مواجهة الجرائم السيبرانية: دراسة مقارنة للقانونَيْن القطري والألماني

النقيب/ عبد الله أحمد السبيعي
باحث أمني وخبير في مجال التدريب، وزارة الداخلية - دولة قطر

النقيب/ حمد عبد الرحمن النصر
باحث أمني، وزارة الداخلية - دولة قطر

مواجهة الجرائم السيبرانية: دراسة مقارنة للقانونَيْن القطري والألماني

النقيب/ عبد الله أحمد السبيعي
باحث أمني وخبير في مجال التدريب، وزارة الداخلية – دولة قطر

النقيب/ حمد عبد الرحمن النصر
باحث أمني، وزارة الداخلية – دولة قطر

المُلخَّص

تستهدف هذه الدراسة تحليل الإطار التشريعي لمواجهة الجرائم السيبرانية من خلال مقارنة تفصيلية بين التشريعين القطري والألماني، استنادًا إلى منهج تحليلي مقارن يركز على النصوص، والتجريم، والتدابير القضائية، وقد ارتكز التحليل على قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014، وقانون العقوبات الألماني (StGB)، ولا سيما المواد (202a – 303b). وقد أظهرت الدراسة توافق النظامين في تجريم أفعال مثل الدخول غير المصرح به، والتجسس، والتلاعب بالبيانات، مع تشديد العقوبة في حال تعلقها بالأمن الوطني أو البنى التحتية الحيوية.

إلا أن التشريع الألماني يمتاز بتفصيل بنيوي يخصص مادة مستقلة لكل صورة جرمية، ويجرم الأفعال التحضيرية صراحةً، ويوفر آليات مرنة للعقوبة (مثل الغرامات اليومية المرتبطة بالدخل). وبالمقابل يجمع القانون القطري عدة أفعال في مواد موحدة ذات صياغة عامة، ويعتمد نظام عقوبات ثابت لا يراعي اختلاف السياقات، كما كشف التحليل عن تفاوت في آليات التعاون الدولي، حيث تعد ألمانيا طرفًا فاعلًا في اتفاقية بودابست، بينما لم تلتحق بها قطر رغم إدراج بعض أحكام التعاون في قانونها.

وتوصي الدراسة بضرورة مراجعة الصياغة التشريعية القطرية لتفصيل الأفعال وتوسيع نطاق التجريم ليشمل الأفعال التحضيرية، وتبني نظام غرامات أكثر مرونة، وتعزيز البنية المؤسسية للتحقيق في الجرائم الرقمية، والانضمام إلى الأطر الدولية ذات الصلة، كما تبرز أهمية إرفاق التوعية المجتمعية الرقمية بهذه التعديلات؛ لضمان تفعيل حماية سيبرانية شاملة تستجيب لطبيعة الجريمة الحديثة.

الكلمات المفتاحية: الجرائم السيبرانية، التشريع القطري، التشريع الألماني، التدابير التشريعية، القانون المقارن.

ABSTRACT

Cybercrime Confrontation: A Comparative Study of Qatari and German Laws

Captain\ ABDULLA AHMED AL-SUBAIEY
Security Researcher and Training Expert, Ministry of Interior – State of Qatar

Captain\ HAMAD ABDULRAHMAN AL-NASR
Security Researcher, Ministry of Interior – State of Qatar

This study aims to analyze the Legislative Framework for Combating Cybercrime through a detailed comparison between Qatari and German legislations, using an analytical comparative methodology focused on legal texts, criminalization mechanisms, and judicial measures. The analysis centers on the Qatari Cybercrime Law No. (14) of 2014 and the relevant provisions of the German Criminal Code (StGB), particularly Sections 202a–303b. The findings reveal convergence in both systems regarding the criminalization of unauthorized access, espionage, and data manipulation, with stricter penalties when national security or critical infrastructure is affected.

However, the German legislation is characterized by a structurally detailed approach, dedicating separate provisions to each type of offense, explicitly criminalizing preparatory acts, and adopting a flexible sentencing model such as income-based daily fines (Tagessätze). In contrast, the Qatari law consolidates multiple offenses into broadly formulated articles and applies fixed penalties that lack contextual flexibility. The study also highlights disparities in international cooperation mechanisms, with Germany being an active party to the Budapest Convention, unlike Qatar, which—despite referencing cooperation—has not yet acceded to the treaty.

The study recommends revising the Qatari legal provisions to disaggregate offenses, expand the scope of criminalization to include preparatory acts, adopt a more flexible penalty system, enhance institutional capacity for digital investigations, and accede to relevant international frameworks. It also emphasizes the need for digital public awareness programs to complement legislative reform and ensure an effective, integrated cybersecurity response.

Keywords: Cyber-crime; Qatari legislation; German legislation; Legislative measures; Comparative law.

المقدمة

أضحت الجرائم السيبرانية في الوقت الحالي واحدةً من أبرز التحديات التي تواجه المجتمعات المعاصرة، بسبب الاعتماد المتنامي على التكنولوجيا الرقمية وما يرافقها من احتمالات متزايدة لاختراق الأنظمة، وسرقة البيانات الشخصية، والاحتيال المالي عبر الإنترنت، فضلاً عن الابتزاز والإساءات الرقمية، وتتسم هذه الجرائم بسرعة تنفيذها وافتقارها للأدلة المادية التقليدية، مما يعقد مسار التحقيق ويزيد من صعوبة ملاحقة مرتكبيها قانونيًا.

وفي ضوء هذه التحديات، تجد الدول نفسها أمام ضرورة مُلِحَّة لتبني تشريعات حديثة قادرة على مجاراة التطورات التقنية المتسارعة، وتوفير حماية فعالة للأفراد والمؤسسات، وتجسّد دولة قطر نموذجاً بارزاً في هذا السياق، اتساقاً مع رؤية قطر الوطنية 2030 التي تمنح التحول الرقمي أولوية استراتيجية، بالتوازي مع تطوير منظومتها القانونية لمجابهة التهديدات السيبرانية وتعزيز الأمن المعلوماتي.

وعلى الجانب الآخر، تعد جمهورية ألمانيا الاتحادية رائدةً في صياغة تشريعات متكاملة لحماية الفضاء السيبراني، مستندةً إلى قوانين وإجراءات صارمة تستهدف الحد من الاعتداءات الإلكترونية على الأفراد والبنى التحتية الرقمية.

وتستهدف الدراسة إجراء مقارنة بين التشريعات القطرية والألمانية في مجال الجرائم السيبرانية، من خلال تحليل قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014، والمواد ذات الصلة في قانون العقوبات الألماني (StGB)، بالتركيز على الأطر القانونية والإجراءات المتبعة في التصدي لجرائم الاعتداء على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، ولذلك تعتمد الدراسة منهجًا تحليليًا مقارنًا يستند إلى تحليل النصوص القانونية ومقارنتها من حيث التجريم، والعقوبة، والتدابير المؤسسية.

وإلى جانب تسليط الضوء على أوجه التوافق والاختلاف في معالجة هذه الجرائم، تبحث الدراسة في التحديات المشتركة التي تواجه النظامين القانونيين عند تطبيق التشريعات على هذا النمط الحديث من الجرائم، كما تسعى الدراسة إلى تقديم توصيات تشريعية عملية مستندة إلى التجارب المقارنة، بما يعزز قدرة المنظومات القانونية على مواجهة هذا النمط المتطور من الجرائم محليًا ودوليًا.

مشكلة الدراسة

مع تطور أشكال الجريمة السيبرانية وازدياد اعتماد الدول على الفضاء الرقمي، أصبحت الحاجة إلى تشريعات فعالة أمرًا مُلِحًّا؛ لضمان الحماية القانونية من الاعتداءات على الأنظمة والشبكات والبيانات الإلكترونية، وتطرح هذه المتغيرات القانونية تحديًا خاصًا فيما يتعلق بكفاية التشريعات الوطنية، ومدى قدرتها على مواكبة التطور التقني، وضمان التنسيق الدولي في مواجهة هذا النمط من الجرائم، وفي هذا السياق تطرح الإشكالية الآتية:

إلى أي مدى يوفر الإطار التشريعي القطري استجابة قانونية فعالة لمواجهة الجرائم السيبرانية، مقارنةً بالتشريع الألماني، من حيث التجريم والتنظيم القانوني والتدابير المرافقة؟

ويتفرع عن هذه الإشكالية الرئيسة السؤالان الآتيان:

1. ما أوجه الشبه والاختلاف بين التشريعين القطري والألماني في تجريم الاعتداء على أنظمة وشبكات المعلومات والمواقع الإلكترونية؟
2. ما أبرز التدابير التشريعية والتدابير القانونية التي يواجهها كل نظام في مواجهة الجرائم السيبرانية؟

أهمية الدراسة

تبرز أهمية هذه الدراسة من عدة أوجه مترابطة؛ إذ تتناول موضوعًا قانونيًا معاصرًا يكتسب أولوية متصاعدة في ظل تنامي الجرائم السيبرانية وتطور أساليبها، مما يستدعي مراجعة التشريعات الوطنية لضمان فاعلية الحماية القانونية، وتزداد أهمية ذلك في دولة قطر، حيث لم يخضع قانون الجرائم الإلكترونية رقم (14) لسنة 2014 لمراجعة هيكلية منذ صدوره، رغم التغيرات التقنية المتسارعة واتساع نطاق الفضاء الرقمي. وتستمد الدراسة أهميتها من تقديمها مقاربة تحليلية مقارنة مع القانون الألماني، الذي يعد من أكثر النماذج تطورًا في مجال التجريم السيبراني وتفصيل الأفعال ومرونة العقوبة، بما يتيح استكشاف بدائل تشريعية قابلة للتكييف في البيئة القطرية.

وتحاول الدراسة ملء الفجوة العلمية في الأدبيات القانونية العربية؛ نظرًا لندرة البحوث المحلية التي تناولت الجرائم السيبرانية في إطار مقارن دقيق يوازن بين بنية النصوص، وفعالية التطبيق، وواقع الممارسات التشريعية، وتنبع أهمية هذا العمل من أثره المحتمل على تطوير السياسة الجنائية الرقمية، وتعزيز البنية القانونية في قطر بما يتماشى مع مقتضيات الأمن السيبراني، ويعزز من التكامل التشريعي مع المعايير الدولية، دون الإخلال بالخصوصية القانونية والسيادية للدولة.

أهداف الدراسة

تسعى هذه الدراسة إلى تحقيق الأهداف الآتية، انسجامًا مع الإشكالية المطروحة ومنهج المقارنة القانونية:

1. تحليل نطاق التجريم في القانونين القطري والألماني، وتحديد صور الأفعال المجرمة ذات الصلة بالاعتداء على الأنظمة، والبيانات، والشبكات الإلكترونية.
2. تقييم مدى فاعلية العقوبات والإجراءات القانونية المصاحبة في كل من التشريعين، من حيث الردع والتناسب.
3. تحديد أوجه القصور في التشريع القطري، ولا سيما في ما يتعلق بتجريم الأفعال التحضيرية وحماية البيانات الحساسة.
4. صياغة توصيات تشريعية عملية وقابلة للتنفيذ تستند إلى المقارنة القانونية، بهدف دعم تطوير السياسات القانونية المتعلقة بالأمن السيبراني في قطر.
5. إبراز أوجه التشابه والاختلاف بين النظامين القانونيين القطري والألماني في المعالجة التشريعية للجرائم السيبرانية، بما يوفر إطارًا مرجعيًا للتقييم والتطوير.

منهجية الدراسة

اعتمدت هذه الدراسة على المنهج التحليلي المقارن في تحليل النصوص التشريعية من حيث البناء والصياغة والمضمون، وتكمن خصوصية هذا المنهج في قدرته على تفكيك النصوص القانونية واستقراء مضامينها، ثم مقارنتها ضمن سياقين تشريعيين مختلفين، مما يتيح إمكانية الكشف عن الفروق الجوهرية في أساليب التجريم والعقاب والتنظيم القانوني.

وقد استخدم هذا المنهج في فحص وتحليل قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014، ومقارنته تفصيلاً مع المواد ذات الصلة في قانون العقوبات الألماني (StGB)، وتحديدًا المواد (202a–303b)، وذلك من حيث: نطاق التجريم، ودقة الصياغة، وتوزيع الأفعال الجرمية، ومرونة العقوبات، ومدى شمول التدابير التشريعية المصاحبة.

ويعد هذا المنهج مناسبًا لطبيعة الدراسة المقارنة، حيث يوفر أدوات علمية منهجية لقياس مدى اتساق القواعد القانونية في النظامين، ومدى فاعلية كل منهما في تحقيق الردع والحماية الرقمية. كما يسهم في تحديد مكامن القوة والقصور من منظور بنيوي وتحليلي، ويوفر خلفية معرفية دقيقة تعزز مصداقية التوصيات التشريعية المقترحة لاحقًا في ضوء نتائج التحليل.

ومن خلال هذا المنهج، سعت الدراسة إلى تجاوز التحليل السردي التقليدي، والانتقال إلى قراءة نقدية تقوم النصوص القانونية محل البحث من حيث مدى مواكبتها للواقع الرقمي، وقدرتها على التعامل مع التحديات المستجدة التي تفرضها الجرائم السيبرانية في السياقين المحلي والدولي على السواء.

الدراسات السابقة والتعقيب عليها

أولاً: منهجية عرض الدراسات

اعتمدت الدراسة على ثلاث ركائز لاختيار الدراسات السابقة وطريقة عرضها:

1. الحداثة الزمنية من (2014–2022) ؛ لضمان مواكبة التطور التشريعي والتقني.
2. تنوع المحاور (إطار جنائي مقارن | سياسات وقائية | تعاون دولي) حتى تغطي الأبعاد الرئيسة لمشكلة البحث.
3. الصلة المباشرة بموضوع الدراسة؛ أي معالجة قصور التشريعات العربية أو الخليجية في مواجهة جرائم التعدي على الأنظمة المعلوماتية، وهو محور بحثنا المقارن (قطري–ألماني).

ثانيًا: عرض مركز لأهم الدراسات السابقة

بناءً على معايير الحداثة الزمنية، وتنوع المحاور، وصلتها المباشرة بمشكلة البحث، تم اختيار ست دراسات أساسية يمكن تلخيصها على النحو الآتي:

1. دراسة «القرصنة السيبرانية: بناء إطار قانوني جنائي منسق لمعالجة القرصنة الإلكترونية في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: دراسة مقارنة بين القوانين الإلكترونية الأردنية والسعودية» [1]: (2019) تعالج أوجه القصور في معاقبة القرصنة داخل التشريعات الأردنية والسعودية، وتقترح معايير موحدة لعقوبات متدرجة تستلهم اتفاقية بودابست، كما تكشف نتائجها حاجة الاتفاقية العربية إلى تعديلات تمس تعريف عناصر الجريمة وآليات ضبط الأدلة الرقمية. هذه الخلاصة تدعم توصيات بحثنا بتفكيك المادة (3) من القانون القطري وتبني مقاربة معيارية أقرب إلى النموذج الأوروبي.

(1) A. Saqf Al Hait, Cyber Hacking: Building a Harmonised Criminal Legal Framework for Addressing Cyber Hacking in the Arab Convention on Combating Information Technology Offences: A Comparative Study between Jordanian & Saudi Cyber Laws (Doctoral dissertation, Anglia Ruskin Research Online (ARRO), 2023).

2. دراسة «الجريمة السيبرانية: المحددات النظرية والسياسات الجنائية وآليات الوقاية والسيطرة»[2]: (2020) تركز على الواقع القطري مستندةً إلى مسح ميداني ومقابلات مع خبراء، وقد بينت أن اختراق المواقع والاحتيال المصرفي يشكلان أبرز أنماط الاعتداء، وأن الدافع المالي هو المحرك الرئيس. وأوصت بتعزيز الوعي وبرامج الحماية التقنية التي تؤكد البعد الوقائي الذي يستحضره بحثنا إلى جانب المعالجة التشريعية.

3. دراسة محمود محمد، (2021)، بعنوان «الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت»[3]: تخلص إلى أن الطبيعة اللامادية للبيانات تجعل القوانين التقليدية عاجزة، وأن كثيرًا من الدول بدأت سن قوانين خاصة أو تعديل العقوبات القائمة لضمان مبدأ الشرعية وعدم إفلات الجناة. وتبرز هذه النتائج الحاجة إلى دينامية تشريعية مستمرة، وهو ما يستجيب له بحثنا عبر اقتراح مراجعات دورية وتوسيع نطاق التجريم.

4. دراسة عبد الله دغش (2014)، بعنوان «المشكلات العملية والقانونية للجرائم الإلكترونية»[4]: تركز على ضرورة وضع صك دولي إلزامي لسد الثغرات التشريعية أمام جرائم عابرة للحدود سريعة التطور. وتؤكد هذه الخلاصة أهمية التعاون الدولي الذي يتبناه بحثنا؛ من خلال الدعوة إلى الانضمام الكامل لاتفاقية بودابست، وتفعيل آليات المساعدة القانونية المتبادلة.

5. دراسة خالد ظاهر، (2022)، بعنوان «دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي»[5]: تبرز التحديات السيبرانية في دول مجلس التعاون، وتبين تفاوت فاعلية التشريعات الجزائية في المنطقة ووجود فجوات قانونية تتطلب نصوصًا أكثر حداثة. هذه النتائج تقدم معيارًا خليجيًا مرجعيًا يسهم بحثنا في رفده بتفصيل مقارنة قطرية – ألمانية تشكل نموذجًا للتطوير الإقليمي.

6. دراسة مريم عبد اللطيف (2022): «مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية»[6]: تظهر تقدم دولة قطر في التعاون الدولي مع غياب اتفاقية دولية

(2) A. L. Nasser, "Cybercrime: Theoretical Determinants, Criminal Policies, Prevention & Control Mechanisms," International Journal of Technology and Systems 5, no. 1 (2020): 3463-.

(3) محمود محمد شرشر، «الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت"، مجلة البحوث القانونية والاقتصادية- المنوفية 54، ع. 3 (2021): 523-580.

(4) عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة (الكويت: جامعة الشرق الأوسط، 2014).

(5) خالد، ظاهر عبدالله جابر السهيل المطيري، «دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي"، مجلة البحوث الفقهية والقانونية، ع. 38 (2022).

(6) مريم عبد اللطيف المسلماني، «مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية"، مجلة القانون والمجتمع، كلية القانون، جامعة قطر، المجلد 10، العدد 2 (2022): 14-59.

شاملة، موصيةً بإنشاء لجان متابعة وتنمية الوعي العام، وينسجم ذلك مع طرحنا الذي يعالج جوانب القوة (التعاون) ويقترح سد ثغرة تجريم الأفعال التحضيرية وتبني غرامات مرنة تربط العقوبة بالدخل.

ثالثًا: التعقيب النقدي

كشفت الدراسات (1) و (5) عن قصور في التجريم التفصيلي؛ إذ إن دمج أفعال متعددة في مادة واحدة يضعف الأثر الردعي ويعقد عملية الإثبات. وقد عالجت هذه الدراسة الإشكالية عبر تفصيل وتحليل المادتين (2) و(3) من القانون القطري، مع مقارنتهما بالمواد (202a–303b) من قانون العقوبات الألماني (StGB)، كما أكدت نتائج الدراسات (3) و (4) الحاجة إلى تشريعات دينامية عابرة للحدود، نظرًا لتخطي الجرائم للحدود الوطنية، وضعف الإلزام القانوني للإطار العربي الحالي.

من هنا، تنطلق هذه الدراسة نحو التوصية بإدراج الأفعال التحضيرية المنصوص عليها في المادة (202c)، واعتماد نظام غرامات مرن يعتمد مبدأ (Tagessätze) القائم على الدخل. وفي جانب آخر أبرزت الدراسة (2) البعد الوقائي والمجتمعي من خلال تسليط الضوء على الدوافع المالية لمرتكبي الجرائم السيبرانية وانتشار ظاهرة الاحتيال المصرفي. وبناءً على ذلك، أضافت الدراسة منظورًا تشريعيًا داعمًا لتوصية بإنشاء برامج توعية وطنية، وربط مقدار العقوبات بالمستوى المالي للمدانين. أما فيما يتعلق بالتعاون الدولي، فقد بينت الدراستان (4) و (6) أهمية الاتفاقيات الدولية في مكافحة الجرائم العابرة للحدود. واستثمارًا لهذه النتائج تقترح دراستنا انضمام دولة قطر الكامل إلى اتفاقية بودابست، مع تفعيل قنوات المساعدة القانونية المتبادلة بشكل عملي ومؤسسي.

وتنطلق هذه الدراسة من حيث توقفت الأدبيات السابقة، فهي لا تكتفي بوصف القصور، بل تتجاوزه إلى تحليل نصي دقيق للمادتين القطريتين، مقدمةً حلولاً تشريعية قابلة للتنفيذ، مستندة إلى النموذج الألماني بما يسد فجوة التجريم التحضيري، ويحسن تدرج العقوبات، ويوطد التعاون الدولي في المجال السيبراني.

خطة الدراسة

تقسم الدراسة إلى مقدمة تمهيدية تتناول مشكلة البحث وأهميته وأهدافه وتساؤلاته، ثم تنتقل إلى عرض منهج الدراسة وأهم الدراسات السابقة والتعقيب عليها.

ويتناول المبحث الأول الإطار المفاهيمي والتنظيمي للجرائم السيبرانية، من خلال استعراض مفهوم الجريمة السيبرانية، وخصائصها، وأنواعها، وأبرز التحديات القانونية والقضائية المرتبطة بها.

أما المبحث الثاني فيمثل القسم التحليلي المقارن للدراسة، حيث يتم تحليل النصوص القانونية ذات الصلة في كل من القانون القطري والقانون الألماني، وذلك من خلال مقارنتها من حيث التجريم، وطبيعة العقوبات، والتدابير التشريعية المصاحبة.

وتختتم الدراسة بخلاصات علمية وتوصيات تشريعية تستند إلى نتائج المقارنة، وتسعى إلى تعزيز الإطار القانوني القطري في ضوء التجربة الألمانية، بما يحقق التوازن بين الحماية القانونية وفعالية التطبيق.

المبحث الأول
مفهوم الجرائم السيبرانية وخصائصها وأنواعها وتحدياتها القضائية

برزت الجرائم السيبرانية كظاهرة حديثة تحمل في طياتها تحديات كبيرة على المستوى القانوني والأمني، وتعنى هذه الظاهرة بالأنشطة غير القانونية التي ترتكب باستخدام الشبكات الحاسوبية والإنترنت، مما يعقد عملية تتبع مرتكبيها وتحديد هويتهم نظرًا لطبيعتها العابرة للحدود. ويهدف هذا المبحث إلى تسليط الضوء على مفهوم الجرائم السيبرانية، واستعراض خصائصها وأنواعها المتعددة، مع التركيز على التحديات القضائية التي تواجهها في سبيل تحقيق العدالة وتطبيق القانون.

المطلب الأول
مفهوم الجرائم السيبرانية

يعد مصطلح «الجرائم السيبرانية» من المفاهيم المستحدثة نسبيًا في الفقه الجنائي، وقد برز مع الانتشار المتسارع للتكنولوجيا الرقمية وشبكات الإنترنت منذ أواخر القرن العشرين. وتتميز هذه الجرائم بأنها لا ترتكب في بيئة مادية تقليدية، بل في فضاء إلكتروني غير ملموس، مما يمنحها خصائص قانونية مغايرة للجريمة الكلاسيكية، ولم يحظَ هذا المفهوم بتعريف موحد في الفقه القانوني، بل تعددت اتجاهات الفقهاء بشأنه؛ فبينما يذهب البعض إلى تعريفها بأنها: «كل سلوك غير مشروع يتم باستخدام الحاسب الآلي أو الشبكة أو أي أداة رقمية»، يرى آخرون أنها: «جرائم ترتكب ضد نظام معلوماتي أو من خلاله، بهدف الاعتداء على سرية البيانات أو سلامتها أو توافرها»، وهناك من يضيف إلى ذلك جرائم المحتوى والاختراق والاحتيال المالي والابتزاز الإلكتروني والتجسس الرقمي.[7]

(7) Abu-taieh, Evon, Auhood Abdullah Alfaries, Shaha Alotaibi, and Ghadah Aldehim. "Cyber Security Crime and Punishment: Concepts, Methodologies, Tools, and Applications." In Multigenerational Online Behavior and Media Use, January 2019. https://doi.org/10.40180-7909-5225-1-978/.ch069

وعرفها البعض بأنها: «هي جريمة ترتكب باستخدام شبكة كمبيوتر أو الإنترنت. ويمكن أن يشمل هذا مجموعة واسعة من الأنشطة، بما في ذلك الأنشطة الإرهابية والتجسس الذي يتم بمساعدة الإنترنت والاختراق غير القانوني لأنظمة الكمبيوتر والجرائم المتعلقة بالمحتوى وسرقة البيانات والتلاعب بها والملاحقة الإلكترونية»[8].

أما من الناحية التشريعية، فلم تحدد معظم القوانين الوطنية تعريفًا دقيقًا للجريمة السيبرانية، بل اعتمدت على تفصيل صور الفعل المجرم ضمن مواد قانونية منفصلة. ويلاحظ أن القانون القطري رقم (14) لسنة 2014 لم يورد تعريفًا جامعًا للمفهوم، بل عرض أفعالاً محددة مجرمة. بينما اعتمد التشريع الألماني منهجية تجزيئية صارمة، عبر تفصيل كل صورة جرمية في مادة مستقلة دون الحاجة لتعريف عام.

وانطلاقًا من ذلك، تعتمد هذه الدراسة مفهومًا وظيفيًا تحليليًا للجريمة السيبرانية؛ بوصفها: «كل فعل ينطوي على استخدام مقصود لأداة رقمية أو نظام معلوماتي بهدف ارتكاب نشاط غير مشروع، يمس بيانات، أو أنظمة، أو حقوق أفراد، أو مؤسسات، سواء أكان ذلك الفعل مباشرًا (كالاختراق) أو غير مباشر (كإعداد أدوات الجريمة)». ويبرز هذا التعريف الطبيعة المركبة للجريمة السيبرانية، ويفسح المجال لتحليل النصوص العقابية ذات الصلة وفقًا لطبيعة الفعل لا مجرد وسيلته، بما ينسجم مع أهداف هذه الدراسة القانونية المقارنة.

المطلب الثاني
خصائص الجريمة السيبرانية

تتميز الجريمة السيبرانية بسمات قانونية وواقعية تجعلها تختلف جوهريًا عن الجرائم التقليدية، لا من حيث الوسيلة فقط، بل من حيث بيئة ارتكاب الجريمة وآثارها وطرق الإثبات[9]. وقد أولت الدراسات الفقهية الحديثة اهتمامًا خاصًا بهذه الخصائص باعتبارها المدخل الأساسي لفهم الطبيعة الخاصة لهذا النمط من الإجرام الرقمي، وأبرز هذه الخصائص ما يلي:

(8) محمد، حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقها: دراسة مقارنة في التشريع الإماراتي والسعودي، والبحريني والقطري والعماني (مصر-الإمارات: دار الكتب القانونية، 2014).

(9) A. L. Nasser, "Cybercrime: Theoretical Determinants, Criminal Policies, Prevention & Control Mechanisms," International Journal of Technology and Systems 5, no. 1 (2020): 3463-.

1. **الطابع غير المادي:** ترتكب الجرائم السيبرانية دون احتكاك مادي مباشر بين الجاني والضحية، مما يمنحها طابعًا غير مادي من حيث الوسيلة والأثر، إذ يكون الاعتداء عادة على بيانات أو أنظمة لا على أشياء مادية محسوسة، وهذا ينعكس على صعوبة التحقق من وقوع الجريمة بالوسائل التقليدية للإثبات[10].

2. **العبور الجغرافي (الطابع العابر للحدود):** لا تقف الجريمة السيبرانية عند نطاق إقليمي محدد، بل قد ترتكب من دولة وتحدث أثرًا في أخرى، مما يثير إشكاليات قانونية تتعلق بالاختصاص القضائي وازدواجية العقوبة وتنفيذ الأحكام الجنائية بين الدول[11].

3. **المهارات التقنية الخاصة:** يتمتع مرتكبو الجرائم السيبرانية غالبًا بخبرة تقنية عالية تمكنهم من تجاوز الأنظمة الأمنية التقليدية، واستخدام أدوات معقدة كالبرمجيات الخبيثة، أو أدوات إخفاء الهوية، مما يصعب عمليات التتبع والتحديد الجنائي[12].

4. **صعوبة الإثبات الرقمي:** نظرًا لأن الأدلة في هذا النوع من الجرائم تكون رقمية، وسريعة الزوال أو قابلة للتعديل، تصبح إجراءات الضبط والتفتيش التقليدية غير كافية، وهو ما فرض على بعض التشريعات اعتماد قواعد جديدة لجمع الأدلة الجنائية الإلكترونية[13].

5. **سهولة التكرار واتساع النطاق:** يلاحظ أن الجريمة السيبرانية يمكن أن تتكرر بسهولة بالغة، وقد تستهدف عددًا كبيرًا من الضحايا في وقت متزامن، كما في حالات اختراق قواعد بيانات ضخمة أو إرسال فيروسات عبر البريد الإلكتروني الجماعي، ما يجعلها أكثر خطورة من الناحية الاجتماعية والاقتصادية[14].

المطلب الثالث
أنواع الجرائم السيبرانية

يعد تصنيف الجرائم السيبرانية من المسائل الإشكالية في الفقه الجنائي المعاصر، نظرًا لتداخل هذه الجرائم مع أنماط إجرامية تقليدية، وتنوع الوسائل التي تستخدم في ارتكابها. ولا يقتصر هذا النوع من الجرائم على الأفعال التي ترتكب عبر الإنترنت فقط،

(10) المطيري، «دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي».

(11) العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة.

(12) Brenner, Susan W. Cybercrime: Criminal Threats from Cyberspace. 1st ed. Santa Barbara, CA: Praeger, 2010.

(13) عدلي دحمان وثامر البشير سعد الدين، التحقيق الجنائي في الجرائم الإلكترونية (لجلفة، الجزائر: كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، 2021).

(14) UNODC. Comprehensive Study on Cybercrime, United Nations Office on Drugs and Crime, Vienna, 2013, pp. 67–69.

بل يشمل أيضًا كافة الأفعال الإجرامية التي تستخدم فيها أي تقنية معلوماتية، سواءً كوسيلة للجريمة، أو كهدف لها، أو كبيئة حاضنة لها[15]، وقد اقترح الفقه عدة تصنيفات وظيفية للجرائم السيبرانية، أبرزها:

1. **الجرائم الواقعة على أنظمة وتقنيات المعلومات:** وهي تشمل الأفعال التي تستهدف الهياكل التقنية ذاتها، مثل أجهزة الحاسوب، الخوادم، الشبكات، وأجهزة الاتصال. وتندرج ضمن هذا النوع جرائم مثل: تعطيل الأنظمة، إرسال فيروسات (Malware)، أو الحرمان من الخدمة (DDoS Attacks).[16]
2. **الجرائم الواقعة على البيانات والمحتوى الرقمي:** تركز هذه الجرائم على البيانات المخزنة أو المنقولة إلكترونيًا، وتشمل: الوصول غير المشروع، سرقة البيانات، الحذف أو التعديل غير المرخص، والتنصت على الاتصالات الإلكترونية. ويعد هذا النوع من الجرائم هو الأكثر شيوعًا.[17]
3. **الجرائم الموجهة ضد الأفراد:** تتعلق هذه الفئة بانتهاك الخصوصية أو التعدي على السمعة والحرية الشخصية، وتشمل: الملاحقة الإلكترونية (Cyberstalking)، والتهديد، والابتزاز، والتشهير الإلكتروني، والتحرش عبر الإنترنت، وهي تختلف من حيث الدافع والنتائج لكنها تتقاطع في وسيلة التنفيذ.[18]
4. **الجرائم الاقتصادية والاحتيالية:** تضم هذه الفئة جرائم مثل: التصيد الإلكتروني (Phishing)، والتزوير الإلكتروني، وغسل الأموال عبر الإنترنت، والاحتيال بواسطة العملات الرقمية، والاختراق المالي للمصارف أو البورصات.[19]
5. **الجرائم ذات الطابع السياسي أو الأمني:** وتشمل الهجمات السيبرانية ذات الأهداف الإرهابية، أو الهجمات على البنية التحتية الحيوية، أو اختراق الأنظمة الحكومية لأغراض تجسسية، وهي من الجرائم المصنفة ذات الخطورة العالية نظرًا لتأثيرها العابر للأفراد والمؤسسات والدول.[20]
6. **الجرائم المرتبطة بالمحتوى غير المشروع:** تتعلق بالمضامين الرقمية التي يعد نشرها أو تداولها جريمة بحد ذاتها، مثل: المواد الإباحية الخاصة بالأطفال، خطاب الكراهية، محتوى التحريض على الإرهاب، أو ترويج العنف، وتخضع هذه الفئة لضوابط تشريعية تختلف من بلد لآخر بحسب الثقافة والنظام القانوني.[21]

(15) Gercke, Marco. Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, 2012, pp. 45–46.

(16) UNODC, Comprehensive Study on Cybercrime, 2013, pp. 90–92, in: https://tinyurl.com/bncy969.

(17) Ibid.

(18) Council of Europe, Explanatory Report to the Budapest Convention, 2001, para. 48, in: https://tinyurl.com/273qyhub.

(19) Ibid

(20) Europol, Internet Organized Crime Threat Assessment (IOCTA), 2022, p. 33, in: https://tinyurl.com/2dborjeo.

(21) INTERPOL, Cybercrime: Online Child Sexual Exploitation, 2021, in: https://tinyurl.com/26pmyplr.

المطلب الرابع
التحديات القضائية في قضايا الجرائم السيبرانية

تواجه السلطات القضائية تحديات متزايدة في التعامل مع الجرائم السيبرانية، نظرًا للطبيعة المتغيرة والسريعة لهذا النوع من الجرائم، إضافة إلى الطبيعة غير المحدودة للإنترنت والنطاق العابر للحدود الوطنية لأنشطة الجرائم السيبرانية، وفيما يلي بعض التحديات القضائية الرئيسة التي تواجه قضايا الجرائم السيبرانية، ويمكن تلخيصها في النقاط التالية:

1. الطبيعة العابرة للحدود (تحديد الاختصاص القضائي):

تثير الجرائم السيبرانية تحديات في تحديد الاختصاص القضائي، نظرًا للطبيعة العابرة للحدود لهذه الجرائم، وقد يكون من الصعب تحديد الدولة المختصة بالتحقيق والمحاكمة، خاصة عندما يكون الجاني والمجني عليه في دول مختلفة، أو عندما ترتكب الجريمة عبر خوادم موزعة في عدة دول، ويمكن ارتكاب الجرائم السيبرانية من ولاية قضائية واحدة بينما تؤثر على الضحايا في ولايات قضائية متعددة، وتحديد الدولة التي لديها ولاية قضائية على حادثة جريمة سيبرانية[22].

2. الافتقار إلى الإجماع القانوني الدولي:

هناك حاجة إلى أطر ومعاهدات قانونية دولية أكثر اتساقًا ومصممة خصيصًا للجرائم الإلكترونية، فالدول لديها تعريفات وقوانين وعقوبات مختلفة للجرائم الإلكترونية، مما يجعل من الصعب توحيد الجهود وتسهيل التعاون الدولي في التحقيق في جرائم الإنترنت وملاحقتها.[23]

3. التحديات في تحديد هوية الجناة (إثبات الجرائم السيبرانية):

يعد جمع وتقديم الأدلة الرقمية من أبرز التحديات في قضايا الجرائم السيبرانية، وتتطلب هذه العملية إجراءات دقيقة لضمان سلامة البيانات وسلسلة الحيازة، مع مراعاة المعايير القانونية لضمان قبولها في المحكمة. كما أن الأدلة الرقمية قد تكون عرضة للتلاعب أو الفقدان، مما يزيد من تعقيد عملية الإثبات، فغالبًا ما يستخدم مجرمو الإنترنت تقنيات لإخفاء هوياتهم ومواقعهم، مثل استخدام خدمات إخفاء الهوية أو خوادم البروكسي أو الاختراق من خلال الأنظمة المخترقة. وهذا يجعل من الصعب تحديد الولاية القضائية التي نشأت منها الجريمة، مما يعوق عملية تحديد هوية الجناة وإلقاء القبض عليهم[24].

(22) Alramamneh and Abuanzeh, "International and National Procedural Framework for Combating Cybercrime".

(23) محمد، " الجريمة المعلوماتية نماذج من تطبيقها: دراسة مقارنة في التشريع الإماراتي والسعودي، والبحريني والقطري والعماني".

(24)I. F. Salim and M. R. Dhafri, "The Criminal Agreement in Cybercrimes in Iraqi, Emirati, and Qatari Law".

4. المساعدة القانونية المتبادلة (التعاون الدولي):

يتطلب التحقيق في الجرائم السيبرانية تعاونًا دوليًا فعالاً، نظرًا للطبيعة العابرة للحدود لهذه الجرائم، ويشمل ذلك تبادل المعلومات والأدلة بين الدول، وتنسيق الجهود بين السلطات القضائية والأمنية. ومع ذلك قد تواجه هذه الجهود تحديات قانونية وإجرائية، مثل اختلاف الأنظمة القانونية، ومتطلبات حماية البيانات، والقيود المتعلقة بالسيادة الوطنية، وقد يستغرق الحصول على الأدلة والتعاون من الولايات القضائية الأجنبية وقتًا وجهدًا بسبب تعقيدات عمليات المساعدة القانونية المتبادلة. وتختلف القوانين والإجراءات الخاصة بتبادل الأدلة وتسهيل التسليم بين البلدان، مما يؤدي إلى تأخيرات وتعقيدات في تحقيقات الجرائم الإلكترونية[25].

5. الاختلافات القانونية (التعامل مع الأدلة الرقمية):

تتطلب الأدلة الرقمية معالجة خاصة لضمان سلامتها وقبولها في المحكمة، ويشمل ذلك استخدام تقنيات متقدمة لجمع وتحليل البيانات، وتدريب القضاة والمدعين العامين على فهم هذه الأدلة وتقييمها بشكل صحيح. كما يجب وضع معايير وإجراءات واضحة للتعامل مع الأدلة الرقمية، بما في ذلك ضمان سلسلة الحيازة، وتوثيق العمليات، والحفاظ على سرية البيانات الحساسة، وقد تنشأ تحديات قضائية بسبب الاختلافات في الأنظمة القانونية والتقاليد القانونية والمعايير الثقافية. وقد تختلف المفاهيم القانونية وتعريفات الجرائم ومتطلبات الأدلة وقوانين الخصوصية بشكل كبير، مما يؤثر على القدرة على جمع الأدلة وملاحقة مجرمي الإنترنت عبر الحدود[26].

6. موارد وخبرات إنفاذ القانون المحدودة:

تتطلب تحقيقات الجرائم الإلكترونية معرفة متخصصة وخبرة فنية قد لا تكون متاحة بسهولة إلا في بعض الولايات القضائية. ويمكن للموارد المالية والتكنولوجية المحدودة أن تعيق قدرة وكالات إنفاذ القانون على التحقيق في الجرائم الإلكترونية وملاحقتها بشكل فعال[27].

7. النزاعات القضائية:

في الحالات التي تطالب فيها بلدان متعددة بالولاية القضائية على حادثة جريمة إلكترونية فقد تنشأ النزاعات، مما يؤدي إلى تحديات قانونية ودبلوماسية، ويتطلب تحديد الولاية القضائية المناسبة وحل النزاعات تعاونًا وتنسيقًا مكثفين بين البلدان المعنية[28].

(25) Ibid.

(26) دحمان وسعد الدين، «التحقيق الجنائي في الجرائم الإلكترونية».

(27) سعيدة بوزنون، «مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة العلوم الإنسانية، ع. 52، ج. 3 (ديسمبر 2019): 47-57.

(28) البداينة، «الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية».

عمومًا، يظهر تحليل البيانات والمعلومات المقدمة أن الجرائم السيبرانية ليست مجرد ظاهرة جديدة تنشأ مع تطور التكنولوجيا، بل هي واقع متنام يعيد صياغة مفاهيم الجريمة والعدالة في العصر الرقمي. فقد اتضح أن هذه الجرائم تعتمد على استغلال الثغرات التقنية والفضاءات الافتراضية التي تفتقر إلى الحدود المكانية والزمنية التقليدية، مما يجعل من الصعب تحديد هوية المجرمين وجمع الأدلة اللازمة لإثبات الجريمة.

ويرى الباحث أن التطور المستمر للتكنولوجيا يتطلب إعادة تقييم وتحديث الأطر القانونية والأمنية؛ لضمان فعالية إجراءات التحقيق والملاحقة القضائية. كما أن الطبيعة متعددة الأبعاد لهذه الجرائم – من حيث خصائصها وأنواعها – تؤكد الحاجة إلى تعاون دولي وثيق لتوحيد الجهود وتبادل الخبرات، مما يعد خطوة أساسية نحو تعزيز الأمان السيبراني على المستويين الوطني والدولي.

المبحث الثاني

مقارنة التشريعات القطرية والألمانية في الجرائم السيبرانية

مع التقدم السريع في التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية في جميع جوانب الحياة، أصبحت الجرائم السيبرانية تهديدًا واقعيًا يؤثر على الأفراد والشركات والحكومات.

ويستهدف هذا المبحث استعراض أوجه الاختلاف والتشابه بين التشريعات القانونية المتعلقة بالجرائم السيبرانية في كل التشريعات القطرية والألمانية لمكافحة الجرائم السيبرانية، من خلال تحليل القوانين المعمول بها، والعقوبات المطبقة، وآليات التحقيق والملاحقة القانونية. فمن خلال مقارنة هذه القوانين، يمكن فهم كيفية تعامل كل دولة مع الجرائم السيبرانية بشكل عملي، وما إذا كانت هناك ثغرات أو تحديات تواجه تطبيق هذه القوانين على أرض الواقع.

المطلب الأول

المقارنة بين التشريعات القطرية والألمانية في النصوص والتجريم

مما لا شك فيه أن الجرائم السيبرانية واحدة من أكبر التحديات التي تواجه الحكومات في عصر التكنولوجيا الرقمية؛ حيث تسعى كل من دولة قطر وجمهورية ألمانيا الاتحادية إلى وضع أطر قانونية واضحة ودقيقة من أجل التصدي إلى هذه الظاهرة، ويمكن طرح مقارنة تفصيلية بين النصوص القانونية المتعلقة بالجرائم السيبرانية في كل من قطر وألمانيا من خلال الآتي:

أولا: التشريع القطري من حيث نص القانون

يمكن النظر إلى التشريع القطري في مجال مكافحة الجرائم السيبرانية من خلال قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، الذي يعد الإطار القانوني الأساسي لمواجهة هذه الجرائم في قطر[29]. ويحدد هذا القانون مختلف أنواع الجرائم الإلكترونية والعقوبات المترتبة عليها، ويتكون من خمسة أبواب رئيسة.

- **الباب الأول**: يشمل التعاريف والمفاهيم الأساسية.
- **الباب الثاني**: يوضح الجرائم الإلكترونية المشمولة في القانون.
- **الباب الثالث**: يتناول الإجراءات القانونية وآليات التحقيق.
- **الباب الرابع**: يركز على التعاون الدولي لمكافحة الجرائم السيبرانية.
- **الباب الخامس**: يتضمن الأحكام العامة المرتبطة بتطبيق القانون.

كما يؤكد التشريع القطري بشكل واضح أهمية حماية البيانات الشخصية، وذلك من خلال قانون حماية البيانات الشخصية رقم (13) لعام 2016[30]، الذي يستهدف تنظيم عمليات معالجة البيانات وضمان حقوق الأفراد في الحفاظ على خصوصية معلوماتهم الشخصية. ويعكس هذا التشريع التزام الدولة بتعزيز الأمن الرقمي وحماية المعلومات في البيئة الإلكترونية.

في 29 ديسمبر 2016، بدأ القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية سريانه، حيث حدد نطاق تطبيقه في المادة الثانية، التي تنص على أنه يقتصر على البيانات الشخصية التي تتم معالجتها إلكترونيًا، أو التي يتم الحصول عليها أو جمعها أو استخراجها تمهيدًا للمعالجة الإلكترونية، أو التي تعالج بمزيج من الطرق الإلكترونية والتقليدية. واستثنى القانون من نطاقه البيانات الشخصية التي يتداولها الأفراد في إطار خاص أو عائلي، وكذلك البيانات الشخصية التي تجمع لأغراض المسوحات والإحصاءات الرسمية، كما كفل القانون حقوق مالكي البيانات الشخصية، وأبرزها الحصول على موافقتهم المسبقة قبل أن يتم استخدام بياناتهم من قبل أي جهة. إضافةً إلى ذلك منحهم الحق في سحب الموافقة، أو الاعتراض على المعالجة، أو طلب حذف بياناتهم، أو تصحيحها، وفقًا للضوابط المنصوص عليها في القانون.

(29) قانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، وزارة العدل – دولة قطر، 2025/02/12، للمزيد، انظر: https://tinyurl.com/29ahrrh9.

(30) قانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، وزارة العدل – دولة قطر، 2025/02/12، للمزيد، انظر: https://tinyurl.com/2cm5hbvm.

وشدد القانون على تجريم أي انتهاك لمواده المتعلقة بحماية خصوصية البيانات الشخصية؛ لضمان أمن وسرية المعلومات، وتعزيز الثقة في البيئة الرقمية.[31]

وسنتطرق للباب الثاني الذي يوضح الجرائم الإلكترونية والمواد المتعلقة بها في القانون القطري، والتي تشمل[32] :

1. جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية

أ. **المادة** 2: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها. وتضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة.

ب. **المادة** 3: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، دون وجه حق، بأي وسيلة، موقعًا إلكترونيًا، أو نظامًا معلوماتيًا، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك. وتضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء، أو حذف، أو إضافة، أو إفشاء، أو إتلاف، أو تغيير، أو نقل، أو التقاط، أو نسخ، أو نشر، أو إعادة نشر بيانات، أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين، أو المستفيدين، أو تدمير، أو إيقاف، أو تعطيل الموقع الإلكتروني، أو النظام المعلوماتي، أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني، أو إلغائه، أو تعديل محتوياته ،أو تصميماته أو طريقة استخدامه أو انتحال شخصية مالكه أو القائم على إدارته.

(31) "حماية البيانات والجرائم الإلكترونية في قطر"، مكتب السليطي للمحاماة والاستشارات القانونية، تم الوصول إليه في 9 فبراير 2025، https://www.alsulaitilawfirm.com/insights-1-9-html-ar.2017.

(32) قانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، وزارة العدل – دولة قطر.

ج. **المادة** 4: يعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من التقط أو اعترض أو تنصت عمدًا، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور.

2. **جرائم المحتوى**

أ. **المادة** 5: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من أنشأ أو أدار موقعًا لجماعة أو تنظيم إرهابي على الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو سهل الاتصال بقيادات تلك الجماعات أو أي من أعضائها، أو الترويج لأفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية.

ب. **المادة** 6: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من أنشأ أو أدار موقعًا إلكترونيًا عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، لنشر أخبار غير صحيحة، بقصد تعريض سلامة الدولة أو نظامها العام أو أمنها الداخلي أو الخارجي للخطر. ويعاقب بالحبس مدة لا تجاوز سنة، وبالغرامة التي لا تزيد على (250,000) مائتين وخمسين ألف ريال، أو بإحدى هاتين العقوبتين، كل من روج أو بث أو نشر، بأي وسيلة، تلك الأخبار غير الصحيحة بذات القصد.

ج. **المادة** 7: يعاقب بالحبس مدة لا تجاوز خمس سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من أنتج مادة إباحية عن طفل بواسطة وسائل تقنية المعلومات، أو استورد أو باع، أو عرض للبيع، أو الاستخدام، أو تداول، أو نقل، أو وزع أو أرسل أو نشر أو أتاح أو بث مادة إباحية عن طفل بواسطة وسائل تقنية المعلومات. ويعاقب بالحبس مدة لا تجاوز سنة، وبالغرامة التي لا تزيد على (250,000) مائتين وخمسين ألف ريال، أو بإحدى هاتين العقوبتين، كل من حاز مادة إباحية عن طفل. ولا يعتد في الجرائم المعاقب عليها في هذه المادة برضا الطفل. ويعتبر طفلاً في حكم هذه المادة كل من لم يتم من العمر ثماني عشرة سنة ميلادية كاملة.

د. **المادة** 8: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من تعدى على أي من المبادئ، أو القيم الاجتماعية، أو نشر أخبارًا، أو صورًا، أو تسجيلات صوتية أو مرئية تتصل بحرمة الحياة الخاصة أو العائلية للأشخاص، ولو كانت صحيحة، أو تعدى على الغير بالسب أو القذف، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

ه. المادة 9: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في تهديد أو ابتزاز شخص، لحمله على القيام بعمل أو الامتناع عنه.

3. **التزوير والاحتيال الإلكتروني**

أ. **المادة** 10: يعاقب بالحبس مدة لا تجاوز عشر سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، كل من زور محررًا إلكترونيًا رسميًا أو استعمله مع علمه بذلك. ويعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، إذا وقع التزوير على محرر إلكتروني غير رسمي واستعمله مع علمه بتزويره.

ب. **المادة** 11: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلًا من الأفعال التالية:

- استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في انتحال هوية لشخص طبيعي أو معنوي.
- تمكن عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات من الاستيلاء لنفسه أو لغيره على مال منقول، أو على سند أو التوقيع عليه، بطريق الاحتيال، أو باتخاذ اسم كاذب، أو بانتحال صفة غير صحيحة.

4. **جرائم بطاقة التعامل الإلكتروني**

أ. **المادة** 12: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلًا من الأفعال التالية:

- استخدام أو حصل أو سهل الحصول دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.
- زور بطاقة تعامل إلكتروني بأي وسيلة كانت.
- صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقات التعامل الإلكتروني.
- استخدم أو سهل استخدام بطاقة تعامل إلكتروني مزورة مع علمه بذلك.
- قبل بطاقات تعامل إلكتروني غير سارية أو مزورة أو مسروقة مع علمه بذلك.

5. **التعدي على حقوق الملكية الفكرية**

أ. **المادة** 13: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في التعدي أو تسهيل التعدي، بأي وسيلة، وفي أي صورة، على حقوق المؤلف، أو الحقوق المجاورة، أو براءات الاختراع، أو الأسرار التجارية، أو العلامات التجارية، أو البيانات التجارية، أو الأسماء التجارية، أو المؤشرات الجغرافية، أو الرسوم والنماذج الصناعية، أو تصاميم الدوائر المتكاملة، المحمية وفقًا للقانون.

وقبل الانتقال إلى استعراض التشريع الألماني، من المهم التوقف عند تحليل المادتين الرئيسيتين في القانون القطري، لما يطرحه مضمونهما من إشكالات قانونية متعددة، كما يلي:

1. **تحليل نقدي للمادتين** (2) **و**(3) **من قانون مكافحة الجرائم الإلكترونية القطري**

أ. على الرغم من الأهمية البالغة التي تمثلها المادتان (2) و (3) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014 في تأطير صور التعدي على أنظمة المعلومات والشبكات الإلكترونية، إلا أن صياغتهما تثير عددًا من الإشكاليات القانونية الجديرة بالتحليل. فقد تم دمج أفعال متعددة ومتميزة من حيث الطبيعة والعناصر الجرمية، ضمن نصوص واحدة، كالدخول غير المشروع، والحذف، والإتلاف، والتغيير، والنشر، والتعدي على بيانات الغير أو استخدامها دون وجه حق. فهذا الدمج يضعف الفاعلية التشريعية من زاويتين: أولًا، من جهة الردع العام، إذ إن عدم التمييز بين الأفعال قد يؤدي إلى شعور بعدم التناسب بين الجريمة والعقوبة؛ وثانيًا، من جهة الإثبات القضائي، حيث يصعب على جهة الادعاء أو المحكمة إثبات الركن المادي والمعنوي لكل فعل على حدة في ظل صياغة كلية غير مفصلة.

ب. وإذ يجدر التنويه إلى أن بعض صور الفعل المجرم قد تستقل بأركان قانونية تختلف عن غيرها (مثلًا: الدخول غير المشروع يختلف في طبيعته القانونية عن الإفشاء أو التلاعب بالبيانات)، فإن جمعها جميعًا تحت مظلة مادتين قد يفرغ بعضها من الحماية الفعلية اللازمة. وعليه، فإن إعادة تفكيك هذه الأفعال في مواد مستقلة، كما هو الحال في التشريع الألماني (مثل المواد 202a و202b و303a و303b من شأنه أن يحقق قدرًا أعلى من الوضوح التشريعي، والتناسب العقابي، والدقة الإجرائية أثناء التحقيق والمحاكمة.

ج. علاوةً على ذلك، فإن الصياغة الحالية لا توضح بشكل كاف الحدود الفاصلة بين الأفعال، مما يثير مخاوف حول التفسير الموسع للنصوص على نحو قد يخل بمبدأ الشرعية الجنائية.

ومن هنا تبرز الحاجة إلى مراجعة بنيوية للمادتين، سواء عبر إعادة توزيع الأفعال بحسب طبيعتها، أو عبر إدراج فقرات توضيحية تبين خصائص كل صورة من صور السلوك الجرمي، ضمانًا لحسن التطبيق، واتساقًا مع المبادئ الدستورية المنظمة للتجريم والعقاب.

ثانيًا: التشريع الألماني من حيث نص القانون (STRAFGESETZBUCH – StGB) [33]

يعد القانون الجنائي الألماني (STRAFGESETZBUCH – StGB) الإطار القانوني الأساسي لمكافحة الجرائم السيبرانية في ألمانيا، حيث يتضمن عدة مواد تعالج مختلف أشكال الجرائم الإلكترونية، مثل

- التجسس على البيانات.
- التصيد الإلكتروني.
- سرقة البيانات.
- التلاعب بالبيانات.
- التخريب الإلكتروني.
- الاحتيال الحاسوبي.
- تزوير البيانات ذات القيمة الإثباتية.
- إنتاج أو حيازة أدوات لارتكاب الجرائم السيبرانية.

تعكس هذه المواد التشريعية التزام ألمانيا بتوفير بيئة إلكترونية آمنة من خلال فرض عقوبات صارمة على الجرائم الرقمية التي تهدد الأفراد والمؤسسات والبنية التحتية للدولة. ومن خلال هذه الأحكام يسعى المشرع الألماني إلى ردع مرتكبي الجرائم السيبرانية وضمان حماية البيانات الرقمية من الاختراق أو التلاعب أو الاستخدام غير المشروع، ويمكن تفصيل هذه المواد في الآتي

1. **التجسس على البيانات - المادة (202a)**[34]:

أ. يعاقب بالسجن لمدة تصل إلى ثلاث سنوات أو بغرامة كل من يحصل لنفسه أو لغيره على وصول غير مصرح به إلى بيانات غير موجهة إليه، والتي تكون محمية بشكل خاص ضد الوصول غير المصرح به، وذلك عن طريق تجاوز وسائل الحماية.

(33) "Strafgesetzbuch (StGB)". Gesetze Im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/.

(34) German Federal Ministry of Justice. n.d. "Section 202a of the Criminal Code (Strafgesetzbuch, StGB)." Gesetze im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/__202a.html.

ب. يقصد بالبيانات تلك التي يتم تخزينها، أو نقلها إلكترونيًا، أو مغناطيسيًا، أو بأي وسيلة أخرى غير مرئية بشكل مباشر.

تستهدف هذه المادة الأفعال التي يقوم فيها الجاني بالوصول غير المصرح به إلى بيانات محمية، مثل اختراق أنظمة الكمبيوتر للوصول إلى معلومات سرية أو شخصية، ويشترط لتطبيق هذه المادة أن تكون البيانات محمية بوسائل تقنية، وأن يتم التحايل على هذه الوسائل للوصول إلى البيانات.

2. **التصيد الإلكتروني (اعتراض البيانات) – المادة (202b)**[35]:

أ. يعاقب بالسجن لمدة تصل إلى سنتين أو بغرامة كل من يحصل لنفسه أو لغيره، دون تصريح، (على بيانات غير موجهة إليه) وفقًا للمادة 202a ، وذلك باستخدام وسائل تقنية من عملية نقل بيانات غير عامة أو من الإشعاع الكهرومغناطيسي لنظام معالجة البيانات، ما لم يكن الفعل يعاقب عليه بعقوبة أشد بموجب أحكام أخرى.

تجرم هذه المادة التنصت غير المصرح به على البيانات أثناء نقلها أو من خلال التقاط الإشارات الكهرومغناطيسية. ويشمل ذلك اعتراض الاتصالات الخاصة أو التنصت على شبكات الواي فاي غير المحمية.

3. **سرقة البيانات – المادة (202d)**[36]:

أ. يعاقب بالسجن لمدة تصل إلى ثلاث سنوات أو بغرامة كل من يحصل لنفسه أو لغيره، أو ينقل، أو ينشر، أو يتيح بأي وسيلة بيانات (وفقًا للمادة 202a غير متاحة للعامة، والتي حصل عليها شخص آخر من خلال فعل غير قانوني، وذلك بقصد تحقيق مكسب لنفسه أو لطرف ثالث أو للإضرار بشخص آخر.

ب. لا يجوز أن تكون العقوبة أشد من العقوبة المقررة للجريمة الأصلية التي تم من خلالها الحصول على البيانات.

ج. لا تنطبق الفقرة (1) على الأفعال التي تهدف حصريًا إلى تنفيذ واجبات رسمية أو مهنية مشروعة، وتشمل على وجه الخصوص:

- الأفعال التي يقوم بها الموظفون العموميون أو وكلاؤهم بهدف استخدام البيانات حصريًا في إجراءات الضرائب، أو الإجراءات الجنائية، أو إجراءات المخالفات الإدارية.

(35) German Federal Ministry of Justice. n.d. "Section 202b of the Criminal Code (Strafgesetzbuch, StGB)." Gesetze im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/__202b.html.

(36) German Federal Ministry of Justice. n.d. "Section 202d of the Criminal Code (Strafgesetzbuch, StGB)." Gesetze im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/__202d.html.

- الأفعال المهنية للأشخاص المشار إليهم في المادة 53 (1) الجملة 1 البند 5 من قانون الإجراءات الجنائية، والتي تتعلق بتلقي البيانات أو تقييمها أو نشرها.

تجرم هذه المادة الحصول أو نقل أو نشر بيانات غير متاحة للعامة إذا تم الحصول عليها بوسائل غير قانونية، وذلك لتحقيق مكاسب شخصية أو للإضرار بالآخرين. تصل العقوبة إلى 3 سنوات سجن أو غرامة، بشرط ألا تتجاوز العقوبة المقررة للجريمة الأصلية. يستثني القانون الموظفين العموميين والصحفيين عند استخدام البيانات في إطار مهام رسمية أو مهنية مشروعة، مثل التحقيقات الجنائية أو الإجراءات الضريبية.

4. **التلاعب بالبيانات (تعديل البيانات) - المادة (303a)** [37]:

أ. يعاقب بالسجن لمدة تصل إلى سنتين أو بغرامة كل من يقوم بشكل غير قانوني بحذف، أو إخفاء، أو تعطيل، أو تعديل بيانات وفقًا للمادة 202a.

ب. يعاقب على الشروع في ارتكاب هذا الفعل.

ج. تسري المادة 202c بما يتناسب مع التحضير لارتكاب جريمة وفقًا للفقرة (1).

تستهدف هذه المادة الأفعال التي تتضمن التلاعب غير المصرح به بالبيانات، مثل حذف أو تعديل أو تعطيل البيانات المخزنة إلكترونيًا. يشمل ذلك التلاعب بملفات أو قواعد بيانات دون إذن.

5. **التخريب الإلكتروني (تخريب الحاسوب) - المادة (303b)** [38]:

أ. يعاقب بالسجن لمدة تصل إلى ثلاث سنوات أو بغرامة كل من يعطل بشكل كبير معالجة البيانات التي تعد ذات أهمية جوهرية لشخص آخر من خلال:

- ارتكاب جريمة وفقًا للمادة 1 (303a).
- إدخال أو نقل بيانات وفقًا للمادة 202a بقصد الإضرار بشخص آخر.
- تدمير، أو إتلاف، أو تعطيل، أو إزالة، أو تعديل نظام معالجة بيانات أو وسيط تخزين بيانات.

ب. إذا كانت معالجة البيانات ذات أهمية جوهرية لمؤسسة تجارية لطرف ثالث، أو لشركة لطرف ثالث، أو لهيئة حكومية، تكون العقوبة السجن لمدة تصل إلى خمس سنوات أو الغرامة.

(37) German Federal Ministry of Justice. n.d. "Section 303a of the Criminal Code (Strafgesetzbuch, StGB)." Gesetze im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/__303a.html.

(38) German Federal Ministry of Justice. n.d. "Section 303b of the Criminal Code (Strafgesetzbuch, StGB)." Gesetze im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/__303b.html.

ج. يعاقب على الشروع في ارتكاب هذا الفعل.

د. في الحالات الخطيرة المنصوص عليها في الفقرة (2)، تكون العقوبة السجن لمدة تتراوح بين ستة أشهر وعشر سنوات. وتعتبر الحالة خطيرة بشكل خاص إذا قام الجاني بِـ:

- التسبب في خسائر مالية كبيرة،

- التصرف بشكل تجاري أو كعضو في عصابة تم تشكيلها لارتكاب جرائم تخريب حاسوبي مستمرة.

- التأثير على توفير السلع أو الخدمات الأساسية للسكان، أو الإضرار بأمن جمهورية ألمانيا الاتحادية من خلال الفعل.

ه. تسري المادة 202c بما يتناسب مع التحضير لارتكاب جريمة وفقًا للفقرة (1).

تجرم هذه المادة أي تدخل غير قانوني في أنظمة معالجة البيانات، مثل التعطيل، الإتلاف، أو التعديل بقصد الإضرار بشخص أو جهة أخرى. وتصل العقوبة إلى 3 سنوات سجن أو غرامة، وترتفع إلى 5 سنوات إذا كان الضرر يؤثر على مؤسسات أو جهات حكومية. الحالات الخطيرة، مثل التسبب في خسائر مالية كبيرة أو تهديد الأمن الوطني، قد تؤدي إلى السجن حتى 10 سنوات، ويعاقب أيضًا على الشروع في الجريمة، مع تطبيق المادة 202c على التحضير لها.

6. **الاحتيال الحاسوبي – المادة (263a)** [39]:

أ. يعاقب بالسجن لمدة تصل إلى خمس سنوات أو بغرامة كل من، بقصد تحقيق مكسب مالي غير مشروع لنفسه أو لطرف ثالث، يلحق ضررًا بممتلكات شخص آخر من خلال التأثير على نتيجة عملية معالجة البيانات عن طريق:

- تصميم برنامج بشكل غير صحيح.

- استخدام بيانات غير صحيحة أو غير مكتملة.

- الاستخدام غير المصرح به للبيانات.

- أي وسيلة أخرى تؤثر على العملية.

ب. تسري الفقرات (2) إلى (6) من المادة 263 بما يتناسب مع هذه المادة.

(39) German Federal Ministry of Justice. n.d. "Section 263a of the Criminal Code (Strafgesetzbuch, StGB)." Gesetze im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/__263a.html.

ج. يعاقب بالسجن لمدة تصل إلى ثلاث سنوات أو بغرامة كل من يقوم بإعداد جريمة وفقًا للفقرة (1) عن طريق:

- إنشاء أو الحصول على أو بيع أو تخزين أو نقل برامج حاسوبية تهدف إلى ارتكاب مثل هذا الفعل.
- أو إنتاج أو الحصول على أو بيع، أو تخزين، أو نقل كلمات مرور ،أو رموز أمان أخرى مناسبة لارتكاب مثل هذا الفعل.

د. في الحالات المذكورة في الفقرة (3)، تسري الفقرتان (2) و (3) من المادة 149 بما يتناسب مع هذه المادة.

تجرم هذه المادة الاحتيال باستخدام أنظمة الحاسوب لتحقيق مكاسب مالية غير مشروعة، مثل التلاعب بالبيانات أو البرامج أو الاستخدام غير المصرح به. تصل العقوبة إلى 5 سنوات سجن أو غرامة. كما يعاقب بالسجن حتى 3 سنوات أو الغرامة على من يعد لهذه الجرائم عبر تطوير أو بيع برامج احتيالية أو حيازة بيانات وصول غير قانونية، وتسري أيضًا بعض أحكام المادة 263 والمادة 149 على هذه الجرائم، مما يعزز من نطاق تطبيقها القانوني.

7. **تزوير البيانات ذات القيمة الإثباتية (ذات الصلة بالأدلة) – المادة (269)** [40]:

أ. يعاقب بالسجن لمدة تصل إلى خمس سنوات أو بغرامة كل من، بقصد التضليل في المعاملات القانونية، يقوم بتخزين أو تعديل بيانات إثباتية بطريقة تجعلها عند إدراكها تبدو وكأنها مستند مزور أو محرف، أو يستخدم بيانات تم تخزينها أو تعديلها بهذه الطريقة.

ب. يعاقب على الشروع في ارتكاب هذا الفعل.

ج. تسري الفقرتان (3) و (4) من المادة 267 بما يتناسب مع هذه المادة.

تجرم هذه المادة تخزين أو تعديل البيانات الإثباتية بشكل يجعلها تبدو كمستندات مزورة، بهدف التضليل في المعاملات القانونية. تصل العقوبة إلى 5 سنوات سجن أو غرامة، كما يعاقب على الشروع في الجريمة. تطبق بعض أحكام المادة 267 لتعزيز العقوبات وضمان شمولية التعامل مع التزوير الرقمي.

(40) German Federal Ministry of Justice. n.d. "Section 269 of the Criminal Code (Strafgesetzbuch, StGB)." Gesetze im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/__269.html.

8. **التحضير للتجسس واعتراض البيانات – المادة (202c)**[41]:

أ. يعاقب بالسجن لمدة تصل إلى سنتين أو بغرامة كل من يقوم بإعداد جريمة وفقًا للمادة 202a أو المادة 202b من خلال:

- إنشاء أو الحصول على أو بيع، أو نقل، أو توزيع، أو إتاحة كلمات المرور، أو غيرها من رموز الأمان التي تتيح الوصول إلى البيانات وفقًا للمادة 2 (202a).
- إنشاء أو الحصول على أو بيع، أو نقل، أو توزيع، أو إتاحة برامج حاسوبية تهدف إلى ارتكاب مثل هذا الفعل.

ب. تسري الفقرتان (2) و (3) من المادة 149 بما يتناسب مع هذه المادة.

تجرم هذه المادة إعداد أو تسهيل الجرائم الإلكترونية عبر إنشاء، أو توزيع، أو بيع كلمات المرور، أو برامج القرصنة التي تتيح الوصول غير المصرح به للبيانات. تصل العقوبة إلى سنتين سجن أو غرامة. كما تطبق بعض أحكام المادة 149 لتعزيز مكافحة الجرائم الإلكترونية التي تهدف إلى اختراق البيانات أو التجسس عليها.

اللائحة العامة لحماية البيانات GDPR – الاتحاد الأوروبي[42]

تعد اللائحة العامة لحماية البيانات GDPR اختصارًا لِـ" General Data Protection Regulation" ، وهي مجموعة من القواعد والقوانين التي تم وضعها من قبل الاتحاد الأوروبي لحماية حقوق جميع مواطني الاتحاد، وتمت الموافقة عليها في 14 أبريل 2016 من قبل المفوضية الأوروبية، وطبقت اللائحة في مايو 2018؛ حيث تمنح الحق للمستخدم بإزالة بياناته، بشكل جزئي أو كامل، من شبكة الإنترنت، كما تعزز حقوق المواطن في حماية بياناته، على أنه تحكمها بعض الضوابط، ومن أهمها:

1. **الحق في الموافقة:** يحق للمستخدم الموافقة الصريحة والواضحة على السماح للشركة بالتصرف في بياناته الخاصة، عكس ما كان عليه الأمر في السابق، فقد كانت الشركات تكتفي بسكوت المستخدم وعدم تحركه لتعديل الخصائص الخاصة ببياناته.
2. **القابلية للنقل:** أقر القانون الجديد حق المستخدمين في نقل بياناتهم وإعادة استخدامها في خدمات أخرى.

(41) German Federal Ministry of Justice. n.d. "Section 202c of the Criminal Code (Strafgesetzbuch, StGB)." Gesetze im Internet. Accessed 122025/02/. https://www.gesetze-im-internet.de/stgb/__202c.html.

(42) European Union. (2016). Regulation (EU) 2016679/ of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data (General Data Protection Regulation), accessed February 19, 2025. Available at: https://tinyurl.com/2bjf3444.

3. **الحق في المحو:** بحيث أصبح بإمكان مستخدمي الإنترنت داخل الاتحاد الأوروبي طلب مسح بياناتهم الشخصية.

4. **الحق في النسيان:** وقد عمدت اللائحة الأوروبية الأخيرة إلى تقنين مبدأ سبق لإحدى المحاكم الأوروبية أن أقرته سنة 2014، وأجبرت من خلاله شركة غوغل على منح المستخدمين الأوروبيين الحق في مسح أي معلومات أو روابط لا يرغبون في أن ترتبط بأسمائهم في الفضاء الرقمي.

يستنتج من استعراض نصوص القانون الجنائي الألماني أن المشرع الألماني اعتمد مقاربة تفصيلية دقيقة في تنظيم الجرائم السيبرانية، حيث يتم تفكيك كل صورة جرمية إلى مادة مستقلة وفقًا لطبيعتها وخطورتها، وهو ما يسهم في وضوح القاعدة القانونية وسهولة تطبيقها من الناحيتين القضائية والإجرائية. وعلى النقيض، يتجه المشرع القطري إلى الجمع بين أفعال متعددة ضمن مادتين رئيستين، مما قد يؤثر على دقة التطبيق العملي ويصعب من عملية التمييز بين الأفعال المختلفة. ويعد هذا الاختلاف البنيوي في التشريع من أبرز الفروقات بين النظامين، مما يفتح الباب أمام مقترحات تطوير الصياغة التشريعية في القانون القطري بما يضمن تجريمًا أوضح وتطبيقًا أكثر فاعلية.

ثالثًا: أوجه التشابه بين التشريعين القطري والألماني

على الرغم من اختلاف السياقات القانونية والاجتماعية التي انبثقت منها كل من المنظومتين القطرية والألمانية، فإن تحليل النصوص القانونية يظهر عددًا من القواسم المشتركة التي تشكل أرضية قانونية متقاربة في التصدي للجرائم السيبرانية، ومنها:

1. يتفق كلا التشريعين على ضرورة وجود إطار قانوني خاص ومستقل لمكافحة الجرائم الإلكترونية، بحيث يتضمن قائمة صريحة بالأفعال الجرمية المرتبطة باستخدام الشبكات والتقنيات الحديثة، فقد أصدرت قطر قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، فيما كرس القانون الجنائي الألماني (StGB) عددًا من المواد المتخصصة التي تتناول ذات الأفعال.

2. يتوافق كلا القانونين في تجريم الوصول غير المصرح به إلى الأنظمة والشبكات الإلكترونية، فبينما تنص المادة (2) من القانون القطري على عقوبات ضد أي دخول غير مشروع، تتناول المادة (§ 202a StGB) من القانون الألماني ذات الفعل بوصفه «تجسسًا على البيانات»، مع اختلاف في التقنيات والصياغات.

3. يشترك النظامان في تجريم التلاعب بالبيانات أو حذفها أو تغييرها دون وجه حق؛ إذ تنص المادة (3) من القانون القطري على عقوبات صارمة لمن يقدم على تعديل أو حذف بيانات، وهو ما يقابله في القانون الألماني المادة (§ 303a) المتعلقة «بتعديل البيانات» و«إتلافها الإلكتروني».

4. يوجد تطابق في مفهوم الحماية الخاصة للبيانات الشخصية؛ إذ نص القانون القطري رقم (13) لسنة 2016 على حماية خصوصية البيانات، بينما يعد نظام الـ GDPR الأوروبي، المطبق في ألمانيا، أحد أكثر الأنظمة صرامة في هذا المجال. ويقر كلا التشريعين بحق الأفراد في التحكم في بياناتهم الشخصية ويفرضان التزامات على الجهات التي تقوم بجمعها أو معالجتها.

5. يتشارك النظامان في تجريم أعمال الاحتيال الإلكتروني والتزوير باستخدام التقنية، فالمادة (11) من القانون القطري تعاقب على انتحال الهوية الإلكترونية والاستيلاء على الأموال بطرق احتيالية، فيما تتضمن المواد (§ 263a و§ 269 StGB) الألمانية أحكامًا مماثلة تتعلق بالاحتيال المعلوماتي والتزوير الرقمي ذي القيمة الإثباتية.

6. يؤكد كلا النظامين أهمية تعزيز التعاون الدولي وتبادل المعلومات في مواجهة الجرائم العابرة للحدود، لا سيما في ظل الطابع غير الإقليمي للفضاء السيبراني. ويظهر ذلك في الباب الرابع من القانون القطري المتعلق بالتعاون الدولي، وفي التزام ألمانيا باتفاقية بودابست، التي تمثل الإطار الأوروبي للتعاون في مكافحة الجرائم السيبرانية.

رابعًا: أوجه الاختلاف بين التشريعين القطري والألماني

على الرغم من وجود قواسم مشتركة بين التشريعين القطري والألماني، إلا أن التحليل المقارن يكشف عن عدد من الاختلافات الجوهرية في البنية القانونية، ومنهجية التجريم، وآلية العقاب، وطبيعة التطبيق القضائي.

1. يتسم التشريع الألماني بتفصيل بنيوي، حيث يفرد لكل صورة من صور السلوك الجرمي مادة مستقلة تُعنى بتحديد عناصر الجريمة وظروفها الخاصة، كما هو الحال في المواد (202a و 202b و 202c و 303a و 303b). وفي المقابل يجمع التشريع القطري عددًا من الأفعال الجرمية ذات الطبيعة المختلفة في نصوص عامة وشاملة (خصوصًا المادتين 2 و3)، مما قد يخلق تداخلًا في المفاهيم ويربك التطبيق القضائي.

2. يظهر القانون الألماني تمييزًا واضحًا بين الأفعال التحضيرية والأفعال التنفيذية، حيث يتم تجريم إعداد أدوات القرصنة أو إنشاء كلمات المرور ضمن المادة (202c)، وهو ما لا

ينص عليه القانون القطري، مما يشير إلى وجود فجوة في تجريم الأفعال القبلية التي تسبق الفعل الجرمي ذاته.

3. على مستوى العقوبات، يعتمد القانون القطري نظامًا تقليديًا ثابتًا في تحديد العقوبات (الحبس والغرامة بمبالغ محددة)، في حين يستخدم القانون الألماني نظام الغرامات اليومية (Tagessätze)، الذي يربط الغرامة بدخل الجاني، مما يضفي طابعًا مرنًا وعادلًا في التنفيذ.

4. في نطاق حماية البيانات الشخصية، رغم صدور القانون القطري رقم (13) لسنة 2016، إلا أن النظام الأوروبي الذي تتبناه ألمانيا (GDPR) يعد أكثر شمولًا من حيث الحقوق المكفولة، وآليات الشكاوى، وحدود المعالجة، وتطبيق مبدأ «الحق في النسيان».

5. من حيث التعاون الدولي، فإن ألمانيا تعد طرفًا في اتفاقية بودابست منذ بدايتها، وتفعل أحكام التعاون القضائي المشترك بشكل عملي. بينما لا تزال قطر خارج هذه الاتفاقية، رغم وجود إشارات في قانونها الوطني للتعاون الدولي. ويعد ذلك عنصرًا فارقًا في التصدي للجرائم السيبرانية العابرة للحدود.

6. التطور الزمني للتشريعات يشير إلى فرق واضح في الدينامية؛ حيث يتم تعديل مواد القانون الألماني بصورة دورية بما يواكب التطورات التقنية، في حين أن القانون القطري، منذ صدوره في 2014، لم يشهد تعديلات بنيوية رغم تطور البيئة الرقمية.

المطلب الثاني

التحديات التشريعية والتدابير القانونية في النظامين القطري والألماني

بعد تحليل النصوص القانونية المتعلقة بالجرائم السيبرانية في كل من دولة قطر وجمهورية ألمانيا الاتحادية، وبيان أوجه التشابه والاختلاف في آليات التجريم والحماية، تبرز الحاجة إلى التعمق في التحديات التي تواجه المنظومتين التشريعيتين في هذا المجال، فضلًا عن استعراض التدابير القانونية والقضائية التي اعتمدها كل نظام. وتستند أهمية هذا المطلب إلى ما أشار إليه المحكمون من ضرورة تجاوز التحليل النظري نحو معالجة فعالية النصوص عند التطبيق، ومدى كفاية التدابير المتخذة، وما إذا كانت توجد فجوات تشريعية أو صعوبات واقعية تحد من فاعلية الردع القانوني.

وعليه، يقسم هذا المطلب إلى أولًا ويتناول التحديات والتدابير في التشريع القطري، وثانيًا ويتناول التحديات والتدابير في التشريع الألماني، ثم يُختتم بخلاصة مقارنة تبرز مكامن القوة والقصور.

أولاً: التحديات والتدابير في التشريع القطري

على الرغم من صدور قانون مكافحة الجرائم الإلكترونية في قطر بموجب القانون رقم (14) لسنة 2014 [43]، فإن الواقع العملي يكشف عن عدد من التحديات التي تعيق تحقيق فاعلية كاملة في مواجهة الجرائم السيبرانية. وتتمثل أبرز هذه التحديات فيما يلي:

1. غياب التفصيل في التجريم: كما بينت الدراسة في المطلب الأول، فإن المادتين (2) و (3) من القانون تتضمنان عددًا من الأفعال الجرمية المتنوعة – كالدخول غير المشروع، والتلاعب، والحذف، والإفشاء – في إطار نصوص واحدة، مما يخلق صعوبة عملية في التكييف القانوني والتوصيف الجنائي الدقيق لكل واقعة على حدة. وقد أشار المحكمون صراحةً إلى أن هذا الدمج يضعف الردع ويعقد الإثبات القضائي[44].

2. عدم تجريم الأفعال التحضيرية: لا يتضمن القانون القطري نصًا يجرم إعداد أدوات الاختراق أو حيازة برامج التسلل، بخلاف ما ينص عليه القانون الألماني المادة 202c [45]، ما يفتح ثغرة أمام نشاط إجرامي سابق للفعل الأساسي، ويقلل من قدرة السلطات على التدخل الوقائي.

3. محدودية الإشارة إلى التدابير القضائية والإجرائية: لا يفصل القانون بشكل كاف آليات التحقيق الرقمية، أو متطلبات الإثبات الفني، ولا يحدد الإجراءات التقنية المتخصصة التي ينبغي اتباعها عند التعامل مع أدلة إلكترونية، مما يخلق صعوبات في تطبيق النصوص أمام القضاء[46].

4. صعوبة التفعيل العملي للتعاون الدولي: رغم إيراد القانون في بابه الرابع لأحكام تتعلق بالتعاون الدولي، فإن قطر ليست طرفًا في اتفاقية بودابست، ما يضعف قدرتها على الاستفادة من آليات المساعدة القانونية المتبادلة المفعلة في الدول الأوروبية، ويقلل من فاعلية ملاحقة الجرائم العابرة للحدود.[47]

5. ثبات نظام العقوبات وعدم مرونته: يعتمد القانون القطري على غرامات ثابتة ومحددة، بغض النظر عن دخل الجاني أو خطورة الفعل، ولا يتماشى مع التوجه الحديث القائم على اعتماد غرامات مرنة [48] (Tagessätze)، ترتبط بالوضع المالي للفرد.

(43) State of Qatar, Law No. 14 of 2014 on Combating Cybercrime, Official Gazette (2014), https://almeezan.qa/LawPage.aspx?id=6366&language=ar.

(44) Ibid

(45) Germany, Strafgesetzbuch (StGB), §202c, accessed April 30, 2025, https://www.gesetze-im-internet.de/stgb/__202c.html.

(46) State of Qatar, Law No. 14 of 2014, Articles 4 and 7.

(47) Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

(48) Ibid., Article 8.

في مقابل هذه التحديات، اعتمد المشرع القطري عددًا من التدابير الجزئية المهمة، أبرزها:

1. صدور قانون حماية البيانات الشخصية رقم (13) لسنة 2016[49].
2. إدماج بعض جوانب التحقيق الرقمي ضمن مهام النيابة العامة والأمن السيبراني في وزارة الداخلية.
3. تنظيم ندوات توعوية بالتنسيق مع جهات حكومية.

إلا أن هذه التدابير لا تزال بحاجة إلى تطوير تشريعي شامل، يضمن تفصيل الأفعال، وتجريم التحضير، وتعزيز التعاون الدولي، وإقرار أدوات استدلال متخصصة.

ثانيًا: التحديات والتدابير في التشريع الألماني

يعد الإطار التشريعي الألماني من أكثر الأنظمة تطورًا ودقةً في تنظيم الجرائم السيبرانية، إلا أن التطبيق العملي يواجه أيضًا مجموعة من التحديات القانونية والتقنية، ولا سيما في ظل التطور السريع للفضاء الرقمي. ويمكن تلخيص أبرز هذه التحديات على النحو التالي:

1. تعقيد البنية القانونية وتشتت النصوص: رغم أن توزيع الجرائم على مواد مستقلة مثل (202a و 202b و 202c و 303a و 303b...) يسهم في وضوح التجريم، إلا أن هذا التشعب يتطلب من جهات التحقيق والقضاء مستوى عاليًا من التخصص لفهم الفروق الدقيقة بين النصوص، مما قد يؤدي إلى تفاوت في التطبيق[50].
2. محدودية النطاق القضائي أمام الجرائم العابرة للحدود: كثير من الجرائم السيبرانية ترتكب من خارج الأراضي الألمانية، ومع أن ألمانيا طرف في اتفاقية بودابست وتملك آليات تعاون فعالة، إلا أن التنفيذ العملي يواجه تأخيرًا وإشكالات في تبادل البيانات مع دول غير موقعة أو ذات أنظمة قانونية مغايرة.[51]
3. صعوبات تحديد هوية الجناة: تعتمد الجرائم السيبرانية غالبًا على إخفاء الهوية (IP masking)، والولوج عبر شبكات مجهولة TOR،VPN، مما يجعل الوصول إلى الجناة الحقيقيين أمرًا بالغ التعقيد، ويستلزم موارد وخبرات متقدمة في التحليل الرقمي.[52]
4. التوازن بين حماية البيانات وفعالية التحقيق: في ظل تطبيق اللائحة العامة لحماية البيانات (GDPR)، تفرض قيود صارمة على الوصول إلى بيانات الأفراد، مما قد يتعارض أحيانًا مع

(49) State of Qatar, Law No. 13 of 2016 on Personal Data Protection, Official Gazette (2016), https://almeezan.qa/LawView.aspx?LawID=7121&language=ar.

(50) Germany, Strafgesetzbuch (StGB), accessed April 30, 2025, https://www.gesetze-im-internet.de/englisch_stgb/

(51) Council of Europe, Budapest Convention, see note 5.

(52) Gercke, Marco, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, 2012, 83–85.

مقتضيات التحقيق في بعض الجرائم الإلكترونية الحساسة، خاصة عندما يتعلق الأمر بجمع الأدلة أو تحليل المحتوى الرقمي الخاص.[53]

5. الحاجة المستمرة إلى تعديل النصوص لمواكبة التهديدات الجديدة: التكنولوجيا تتطور بوتيرة أسرع من التشريعات، ويجد المشرع الألماني نفسه مطالبًا بتحديث القانون بشكل متكرر، كما حصل في السنوات الأخيرة عند إدراج بعض أنواع الهجمات مثل هجمات «الفدية الرقمية» أو «هجمات تعطيل الخدمة DDoS"[54].

مقابل هذه التحديات، اعتمد النظام الألماني عددًا من التدابير القانونية والتقنية الرائدة، منها:

1. النص الصريح على تجريم الأفعال التحضيرية المادة 202c.
2. استخدام نظام الغرامات اليومية (Tagessätze) المرتبط بدخل الجاني.
3. إدراج الجرائم السيبرانية ضمن الجرائم المنظمة على المستوى الفيدرالي.
4. تفعيل التعاون الدولي بموجب اتفاقية بودابست.
5. إنشاء وحدات متخصصة في الادعاء العام والشرطة الفيدرالية للتحقيق الرقمي والتحليل الجنائي الإلكتروني.

وتشير هذه التدابير إلى أن النظام الألماني لا يكتفي بتجريم الأفعال، بل يربطها بإطار مؤسسي وتشغيلي يسهم في رفع مستوى الجاهزية القانونية والتقنية على السواء، ومن خلال ما سبق يتضح أن التشريع القطري يواجه عددًا من التحديات البنيوية، أبرزها الدمج الكلي لصور جرمية متعددة في مواد موحدة، وغياب تجريم الأفعال التحضيرية، ويحتاج إلى المزيد من المرونة في نظام العقوبات، كما أن تقييد التعاون الدولي يحد من فاعلية الردع القانوني ويصعب التطبيق العملي.

في المقابل، يتميز التشريع الألماني ببنية تفصيلية تفرد لكل فعل مادة مستقلة، وتدرج التحضير كجريمة قائمة بذاتها، وتفعل أدوات التعاون الدولي بموجب اتفاقيات نافذة، كما يعتمد نظام عقوبات مرن يرتبط بالدخل ويراعي العدالة النسبية.

ومع ذلك، لا يخلو النظام الألماني من تحديات واقعية، مثل تعقيد ملاحقة الجناة في بيئة عابرة للحدود، والتوازن الصعب بين حماية البيانات وفعالية التحقيق. ويخلص هذا المطلب

(53) European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016679/, accessed April 30, 2025, https://gdpr.eu.

(54) Germany, StGB, §40, https://www.gesetze-im-internet.de/stgb/__40.html.

إلى أن فعالية أي نظام قانوني في مواجهة الجرائم السيبرانية لا تقتصر على النصوص التشريعية، بل تتطلب إجراءات مؤسسية مكملة، واستجابة مرنة للتحولات التقنية المتسارعة، مع إشراك دائم للجهات القضائية والأمنية والمجتمع المدني في تطوير تلك الأطر باستمرار.

المطلب الثالث
مقارنة التشريع القطري والألماني في (جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية)

تأتي جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية في صلب التحديات المعاصرة التي تواجه الأمان الرقمي، حيث تشكل حجر الزاوية في حماية البنية التحتية الحيوية للمعلومات. وفي ظل التطور التكنولوجي السريع واعتماد المجتمعات على الأنظمة الرقمية في جميع جوانب الحياة، يبرز من هذا المطلب مقارنة دقيقة بين التشريع القطري والألماني لمواجهة هذه الجرائم. وتهدف المقارنة إلى استعراض أوجه التشابه والاختلاف في نصوص التشريع والعقوبات المقررة، وذلك بهدف تقديم رؤية متكاملة تظهر مدى كفاءة كل نظام في التصدي للتحديات الأمنية الناجمة عن الجرائم السيبرانية.

أولًا: أوجه التشابه بين التشريع القطري والألماني في (جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية) [55]:

البند	المشرع القطري	المشرع الألماني
تجريم الوصول غير المصرح به	المادة (2) والمادة (3) تجرمان الدخول بغير وجه حق إلى موقع إلكتروني أو نظام معلوماتي، سواء لأجهزة الدولة أو غيرها، مع مضاعفة العقوبة إذا ترتب على ذلك الحصول على بيانات تمس الأمن أو تدمير البيانات أو الإضرار بالمستخدمين.	المادة (202a) تعاقب على الوصول إلى بيانات محمية عن طريق تجاوز وسائل الحماية، وهي تشمل أنظمة المعالجة أو أجهزة الحاسوب أو الخوادم طالما أنها مخزنة إلكترونيًا أو مغناطيسيًا ومحمية بشكل خاص.

(55) تم إعداد هذا الجدول من قبل الباحث استنادًا إلى تحليل ومقارنة الأحكام الواردة في القانون القطري لمكافحة الجرائم الإلكترونية (رقم 14 لسنة 2014) والقانون الجنائي الألماني (Strafgesetzbuch – StGB)، وذلك بهدف تحديد أوجه التشابه في التشريعات المتعلقة بجرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، من حيث تجريم الوصول غير المصرح به، اعتراض البيانات، التلاعب بها أو إتلافها، تشديد العقوبات في الحالات الخطيرة، واستهداف الأدوات التحضيرية للجريمة الإلكترونية.

التنصت على البيانات	المادة (4) تجرم التقاط أو اعتراض أو تنصت أي بيانات مرسلة عبر الشبكة المعلوماتية دون وجه حق.	المادة (202b) تجرم اعتراض البيانات في سياق نقلها (بشكل غير علني) أو عبر الإشعاع الكهرومغناطيسي لنظام المعالجة.
معاقبة التلاعب بالبيانات أو إتلافها	المادة (2) والمادة (3) تنصان على تشديد العقوبة إذا أدى الدخول غير المصرح به إلى إلغاء، أو حذف، أو إضافة، أو إفشاء، أو إتلاف، أو تغيير بيانات إلكترونية، أو تعطيل الموقع ،أو النظام المعلوماتي.	المادة (303a) تجرم الحذف أو التعطيل أو التعديل غير المشروع للبيانات. والمادة (303b) تتناول تعطيل معالجة البيانات أو إتلاف أنظمة المعالجة بشكل كبير.
تشديد العقوبات في الحالات الخطيرة	ينص على مضاعفة العقوبة في حال الحصول على بيانات تمس أمن الدولة أو اقتصادها (المادة 2)، أو إذا تم إلحاق ضرر بالمستخدمين، أو تدمير أو تعطيل النظام (المادة 3).	ينص على تشديد العقوبة (قد تصل إلى 5 سنوات أو 10 سنوات في الحالات الخطيرة) إذا كانت معالجة البيانات ذات أهمية جوهرية لمؤسسة أو لهيئة حكومية، أو إذا ترتب خسائر كبيرة أو مساس بأمن الدولة (المادة 303b).
استهداف الأدوات التحضيرية للجريمة الإلكترونية	وإن لم ينص صراحة على مادة مستقلة لتجريم إعداد الأدوات الإجرامية، لكنه يجرم الدخول أو الاستخدام بغير وجه حق (المادة 3) بما يشمل تقنيًا امتلاك أو استخدام وسائل تساعد في الاختراق، وكذلك إمكانية تجريم الشروع.	المادة (202c) تجرم التحضير للتجسس أو الاعتراض عبر إنشاء، أو حيازة، أو بيع برامج، أو كلمات مرور، أو رموز أمان تستعمل في الاختراق.

ثانيًا: أوجه الاختلاف بين التشريع القطري والألماني في (جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية) [56]:

البند	المشرع القطري	المشرع الألماني
التفصيل التشريعي والصياغة	• يستخدم تعابير واضحة وصريحة مثل "موقع إلكتروني"، "نظام معلوماتي"، "شبكة معلوماتية". • يجمع أكثر من صورة للفعل الإجرامي تحت المادة نفسها (مثلًا المادة 2 والمادة 3 تشملان الدخول غير المشروع والتخريب والسرقة الإلكترونية... إلخ).	• يعتمد على مصطلحات أكثر عمومية ("بيانات محمية"، "نظام معالجة بيانات")، والتي يفهم منها شموله للمواقع والشبكات والأنظمة. • يقسم الأفعال على عدة مواد مستقلة (202a للتجسس، 202b للاعتراض، C202 للتحضير... إلخ).
عقوبات الحبس والغرامة	• يضع عقوبة حبس لا تجاوز 3 سنوات أو سنتين (بحسب المادة)، مع تحديد سقف للغرامة (500 ألف ريال أو 100 ألف ريال). • ينص على مضاعفة العقوبة في حال توافر ظروف مشددة.	• يضع مدة حبس تصل إلى 3 سنوات أو 5 سنوات أو 10 سنوات في الحالات الخطيرة. • لا يحدد سقفًا عدديًا للغرامة في نص المادة، إنما تقدر وفق نظام "الغرامة اليومية "(Tagessätze)، مما يضفي مرونة عند تحديد مقدارها.
حالة استهداف البيانات الحساسة للدولة	• صراحةً يقرر عقوبة مضاعفة إذا كانت البيانات تمس الأمن الداخلي أو الخارجي للدولة أو الاقتصاد الوطني (المادة 2)، أو إذا تعلق الأمر بأجهزة الدولة وهيئاتها.	• يرفع العقوبة إذا كان النظام أو البيانات "ذات أهمية جوهرية" (مؤسسة حيوية أو هيئة حكومية) أو إذا تأثر أمن الدولة. لكن معيار "الأهمية الجوهرية" (besonders schwere Fall) يترك تقديرًا أوسع للقضاء لتحديد ما إذا كانت الحالة خطيرة.

(56) تم إعداد هذا الجدول من قبل الباحث استنادًا إلى تحليل ومقارنة الأحكام الواردة في القانون القطري لمكافحة الجرائم الإلكترونية (رقم 14 لسنة 2014) والقانون الجنائي الألماني (Strafgesetzbuch – StGB)، وذلك بهدف تحديد أوجه الاختلاف في التشريعات المتعلقة بجرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية من حيث الصياغة القانونية، العقوبات، استهداف البيانات الحساسة، والتحريض أو الاشتراك في الجرائم الإلكترونية.

التحريض أو الاشتراك في الجرائم الإلكترونية	• لم ينص صراحةً في المواد (2، 3، 4) على تحضير الأدوات (برامج الاختراق) أو التحريض عليها، لكن المادة (3) تشدد العقوبة إذا تم "تجاوز الدخول المصرح به" أو "استمر في التواجد" بعد علمه باللاشرعية، ويمكن الاستناد لمواد عامة بشأن الاشتراك والتحريض.	• خصص المادة (202c) لتجريم مجرد الإعداد والتحضير لهذه الجرائم (ببرامج، كلمات مرور، إلخ)، وهي مادة واضحة بهذا الخصوص.
تجزئة الأفعال مقابل دمجها في نص واحد	• المزج بين عدد من الأفعال ضمن المادة (2) و(3) (الدخول، الإتلاف، التعطيل، النسخ، النشر... إلخ).	• ينتهج أسلوب التفصيل في مواد مختلفة، فيتوزع الفعل الإجرامي (تجسس، اعتراض، تحضير، تعديل البيانات، تخريب الحاسوب) على مواد مستقلة بكل فعل.

النتائج:

في ضوء النص ومجريات الدراسة المقارنة بين التشريعات القطرية والألمانية في مجال الجرائم السيبرانية، يمكن بلورة النتائج على النحو الآتي:

1. **تطور التشريعات استجابةً للجرائم السيبرانية**: أظهرت الدراسة أن كلًا من قطر وألمانيا طورت أطرًا قانونية للتعامل مع الجرائم السيبرانية التي تشهد تطورًا مستمرًا. ففي قطر جاء قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، بينما يستعين المشرع الألماني بمجموعة مواد متفرقة ضمن قانون العقوبات (StGB) لمواجهة الجرائم الإلكترونية بأشكالها المختلفة.

2. **وجود قواسم مشتركة في التجريم**، يتشابه التشريعان في تجريم الأفعال الآتية:
   أ. الوصول غير المصرح به للأنظمة أو البيانات.
   ب. اعتراض البيانات أو التنصت عليها دون تصريح.
   ج. التلاعب بالبيانات أو إتلافها أو حذفها بغير وجه حق.
   د. تشديد العقوبات في حال كانت البيانات أو الأنظمة ذات حساسية خاصة، أو ترتب على الجريمة أضرار مالية كبيرة أو تهديد لأمن الدولة.

3. **اختلاف مستويات التفصيل والصياغة**

أ. **التشريع القطري**: يميل إلى استخدام مصطلحات واضحة (مثل "موقع إلكتروني" و"نظام معلوماتي" و"شبكة معلوماتية")، ويتضمن في مواد محدودة عدة صور من الجريمة (كما في المواد 2، 3 من قانون رقم 14).

ب. **التشريع الألماني**: يعتمد على تعابير تقنية عامة نسبيًا (مثل "بيانات محمية" و"نظام معالجة بيانات")، ويقسم الجرائم على مواد مستقلة (202a للتجسس، 202b للاعتراض، 202c للتحضير...)، مما يجعله أكثر تفصيلًا في توزيع الأفعال.

4. **تفاوت العقوبات وآلية تحديد الغرامات**

أ. **في قطر**: العقوبات محددة بسقف أقصى للغرامة (500 ألف ريال أو 100 ألف ريال)، والحبس الذي لا يتجاوز 3 سنوات أو 2 سنة بحسب الحالة، مع مضاعفة العقوبة في الظروف المشددة.

ب. **في ألمانيا**: أقصى العقوبات قد تصل إلى 3 أو 5 أو حتى 10 سنوات في الحالات الخطيرة جدًا، ولا يوجد سقف عددي للغرامة في نص القانون؛ إذ يطبق نظام "الغرامة اليومية"(Tagessätze) الذي يعتمد على الدخل المادي للجاني.

5. **حماية البيانات الحساسة وأمن الدولة**

أ. يشدد القانون القطري العقوبات إذا تعلق الاختراق ببيانات تخص أجهزة الدولة أو تمس الأمن الداخلي أو الخارجي أو الاقتصاد الوطني.

ب. في ألمانيا، يعتبر التخريب الإلكتروني "خطيرًا بشكل خاص" إذا أثر على بنى حيوية أو مؤسسات حكومية، أو أدى إلى خسائر مالية كبيرة أو هدد الأمن الاتحادي.

6. **التعامل مع الأدوات التحضيرية**

أ. المشرع الألماني (المادة 202c) ينص صراحةً على تجريم حيازة أو إنتاج أو نشر أدوات تقنية (برامج أو كلمات مرور) مخصصة للاختراق والتجسس.

ب. المشرع القطري لا يخصص مادة مستقلة لذلك، لكنه يجرم أفعال الدخول غير المشروع تحت المادة (3)، ما يعني أن الأدوات التحضيرية مغلفة ضمن الأفعال الأصلية أو يستفاد من المواد العامة للشروع أو الاشتراك.

7. **عدم وجود تعريف موحد للجريمة السيبرانية في ألمانيا**: القانون القطري يذكر ضمن قانون مكافحة الجرائم الإلكترونية (المادة الأولى) تعريفات واضحة لمصطلحات تقنية عدة؛ فيما لا يتوفر في القانون الألماني تعريف موحد لمصطلح "الجريمة الإلكترونية"، بل يتناول الأفعال في مواد مختلفة ضمن قانون العقوبات.

8. **التعاون الدولي ومواجهة الطبيعة العابرة للحدود**: كلا النظامين يعترف بأهمية التعاون الدولي، وإن كان ذلك يظهر بوضوح في القانون القطري (الباب الرابع المتعلق بالتعاون الدولي) وفي عضوية ألمانيا في اتفاقيات أوروبية (مثل اتفاقية بودابست 2001). وينسجم هذا مع الصفة العابرة للحدود التي تتسم بها الجرائم السيبرانية.

9. **الحاجة لاستمرار التطوير والتكيف**: تبين الدراسة أن الجرائم السيبرانية تتطور بسرعة، ما يستدعي مراجعات دورية للقوانين الوطنية لتغطية المستجدات التقنية. ففي حين قطعت ألمانيا شوطًا متقدمًا في بناء إطار تشريعي مفصل وقابل للتعديل، فإن قطر عززت قوانينها مؤخرًا مع وجود مساحة للاستمرار في مواءمة أفضل الممارسات الدولية.

10. **أهمية نشر الوعي وبناء القدرات**: تؤكد النتائج ضرورة أن تواكب الجهود التشريعية إجراءات توعوية شاملة للأفراد والمؤسسات، والاستثمار في خبرات التحقيق الرقمي وبناء القدرات التقنية للأجهزة المختصة، إذ يعد ذلك مكملًا أساسيًا لنجاعة القوانين في مواجهة الجرائم السيبرانية.

الخلاصة

خلصت هذه الدراسة، عبر التحليل المقارن بين التشريعين القطري والألماني في مجال مكافحة الجرائم السيبرانية، إلى عدد من النتائج الجوهرية التي تكشف عن تباين واضح في منهجية التجريم وبنية النصوص القانونية وآليات التطبيق. يتضح أن التشريع القطري يجمع أفعالاً جرمية مختلفة في مادتين عامتين (المادتين 2 و3 من قانون مكافحة الجرائم الإلكترونية)، مما يؤدي إلى صعوبة تحديد الوصف القانوني الدقيق، وتحديات في الإثبات، وعدم توازن بين الجريمة والعقوبة المقررة لها.

كما كشفت الدراسة عن غياب تجريم الأفعال التحضيرية في القانون القطري، وعدم تبني نظام غرامات مرن يراعي الوضع المالي للجاني (كما هو الحال في النموذج الألماني عبر مبدأ (Tagessätze)، إضافةً إلى محدودية التفعيل العملي للتعاون القضائي الدولي، نتيجة عدم انضمام دولة قطر إلى اتفاقية بودابست.

في المقابل، أبرز التحليل القانوني أن التشريع الألماني يتفوق من حيث الدقة البنيوية وتفصيل كل سلوك إجرامي في مادة مستقلة، وتجريم الأفعال السابقة على الجريمة (202c)، وتوفير بيئة قانونية مرنة قادرة على مواكبة تطورات الفضاء الرقمي. إلا أن هذا النظام لا يخلو من تحديات واقعية، من أبرزها صعوبة ملاحقة الجرائم العابرة للحدود وتعقيدات التوازن بين حماية الخصوصية وفعالية التحقيق، وخاصة في ظل تطبيق صارم للائحة GDPR.

وعليه، تشير الدراسة الحاجة لمراجعة للتشريع القطري، تنطلق من تعزيز التجريم التفصيلي، وتجريم التحضير، واعتماد نظام عقوبات مرن، مع تطوير البنية الإجرائية الرقمية وتفعيل التعاون الدولي، بما ينسجم مع الخصوصية الدستورية والقانونية لدولة قطر. كما تبرز هذه الدراسة أهمية استلهام التجارب المقارنة لا بوصفها نماذج جامدة، بل كمرجعيات مرنة تسهم في بناء منظومة وطنية أكثر تماسكًا واستجابةً للتحديات السيبرانية المعاصرة.

التوصيات

1. **تفكيك المادة (2) والمادة (3) من قانون الجرائم الإلكترونية القطري إلى مواد مستقلة ومفصلة:** بناءً على ما كشفت عنه المقارنة مع القانون الألماني في المبحث الثاني – المطلب الأول، فإن دمج صور جرمية متعددة (مثل الدخول غير المشروع، والحذف، والإفشاء) ضمن مادة واحدة، يضعف من الأثر الردعي ويعقد عملية الإثبات، خلافًا للنموذج الألماني الذي يفرد لكل سلوك مادة خاصة به كما في المواد (202a–303b StGB).
2. **إدراج نص تشريعي مستقل يجرم الأفعال التحضيرية للجريمة السيبرانية:** مثل إنتاج أو توزيع أدوات الاختراق أو كلمات المرور غير القانونية، وذلك على غرار المادة (202c) من قانون العقوبات الألماني، وهو ما يمثل فجوة تشريعية حالية في القانون القطري تم رصدها في المبحث الثاني – المطلب الثاني.
3. **التحول إلى نظام غرامات مرن (Tagessätze) يراعي دخل الجاني:** بدلًا من نظام الغرامات الثابتة، بما يعزز مبدأ التناسب ويحقق عدالة أكثر فاعلية في العقوبات المالية. وتستند هذه التوصية إلى التحليل المقارن لأثر نظام الغرامات في كلا القانونين، وخاصة المادة (303b) في القانون الألماني.
4. **الحث على تفعيل انضمام دولة قطر إلى اتفاقية بودابست لمكافحة الجرائم السيبرانية:** لما لذلك من دور في تسهيل التعاون الدولي، وتبادل الأدلة، وتسريع المساعدة القانونية المتبادلة، خصوصًا في ظل التحديات العابرة للحدود التي تناولها البحث في المبحث الثاني – المطلب الثاني.
5. **تطوير البنية المؤسسية للتحقيق الرقمي داخل النظام القضائي القطري:** من خلال إنشاء وحدات متخصصة في الأدلة الإلكترونية والتحليل الجنائي الرقمي، وتحديث الإجراءات المتبعة في جمع وتحليل البيانات، وهي نقطة أثيرت صراحةً في ملاحظات المحكمين حول غياب المعالجة الإجرائية داخل المواد القانونية الحالية.
6. **مراعاة الخصوصية التشريعية والدستورية لدولة قطر عند اقتراح التعديلات:** ولا سيما في القضايا التي قد تتقاطع مع القواعد المستمدة من الشريعة الإسلامية أو مع النظام العام. وينبغي في هذا السياق عرض التوصيات على الجهات التشريعية المختصة لدراسة مدى مواءمتها مع المبادئ الدستورية المعمول بها.

المراجع

أولاً: المراجع باللغة العربية

- عبد الله، دغش العجمي. 2014. "المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة". الكويت: جامعة الشرق الأوسط.
- مريم، عبد اللطيف المسلماني. 2022. "مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية." مجلة القانون والمجتمع، كلية القانون، جامعة قطر 10, no. 2: 14–59.
- محمد، حماد مرهج الهيتي. 2014. "الجريمة المعلوماتية نماذج من تطبيقها: دراسة مقارنة في التشريع الإماراتي والسعودي، والبحريني، والقطري، والعماني". مصر– الإمارات: دار الكتب القانونية.
- ذياب، موسى البداينة. 2014. "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية". عمان، الأردن: كلية العلوم الاستراتيجية.
- خالد، ظاهر عبد الله جابر السهيل المطيري. 2022. "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي." مجلة البحوث الفقهية والقانونية، no. 38.
- عدلي، دحمان، وسعد الدين، ثامر البشير. 2021. "التحقيق الجنائي في الجرائم الإلكترونية". الجلفة، الجزائر: كلية الحقوق والعلوم السياسية، جامعة زيان عاشور.
- سعيدة، بوزنون. 2019. "مكافحة الجريمة الإلكترونية في التشريع الجزائري." مجلة العلوم الإنسانية. 52
- شرشر، محمود. 2021. "الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت." مجلة البحوث القانونية والاقتصادية 12, no. 2..
- عبد الله، عبد الكريم. 2007. "جرائم المعلوماتية والإنترنت". بيروت: الحلبي الحقوقية.
- الفيل، علي. 2011. "الإجرام الإلكتروني" (الطبعة الأولى). بيروت: زين دار النشر.
- دولة قطر. قانون مكافحة الجرائم الإلكترونية. بوابة الميزان القانونية. Accessed October 28, 2024.

https://www.almeezan.qa/LawArticles.aspx?LawTreeSectionID=16513&lawId=6366&language=ar.

ثانيًا: المراجع باللغة الإنجليزية

- Saqf Al Hait, A. 2023. Cyber Hacking: Building a Harmonised Criminal Legal Framework for Addressing Cyber Hacking in the Arab Convention on Combating Information Technology Offences: A Comparative Study between Jordanian & Saudi Cyber Laws. Doctoral dissertation, Anglia Ruskin Research Online (ARRO).
- Nasser, A. L. 2020. "Cybercrime: Theoretical Determinants, Criminal Policies, Prevention & Control Mechanisms." International Journal of Technology and Systems 5, no. 1: 34–63.
- Salim, I. F., and M. R. Dhafri. 2024. "The Criminal Agreement in Cybercrimes in Iraqi, Emirati, and Qatari Law." Kurdish Studies 12, no. 2: 4060–4087.
- Alramamneh, I. M., and A. Abuanzeh. 2023. "International and National Procedural Framework for Combating Cybercrime." International Journal of Cyber Criminology 17, no. 2: 330–349.
- Joyce, H. 2018. Cybercrime Legislation in the GCC Countries Fit for Purpose? Chatham House: The Royale Institute of International Affairs.
- German Federal Ministry of Justice. n.d. German Criminal Code (Strafgesetzbuch, StGB). Gesetze im Internet. Accessed October 28, 2024. https://www.gesetze-im-internet.de/englisch_stgb/index.html.