الواقعية لكل نوع، وبيان الأدوات المستخدمة في تنفيذ كل منها، بما يسهم في بلورة رؤية متكاملة حول مشهد الجريمة في العصر الرقمي كما في الجدول أدناه:-

جدول رقم (1): تصنيف الجرائم حسب الوسيلة والتقنية المستخدمة

النوع	الوسيلة	الهدف	الاتصال بالإنترنت	مثال
الجريمة العامة	أدوات تقليدية، " أسلحة بيضاء	تحقيق مكاسب غير قانونية من خلال ارتكاب أفعال غير مشروعة	لا يوجد	سرقة متجر أو اعتداء جسدي..الخ.
الجريمة الإلكترونية	أي جهاز إلكتروني	تنفيذ جريمة باستخدام الأجهزة	ليس بالضرورة	تخرين بيانات عبرUSB

DOI: https://doi.org/10.61856/krp0q603

الجريمة المعلوماتية	المعلومات والبيانات	سرقة أو تلاعب بالمعلومات	ليس بالضرورة	سرقة قاعدة بيانات
الجريمة السيبرانية	الإنترنت والشبكات	جريمة عبر الفضاء السيبراني	ضروري	اختراق موقع إلكتروني

المطلب الثاني: مفهوم الأمن السيبراني

المفهوم اللغوي:الأمن: لغةً هو نقيض الخوف، ويعني الطمأنينة والاستقرار والسلامة من كل مكروه أما كلمة سيبراني: مشتق من الكلمة الإنجليزية Cyber، وهي مأخوذة من Cybernetics". وتعني علم التحكم أو الحوكمة، ثم تطور استخدامها للدلالة على الفضاء الرقمي أو العالم الافتراضي المتصل بالشبكات الحاسوبية.

وبذلك فإن "الأمن السيبراني" لغويًا يعني: ضمان الطمأنينة والسلامة في الفضاء الرقمي أو العالم الافتراضي

المفهوم الاصطلاحي:الأمن السيبراني: يُعرف اصطلاحاً بأنه مجموعة من الإجراءات والتقنيات المصممة لحماية الأنظمة الرقمية والبيانات الحساسة من التهديدات الإلكترونية. مع زيادة الاعتماد على التكنولوجيا الرقمية، أصبح الأمن السيبراني ضروريًا للحفاظ على سلامة المعلومات.

المفهوم الإجرائي للأمن السيبراني: في سياق هذه الدراسة، يُقصد بالأمن السيبراني – إجرائيًا – مجموعة السياسات والتدابير التشريعية والتنظيمية والتقنية التي تعتمدها الدولة والمؤسسات بهدف الوقاية من الجرائم السيبرانية، والتصدي لها، وتأمين سلامة البنية التحتية الرقمية، وحماية خصوصية الأفراد وحقوقهم في الفضاء الرقمي.

ويشمل ذلك أنشطة الحماية المسبقة، والرصد والتصدي للهجمات، والاستجابة للطوارئ الرقمية، وفقًا لما تنص عليه القوانين الوطنية كقانون جرائم المعلوماتية السوداني، والمعايير الدولية كـ(GDPR) والاتفاقيات الخاصة بالتعاون في مكافحة الجريمة السيبرانية.

أهمية الأمن السيبراني:

التحولات التقنية المتسارعة واعتماد المجتمعات الحديثة على الفضاء الرقمي في شتى جوانب الحياة، أظهرت أهمية الأمن السيبراني كضرورة استراتيجية لحماية المعلومات والأنظمة من التهديدات المتزايدة. فمع تنامي الاعتماد على التكنولوجيا في القطاعات الحيوية، أصبحت الهجمات السيبرانية تمثل تهديداً مباشراً لسرية البيانات وسلامة البنية التحتية، مما يجعل الأمن السيبراني أداة محورية في الحفاظ على الاستقرار المؤسسي والأمن القومي. وتكمن أهمية الأمن السيبراني في النقاط التالية :

1. حماية البيانات والمعلومات الحساسة (المالية ، الصحية ..الخ).
2. ضمان استمرارية الخدمات والأنظمة.
3. الوقاية من الهجمات الإلكترونية والاختراقات.
4. حماية البنية التحتية الحيوية.
5. يقلل من الخسائر المالية الناتجة عن الجرائم السيبرانية.
6. يقوي ويعزز الثقة في البيئة الرقمية.
7. يدعم الأمن القومي والسيادة الرقمية.
8. الامتثال للأنظمة والقوانين المتعلقة بحماية البيانات.
9. يعزز الأمان في المعاملات الإلكترونية.
10. مواجهة التهديدات السيبرانية المتطورة.

المبحث الثاني: آثار الأمن السبراني

إن آثار جريمة الأمن السيراني تتجاوز الجوانب التقنية لتطال الأبعاد الاجتماعية والاقتصادية والقانونية. فمع تزايد الاعتماد على الفضاء الرقمي في مختلف مجالات الحياة، أصبحت حماية المعلومات والبنية التحتية الرقمية ضرورة ملحّة لضمان استقرار المجتمعات واستدامة التنمية. وتأتي هذه الدراسة لتسلّط الضوء على الآثار المترتبة على الأمن السيبراني، من خلال تحليل انعكاساته على السلوك الاجتماعي، والنمو الاقتصادي، ولبيان تلك الفجوات القانوني الذي ينظم هذا المجال الحيوي.

ووفقا لتقرير صادر عن شركة Cybersecurity Ventures، من المتوقع أن تصل الخسائر العالمية الناتجة عن الجرائم السيبرانية إلى 10.5تريليون دولار سنويًا ببلوغ هذا العام 2025، مقارنة بـ3 تريليونات فقط في 2015، ما يدل على التسارع الخطير في حجم التهديدات (Cybersecurity Ventures. 2020).

الآثار الاجتماعية والاقتصادية للأمن السيبراني.

تعد هذه الأثار منفردة أو مجتمعة مهدداً أساسياً ويعد الأمن السيبراني عاملاً أساسياً في حماية المجتمعات الحديثة من التهديدات الرقمية المتزايدة، إذ تؤثر الهجمات السيبرانية بشكل مباشر على النسيج الاجتماعي من خلال زعزعة الثقة في المنصات الرقمية، وانتشار الجرائم الإلكترونية مثل الابتزاز والتشهير وسرقة الهوية.

وفي ظل الاعتماد على التكنولوجيا في الحياة اليومية، أصبح لضعف الأمن السيبراني آثار اجتماعية عميقة، تشمل القلق المجتمعي، وانتهاك الخصوصية، وتفكك العلاقات الاجتماعية، مما يستدعي تكامل الجهود لحماية الأفراد والمجتمعات من هذه المخاطر.

المطلب الأول الأثار الاجتماعية (حماية الخصوصية):

إن حماية الخصوصية أبرز الجوانب الاجتماعية المرتبطة بالأمن السيبراني، إذ تمثل الخصوصية الرقمية حقًا أساسيًا للفرد في العصر الرقمي. ومع تزايد استخدام التقنيات الحديثة وتبادل المعلومات عبر الإنترنت، أصبحت البيانات الشخصية عرضة للاختراق والانتهاك، مما يهدد شعور الأفراد بالأمان والثقة في التعاملات الإلكترونية. ويؤدي غياب الضوابط السيبرانية الفعّالة

DOI: https://doi.org/10.61856/krp0q603

إلى انتهاك خصوصيات الأفراد ونشر معلوماتهم الحساسة، ما يترتب عليه آثار نفسية واجتماعية، مثل العزلة والخوف والابتعاد عن الفضاء الرقمي. لذا، يُعد تعزيز حماية الخصوصية من أهم أهداف السياسات السيبرانية لضمان استقرار المجتمع ورفاهه الرقمي. يُساهم الأمن السيبراني في حماية البيانات الشخصية من الاستغلال غير القانوني، ويقوي الثقة بين المستخدمين والتكنولوجيا.

الآثار الاجتماعية العامة للأمن السيبراني:

أصبحت مسألة الأمن السيبراني مرتبطة بشكل وثيق بالحياة الاجتماعية للأفراد، حيث انعكس تطور التهديدات الرقمية على أنماط السلوك والتفاعل داخل المجتمع. فمن ناحية، أدى توفر أنظمة حماية رقمية فعالة إلى شعور عام بطمأنينة أكبر عند استخدام التطبيقات والخدمات الرقمية، لا سيما في قطاعات مثل التعليم، الصحة، والتعاملات البنكية.

الضوابط القانونية والتقنية في تساهم في تقليص فرص استغلال البيانات الشخصية، مما يخفف من حالات الابتزاز الإلكتروني والانتهاكات الأخلاقية المرتبطة بالتشهير أو نشر معلومات خاصة دون إذن.

في المقابل، ما زال غياب التوعية الرقمية الكافية في بعض المجتمعات يولد فجوة معرفية تؤثر على شرائح واسعة من السكان، وتحدّ من قدرتهم على الاستفادة الكاملة من الفرص الرقمية. هذه الفجوة لا تقتصر على الجانب التقني فحسب، بل تمتد إلى شعور بالخوف أو الحذر المفرط أثناء استخدام الوسائل الرقمية، ما قد يضعف من جودة التفاعل الاجتماعي والثقة بين الأفراد.

علاوة على ذلك، فإن زيادة الاعتماد على المنصات الرقمية في الحياة اليومية أعاد تشكيل المفاهيم الاجتماعية التقليدية حول الخصوصية، الرقابة الذاتية، وحدود التعبير، مما يفرض تحديات جديدة أمام الأفراد والمؤسسات في التكيف مع الواقع وفي ضوء ذلك، يمكن تلخيص أبرز الآثار الاجتماعية التي يُحققها الأمن السيبراني في النقاط التالية:

- تعزيز الثقة في التعاملات الرقمية والخدمات الإلكترونية.
- حماية الخصوصية والبيانات الشخصية للأفراد.
- الحد من الجرائم الإلكترونية مثل الابتزاز والتشهير والاحتيال.
- تعزيز وعي الأفراد والمجتمع بأهمية الأمن الرقمي.
- تقليل الفجوة الرقمية من خلال توفير بيئة رقمية آمنة للجميع.
- التأثير على العلاقات الاجتماعية نتيجة الخوف من الاختراقات أو التجسس.

ويُعد الحد من الجرائم الإلكترونية من أبرز هذه الآثار، إذ يسهم الأمن السيبراني بشكل فعّال في التصدي للأنشطة الضارة مثل الاحتيال والتشهير، مما يقلل من انعكاساتها السلبية على الأفراد والمجتمع. ومع ازدياد التهديدات الرقمية، أصبحت الحاجة ملحة إلى تبني أدوات قانونية وتقنية قادرة على حماية الأفراد من الانتهاكات التي تمس خصوصيتهم واستقرارهم الاجتماعي.

ثانياً الأثر الاقتصادي: (التكلفة الاقتصادية)

امتد تأثير الأمن السيبراني إلى الجوانب الاقتصادية بشكل كبير، حيث تُعد الهجمات السيبرانية مصدرًا لخسائر مالية مباشرة وغير مباشرة على الأفراد، والشركات، والدول. فاختراق الأنظمة البنكية، وسرقة البيانات المالية، وتعطيل الخدمات الإلكترونية الحيوية يمكن أن يؤدي إلى شلل اقتصادي مؤقت، وانخفاض ثقة المستثمرين، وتكاليف باهظة لاستعادة الأنظمة وتعويض المتضررين. كما يتطلب تعزيز الأمن السيبراني استثمارات مستمرة في البنية التحتية التقنية والتدريب، مما يجعل الأمن السيبراني عنصرًا محوريًا في الحفاظ على الاستقرار الاقتصادي، وضمان استدامة النمو في البيئة الرقمية المتطورة.

التكاليف الاقتصادية للهجمات السيبرانية:

إن تتسبب التهديدات السيبرانية في آثار متعددة الجوانب. على الصعيد مثلاً القانوني، يؤدي اختراق الأنظمة إلى انتهاك الخصوصية، وتسريب بيانات حساسة قد تشمل معلومات مالية أو صحية، مما يستوجب تحديث الإطار التشريعي بشكل مستمر. أما من الناحية الاجتماعية، فالتعرض المتكرر للهجمات الإلكترونية يخلق مناخًا من انعدام الثقة في الخدمات الرقمية، خاصة إذا ما فشلت الجهات المختصة في توفير الحماية الكافية. كما يؤثر ذلك على الأمن النفسي للمستخدمين، كما في حالة تعرض الأشخاص للابتزاز أو التحرش الإلكتروني. من الجانب الاقتصادي، تفقد الشركات أموالًا طائلة نتيجة للهجمات؛ فوفقًا لتقرير IBM لعام 2023، بلغ متوسط تكلفة اختراق البيانات عالميًا حوالي 4.45مليون دولار لكل حادثة. أما الدول، فتواجه تهديدًا لأمنها القومي، حيث يمكن للهجمات أن تستهدف البنية التحتية الحيوية كشبكات الكهرباء أو الاتصالات (IBM Security. 2023). تؤدي الهجمات الإلكترونية إلى خسائر مالية فادحة للشركات والحكومات، مما يزيد من الحاجة إلى استثمار المزيد في تقنيات الحماية. وهذا مما يدفعنا وجميع المتخصصين إلى زيادة وتقوية الاقتصاد الرقمي في كل المجالات والتي ترتبط بسلسة واحدة وهي الاقتصاد المحلي والإقليمي والعالمي.

وذلك بأن الأمن السيبراني يساهم في خلق بيئة رقمية آمنة تشجع الاستثمار والنمو الاقتصادى محلياً وتفتح الباب للعالم بالتبادل والتداخل التنموي والذي ينتج بدوره عدة مزايا نلخصها في النقاط التالية والتي تساهم في:-

- تقليل الخسائر المالية الناتجة عن الهجمات السيبرانية.
- حماية الاستثمارات في البنية التحتية الرقمية والتقنية.
- تعزيز مناخ الأعمال وزيادة ثقة المستثمرين والعملاء.
- رفع تكلفة تشغيل الأنظمة نتيجة الحاجة المستمرة لتحديث الحماية.
- دفع عجلة الابتكار في مجال تقنيات الأمن السيبراني.

DOI: https://doi.org/10.61856/krp0q603

- التأثير على التجارة الإلكترونية في حال ضعف التدابير الأمنية.

المطلب الثاني: الفجوات التشريعية من خلال أثار الأمن السيبراني

الفضاء الرقمي أوجد تحديات قانونية غير مسبوقة تتعلق بكيفية تنظيم وحماية هذا الفضاء من التهديدات السيبرانية المتزايدة. فقد فرض الأمن السيبراني واقعًا قانونيًا جديدًا يتطلب تطوير أطر تشريعية وتنظيمية قادرة على التعامل مع الجرائم الإلكترونية وتعقيداتها التقنية. كما أثار العديد من الإشكاليات القانونية المتعلقة بتحديد الاختصاص القضائي، وسبل الإثبات الرقمي، وحماية حقوق الأفراد في بيئة غير مادية. ومن هنا، بات الأمن السيبراني لا يقتصر على كونه مسألة تقنية فحسب، بل أصبح أيضًا مسألة قانونية جوهرية تستدعي مراجعة وتحديث القوانين المحلية والدولية بما يتماشى مع التحولات الرقمية.

التشريعات الدولية:

بدأت الدول في إدراك أهمية التشريعات المتعلقة بجرائم المعلوماتية منذ أواخر القرن العشرين، حيث كانت ماليزيا من أوائل الدول التي بادرت إلى سن قانون خاص في هذا المجال، وذلك بإصدار قانون جرائم الحاسوب (Computer Crimes Act) عام 1997، والذي خضع لتعديلات لاحقة لمواكبة التطورات التقنية وأساليب الجريمة الإلكترونية.

أما في العالم العربي، فقد كانت المملكة العربية السعودية من الدول السباقة، حيث أصدرت نظام مكافحة جرائم المعلوماتية عام 2007، وقد صدر هذا النظام عن هيئة الاتصالات وتقنية المعلومات بالتنسيق مع وزارة الداخلية، وشكّل نقلة نوعية في التعامل مع الجرائم الإلكترونية. وفي نفس العام، أصدر السودان أيضًا قانون جرائم المعلوماتية لسنة 2007، وهو قانون متقدم نسبيًا بمقاييس المنطقة، وقد خضع لتعديل لاحق في عام 2020 لمواكبة التحديات الرقمية المتسارعة.

وفي دولة قطر، صدر قانون مكافحة الجرائم الإلكترونية رقم 14 لسنة 2014، والذي يعد من القوانين الحديثة المتقدمة في المنطقة من حيث شموليته وطابعه الردعي، ويساهم في تعزيز الأمن السيبراني الوطني.

أما الأردن، فقد أقر قانون الجرائم الإلكترونية لأول مرة في عام 2015، وتم تعديله في عام 2023، غير أن التعديلات الأخيرة أثارت جدلاً واسعًا بسبب مخاوف من تقييد الحريات العامة وحرية التعبير على الإنترنت.

وفي جمهورية مصر العربية، صدر قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، وهو أول قانون شامل ومفصل في مصر ينظم الجرائم الإلكترونية، ويُعتبر تطورًا تشريعيًا مهمًا يتماشى مع متطلبات البيئة الرقمية الحديثة والجدول التالي يوضح ذلك.

جدول رقم (2): بعض القوانين لمكافحة الجرائم الإلكترونية في بعض الدول العربية والآسيوية

الدولة	اسم القانون	سنة الصدور الأولى	التعديلات
ماليزيا	قانون جرائم الحاسوب(Computer Crimes Act)	1997	تم تعديله لاحقًا عدة مرات
السعودية	نظام مكافحة جرائم المعلوماتية	2007	لا توجد تعديلات رسمية معلنة حتى الآن
السودان	قانون جرائم المعلوماتية	2007	تعديل في عام 2020
قطر	قانون مكافحة الجرائم الإلكترونية رقم 14	2014	لا توجد تعديلات معلنة حتى الآن
الأردن	قانون الجرائم الإلكترونية	2015	تعديل موسّع في عام 2023
مصر	قانون مكافحة جرائم تقنية المعلومات رقم 175	2018	لا توجد تعديلات حتى الآن

التشريعات السودانية:

يُعد السودان واحدًا من الدول التي بدأت تسعى لمواكبة التطورات المتسارعة في مجال الأمن السيبراني، في ظل تصاعد التهديدات الرقمية وتزايد استخدام التكنولوجيا في مختلف جوانب الحياة شهدت البيئة القانونية في السودان محاولات جادة للتصدي للتحديات التي فرضها تطور الفضاء الرقمي وظهور الجرائم السيبرانية، حيث تم سن قانون جرائم المعلوماتية لسنة 2007 وتعديله لاحقًا في عام 2020، بهدف تنظيم استخدام الوسائط الإلكترونية ومكافحة الجرائم التي ترتكب عبر الإنترنت (قانون جرائم المعلوماتية، 2020). ورغم أن هذه التشريعات شكلت خطوة مهمة نحو ضبط السلوك الإلكتروني، إلا أنها لا تزال تعاني من عدة جوانب قصور، أبرزها غياب التعريفات الدقيقة لبعض الجرائم السيبرانية، وضعف العقوبات الرادعة، وافتقارها للتكامل مع المعايير الدولية الحديثة. ومن هنا، تبرز الحاجة إلى تحديث الإطار القانوني السوداني ليواكب التطور التقني السريع، ويحقق التوازن بين حماية الأمن الرقمي وضمان الحقوق والحريات الأساسية للمواطن.

قانون الجرائم المعلوماتية السوداني لعام 2007 يُعد من أوائل المحاولات لتقنين الجرائم الإلكترونية. ومع ذلك، هناك فجوات في التشريع تجعل من الصعب مواجهة التهديدات المعقدة الحديثة مثل الجرائم عبر الحدود.

التشريعات الدولية:

تشكل التشريعات والمعايير الدولية إطارًا ضروريًا لتنظيم وحماية الفضاء السيبراني على المستوى العالمي، نظراً لطبيعة الجرائم السيبرانية العابرة للحدود وتأثيرها الواسع على الأمن والاستقرار الدوليين وتُعد اللائحة العامة لحماية البيانات (GDPR) نموذجًا يحتذى به، حيث تضع معايير صارمة لحماية البيانات وفرض غرامات مالية كبيرة على المخالفين.

التحديات القانونية في مواجهة التهديدات السيبرانية في السودان بالرغم من قدم قانون مكافحة جرائم المعلوماتية نسبياً مقارنة ببقية الدولة لسنة 2007، والذي يُعد خطوة أولى في تنظيم المجال السيبراني، إلا أن هناك فجوة قانونية كغياب آليات التحقيق الرقمي وغياب هيئة أمن سيبراني أو وكالة أو تأسيس صريح لهيئة وطنية تشرف على هذا القانون ومراقبته. وأيضاً عدم إفراد مواد متخصصة لإدارة الأدلة الرقمية أو إجراءات الضبط والتحليل. وفي المادة 5 (فقرة 3) تنص على معاقبة كل من يدخل شبكة

DOI: https://doi.org/10.61856/krp0q603

معلومات أو اتصالات بقصد الحصول على بيانات تتعلق بالأمن القومي، الاقتصاد الوطني، البنية التحتية أو "معلومات حساسة"، بعقوبة تصل إلى 10 سنوات سجن أو غرامة أو كليهما. لكن مصطلحات مثل "الأمن القومي" و"المعلومات الحساسة" غير معرفة، مما يسمح بتأويل واسع وغير محكم أيضا لا تزال تواجه عددًا من التحديات الجوهرية التي تحد من قدرتها على التصدي للتهديدات السيبرانية المتنامية والمعقدة. وتتمثل أبرز هذه التحديات في خمس فجوات رئيسية:

أولًا: فجوة التحديث التشريعي

بالرغم من قدم قانون جرائم المعلوماتية في السودان الذي صدر في العام 2007 وحوى (29) مادة الا أنه يتسم بالجمود مقارنةً بالتطور السريع في أساليب وتقنيات الجريمة السيبرانية وقانون 2018 لم يغطي كافة الجوانب الحديثة وكذا التعريف الدقيق مثل أنواع هجمات الفدية (Ransomware) وهجمات الهندسة الاجتماعية (Social Engineering)، لم يتم تناولها بوضوح في النصوص الحالية، ما يجعل أدوات التجريم والمساءلة القانونية قاصرة عن ملاحقة الجناة في ظل غياب توصيف قانوني دقيق لتلك الأنماط.

ثانيًا: فجوة الشمول:

يركّز التشريع السوداني على المعالجة الجنائية للجرائم الإلكترونية دون أن يُغطي الجوانب الوقائية والتنظيمية، كإلزام المؤسسات بحماية بيانات المستخدمين أو فرض الإفصاح الإجباري عند حدوث خروقات سيبرانية. كما يغيب عن القانون تنظيم المسؤولية المدنية، ما يُضعف من حماية الحقوق الرقمية للأفراد ويقلل من الحوافز المؤسسية للاستثمار في الأمن السيبراني.

ثالثًا: فجوة الإثبات الرقمي:

يُشكّل غياب نظام متكامل للتعامل مع الأدلة الرقمية يقف عائقًا أمام تطبيق العدالة. فلا توجد قواعد إجرائية واضحة لجمع أو حفظ أو تقديم الأدلة السيبرانية أمام المحاكم، مما يُفرز إشكالات عديدة تتعلق بسلامة الإجراءات وشرعية الأدلة، لا سيما في الجرائم التي تتطلب تتبع أنشطة افتراضية دقيقة أو تحليل بيانات عبر بيئات سحابية دولية (إبراهيم قسم السيد، 2021جرائم المعلومات).

رابعاً: فجوة المؤسسات والاختصاص:

لا توجد جهات متخصصة على مستوى أجهزة العدالة السودانية (الشرطة، النيابة، القضاء) تتولى حصريًا التحقيق والبت في القضايا السيبرانية، كما تفتقر الكوادر المعنية إلى التدريب التقني والقانوني اللازم لمواكبة تعقيدات هذا النوع من الجرائم. ويُسهم ذلك في بطء الإجراءات القضائية وضعف الردع العام.

خامسًا: فجوة التعاون الدولي:

الجريمة السيبرانية بطبيعتها لا تعرف حدودًا جغرافية، ما يجعل التعاون الدولي أداة محورية في مكافحتها. ومع ذلك، فإن السودان لم يطور بعد أطرًا قانونية ملائمة أو اتفاقيات ثنائية ومتعددة الأطراف تتيح تبادل المعلومات والتحقيقات المشتركة أو تسليم المتهمين. هذا القصور يُعقّد من فرص تعقب الجناة ويضعف من فعالية ملاحقتهم.

الإجراءات العامة في الأنظمة القضائية

أولًا: التبليغ/الشكوى: تقديم البلاغ إلى النيابة العامة أو الشرطة المتخصصة، مصحوبًا بأدلة رقمية مثل رسائل، عناوين IP، أو تسجيلات.

ثانيًا: التحقيق الفني والجنائي: يقوم خبراء الأدلة الرقمية بإجراء فحص فني للجهاز أو الحساب لإنشاء تقرير Forensic Report .

ثالثًا توجيه التهمة: النيابة تصدر لائحة اتهام بناءً على الأدلة والمواد القانونية ذات الصلة.

رابعًا: الإحالة للمحكمة: تُحال القضية إلى المحكمة المختصة (جنائية أو متخصصة).

خامسًا: المحاكمة: تشمل جلسات استماع للشهود، تقييم الأدلة الرقمية، والمرافعات القانونية.

سادسًا: الحكم والاستئناف: يصدر الحكم وقد يُستأنف أمام محكمة أعلى درجة.

الإجراءات المتبعة في السودان – قانون مكافحة جرائم المعلوماتية (2018/2020)

الجهات والإجراءات:

1. التحقيق: بواسطة "إدارة مكافحة جرائم المعلومات"، مع طلب تقارير فنية من هيئة الاتصالات أو خبراء مستقلين.
2. النيابة: نيابة جرائم المعلوماتية تختص بتوجيه الاتهامات.
3. المحاكم: تُنظر القضايا في المحاكم الجنائية العامة؛ لا توجد محاكم متخصصة.

إذا لا توجد مواد خاصة بالتقاضي الإلكتروني داخل قانون الإجراءات الجنائية (1991).

- غياب محاكم ونيابات مدربة على الأدلة الرقمية.
- بطء الإجراءات بسبب ضعف المعدات والتنسيق الفني.

وبالمقابل الإجراءات المتبعة في دولة قطر – قانون الجرائم الإلكترونية رقم 14 لسنة 2014.

الجهات والإجراءات:

1. التحقيق: يتم عبر قسم الجرائم الإلكترونية التابعة لوزارة الداخلية.
2. النيابة: توجد نيابة متخصصة مختصة بالجرائم الرقمية.
3. المحاكم: يستقبل القضاء القطري الأدلة الرقمية بشروط التوثيق الرسمي.

يوجد إطار قانوني متكاملا أي أن قانون الإجراءات الجنائية ينص في الفصل الثالث (المادة 14 وما بعدها) على إجراءات التحقيق الرقمي، حفظ الأدلة، التعاون مع مزودي الخدمة، والتوثيق ...الخ.

DOI: https://doi.org/10.61856/krp0q603

جدول يوضح ملخص الفجوة التشريعية بين التشريع السوداني والتشريع القطري من ناحية الإجراءات المتبعة والاختصاص القضائي والمؤسسي والكوادر والسند التشريعي لذلك وفق الجدول أدناه.

جدول رقم (3): الفجوات التشريعية بين التشريع السوداني والقطري

العنصر	السودان (2018/2020)	قطر (2014)
نصوص خاصة بالإجراءات	غياب مواد إجرائية واضحة في قانون 1991؛ لا اختصاص قضائي إلكتروني.	مواد متخصصة تحدد آليات التحقيق الرقمي (المادة 14–20)
الاختصاص المؤسسي	نيابة عامة وعدد محدود من التحقيقات التقنية.	وجود نيابة وقضاء متخصّص واعتماد على توثيق الأدلة رسميًا
الكادر الفني	محدود ومفتقر لتدريب منهجي في الأدلة الرقمية.	كوادر مؤهلة ضمن وزارة الداخلية ويطبقون إجراءات معيارية.
السند التشريعي	نقص في ربط التشريع التقني بقانون الإجراءات.	تنظيم متكامل بين القانون والإجراءات القضائية والفنية.

تُبيّن هذه التحديات أن الإصلاح القانوني في مجال الأمن السيبراني يجب أن يكون شاملًا ومترابطًا، بحيث لا يقتصر على تعديل القوانين، بل يشمل بناء مؤسسات متخصصة، ورفع كفاءة الكوادر، وتطوير آليات الإثبات والتعاون الدولي، لضمان بيئة رقمية أكثر أمانًا وعدالة.

1. نقص التشريعات المحدثة: لا تزال جزء من القوانين السودانية غير مهيأة لمواكبة التطورات التكنولوجية. بالإضافة إلى ضعف التعاون الدولي خاصة أن معظم أو غالب الجرائم السيبرانية ما تكون عابرة للحدود وهذا يستدعي تعاونًا دوليًا أوسع واحداث اتفاقيات جديدة.

المبحث الثالث: تحقيق الأمن السيبراني من خلال التشريع السوداني والقطري

إن دراسة النظم في ضوء المعايير الدولية من القضايا الأساسية لفهم الفجوات، ولذلك تأتي أهمية المقارنة بين التشريع السوداني والنظام الدولي، لا سيما عند النظر في تجربة ناجحة مثل دولة قطر، التي حققت تقدمًا ملحوظًا في مواءمة سياساتها القانونية خاصة في حماية البيانات الشخصية حيث وضعت قطر إطارًا قانونيًا متكامًلا يشمل قانون حماية البيانات الشخصية (2016)، واستحدثت مؤسسات متخصصة مثل وزارة الاتصالات وتقنية المعلومات ووحدة الاستجابة للطوارئ السيبرانية (Qatar Computer Emergency Response Team) (Q-CERT). وممارساتها مع المعايير الدولية (قانون حماية الخصوصية والبيانات الشخصية، قطر: 2016).

وتفتح هذه المقارنة المجال لتحليل أوجه التشابه والاختلاف، وتسليط الضوء على التحديات والإمكانات في سبيل تحقيق التكامل مع الأطر العالمية. فنجد أن القانون السوداني يُركز على العقوبات الجنائية، بينما تتبنى التشريعات الدولية لوائح مثل اللائحة العامة لحماية البيانات والتي تعرف اختصارًا (GDPR) وهي تشريع أوروبي صدر في مايو 2018 من قبل الاتحاد الأوروبي لتنظيم كيفية جمع واستخدام وتخزين البيانات الشخصية للأفراد داخل دول الاتحاد الأوروبي، ويُعد من أقوى وأشمل القوانين في العالم في مجال حماية الخصوصية الرقمية بحيث أن تنتهج نهجًا شاملًا يشمل الوقاية والحماية، بالرغم من ذلك إلا أن السودان يحتاج إلى تشريعات مخصصة لحماية البيانات الشخصية، مما يعرض الأفراد والشركات لمزيد من المخاطر وبالتفصيل في المقارنة التالية.

المطلب الأول مقارنة التشريعات مقارنة بين القانون السوداني والقطري في مكافحة الجرائم الإلكترونية

1. حداثة التشريع وتحديثه

السودان: صدر قانون جرائم المعلوماتية في عام 2007، ومن ثم ألغي في المادة 2 من قانون 2018 على أن تظل جميع القواعد والأوامر التي صدرت بموجبه سارية إلى أن تلغى وتعدل ((إبراهيم قسم السيد-قانون جرائم المعلومات، 2021:). ليحل بديله قانون 2018 المعدل 2020م ومن الملاحظ أنه أضاف كلمة (مكافحة)، القانون الأول يسمى قانون جرائم المعلوماتية والأخير أصبح قانون مكافحة جرائم العلوماتية ومنذ ذلك الحين لم يشهد تحديثات جوهرية، مما يجعله غير مواكب للتطورات السريعة في مجال الجرائم الإلكترونية، مثل الهجمات باستخدام الذكاء الاصطناعي أو العملات الرقمية .

قطر: أصدرت قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، والذي يُعتبر أكثر حداثةً وشمولًا حيث يتضمن فصولًا متعددة تغطي مختلف أنواع الجرائم الإلكترونية، بما في ذلك التعدي على أنظمة المعلومات، جرائم المحتوى، التزوير والاحتيال الإلكتروني، وجرائم بطاقات التعامل الإلكتروني (قانون مكافحة الجرائم الإلكترونية بقطر، 2014).

2. شمولية النصوص القانونية

السودان :يركز القانون السوداني بشكل أساسي على الجانب الجنائي، مع غياب واضح للتنظيمات المتعلقة بحماية البيانات الشخصية، والإفصاح الإجباري عن الخروقات الأمنية، والمسؤولية المدنية للمؤسسات .

قطر: يتضمن القانون القطري مواد تنظم حماية البيانات، مثل المادة (2) التي تُلزم مزودي الخدمة بالحفاظ على سرية المعلومات، والمادة (23) التي تنص على التعاون الدولي في العقوبات والردع

DOI: https://doi.org/10.61856/krp0q603

في السودان أذا أخذنا نموذج للمادة (7) إيقاف شبكات المعلومات أو الاتصالات ونظم المعلومات وقواعد البيانات وتعطيلها فإن: العقوبات في القانون السوداني تتراوح بين الغرامات والسجن (8 سنوات) في حالة الاتلاف أو الدخول غير المصرح لقواعد البيانات أو الحذف أو ايقافها أو تعطيله أو تدمير البرامج ولا تتجاوز الـ (20 عامًا) اذا كانت تمس الأمن القومي، لكنها قد لا تكون رادعة بما يكفي في ظل تطور أساليب الجرائم الإلكترونية، خاصة في جانب الغرامة الذي ترك لتقدير المحكمة وهذا في تقديرنا بعدم تحديد حد أدنى أو أقصى للغرامات في النصوص بشكل واضح يضعف من فعالية الردع المالي.
أما في قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014، تعالج المادة (6) والمادة (7) حالات مشابهة، وتنص على ما يلي:
من يتعمد تعطيل شبكة معلوماتية أو الدخول غير المشروع أو إتلاف البيانات أو حذفها أو تعديلها، يعاقب: بالسجن لمدة لا تقل عن سنة ولا تتجاوز 10 سنوات، وبغرامة لا تقل عن 200,000 ريال قطري ولا تتجاوز 500,000 ريال قطري.

- أما إذا استهدف الفعل نظمًا معلوماتية تخص الأمن القومي أو المصالح العليا للدولة:

العقوبة تصل إلى السجن المؤبد.

التعاون الدولي:

السودان: لا يتضمن القانون السوداني نصوصًا واضحة تسهل التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، مما يُعيق ملاحقة الجناة عبر الحدود .
قطر: تنص المادة (23) من القانون القطري على التعاون الدولي، مما يُعزز من قدرة الدولة على ملاحقة الجرائم الإلكترونية ذات الطابع العابر للحدود.
الجدول التالي يوضح أوجه المقارنة وإيجاد الفجوات وفق المحاور المبية أدناه:

الجدول رقم (4): مقارنة بين القانون السوداني والقطري في مكافحة الجرائم الإلكترونية

المحور	النظام القطـــــري	النظام السوداني
حداثة التشريع وتحديثه	أصدر قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، حديث وشامل، يغطي أنواع متعددة من الجرائم الإلكترونية.	صدر قانون مكافحة الجرائم الإلكترونيةلأول مرة 2007 وعدل 2018 وملحق 2020 ، بدون تحديثات جوهرية، وغير مواكب للتطورات الحديثة والأمن السيبراني كالذكاء الاصطناعي والعملات الرقمية.
شمولية النصوص القانونية	يتضمن مواد لحماية البيانات (مثل الحفاظ على سرية المعلومات)، ويشمل نصوصًا للتعاون الدولي في مكافحة الجرائم.	يركز على العقوبات الجنائية، ويفتقر لتنظيم حماية البيانات الشخصية، وعدم وجود إفصاح إجباري عن الخروقات أو مسؤولية مدنية واضحة.
العقوبات والردع	عقوبات صارمة، مثل الحبس حتى 10 سنوات وغرامات تصل إلى 500,000 ريال قطري، خاصة في الجرائم التي تهدد الأمن الوطني.	عقوبات بين غرامات وسجن، لكنها قد لا تكون رادعة كفاية في ظل تطور الجرائم الإلكترونية لترك التحديد المالي لتقديرات المحكمة.
.التعاون الدولي	ينص على التعاون الدولي بشكل واضح، مما يعزز قدرة الدولة على مواجهة الجرائم الإلكترونية العابرة للحدود.	لا يحتوي على نصوص واضحة تسهل التعاون الدولي، مما يعيق ملاحقة الجناة عبر الحدود.
الإجراءات والإثبات	يستند في الإجراءات والإثبات على قانون الإجراءات الجنائية	يستند في الإجراءات والإثباتات1994-1991 على قانون الإجراءات الجنائية
عدد المواد	54 مادة	29مادة لأول مرة في ومن ثم عدلت 48 مادة+ ملحق

بالرغم من أقدمية التشريع السوداني يُظهر القانون القطري تقدمًا ملحوظًا في مواكبة التحديات الحديثة للجرائم الإلكترونية من خلال تحديث التشريعات، شمولية النصوص، فرض عقوبات رادعة، وتعزيز التعاون الدولي. في المقابل، يحتاج القانون السوداني إلى مراجعة شاملة لتحديثه وتوسيعه ليشمل الجوانب التنظيمية والوقائية، بالإضافة إلى تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية بفعالية .
ويرى الباحث من خلال دراسته هذه أن الفجوات التشريعية القائمة تمثل عائقًا رئيسيًا أمام جهود مكافحة الجريمة السيبرانية في السودان، وأن هذه الفجوات تتداخل مع تحديات مجتمعية واقتصادية وسياسية تؤثر سلبًا على فعالية الاستجابة الوطنية. كما يؤكد الباحث أن سد هذه الفجوات من خلال تطوير تشريعات متينة وفعالة، ذات قدرات رادعة، يعد خطوة ضرورية لتحويل التحديات إلى فرص حقيقية تعود بالنفع على المجتمع والاقتصاد والسياسة. فبتطبيق هذه التشريعات الحديثة، يمكن تعزيز الثقة في البيئة الرقمية، وتحقيق استقرار اقتصادي أكبر، وتعزيز التعاون الدولي، مما يجعل الأمن السيبراني ركيزة أساسية للتنمية المستدامة.
الخاتمة: في ضوء ما تناولته هذه الدراسة، تبيّن أن الأمن السيبراني يمثل قضية متعددة الأبعاد تتجاوز الجوانب التقنية لتشمل آثارًا قانونية، اجتماعية واقتصادية واضحة. وقد أظهرت نتائج البحث وجود ثغرات قانونية في الإطار التشريعي السوداني تُضعف من قدرته على التصدي للتحديات الناشئة عن تطور الجرائم الإلكترونية، بالرغم من بعض المحاولات التشريعية كقانون مكافحة الجرائم المعلوماتية لسنة 2018، وقد أظهرت المقارنة مع المعايير الدولية، وعلى رأسها اللائحة الاوربية العامة لحماية البيانات (GDPR)، أهمية تبني نموذج تشريعي أكثر حداثةً وشمولًا، يستند إلى مبادئ حماية الخصوصية وحقوق الأفراد، ويعزز من قدرة الدولة على الاستجابة للتهديدات السيبرانية ذات الطابع العابر للحدود. وبناءً على ما تقدم، فإن تعزيز منظومة الأمن السيبراني يتطلب نهجًا تكامليًا يجمع بين التشريع الفعّال ليسهم في حماية الفضاء الرقمي وضمان أمن واستقرار المجتمع والدولة.

DOI: https://doi.org/10.61856/krp0q603

النتائج:

1. وجود فجوات في التشريعات السودانية: القوانين السودانية غير مهيأة لمواكبة التهديدات السيبرانية المعقدة.
2. نقص التعاون الدولي في مكافحة الجرائم السيبرانية: الجرائم السيبرانية غالبًا ما تكون عابرة للحدود وتحتاج إلى استجابة منسقة بين الدول.
3. عدم وجود تشريعات مخصصة لحماية البيانات الشخصية: عدم وجود قوانين لحماية البيانات يجعل الأفراد والشركات عرضة للمخاطر.
4. عدم كفاية التشريعات في مواجهة الجرائم السيبرانية الحديثة: التشريعات الحالية تركز على العقوبات الجنائية فقط دون التعامل مع الوقاية والتوعية.
5. أظهرت الدراسة أن الجرائم السيبرانية ذات طبيعة عابرة للحدود، وأن غياب التنسيق الدولي والإقليمي وضعف تبادل المعلومات والخبرات بين الدول يحدّ من فعالية الجهود الوطنية في مكافحتها.
6. الافتقار إلى تدريب الكوادر القانونية: عدم تدريب القضاة والمحامين على التعامل مع الجرائم السيبرانية.

التوصيات:

1. تحديث التشريعات الوطنية: مراجعة القوانين السودانية لتشمل جرائم سيبرانية معقدة مثل القرصنة العابرة للحدود.
2. تقوية التعاون الدولي: إنشاء اتفاقيات إقليمية ودولية لمكافحة الجرائم السيبرانية.
3. تشريع حماية البيانات الشخصية: تطوير قوانين لحماية البيانات الشخصية وتوفير آليات قانونية لحمايتها.
4. زيادة التشريعات الوقائية: تبني نهج شامل يتضمن الوقاية، الحماية، والعقوبات.
5. ضرورة تعزيز الشراكات الدولية والإقليمية لتبادل المعلومات والخبرات، وتوسيع نطاق التعاون في مجال مكافحة الجرائم السيبرانية عبر الحدود، بما يضمن مواجهة فعّالة للتحديات الأمنية المشتركة الناتجة عن الطابع العابر للحدود لهذه الجرائم
6. تدريب الكوادر القانونية: تدريب القضاة والمحامين على التعامل مع الجرائم السيبرانية وتعريفهم بأحدث التقنيات.

References

Al-Qur’ān al-Karīm

Al-Ḥay’ah al-‘Āmmah li-al-Isti‘lālāt. (2018). Qānūn mukāfaḥat jarā’im taqniyyat al-ma‘lūmāt raqm 175 li-sanat 2018. Jumhūrīyah Miṣr al-‘Arabīyah. Retrieved from https://www.cc.gov.eg/

Al-Mamlakah al-‘Arabīyah al-Su‘ūdīyah. Retrieved from https://laws.boe.gov.sa/

Al-Mamlakah al-Urdunīyah al-Hāshimīyah. Retrieved from http://www.lob.jo/

Al-Qānūn al-jarā’im al-ma‘lūmātiyyah al-Sūdānī li-‘ām 2007. (D.T). Madwanat al-Duktur Ibrāhīm Qism al-Sayyid li-al-Dirāsāt wa-al-Buḥūth al-Qānūniyyah.

Al-Qur’ān al-Karīm. (D.T).

Aziz, S. (2024). Impact of cybercrime legislation on cybersecurity measures in financial institutions in Pakistan. *American Journal of Law*, 6(2), 23–33. Retrieved from https://ajpojournals.org/journals/AJL/article/view/2302/2973

Bawwābah Ḥukumī. (2014). Qānūn raqm (14) li-sanat 2014 bi-sha’n mukāfaḥat al-jarā’im al-iliktrūniyyah. Dawlat Qaṭar. Retrieved from https://www.almeezan.qa/LawPage.aspx?id=6366&language=ar

Cybereason. (2022). *Cybersecurity Losses & Trends 2022: A Global Perspective*. Retrieved from https://www.cybereason.com

DOI: https://doi.org/10.61856/krp0q603

Dīwān al-Tashrīʿ wa-al-Raʾy. (2015, 2023). Qānūn al-jarāʾim al-iliktrūniyyah wa-taʿdīlātuhā. Al-Sūdān.

European Union. (2016). *General Data Protection Regulation (GDPR)*. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fortinet. (2021). *Cybersecurity Threat Landscape*. Retrieved from https://www.fortinet.com

Government of Malaysia. (1997). *Computer Crimes Act 1997*. Retrieved from https://www.cljlaw.com/public/bills/act563.pdf

Hayʾat al-Khubarāʾ bi-Majlis al-Wuzarāʾ. (2007). Niẓām mukāfaḥat jarāʾim al-maʿlūmātiyyah. Al-Mamlakah al-ʿArabīyah al-Suʿūdīyah.

Khan, H., Shabbir, S. S., Ali, A., & Qureshi, A. N. (2024). Revamping cybercrime laws in Pakistan: A comparative analysis of Pakistan and United Kingdom. *International Journal of Human and Society*, 4(1). Retrieved from https://ijhs.com.pk/index.php/IJHS/article/view/523

Kshetri, N. (2017). *Cybercrime and cybersecurity in the global South*. Palgrave Macmillan.

Montesquieu. (1750). *Rūḥ al-qawānīn* (ṭ. 2).

Sharaf, Aḥmad. (2021). *Mafāhīm fī al-amn al-saybarnī*. Dār al-Fikr al-Jāmiʿī, al-Iskandarīyah.

Stallings, W., & Brown, L. (2018). *Cybersecurity: Principles and Practice* (2nd ed.).

Statista. (2021). *Cybercrime: Estimated Global Damage Due to Cybercrime from 2020 to 2025*. Retrieved from https://www.statista.com

The World Economic Forum. (2022). *The Global Risks Report 2022*. Retrieved from https://www.weforum.org

United Nations. (2020). *Cybersecurity and its Economic Impact*. Retrieved from https://www.un.org

Wizārat al-ʿAdl al-Sūdānīyah. (2007, 2020). Qānūn jarāʾim al-maʿlūmātiyyah wa-taʿdīlihā. Al-Sūdān.