

فاعلية الأطر القانونية القطرية والدولية في الحماية الجنائية للبيانات الشخصية

“دراسة تحليلية”

الدكتور / محمد براء باسل أبو عنزة

أستاذ القانون الجنائي المساعد - جامعة لوسيل

mabuanzeh@lu.edu.qa

الباحث / عبد الحميد الأسمر الرويلي

ماجستير العدالة الجنائية الدولية - جامعة قطر

202300467@lu.edu.qa

تاريخ الاستلام : 2025 / 11 / 23 - تاريخ التحكيم : 2026 / 01 / 19 - تاريخ القبول : 2026 / 02 / 11

ملخص البحث

شهد الفضاء الرقمي في السنوات الأخيرة تطوراً متسارعاً في تقنيات المعلومات وشبكات الاتصال؛ مما أدى إلى تحول البيانات الشخصية إلى أصول رقمية حساسة وذات أهمية بالغة حيث ترتبط في حياة الأفراد والمؤسسات والدول. وقد رافق هذا التطور تصاعد غير مسبوق في التهديدات الرقمية التي باتت تستهدف الخصوصية والبيانات الشخصية، مستغلة بذلك الفجوات والتحديات القانونية على المستويين الوطني والدولي، التي تعيق عملية التصدي لها.

ويهدف هذا البحث إلى دراسة الأطر القانونية القطرية والدولية القائمة التي تعنى بخصوصية الأفراد وبياناتهم الشخصية، وتقييم مدى فاعليتها في مكافحة التهديدات الرقمية المتزايدة والمعقدة، مع تسليط الضوء على التحديات القانونية المرتبطة بها، على المستويين القطري والدولي.

وقد اعتمد الباحثان في معالجة هذا الموضوع المنهج الوصفي والتحليلي، مستعينين في سياق الوصف والتحليل بالمنهج النقدي، وذلك لتفكيك التحديات القانونية ذات الصلة. واستند البحث إلى مجموعة من القوانين القطرية والاتفاقيات الدولية.

وقد خلص البحث إلى مجموعة من التوصيات المقترحة، التي يتمنى الباحثان أن تسهم في معالجة التحديات القانونية، وتعزيز فاعلية الجهود الرامية إلى مكافحة التهديدات الرقمية التي تستهدف البيانات الشخصية؛ بما يعزز بناء بيئة رقمية أكثر أمناً واستدامة.

الكلمات المفتاحية:

البيانات الشخصية - التعاون الدولي - الحماية الجنائية - الخصوصية - الجرائم الإلكترونية.

The Effectiveness of Qatari and International Legal Frameworks in the Criminal Protection of Personal Data

An Analytical Study

Dr. Mohammed Bara Basel Abuanzeh

Assistant Professor of Criminal Law

Lusail University

mabuanzeh@lu.edu.qa

ABDULHAMED ALASMAR AL-RUAILE

Master's in International Criminal Justice

202300467@lu.edu.qa

Received : 23 / 11 / 2025 - Peer-reviewed : 19 / 01 / 2026 - Accepted : 11 / 02 / 2026

Abstract:

In recent years, the digital space has witnessed rapid advancements in information technologies and communication networks, transforming personal data into highly sensitive and valuable digital assets that are deeply intertwined with the lives of individuals, institutions, and states. This technological progress has been accompanied by an unprecedented rise in cyber threats targeting privacy and personal data, exploiting legal gaps and challenges at both the national and international levels, which hinder effective response mechanisms.

This study aims to examine the existing Qatari and international legal frameworks concerned with individuals' privacy and personal data, and to assess their effectiveness in addressing the growing and complex cyber threats. The research also highlights the legal challenges associated with these frameworks at both the national and international levels.

The researchers employed a descriptive and analytical methodology, supported by the critical approach within the process of description and analysis, in order to deconstruct the relevant legal challenges. The study relies on a range of Qatari laws and international conventions.

The research concludes with a set of proposed recommendations that are hoped to contribute to addressing the identified legal challenges and enhancing the effectiveness of efforts to combat cyber threats targeting personal data—ultimately fostering a safer and more sustainable digital environment.

Key Words:

Personal Data - International Cooperation - Criminal Protection - Privacy - Cybercrime.

المقدمة

تمهيد:

في ظل التزايد العالمي في الاعتماد على المحتوى الرقمي وشبكات الاتصال، أصبحت الحماية الجنائية للبيانات الشخصية مسألة حيوية تتطلب اهتماما خاصا. فقد أدركت الدول ومنها دولة قطر أهمية هذه القضية؛ مما دفعها إلى إصدار قوانين، وعقد اتفاقيات، وتطوير تقنيات، لضمان حماية الخصوصية والبيانات الشخصية من الانتهاكات والتهديدات الرقمية. تسعى هذه الجهود إلى تحقيق توازن بين حق الأفراد في الخصوصية وحماية بياناتهم الشخصية من التهديدات الرقمية، وبين ضرورة السماح بالوصول إلى هذه البيانات ومعالجتها في ظل الانتشار الواسع للخدمات الرقمية وتطور الجرائم المرتبطة بها.

جاء هذا البحث ليستعرض هذه القضية الحساسة، وما يرتبط بها من تحديات؛ لتحسين الحماية الجنائية للبيانات الشخصية، وتعزيز الأمن الرقمي.

أهمية البحث:

تتجلى أهمية هذا البحث في تسليط الضوء على حماية حق الفرد في خصوصيته وصون بياناته الشخصية من أي انتهاك أو تهديد رقمي؛ لا سيما في ظل التحولات الرقمية المتسارعة التي يشهدها العالم. هذه التحولات التي تشمل المجالات الخدمية والإجرامية التي تتسم بالتعقيد والانفتاح ولا تعرف حدودا جغرافية أو توقيتات ثابتة؛ مما يهدد حقوق الإنسان الأساسية، فهذا البحث يعالج واحدة من أكثر القضايا ارتباطا بالحياة اليومية للأفراد، وهي أمن بياناتهم الرقمية.

كما تزداد أهمية البحث مع التطور المستمر في الأطر القانونية المتعلقة بحماية البيانات

الشخصية على المستويين المحلي والدولي. هذا يستدعي الحاجة لمراجعة وتحليل هذه الأطر لضمان فاعليتها وتحديد الثغرات والتحديات التي تواجهها.

إن حماية البيانات الشخصية تعتبر أمراً جوهرياً في بناء وتعزيز الثقة في استخدام التقنيات الحديثة، وأي تراجع في هذه الحماية قد يؤدي إلى فقدان الثقة العامة في النظم الرقمية والخدمات التي تقدمها؛ مما ينعكس سلباً على تطور الحضارة الإنسانية وازدهارها.

ومما يزيد من أهمية البحث هو مساهمته في تعزيز الدراسات والعلوم القطرية والعربية التي بحاجة لمثل هذه الدراسات، كما أنه يشكل مرجعاً مهماً للباحثين في مجال الخصوصية والبيانات الشخصية في العصر الرقمي.

إشكالية البحث:

مع تصاعد التهديدات الرقمية والانتهاكات المتزايدة للخصوصية والبيانات الشخصية، التي تؤدي إلى أضرار جسيمة تطال الأفراد والبنية المعلوماتية سواء في دولة قطر أم في غيرها من الدول، يبرز تساؤل حول فاعلية الأطر القانونية القطرية والدولية في حماية البيانات الشخصية، ويزداد هذا التساؤل مع الاعتماد المتزايد على البيئة الرقمية وانتشار خدماتها وجرائمها العابرة للحدود والمرتبطة بالبيانات الشخصية؛ مما يطرح تحديات قانونية تتطلب حلول فعالة.

أسئلة البحث:

في ضوء ما تقدم وبناء على إشكالية البحث؛ فإنه ينبغي الإجابة على الأسئلة التالية:

- 1 - ما الأطر القانونية القطرية والدولية المعمول بها لحماية البيانات الشخصية؟
- 2 - ما أبرز التحديات التي تواجه التشريعات القطرية والدولية لحماية البيانات الشخصية في العصر الرقمي؟

أهداف البحث:

يهدف البحث إلى تحقيق مجموعة من الغايات أهمها ما يلي:

1 - استعراض وتحليل أهم الأطر القانونية القطرية والدولية المعمول بها؛ لتوفير الحماية الجنائية للبيانات الشخصية.

2 - الوقوف على أبرز التحديات التي تواجه الأطر القانونية القطرية والدولية لحماية البيانات الشخصية، وسبل التغلب عليها.

منهج البحث:

اعتمد الباحثان المنهج الوصفي التحليلي، وذلك لملاءمته طبيعة موضوع البحث وإشكاليته، التي تتطلب الوقوف على الأطر القانونية القائمة لحماية البيانات الشخصية من التهديدات الرقمية، وتحليل مدى كفايتها وفعاليتها في تحقيق الحماية الجنائية المنشودة.

وقد تم توظيف المنهج الوصفي في رصد وتوصيف الإطار القانوني المنظم لحماية البيانات الشخصية، من خلال استعراض القوانين القطرية ذات الصلة، وأهم الاتفاقيات والمواثيق الدولية المعمول بها، بهدف تقديم صورة دقيقة للوضع القانوني القائم.

كما تم استخدام المنهج التحليلي في تحليل هذه النصوص القانونية، وبيان نطاق تطبيقها، والكشف عن أوجه القصور أو الثغرات القانونية التي قد تضعف من فاعلية الحماية الجنائية للبيانات الشخصية، وذلك من خلال ربط النصوص القانونية بالتحديات العملية التي تفرضها التهديدات الرقمية المتزايدة.

وقد تم اختيار هذا المنهج دون غيره من المناهج؛ لكون البحث لا يستهدف إجراء دراسة

إحصائية أو ميدانية، ولا يقتصر على المقارنة البحتة، وإنما يهدف إلى تحليل الإطار القانوني القائم وتقويمه في ضوء الواقع الرقمي المتغير، وصولاً إلى استخلاص نتائج وتقديم توصيات قانونية عملية تساهم في تعزيز الحماية الجنائية للبيانات الشخصية.

خطة البحث:

ينقسم البحث بشكل عام إلى مبحثين، وهما:

المبحث الأول: الأطر القانونية القطرية والدولية لحماية البيانات الشخصية

المبحث الثاني: حماية الخصوصية في زمن العولمة الرقمية وتحديات التعاون الدولي

وخاتمة تحتوي على أهم النتائج والتوصيات.

المبحث الأول

الأطر القانونية القطرية والدولية لحماية البيانات الشخصية

أصبحت البيانات الشخصية في العصر الحديث من الأصول الحيوية التي تحظى بأهمية متزايدة، وينظر إليها على أنها وسيلة لفهم الأفراد وتلبية احتياجاتهم في مختلف القطاعات، مثل: التجارة الإلكترونية، والرعاية الصحية، والتعليم، والصيرفة، والخدمات الحكومية، وغيرها.

وعرف القانون القطري البيانات الشخصية بأنها: «بيانات عن الفرد الذي تكون هويته محددة، أو يمكن تحديدها بصورة معقولة، سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى»،⁽¹⁾ كما تعرف البيانات الشخصية بأنها: «كل معلومة تتعلق بالشخص الطبيعي المحدد الهوية أو الذي يكون قابلاً للتعرف على هويته». ⁽²⁾ ويمكن أن نعرف البيانات الشخصية بأنها: أي بيان أو معلومة رقمية أو تقليدية تدل على شخص طبيعي بشكل مباشر أو غير مباشر. ومن هنا يتضح أن البيانات الشخصية جزء مهم من الخصوصية.

وقد عرف المحاميان صامويل وارن ولويس برانديز في مقالتهما المعنونة بالحق في الخصوصية بأن الخصوصية هي: «حق المرء في أن يترك وشأنه»،⁽³⁾ ومع التطور التقني أصبحت البيانات الشخصية من أهم مظاهر الخصوصية وانتقلت من مجرد كونها معلومات بسيطة إلى معلومات ذات طابع حساس؛ مما جعل منها ثروة قيمة، كما جعلها محط اهتمام الدول والقوانين والمنظمات الدولية.

1 - قانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، مادة 1، دولة قطر.

2 - طارق جمعة السيد راشد، «الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي دراسة مقارنة»، مجلة القانون والاقتصاد، جامعة القاهرة، كلية الحقوق، مج 92، ع 3، أغسطس 2019م، 190-314، ص 218.

3 - Samuel D. Warren; Louis D. Brandeis 'The Right to Privacy' Harvard Law Review, Vol. 4, No. 5. (December 15, 1890), pp. 193-220: 193

ويعتبر الإطار القانوني لحماية البيانات الشخصية من الركائز الأساسية في مواجهة التهديدات الرقمية المتزايدة وتنظيم التعامل مع البيانات والخصوصية. ويهدف هذا المبحث إلى الوقوف على أبرز الأطر القانونية القطرية والدولية التي تنظم حماية البيانات الشخصية.

المطلب الأول

الأطر القانونية القطرية لحماية البيانات الشخصية

تعد الخصوصية وحماية البيانات الشخصية من الحقوق الأساسية التي حظيت باهتمام خاص في دولة قطر، ومع تسارع التطورات التقنية وازدياد الاعتماد على المحتوى الرقمي، أدركت دولة قطر أهمية وضع إطار قانوني متين يضمن حماية البيانات الشخصية ويعزز الثقة في البيئة الرقمية، بحيث يشمل هذا الإطار القانوني حماية حق الخصوصية والبيانات الشخصية؛ مما يعزز الثقة في الفضاء الرقمي. ونعرض في الفروع التالية أهم التشريعات المعنية بحماية البيانات الشخصية وحفظ الخصوصية.

الفرع الأول

الدستور القطري

الدستور القطري أرسى المبادئ الأساسية لحرمة الحياة الخاصة، كما جاء في نص المادة 37 منه؛ فقد أعطى الدستور بذلك أساساً صلباً لحماية الخصوصية كحق دستوري لا يمكن المساس به إلا وفق القانون، ومنح في ذات الوقت للخصوصية مكانة مهمة، عندما نص على حرمة الحياة الخاصة، ومنع الاعتداء عليها أو التدخل فيها، وما البيانات الشخصية إلا امتداد لتلك الحياة الخاصة.

الفرع الثاني

قانون العقوبات

جاء في قانون العقوبات القطري رقم 11 لسنة 2004 مجموعة من النصوص التي تساهم في الحفاظ على حق الخصوصية وحماية البيانات الشخصية، وجرمت بعض الأفعال في هذا السياق مثل: دخول المساكن، وفض الرسالة والبرقيات الخاصة، وتصوير الأفراد دون رضاهم، وغيرها. وقد جاء القانون القطري موفقا في تشديد العقوبة على من حصل على بيانات شخصية من خلال التجسس على الأفراد وهددهم بنشرها إذا لم ينصاعوا لمطالبه.⁽⁴⁾

ولا يقتصر دور هذه النصوص على حماية الحياة الخاصة فحسب، بل يمتد ليشمل حماية غير مباشرة للبيانات الشخصية من خلال تجريم السلوك الإجرامي الذي يستهدف الحصول عليها واستغلالها بغير وجه حق. فتعد أفعال دخول المساكن وفض الرسائل وتصوير الأفراد دون رضاهم من صور السلوك الإجرامي التي قد تستخدم كوسيلة للوصول إلى بيانات شخصية أو معلومات خاصة؛ سواء بصورتها المادية أم الرقمية. كما تتجلى الحماية الجنائية للبيانات الشخصية بوضوح في تشديد العقوبة على من يحصل على هذه البيانات عن طريق التجسس أو التهديد بنشرها، وهو ما يبين تصدي القانون لخطورة استغلال البيانات الشخصية كأداة للابتزاز أو الضغط غير المشروع، حيث يشكل هذا القانون دعامة أساسية مكملة للحماية الجنائية المقررة للبيانات الشخصية في القوانين الرقمية الخاصة.

وتطبيقا لذلك ولبيان خطورة التعدي على الخصوصية في الواقع العملي، قضت المحكمة بإدانة متهم استولى دون وجه حق على الحساب الشخصي لزوج المجني عليها، وتمكن من الحصول على صور خاصة وخادشة للحياء، ثم قام بتهديدها بنشر تلك الصور عبر الشبكة

4 - قانون العقوبات الصادر بالقانون رقم 11 لسنة 2004، المواد: 323 و324 و333، وكذلك المادة 333 مكرر والتي أضيفت بموجب القانون رقم 14 لسنة 2024 بتعديل بعض أحكام قانون العقوبات رقم 11 لسنة 2004، دولة قطر.

المعلوماتية ومواقع التواصل الاجتماعي، وكان هذا التهديد مقرونا بطلب معاشرتها جنسيا. وقد اعتبرت المحكمة أن هذا السلوك يشكل اعتداء جسيما على الخصوصية وانتهاكا للبيانات الشخصية، إلى جانب توفر أركان جرائم الدخول غير المشروع، والتهديد، وتعتمد الإزعاج؛ مما استوجب توقيع عقوبة السجن لمدة عشر سنوات، تأكيداً على جسامه الجرائم الرقمية التي تستهدف البيانات الشخصية.⁽⁵⁾

الفرع الثالث

قانون الإجراءات الجنائية

جاء في قانون الإجراءات الجنائية القطري رقم 23 لسنة 2004 مجموعة من القيود التي تلتزم بها السلطة. تهدف هذه القيود إلى الحفاظ على حرمة الحياة الخاصة وحقوق الخصوصية الفردية، وأهمها ما يلي:⁽⁶⁾

- 1 - لا يجوز لمأمور الضبط أن يقوم بفض الأوراق والظروف المختومة، بل يجب عرضها على النيابة العامة.
- 2 - لا يجوز تفتيش المساكن إلا بأمر كتابي من النيابة العامة بناء على تحريات تكشف أن حائز المسكن أو المقيم فيه ارتكب جنائية أو جنحة أو اشتراك في ارتكابها أو وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة، كما أن الأصل عدم جواز تفتيش المساكن في الليل.
- 3 - لا يجوز تفتيش الأنثى إلا بمعرفة أنثى.

5 - جمهورية مصر العربية، محكمة النقض، الدائرة الجنائية، الطعن رقم 22830 لسنة 88 القضائية، جلسة السبت الموافق 11 من سبتمبر سنة 2021م، برئاسة المستشار: أحمد الخولي نائب رئيس المحكمة.

6 - قانون الإجراءات الجنائية الصادر بالقانون رقم 23 لسنة 2004، المواد: 51 و53 و75 و77 و83، دولة قطر.

4 - نصت المادة 77 من قانون الإجراءات الجنائية القطري⁽⁷⁾ بشأن المراقبة على مجموعة من القيود لحماية الخصوصية الفردية منها:

- أ - لا تجوز المراقبة في الجرائم الثلاث المنصوص عليها إلا بأمر كتابي من النائب العام.
- ب - لا تجوز المراقبة في غير الجرائم المنصوص عليها إلا بأمر من أحد قضاة المحكمة.
- ج - يجب أن يكون الأمر بالمراقبة لمدة لا تزيد على ثلاثين يوم، ولا يجوز تجديد أمر المراقبة إلا إذا توفرت مبررات لذلك.

د - في غير الحالات السابقة لا تجوز مراقبة جهاز اتصال كالهاتف في قضايا المضايقة والإزعاج والقتل والسب في غير علانية عبر الهاتف إلا بناء على شكوى المجني عليه في هذه الجريمة، ومن يصدر الأمر بالمراقبة هو النائب العام أو من يقوم مقامه، ويجب أن يكون الأمر بالمراقبة لمدة لا تزيد على ثلاثين يوما ، ولا يجوز تجديد أمر المراقبة إلا إذا توفرت مبررات لذلك.⁽⁸⁾

هذه القيود الواردة على الإجراءات الجنائية تساهم في الحفاظ على الخصوصية الفردية وحماية البيانات الشخصية من الاطلاع غير القانوني عليها، وتعزز حرمة الحياة الخاصة.

الفرع الرابع

قانون البصمة الوراثية

يرتبط قانون البصمة الوراثية رقم 9 لسنة 2013 بحماية البيانات الشخصية ذات الطبيعة الخاصة؛ إذ ينظم جمع وحفظ واستخدام بيانات البصمة الوراثية في إطار محدد، ويقصر

7 - قانون الإجراءات الجنائية الصادر بالقانون رقم 23 لسنة 2004، المادة 77، دولة قطر.

8 - قانون الإجراءات الجنائية الصادر بالقانون رقم 23 لسنة 2004، المادة 83، دولة قطر.

معالجتها على الأغراض التي يحددها القانون، مع إخضاعها لضوابط إجرائية تهدف إلى منع إساءة استخدامها نظرا لما تمثله هذه البيانات من ارتباط مباشر بخصوصية الفرد وسلامته الجينية، كما يحظر القانون الاطلاع على هذه البيانات إلا بإذن من وزير الداخلية أو النيابة العامة أو المحكمة المختصة.

الفرع الخامس

قانون مكافحة الجرائم الإلكترونية

يعتبر قانون مكافحة الجرائم الإلكترونية رقم 14 لسنة 2014 هو الأساس في مكافحة أهم الجرائم التي تنتهك الخصوصية والبيانات الشخصية كالدخول غير المشروع، والتجسس على الخصوصية والبيانات، وإفشاء الأسرار الشخصية، وانتحال الهوية، وغيرها.

وتجدر الإشارة إلى أن هذا القانون أدرك تطور مفهوم الخصوصية، فلم تعد الخصوصية مرتبطة في الأماكن المغلقة، بل أصبحت تشمل حتى الأماكن العامة، وهو توجه حديث لمواجهة الاستغلال السيئ لتقنيات التصوير الفوري والنشر عبر المنصات الرقمية. وتأكيدا على ذلك صدر مؤخرا تعديل على هذا القانون حيث عزز مفهوم الخصوصية في الأماكن العامة، كما عزز مبدأ الموافقة الشخصية، وهذا من نتائج التطور التقني الذي أصبح يتغذى على الخصوصية والبيانات الشخصية.⁽⁹⁾

لقد نظم هذا القانون عملية التفتيش الرقمي. فالتفتيش يعتبر أحد أهم الإجراءات

9 - انظر: قانون رقم 11 لسنة 2025 بتعديل بعض أحكام قانون مكافحة الجرائم الإلكترونية رقم 14 لسنة 2014، دولة قطر، صدر هذا القانون بتاريخ 21 يوليو 2025م، وينص على إضافة مادة جديدة وهي مادة 8 مكرر، وتنص على تجريم كل من تعدى على خصوصية الأفراد أثناء تواجدهم في الأماكن العامة، من خلال نشر أو تداول صور أو مقاطع فيديو لهم، دون علمهم أو رضائهم، أو في غير الأحوال المصرح بها قانونا، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

الجنائية في الكشف عن الجرائم وتتبع المجرمين، كما أنه في الوقت نفسه من أخطر الإجراءات التي تنتهك البيانات الشخصية. ولذلك؛ فإن التفتيش التقليدي أو الرقمي ليس أمراً متروكاً لأي شخص أو أي جهة، وبالنظر إلى خطورة هذا الإجراء وانتهاكه لحق الإنسان في الخصوصية وحرمة حياته الخاصة؛ فقد حرصت الكثير من الدول ومنها دولة قطر على إحاطة التفتيش الرقمي بمجموعة من القيود، ولذلك حدد القانون سلطة التفتيش وهي النيابة العامة التي لها الصلاحية لإصدار أوامر بالتفتيش، وهذا يشمل حالات الجرائم الرقمية أو الانتهاكات التي تتطلب التحقيق.⁽¹⁰⁾

جاء في المادة 14 من قانون مكافحة الجرائم الإلكترونية القطري رقم 14 لسنة 2014 على أن للنيابة العامة أو من تندبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة. ويجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة. فإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.

إن هذه المادة تضع إطاراً قانونياً لضمان أن عمليات التفتيش في الجرائم الرقمية تتم بطريقة قانونية وعادلة، مع احترام حقوق الأفراد وخصوصيتهم، فلا يجوز تفتيش أنظمة المعلومات للأفراد والأجهزة الشخصية كالهواتف والحواسيب والسحابة الرقمية والبريد الرقمي ووسائل التخزين إلا بإذن من النيابة العامة ضماناً لصون الخصوصية الفردية. كما أنه لا يجوز للنيابة العامة - وفق هذه المادة - أن تصدر أمر التفتيش إلا إذا كان مسبباً ومحدداً، وأنه لا يجوز تجديد أمر التفتيش إلا إذا كانت هناك مبررات قائمة.

10 - انظر: قانون مكافحة الجرائم الإلكترونية الصادر بالقانون رقم 14 لسنة 2014، المادتان: 14 و17، دولة قطر. / قانون الإجراءات الجنائية الصادر بالقانون رقم 23 لسنة 2004، المادتان: 23 و77، دولة قطر.

ونرى ضرورة أن يحدد أمر التفتيش نوع الأجهزة، أو البريد، أو الحسابات، أو الأرقام المقصودة من أمر التفتيش، كما يحدد النطاق الزمني للتفتيش فيها، ولا يتم أخذ أي معلومات لا صلة لها بالتفتيش، وأن يتم حذف كافة البيانات بعد انتهاء الإجراءات.

ويرى الباحثان أن توظيف تقنيات الذكاء الصناعي في عمليات التفتيش يمكن أن يساهم بشكل كبير في تعزيز حماية الخصوصية. فمن خلال الاعتماد على أنظمة الذكاء الصناعي، يمكن لتلك التقنيات تفحص الأجهزة أو الأنظمة الإلكترونية بطريقة دقيقة، بحيث تقتصر عملية التفتيش على استخراج البيانات والمعلومات المتعلقة بالجريمة فقط، دون المساس بالبيانات الأخرى غير ذات الصلة.

وهذا الأسلوب لا يقتصر فقط على تسهيل وتسريع إجراءات التحقيق، بل يوفر أيضا حماية إضافية لخصوصية الفرد المعني بالتفتيش، بالإضافة إلى حماية خصوصية الآخرين الذين قد تكون بياناتهم محفوظة على الجهاز محل التحقيق.

كما نصت المادة 17 من قانون مكافحة الجرائم الإلكترونية القطري على أن للنيابة العامة أن تأمر بالجمع والتسجيل الفوري لأية بيانات، أو معلومات إلكترونية، أو بيانات مرور، أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات.

هذه المادة أعطت للنيابة العامة الحق بأن تأمر بالجمع والتسجيل الفوري لأي بيانات أو معلومات بما فيها البيانات الشخصية أو البيانات المرتبطة بالخصوصية، ولكن اشترطت هذه المادة شرطين، أحدهما بأن يكون هناك تحقيق قائم، والآخر أن يكون الأمر بالجمع والتسجيل لازما لمصلحة التحقيق.

ومن الجدير بالذكر أن القانون⁽¹¹⁾ وضع مجموعة من الالتزامات على مزودي الخدمة ومن

11 - انظر: قانون مكافحة الجرائم الإلكترونية الصادر بالقانون رقم 14 لسنة 2014، دولة قطر، المادة 21 والتي نصت على

يعالج البيانات الشخصية، وبالتالي يتعين على مزودي الخدمة⁽¹²⁾ أو المراقبين أو المعالجين الالتزام باتخاذ جميع الإجراءات اللازمة لحماية الخصوصية والبيانات الشخصية التي تصل إليهم بصورة قانونية؛ بما في ذلك تأمين الخوادم وأنظمة الحماية بشكل كاف؛ لأن أي إهمال في تأمين هذه البيانات، مثل تقاعس شركة اتصال عن تأمين خوادمها؛ قد يتيح للمخترقين الوصول إلى بيانات المشتركين وسرقتها؛ مما يشكل انتهاكا صريحا لالتزامات حماية الخصوصية والأمان.

مزودو الخدمة والمراقبون والمعالجون بحكم عملهم يمتلكون المعلومات الضرورية للمستخدمين، وذلك في سبيل تفعيل الخدمات التي يقدمونها؛ بما في ذلك البيانات الشخصية وبيانات المرور والمحتوى الرقمي ومعلومات الاتصال، وهم من أهم الجهات التي يعتمد عليها التحقيق الجنائي في كشف الجرائم ومعرفة مرتكبيها.

الفرع السادس

قانون حماية خصوصية البيانات الشخصية

يعد قانون حماية خصوصية البيانات الشخصية رقم 13 لسنة 2016 الأول من نوعه في دول مجلس التعاون لدول الخليج العربية الذي يختص بحماية البيانات الشخصية، كما يعد من القوانين الشاملة والمتقدمة في المنطقة، ويهدف إلى تعزيز حماية البيانات الشخصية وضمان استخدامها وفق معايير محددة تحترم الخصوصية.

وتدخل البيانات الشخصية في الخصوصية المعلوماتية التي تعالج بطريقة آلية، والتي يود

مجموعة من الالتزامات على مزود الخدمة. والمادة 22 والتي تنص على مجموعة من الالتزامات التي تلتزم بها أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها. / قانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، مادة 13، دولة قطر.

12 - عرفت المادة الأولى من قانون مكافحة الجرائم الإلكترونية الصادر بالقانون رقم 14 لسنة 2014 مزود الخدمة بأنه: أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة تخزين المعلومات.

كل شخص - منطقيا - المحافظة عليها وحمايتها من أي اعتداء، وتبرز أهمية توفير الإطار القانوني لحماية البيانات الشخصية من خلال ظهور العلاقة القوية بين حق الإنسان في الخصوصية من جهة وبين التقنيات الرقمية الحديثة من جهة أخرى؛ سواء في جمع المعلومات أم في مشاركتها أو معالجتها بشكل عام.⁽¹³⁾ ويشتمل هذا القانون بشكل عام على 32 مادة تحوي ما يلي:

أولا: التعريفات والأحكام العامة

يحتوي هذا الفصل على التعريفات الأساسية للمصطلحات المستخدمة في القانون، مثل البيانات الشخصية، المراقب، المعالج، وتدفق البيانات عبر الحدود وغيرها.

ثانيا: حقوق الأفراد أصحاب البيانات

ينص القانون على حقوق واضحة للأفراد تتعلق ببياناتهم الشخصية تشمل ما يلي:

ثالثا: حق الموافقة

لا يجوز معالجة البيانات الشخصية إلا برضا وموافقة الفرد صاحب البيانات، و «لا يكفي مجرد رضا الفرد المعني بالبيانات، وإنما يجب بجانب ذلك أن يكون الرضا صحيحا»،⁽¹⁴⁾ فلا يجوز إجباره على الموافقة دون رضاه التام، ولا يجوز التحايل على الفرد للحصول على موافقته، وإنما يجب أن تكون الموافقة مبنية على الوضوح والوعي، كما يحق للفرد سحب موافقته السابقة على معالجة بياناته الشخصية. وهذا الحق من الحقوق الأساسية التي نصت عليها القوانين

13 - انظر: جمعة السيد راشد، «الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والمقارن»، المجلة القانونية والقضائية، دولة قطر: وزارة العدل - مركز الدراسات القانونية والقضائية، مج11، ع2، 2017م، 75-138، ص 78-79.

14 - ياسر أحمد بدر محمد، «الإطار النظامي لحماية حق الأفراد في مواجهة مخاطر معالجة بياناتهم ذات الطابع الشخصي: دراسة مقارنة بين نظام حماية البيانات الشخصية السعودي واللائحة العامة الأوروبية لحماية البيانات»، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، مركز الدراسات والبحوث، مج31، ع83، يوليو 2022م، 69-128، ص 90.

كالقانون الفرنسي⁽¹⁵⁾ والاتفاقيات كالاتحاد الأوروبية والاتفاقية الإفريقية⁽¹⁶⁾ ونرى أنه ينبغي منح الفرد الحق في تقييد موافقته بمدة محددة تنتهي بعدها هذه الموافقة ما لم ينص القانون على خلاف ذلك.

رابعاً: حق التحكم

للأفراد الحق في الاطلاع على بياناتهم وأخذ نسخة منها، وتعديلها وتصحيحها، وحذفها ومحوها، أو الاعتراض على معالجتها إذا كانت المعالجة غير ضرورية.

إن تحكم الفرد في بياناته الشخصية ومراقبتها ومتابعة آلية التعامل معها من قبل المراقبين والمعالجين والطرف الثالث، هو حق من الحقوق الأساسية للفرد صاحب البيانات، وهو حق يعزز ما يطلق عليه البعض مبدأ السيادة الرقمية الفردية⁽¹⁷⁾.

ومن المسائل المهمة التي ينبغي الوقوف عندها بشأن حق الفرد بالتحكم في بياناته هي مسألة حق النسيان، فحق النسيان هو: «حق مستخدم الإنترنت في المحافظة على ماضيه الرقمي وبقائه في حيز النسيان والسيطرة على معلوماته التي مضت فترة زمنية على بثه عبر الإنترنت مع محوها آلياً عند تركه مراجعتها خلال فترة يحددها هو بنفسه مسبقاً عند بثه

15 - قانون تكنولوجيا المعلومات والملفات والحريات المدنية رقم 78-17 لسنة 1978م المؤرخ في 6 يناير 1978م والمعدل بالقانون رقم 801 لسنة 2004م، والمعدل بالقانون رقم 1125 لسنة 2018م، الجمهورية الفرنسية، مادة 5 والتي أحالت شروط الموافقة إلى اللائحة الأوروبية لحماية البيانات الشخصية (GDPR).

16 - انظر: الاتحاد الأوروبي، البرلمان الأوروبي والمفوضية الأوروبية، اللائحة العامة لحماية البيانات (GDPR)، قانون رقم 679/2016م، المادة 6 بند 1 والمادة 7/ اتفاقية الاتحاد الإفريقي رقم XXV (EX.CL/846) بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، التي تم اعتمادها في مدينة مالابو عاصمة جمهورية غينيا الاستوائية، في الدورة العادية الثالثة والعشرين لقمة رؤساء دول وحكومات الاتحاد الإفريقي، بتاريخ 27 يونيو 2014م، المادة 13 المبدأ 1.

17 - انظر: أحمد محمد عبد الغفار، «مبدأ السيادة الرقمية الفردية على البيانات»، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون، ع43، أكتوبر 2023م، 767-862، ص777، والتي جاء فيها: السيادة الرقمية الفردية أو حق الاستقلال المعلوماتي الفردي، هو حق يمنح الفرد استقلالية معينة في إدارة بياناته الشخصية، فلكل فرد الحق في تقرير ومراقبة استخدام البيانات الشخصية المتعلقة به.

للمعلومة»،⁽¹⁸⁾ فحق النسيان أو حق المحو هو تمكين الفرد من محو وإزالة بياناته الشخصية أو طمسها، إما يدويا أو بشكل آلي تلقائي.

ورغم أن القانون القطري لم يستخدم مصطلح حق النسيان صراحة في قانون حماية خصوصية البيانات الشخصية؛ إلا أنه أقر مضمون هذا الحق بشكل واضح من خلال مجموعة من الحقوق⁽¹⁹⁾ المتصلة بحق النسيان وهي: طلب حذف البيانات الشخصية في حالة سحب الموافقة، أو إذا كانت المعالجة غير ضرورية، أو كانت زائدة على متطلباتها، أو تمييزية، أو مجحفة، أو مخالفة للقانون. وكذلك عدم احتفاظ المراقب بالبيانات الشخصية لمدة تزيد على المدة الضرورية لتحقيق الأغراض التي جمعت هذه البيانات من أجلها. كما أشار القانون إلى حق الاعتراض على معالجة البيانات. وقيام المراقب بإبلاغ الفرد بأي انتهاك لبياناته الشخصية، وهذا الأمر يعزز من حماية البيانات الشخصية بحيث يتم التركيز على هذا الانتهاك والحد منه في المستقبل؛ مما يتيح للأفراد طلب إزالة البيانات المتضررة. كما أشار القانون إلى حق طلب تصحيح البيانات. وفيما يتصل ببيانات الأطفال، نص القانون على حق ولي الأمر في طلب حذف أو محو أو وقف معالجة البيانات الشخصية المتعلقة بالطفل، وهو ما يعد تطبيقا عمليا لمضمون حق النسيان في إطار فئة تستوجب حماية خاصة.

يرى الباحثان أهمية تعزيز حق النسيان للأفراد، إضافة الحق للفرد في تحديد مدة زمنية ينبغي عن انتهائها حذف بياناته الشخصية التي حددها، كما تنتهي عندها صلاحية الموافقة، وألا تترك الموافقة وبيانات الفرد الشخصية عند المعالج أو المراقب بشكل أبدي أو بدون معايير واضحة. وكذلك إدراج فئات أخرى في توفير الحماية لهم مثل: الحماية لبيانات الأطفال، كالمصابين بعاقة عقلية، أو المرضى المغمى عليهم، أو كبار السن المصابين بالنسيان، فهؤلاء

18- عبد الكريم صالح عبد الكريم وألند صلاح الدين تمر، «الحق في النسيان الرقمي والمسؤولية التقصيرية الناجمة عن انتهاكه - دراسة تحليلية مقارنة»، مجلة الحقوق، جامعة الكويت، مج48، ع3، سبتمبر 2024م، 367-412، ص 374.

19- قانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، المواد: 5 و6 و17، دولة قطر.

يشابهون الأطفال في عجزهم وضعفهم عن حماية بياناتهم الشخصية، وبالتالي يوصي الباحثان باعتبار بياناتهم بيانات حساسة بأن يتم تعديل كلمة (والأطفال) في المادة 16 من القانون القطري رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية لتصبح (والأطفال ومن في حكمهم).

خامسا: حق الشفافية

يلزم المراقب بإبلاغ الفرد عن معالجة بياناته الشخصية وعن الغرض من تلك المعالجة، وعن الأغراض المشروعة التي يرغب المراقب أو أي طرف آخر في معالجة البيانات الشخصية من أجلها، وعن أي إفصاح محتمل، وإخطار الفرد بأي إفشاء أو إخلال متعلق ببياناته الشخصية، كما يحق للفرد الاعتراض على المعالجة، وأن يتقدم بشكوى فيما يتعلق ببياناته الشخصية.

ويرى الباحثان أن القانون القطري أقر حق الفرد في الاعتراض على معالجة بياناته الشخصية متى كانت غير ضرورية أو زائدة أو تنطوي على تمييز أو كانت مجحفة أو مخالفة للقانون، ويدخل ضمن نطاق هذا الحق المعالجات المؤتمتة وممارسات التنميط⁽²⁰⁾ غير المشروع؛ لما تسببه من مخاطر تمس حقوق الأفراد وخصوصيتهم. وعلى الرغم من ذلك يرى الباحثان أهمية تعزيز هذا الحق من خلال النص عليه بصورة أكثر تفصيلا ووضوحا، وبما يضمن تمكين الفرد من الاعتراض الصريح على المعالجات المؤتمتة والتنميط، وإتاحة إمكانية الموافقة المسبقة عليها في نطاق محدد، مع ضمان حقه بسحب تلك الموافقة في أي وقت، فذلك يعزز مبدأ السيطرة على البيانات والتحكم بالمعالجات التي تتم عليها.

20 - مرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، دولة الإمارات العربية المتحدة، مادة 1 والتي جاء بنصها تعريف التنميط كالتالي: التنميط: «شكل من أشكال المعالجة المؤتمتة بحيث تتضمن استخدام البيانات الشخصية لتقييم جوانب شخصية معينة ومرتبطة بصاحب البيانات، ومن بينها تعليل أو توقع الجوانب المتعلقة بأدائه أو وضعه المالي، أو صحته أو تفضيلاته الشخصية أو اهتماماته أو سلوكه أو مكانه أو تحركاته أو موثوقيته». فالتنميط هو استخدام البيانات الشخصية للفرد بواسطة برامج أو خوارزميات بشكل آلي؛ لتكوين فكرة أو صورة مفصلة عن سلوك ذلك الشخص وخصائصه وتفضيلاته أو توقع ما قد يفعله مستقبلا.

سادسا: التزامات المراقبين والمعالجين

يتعين على المراقبين والمعالجين الالتزام بمعالجة البيانات الشخصية بأمانة ومشروعية، وبحماية البيانات الشخصية من الفقد، أو التلف، أو الإفشاء، أو الوصول غير المصرح به. كما يفرض القانون إعداد سياسات حماية الخصوصية، وضمان سرية البيانات، وجودة من يقوم بالمراقبة والمعالجة، وتلقي الشكاوى والنظر فيها، وإدارة البيانات، وتمكين الأفراد من ممارسة حقوقهم. كما يتعين على المراقب ألا يتخذ أي إجراءات أو قرارات تقيد أو تمنع تدفق البيانات الشخصية إلى خارج الدولة إلا إذا كانت المعالجة مخالفة للقانون أو تضر بالفرد، وأن على المراقب التحقق من أن نقل البيانات الشخصية يتوافق مع الأغراض المشروعة التي جمعت البيانات لأجلها.

ويرى الباحثان أنه من الأفضل أن ينص القانون القطري على الحالات التي يجوز أو لا يجوز فيها نقل البيانات الشخصية عبر الحدود، كعدم نقل البيانات إلا لدولة فيها قانون يضمن حمايتها، أو أن تكون هناك اتفاقية ثنائية أو متعددة الأطراف لحماية البيانات بين دولة قطر وبين تلك الدولة، أو بموافقة الفرد صاحب البيانات بشرط عدم الإضرار بالمصلحة العامة. فهذا الأمر يوفر حماية جنائية استباقية للبيانات الشخصية من التعرض للانتهاك في مكان لا يطاله القانون القطري.

سابعا: البيانات الحساسة أو البيانات الشخصية ذات الطبيعة الخاصة

يعطي القانون القطري اهتماما خاصا للبيانات الحساسة⁽²¹⁾ مثل: البيانات الصحية، والعرقية، والدينية، وسجلات الأطفال، والعلاقات الزوجية، والحالة الجنائية. ويحظر معالجتها إلا بتصريح مسبق من الجهة المختصة، مع فرض إجراءات أمان إضافية. ويشترط القانون وضع

21 - قانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، مادة 16، دولة قطر.

سياسات خاصة لحماية بيانات الأطفال. كما يمكن إضافة أصناف أخرى من البيانات الشخصية ذات الطبيعة الخاصة؛ إذا كان من شأن سوء استخدامها أو إفشائها إلحاق ضرر بالفرد.

إن إمكانية إضافة أصناف جديدة من البيانات الشخصية كبيانات حساسة في القانون القطري قد تعد ميزة تمنح القانون مرونة لمواكبة التطورات التقنية المتسارعة. ومع ذلك، قد يواجه هذا التوجه انتقاداً لافتقاره إلى الوضوح بشأن البيانات التي يمكن تصنيفها كحساسة؛ مما قد يؤدي إلى توسع غير محدد وغير منصوص عليه صراحة في القانون. ونرى أن النصوص القانونية المتعلقة بالبيانات الحساسة يجب أن تكون واضحة ومحددة، نظراً لتأثيرها المباشر على حياة الأفراد وحقوقهم. فكل فرد له بيانات حساسة خاصة به، ويجب أن يكون من حقه معرفة البيانات التي يعتبرها القانون حساسة؛ مما يستدعي تضمينها بشكل صريح ودقيق في نصوص القانون.

البيانات البيومترية أو البصمة الحيوية⁽²²⁾ أصبحت عنصراً محورياً في الحياة العامة، حيث تستخدم على نطاق واسع كوسيلة معتمدة لصلاحيات الدخول وتحديد هوية المستخدمين في العديد من المجالات والتقنيات. تعتمد هذه البيانات في التطبيقات الهاتفية لتقديم خدمات متنوعة مثل: الخدمات المصرفية والصحية، وتسجيل الحضور في العمل، والخدمات الحكومية. ومع ذلك؛ فإن هذه البيانات تشكل هدفاً جذاباً للمجرمين الذين قد يستغلونها في ارتكاب الجرائم، مثل: سرقتها رقمياً لانتحال شخصية أصحابها أو الوصول غير المصرح به إلى الأنظمة الحكومية أو الشخصية؛ مما يؤدي إلى انتهاك الخصوصية.

22 - مرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، دولة الإمارات العربية المتحدة، مادة 1 والتي جاء بنصها تعريف البيانات البيومترية كالتالي: البيانات الحيوية البيومترية: البيانات الشخصية الناتجة عن المعالجة باستخدام تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لصاحب البيانات، والتي تسمح بتحديد أو تؤكد التحديد الفريد لصاحب البيانات، مثل: صورة الوجه أو بيانات البصمة. / قانون رقم 17 لسنة 2025 بشأن البصمة الحيوية، دولة قطر، عرف البصمة الحيوية بأنها: الخصائص الفسيولوجية (الجسدية)، وهي عينة من صوت أو يد أو وجه أو عين أو أسنان، أو أي عضو آخر من أعضاء الإنسان يحددها الوزير، والتي يمكن مقارنتها أو قياسها بشكل علمي لتمييز شخص ما عن الأشخاص الآخرين.

ثامنا: الإعفاءات

ينص قانون حماية البيانات الشخصية القطري على حالات استثنائية يمكن فيها معالجة البيانات دون الالتزام الكامل ببعض المواد، وذلك لأسباب منصوص عليها مثل: حماية الأمن الوطني والأمن العام، ومنع أي جريمة جنائية، أو جمع معلومات عنها، أو التحقيق فيها، وكذلك مثل تنفيذ التزام قانوني أو أمر من محكمة، أو تحقيق أغراض البحث العلمي الذي يجرى للمصلحة العامة، أو حماية المصالح الحيوية للفرد.

ومن بين حالات إعفاء المراقب من بعض الالتزامات القانونية هي تصرف المراقب من أجل حماية المصالح الحيوية للفرد،⁽²³⁾ فيعفى المراقب مثلا من أخذ موافقة الفرد لمعالجة البيانات الشخصية أو من حذفها من أجل تحقيق المصالح الحيوية للفرد مثل: إنقاذ حياة الفرد في حالة طيبة طارئة؛ فإذا كان الشخص في حالة طيبة حرجة وغير قادر على تقديم موافقته، يجوز للمستشفى أو الجهة الطبية معالجة بياناته الشخصية مثل: سجله الطبي أو بياناته الصحية لتقديم الرعاية العاجلة أو إنقاذ حياته. أو إذا كان الفرد مصابا بمرض معد يشكل خطرا على حياته وعلى المجتمع، يجوز للمستشفى أو للجهة الصحية معالجة بياناته الشخصية أو الإفصاح عنها للسلطات الصحية دون موافقته للسيطرة على انتشار المرض وحماية صحته وصحة الآخرين. وكذلك في حالات إجلاء الأشخاص أثناء الكوارث الطبيعية مثل: الزلازل أو الفيضانات؛ فيمكن للجهات المختصة معالجة أو تبادل بيانات شخصية مثل: بيانات الإقامة أو الموقع الجغرافي لضمان إجلاء الأشخاص المتأثرين وحمايتهم من الخطر الوشيك.

وحتى لا يتم استغلال هذا الإعفاء بشكل غير مبرر، يجب أن يتم ربطه بضابط المصلحة المتحققة فعليا للفرد، بحيث يكون الهدف من المعالجة واضحا وضروريا لتحقيق منفعة حقيقية وجوهريّة، وفي هذا السياق تقول القاعدة الفقهية الإسلامية إن: «كل متصرف عن

23 - قانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، مادة 15، دولة قطر.

الغير فعليه أن يتصرف بالمصلحة»⁽²⁴⁾ وهذه القاعدة تشدد على أن أي إجراء يتخذ نيابة عن الآخرين يجب أن يحقق منفعة حقيقية ومباشرة لهم. وكذلك قاعدة تصرف الإمام على الرعية منوط بالمصلحة، والرعية هنا هي كل فرد يقع تحت الولاية العامة، وهذه القاعدة تؤكد أن أي تصرف يمارس في إطار السلطة يجب أن يكون هدفه الأساسي هو تحقيق المصلحة العامة أو الخاصة حسب مقتضى الحال وإلا لن يكون التصرف صحيحاً.⁽²⁵⁾ فالتصرف الصحيح يجب أن يحقق مصلحة الفرد الذي يقع هو وخصوصيته وبياناته الشخصية ضمن النطاق القانوني استناداً إلى مبدأ إقليمية القانون واستثناءاته من حيث الاختصاص العيني أو الشخصي أو حتى الاختصاص الشامل⁽²⁶⁾ خصوصاً أن البيانات الشخصية عابرة للحدود الجغرافية.

بناء على ما سبق؛ يجب أن تحدد المصلحة المرتبطة بالإعفاء في القانون القطري بوضوح، مع وجود آليات للرقابة والمساءلة لضمان أن هذا الإعفاء يستخدم فقط في الحالات الاستثنائية التي تحقق فعلاً حماية المصالح الحيوية للفرد، وفي هذا السياق نقترح تطبيق بعض الآليات مثل: الحصول على موافقة لاحقة أو إشعار ما بعد الطوارئ، مع الاحتفاظ بسجل واضح للأسباب والمبررات التي جعلت المراقب يتصرف بناء على المصالح الحيوية للفرد دون موافقته، مع عرض هذه الأسباب والمبررات على الفرد صاحب البيانات أو وليه، مع حقه بالطعن على ذلك أمام القضاء.

تاسعاً: الاتصالات الإلكترونية لغرض التسويق المباشر

يتعلق هذا الفصل بتنظيم التسويق المباشر عبر الوسائل الرقمية، مثل: البريد الرقمي،

- 24 - تاج الدين عبد الوهاب بن علي بن عبد الكافي السبكي (المتوفى 771هـ)، الأشباه والنظائر، تحقيق: عادل أحمد عبد الموجود وعلي محمد معوض، ط1، دار الكتب العلمية، بيروت، 1411هـ/1991م، ج1، ص 310.
- 25 - سلطان بن عبد الرحمن بن عبد القادر العبيدان، «التأصيل الفقهي لنظام حماية البيانات الشخصية السعودي»، مجلة أبحاث، اليمن: كلية التربية بجامعة الحديدة، مج11، ع2، يونيو 2024م، 460-541، ص 485.
- 26 - انظر: علي حسين الخلف وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، دار المكتبة القانونية، بغداد، ط1، 1982م، ص 86 - 108.

الرسائل النصية القصيرة، أو أي وسيلة اتصال رقمية أخرى، وألا يتم التسويق إلا بموافقة الفرد والالتزام بالغرض الذي منح الفرد بياناته الشخصية لأجلها، والهدف من ذلك هو حماية الأفراد من الإزعاج والاختراق غير المرغوب فيه لخصوصيتهم عن طريق رسائل التسويق، والتي قد تستغل في ارتكاب الجرائم الرقمية.

عاشرا: العقوبات

يفرض هذا القانون عقوبات على المخالفين تتراوح بين غرامات تصل إلى خمسة ملايين ريال قطري، حسب طبيعة وحجم الانتهاك. كما يتحمل الأشخاص الاعتباريون مسؤولية قانونية مستقلة عن أفعالهم.

حادي عشر: أحكام ختامية:

تتناول الأحكام الختامية من قانون حماية البيانات الشخصية القطري حق الأفراد في تقديم الشكاوى ضد مخالفات القانون إلى الإدارة المختصة التي بدورها تحقق وتصدر قرارات ملزمة قابلة للتظلم أمام الوزير، كما يعزز القانون التنسيق بين الجهات المهنية لحماية البيانات، ويبطل أي عقود مخالفة للقانون.

الفرع السابع

قانون مكافحة الإرهاب

منح قانون مكافحة الإرهاب رقم 27 لسنة 2019 صلاحيات استثنائية للنياحة العامة تمس البيانات الشخصية كما ورد في المواد 24 و 25 و 26 منه، بحيث تشمل المراقبة السمعية والبصرية، اعتراض الاتصالات، دخول نظم المعلومات، وضبط الرسائل ومراقبة الاتصالات والاطلاع على البيانات المالية مع اشتراط التسييب والتحديد الزمني والرقابة القضائية؛ بما

يعكس محاولة لتحقيق توازن بين متطلبات الأمن وحماية البيانات الشخصية؛ لا سيما أن هذه البيانات قد تتعدى الشخص محل المراقبة إلى محيطه الاجتماعي.

الفرع الثامن

قانون البصمة الحيوية

صدر في دولة قطر قانون رقم 17 لسنة 2025 بشأن البصمة الحيوية، أو ما يعرف بالبيانات البيومترية، وهي بيانات شخصية حساسة دالة على صاحبها، حيث يعد هذا القانون من القوانين الحديثة ذات الأثر المباشر على البيانات الشخصية؛ لما تنطوي عليه البصمة الحيوية من حساسية عالية وقدرة دقيقة على التعريف بالأشخاص.

وقد نظم القانون تبادل بيانات البصمة الحيوية مع الجهات القضائية الأجنبية والمنظمات الدولية، وفقا للقوانين المعمول بها في الدولة، وبشرط المعاملة بالمثل، وبعد موافقة النائب العام، مع مراعاة خصوصية وسرية هذه البيانات، وهذا ما يبرز البعد الدولي لحماية البصمة الحيوية في مواجهة الجرائم الرقمية العابرة للحدود.

وإلى جانب ذلك؛ أضفى القانون حجية في الإثبات على بيانات البصمة الحيوية المحفوظة في قاعدة البيانات ما لم يثبت العكس، وهو ما يعكس الثقة القانونية في الوسائل التقنية الحديثة المعتمدة على البيانات الشخصية، الأمر الذي يمنح هذه البيانات دورا محوريا في الإثبات الجنائي؛ خصوصا في الجرائم الرقمية التي يصعب تحديد هوية الجاني فيها بالوسائل التقليدية.

كما أن هذا القانون أرسى مجموعة من الضمانات التي تكفل حماية بيانات البصمة الحيوية والحد من التعسف في استخدامها، حيث نص على الحالات التي يجوز فيها الرجوع إلى قاعدة بيانات البصمة الحيوية على سبيل الحصر، وذلك بناء على أمر من النيابة العامة أو المحكمة المختصة، كما أقر مبدأ سرية هذه البيانات وحظر الاطلاع عليها أو استخدامها إلا

في الأغراض المحددة بالقانون، وذلك بهدف تحقيق الموازنة بين المتطلبات الأمنية وضمانات الخصوصية ومقتضيات العدالة الجنائية.⁽²⁷⁾

المطلب الثاني

الأطر القانونية الدولية لحماية البيانات الشخصية

لا تقتصر الجهود القانونية الرامية إلى حماية حق الأفراد في الخصوصية والبيانات الشخصية على الإطار الوطني فحسب، بل تمتد أيضا إلى الساحة الدولية من خلال القوانين والاتفاقيات الدولية والمواثيق الأممية، التي أكدت على أن الخصوصية تعد من الحقوق الإنسانية الأساسية. ينبع هذا الاهتمام من إدراك عالمي بأن التحديات الناتجة عن التقنيات الحديثة والانفتاح الرقمي العابر للحدود وما يصحب ذلك من جرائم وانتهاكات لا يمكن مواجهتها حصرا بنهج محلي، بل يستلزم ذلك تعاونا دوليا واتفاقات عابرة للقارات.

لقد ظهرت العديد من الاتفاقيات الدولية التي اهتمت بحماية البيانات الشخصية والخصوصية الإنسانية وجعلتها من الحقوق الأساسية المعترف بها دوليا، ولأهمية هذا الحق، حرصت هذه الاتفاقيات الدولية على تضمين نصوص خاصة تعزز من حماية الخصوصية.

الفرع الأول

أبرز الاتفاقيات الدولية في حماية حق الخصوصية الإنسانية

أولا: الإعلان العالمي لحقوق الإنسان

يعد الإعلان العالمي لحقوق الإنسان لعام 1948م أحد أبرز الوثائق الدولية التي أرسيت الأسس القانونية لحماية الخصوصية كحق من حقوق الإنسان الأساسية. وقد نص هذا الإعلان
27 - قانون رقم 17 لسنة 2025 بشأن البصمة الحيوية، دولة قطر. صدر هذا القانون في 1 سبتمبر 2025م.

صراحة على حماية الخصوصية، حيث جاء فيه: «لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته. ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات».⁽²⁸⁾

يشير هذا النص إلى ضرورة احترام الحياة الخاصة للأفراد، ومنع أي تدخل غير مشروع أو تعسفي في شؤونهم الخاصة؛ سواء كان ذلك من قبل الأفراد أم الجهات الحكومية، كما أكد النص على حرمة المساكن والمراسلات والحياة الأسرية، ما يعني أن حماية الخصوصية تمتد إلى جميع جوانب حياة الإنسان؛ سواء المادية مثل المسكن أم المعنوية مثل المراسلات، كما يؤكد النص بأن على الدول توفير الحماية القانونية للأفراد ضد أي تدخل يمس خصوصيتهم أو ينتهكها.

ثانيا: الاتفاقية الأوروبية لحقوق الإنسان

بعد تأكيد الإعلان العالمي لحقوق الإنسان على حرمة الحياة الخاصة، جاءت الاتفاقية الأوروبية لتعزز هذا المبدأ ضمن إطار إقليمي، فحرصت هذه الاتفاقية على احترام حق الخصوصية، ونصت على أنه: «لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته. -2 لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقا للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحرياتهم».⁽²⁹⁾

يعد هذا النص من أهم النصوص القانونية الدولية التي تؤكد على الحق في الخصوصية باعتباره أحد الحقوق الأساسية التي يجب صونها وحمايتها. ويذكر البند الأول من هذا النص على حق كل إنسان في احترام حياته الخاصة والعائلية ومسكنه ومراسلاته؛ مما يعكس إدراكا عميقا

28 - الإعلان العالمي لحقوق الإنسان 1948م، المادة 12.

29 - الاتفاقية الأوروبية لحقوق الإنسان 1950م، المادة 8.

لأهمية حماية الأفراد من التدخلات غير المبررة في حياتهم الشخصية؛ سواء من قبل السلطات العامة أم غيرها. كما يضع البند الثاني إطارا استثنائيا يسمح بتقييد هذا الحق، ولكنه يشترط أن تكون هذه القيود محددة وفقا للقانون، ومبررة بمقتضيات الضرورة ولمصالح محددة مثل حفظ النظام ومنع الجريمة.

ثالثا: العهد الدولي الخاص بالحقوق المدنية والسياسية

نص العهد الدولي الخاص بالحقوق المدنية والسياسية⁽³⁰⁾ على أنه لا يجوز تعريض أي شخص - على نحو تعسفي أو غير قانوني - لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته. ومن حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس.

يعد العهد الدولي للحقوق المدنية والسياسية أحد أهم الوثائق الدولية الملزمة التي تناولت حماية الحق في الخصوصية كجزء أساسي من حقوق الإنسان، ويمثل مرجعا عالميا لحماية الخصوصية، ويلزم الدول الأطراف بتوفير ضمانات قانونية واضحة تمنع أي انتهاك لهذا الحق. وتجدر الإشارة أن دولة قطر انضمت إلى العهد الدولي الخاص بالحقوق المدنية والسياسية في عام 2018م،⁽³¹⁾ وذلك استنادا إلى المادة 68 من الدستور.⁽³²⁾

رابعا: اتفاقية بودابست:

إن الاتفاقية المتعلقة بمكافحة الجريمة الرقمية المعروفة باتفاقية بودابست،⁽³³⁾ تعد

30 - العهد الدولي الخاص بالحقوق المدنية والسياسية 1966م، المادة 17.

31 - مرسوم رقم 40 لسنة 2018 بالموافقة على انضمام دولة قطر إلى العهد الدولي الخاص بالحقوق المدنية والسياسية، دولة قطر. علما أن دولة قطر تحفظت على بعض المواد ولم توافق عليها. ونرى أن أي مادة في الاتفاقيات الدولية تخالف أحكام الشريعة الإسلامية لا ينبغي الموافقة عليها، ومن ذلك تحفظ دولة قطر على المادة 23 البند 4 لمخالفته أحكام الشريعة الإسلامية.

32 - الدستور الدائم 2004م، المادة 68، دولة قطر.

33 - مجلس أوروبا، اللجنة الوزارية، مجموعة المعاهدات الأوروبية رقم 185، الاتفاقية المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست)، تم التوقيع على هذه الاتفاقية في العاصمة المجرية بودابست بتاريخ 8 نوفمبر 2001م.

أول معاهدة دولية تهدف إلى مواجهة الجرائم الرقمية وتعزيز التعاون الدولي لمكافحتها، وتلزم الدول بسن الحد الأدنى من القوانين الضرورية للتعامل مع الجرائم الرقمية.⁽³⁴⁾ ومن أبرز الأفعال المجرمة التي تنتهك الخصوصية الواردة في اتفاقية بودابست هي: الدخول غير المشروع، اعتراض البيانات، والتدخل في البيانات والنظام.

خامسا: اتفاقيات أخرى اهتمت بالخصوصية

تجدر الإشارة إلى أن هناك العديد من الاتفاقيات الدولية والإقليمية - لا يسع المجال لذكرها - التي أولت اهتماما بالغا بحماية الحق في الخصوصية، مثل: ما نص عليه الميثاق العربي لحقوق الإنسان على الحق في الخصوصية،⁽³⁵⁾ وكذلك ما نص عليه إعلان القاهرة حول حقوق الإنسان في الإسلام الذي أكد على حرمة الحياة الخاصة،⁽³⁶⁾ وأيضا ما جاء في المادة 11 من ميثاق سان خوسيه.⁽³⁷⁾

وقد انعكس هذا الاهتمام في دساتير وقوانين الدول الوطنية، حيث ترسخت مبادئ حماية الخصوصية في المنظومات القانونية، وصولا إلى الاجتهادات والأحكام القضائية. ومن أبرز ما أكدت عليه المحكمة الدستورية العليا في أحكامها، التشديد على احترام حرمة الحياة الخاصة وصونها من أي اعتداء، وقد جاء في أحد أحكامها أن: «قضاء هذه المحكمة قد جرى على أن ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغوارا لا يجوز النفاذ إليها، وينبغي دوما ألا يقتحمها أحد ضمانا لسريتها وصونا لحرمتها، فلا يكون اختلاس بعض جوانبها مقبولا، وهذه المناطق من خواص الحياة ودخائلها».⁽³⁸⁾

34 - سامي جاد واصل، «التعاون الدولي في مكافحة الجريمة الإلكترونية»، مجلة القانون والتكنولوجيا، كلية القانون بالجامعة البريطانية في مصر، مج3، ع1، أبريل 2023م، 13-99، ص 53.

35 - الميثاق العربي لحقوق الإنسان، تونس 2004م، المادة 21.

36 - إعلان القاهرة حول حقوق الإنسان في الإسلام، القاهرة 1990م، المادة 4.

37 - الاتفاقية الأمريكية لحقوق الإنسان المعروفة باسم ميثاق سان خوسيه 1969م، المادة 11.

38 - جمهورية مصر العربية، حكم المحكمة الدستورية العليا، قضية رقم 56 لسنة 18 القضائية، الجلسة العلنية المنعقدة في تاريخ 15 رجب 1418هـ الموافق 15 نوفمبر 1997م، الجريدة الرسمية العدد 48 في 27 نوفمبر 1997 صفحة 2925.

تظهر هذه الأطر القانونية الدولية أن الخصوصية ليست مجرد حق فردي، بل هي حجر زاوية في تعزيز حقوق الإنسان عامة، وتؤكد على ضرورة التوازن بين الحفاظ على الخصوصية وحماية الأمن والمصلحة العامة، واستناداً إلى هذا الأساس الواسع لحماية الخصوصية وحرمة الحياة الخاصة، وقد ظهرت لاحقاً تنظيمات دولية أكثر تخصصاً بشأن البيانات الشخصية.

الفرع الثاني

أبرز الاتفاقيات الدولية لحماية البيانات الشخصية

تعد حماية البيانات الشخصية جزءاً لا يتجزأ من حماية الخصوصية. وعلى الرغم من أن الأطر القانونية الدولية قد ركزت بشكل عام على حماية الخصوصية كحق أساسي للإنسان؛ إلا أن الحاجة إلى حماية البيانات الشخصية بشكل خاص دفعت المجتمع الدولي إلى وضع اتفاقيات دولية متخصصة في تنظم جمع البيانات الشخصية ومعالجتها، وتأتي هذه الأطر استجابة للتحديات التي يفرضها الفضاء الرقمي، لا سيما في ظل التوسع الهائل في تبادل البيانات بين الدول والشركات العالمية وزيادة الجرائم الرقمية.

أولاً: اللائحة العامة لحماية البيانات (GDPR)

تعتبر اللائحة العامة لحماية البيانات الأوروبية⁽³⁹⁾ واحدة من أكثر القوانين شمولاً وتنظيماً لحماية البيانات الشخصية، وتهدف اللائحة إلى منح الأفراد في الاتحاد الأوروبي سيطرة أكبر على بياناتهم الشخصية، وفق مبادئ الشرعية والإنصاف والشفافية والدقة والسرية والنزاهة

39 - الاتحاد الأوروبي، البرلمان الأوروبي والمفوضية الأوروبية، اللائحة العامة لحماية البيانات (GDPR)، قانون رقم 679/2016م، تاريخ الاعتماد 27 أبريل 2016م بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات، ومرت هذه اللائحة بفترة انتقالية لمدة عامين وذلك للسماح للشركات والمؤسسات بترتيب أوضاعها مع المتطلبات الجديدة؛ لتصبح اللائحة سارية المفعول اعتباراً من تاريخ 25 مايو 2018م، وإلغاء القانون EC

والمساءلة في معالجة البيانات⁽⁴⁰⁾، وخلق بيئة آمنة لتداول البيانات داخل الاتحاد الأوروبي وخارجه.

تحتوي اللائحة على 99 مادة تشمل الأحكام العامة، ومبادئ معالجة البيانات الشخصية، وحقوق الفرد صاحب البيانات كحق العلم والوصول والتصحيح، كما تتناول التزامات الأطراف التي تجمع وتعالج البيانات، مثل: المراقب والمعالج ومسؤول البيانات، وتشمل البيانات الشخصية عبر الحدود، كما تتحدث عن الانتهاكات والمسؤولية والعقوبات.

إن هذه اللائحة تعتبر من أكثر القوانين شمولاً ودقة في حماية البيانات على المستوى العالمي، كما أنها معياراً للدول في سن قوانينها الوطنية لحماية البيانات الشخصية.

ثانياً: اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي

تهدف الاتفاقية الإفريقية⁽⁴¹⁾ إلى إرساء إطار قانوني إقليمي موحد ينظم حماية البيانات داخل الدول الأعضاء، ويضمن معالجتها وفق مبادئ الخصوصية. إلى جانب تعزيز الأمن الرقمي ومكافحة الجرائم الرقمية، وحماية البنية التحتية الرقمية في القارة الإفريقية.

ورغم ما يواجه تنفيذ هذه الاتفاقية من تحديات عملية، مثل: نقص الموارد الفنية والبشرية وضعف البنية التحتية الرقمية في بعض الدول الإفريقية؛ فإنها تظل نموذجاً قانونياً متقدماً في مجال حماية البيانات الشخصية.

40 - Davit Marikyan, Savvas Papagiannidis, Omer F. Rana, and Rajiv Ranjan, "General Data Protection Regulation: A Study on Attitude and Emotional Empowerment," Behaviour & Information Technology, Taylor & Francis, Vol. 43, No. 14, 2024, pp. 3561-3577: 3563.

41 - اتفاقية الاتحاد الإفريقي رقم XXV / 846 .CL (EX) بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، التي تم اعتمادها في مدينة مالابو عاصمة جمهورية غينيا الاستوائية، في الدورة العادية الثالثة والعشرين لقمة رؤساء دول وحكومات الاتحاد الإفريقي بتاريخ 27 يونيو 2014م.

وفي المقابل، يلاحظ غياب اتفاقية إقليمية مماثلة على مستوى قارة آسيا تضاهي اللائحة العامة لحماية البيانات الأوروبية (GDPR)، أو الاتفاقية الإفريقية. كما تفتقر الدول العربية؛ سواء على مستوى جامعة الدول العربية أم دول مجلس التعاون الخليجي إلى اتفاقية إقليمية موحدة تعنى بحماية البيانات الشخصية.

ونرى أنه في الوقت الحالي من الضروري صياغة اتفاقية خليجية موحدة لحماية البيانات الشخصية، وتجدر الإشارة إلى اتفاقية الأمم المتحدة لمكافحة الجريمة الرقمية، حيث تضمنت عددا من الأحكام التي تعنى بحماية البيانات الشخصية،⁽⁴²⁾ وتعد هذه الاتفاقية أول إطار دولي شامل وملزم قانونا لمواجهة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية. كما تكتسب هذه الاتفاقية أهمية خاصة في مجال مكافحة الجرائم الرقمية العابرة للحدود، لما تطرحه من آليات لتعزيز التعاون الدولي وتبادل الأدلة الرقمية.

بناء على ما سبق؛ يتبين أن الجهود القانونية لتحقيق حماية فعالة للخصوصية والبيانات الشخصية قطعت أشواطاً مهمة. ومع ذلك، ما زالت هذه المنظومات تواجه جملة من التحديات العملية والقانونية التي تعيق تطبيقها على أرض الواقع؛ سواء على المستوى الوطني أم الدولي.

42 - انظر: الجمعية العامة للأمم المتحدة، الدورة التاسعة والسبعون، البند 108 من جدول الأعمال، قرار رقم 79/243، اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، المواد: 7 و 8 و 9 و 10 و 12 و 13 و 14 و 16. بتاريخ 24 ديسمبر 2024م في نيويورك اعتمدت الجمعية العامة للأمم المتحدة اتفاقية جديدة ملزمة قانوناً تهدف إلى منع ومكافحة الجريمة السيبرانية، لتتوج بذلك عملية تفاوض استمرت خمس سنوات. واعتمدت الجمعية العامة القرار دون تصويت. وتفاوضت الدول الأعضاء في الأمم المتحدة، بمشاركة المجتمع المدني، والمؤسسات الأكاديمية، والقطاع الخاص، على نص الاتفاقية على مدار خمس سنوات، حيث اكتملت صياغة مسودتها النهائية في 9 أغسطس 2024م. وتم فتح الاتفاقية للتوقيع عليها في مدينة هانوي بفييتنام في أكتوبر 2025م وتدخل الاتفاقية حيز التنفيذ بعد 90 يوماً من تصديق الدولة الأربعين عليها. وقد وقعت دولة قطر على الانضمام لهذه الاتفاقية الدولية في 25 أكتوبر 2025م، لمزيد من التفصيل انظر: الرابط التالي: جدول الأعمال - الدورة 79 للجمعية العامة. / الموقع الرقمي الرسمي لوكالة الأنباء القطرية (قنا)، خبر بعنوان: اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية.. خطوة محورية نحو التصدي للتهديدات الرقمية، تاريخ 13 نوفمبر 2025م، على الرابط التالي: <https://tinyurl.com/ye26ye2s>

المبحث الثاني

حماية الخصوصية

في زمن العولمة الرقمية

وتحديات التعاون الدولي

نتناول في هذا المبحث من خلال المطلب الأول التحديات القانونية التي يواجهها المشرع القطري في مجال تأمين الخصوصية وحماية البيانات الشخصية، من حيث مدى كفاية الإطار التشريعي الوطني وضماناته العملية. أما المطلب الثاني فنركز من خلاله على التحديات ذات البعد الدولي، والمتعلقة بآليات التعاون بين الدول في حماية الخصوصية والبيانات الشخصية، وما يترتب عليها من إشكاليات قانونية وتطبيقية في ظل الطبيعة العابرة للحدود للفضاء الإلكتروني.

المطلب الأول

التحديات القانونية الوطنية في تأمين البيانات الشخصية

تواجه الدول ومنها دولة قطر تحديات قانونية متزايدة في تأمين البيانات الشخصية من الجرائم والتهديدات الرقمية، وذلك في ظل التطور السريع للتقنية والاعتماد المتزايد على المعاملات الرقمية. فبينما تسعى القوانين الوطنية إلى حماية البيانات الشخصية من الجرائم والتهديدات؛ فإن التطور السريع لأساليب الاختراق والاستغلال الرقمي يجعل من الصعب على القوانين المحلية مواكبة هذه التهديدات بفاعلية. ونعرض بالفروع التالية أبرز التحديات القانونية الوطنية في حماية البيانات الشخصية من الجرائم والانتهاكات الرقمية.

الفرع الأول

عدم وجود تنظيم قانوني واضح للتقنيات الحديثة

لا تزال العديد من الدول، ومنها دولة قطر، بحاجة إلى إطار قانوني شامل ومتكامل وقوي ينظم استخدام التقنيات الحديثة مثل: الذكاء الصناعي، وشبكة الأشياء أو إنترنت الأشياء (IoT)، ومعالجة البيانات الضخمة (Big Data)، الحوسبة السحابية، والأجهزة القابلة للارتداء، وتقنيات المدن الذكية، فهذه التقنيات تقوم بمعالجة البيانات الشخصية، والأطر الوطنية الحالية لا توفر حماية قانونية متكاملة لمواجهة المخاطر القانونية والتقنية التي قد تنشأ عن استخدام هذه التقنيات؛ مما يؤدي إلى فجوات قانونية يمكن استغلالها في الجرائم الرقمية والانتهاكات، ويزيد من صعوبة ضمان الامتثال القانوني وحماية الخصوصية والبيانات الشخصية بفاعلية.

فالأفعال؛ مثل: استخدام الذكاء الصناعي وتوجيهه للاحتيال على الضحية دون تدخل من المبرمج الأول قد ينشئ إشكالية في تحديد المسؤولية الجنائية لمثل هذه الأفعال التي لم ينظمها القانون بشكل واضح حتى الآن؛ مما قد يؤدي إلى فجوات قانونية تستغل للإفلات من العقاب، ولذلك بدأت الدول، مثل: دولة قطر بوضع بعض الخطط لتسخير التقنيات الحديثة كالذكاء الصناعي واستخدامه في تعزيز الأمن المعلوماتي وحماية البيانات الشخصية من الاستغلال عبر الشبكة العالمية،⁽⁴³⁾ إلا أن الطريق ما زال في البداية، وبالتالي؛ فإن مثل

43 - انظر: عمر محمد منيب إدليبي، المسؤولية الجنائية الناتجة عن أعمال الذكاء الاصطناعي، رسالة ماجستير، كلية القانون، جامعة قطر، يناير 2023م، ص 49 و50 / الموقع الرقمي لمركز قطر للتطور المهني، استراتيجية قطر الوطنية في مجال الذكاء الاصطناعي، متوفر على الرابط: ثورة الذكاء الاصطناعي: قطر على المسار الصحيح | QCDC تاريخ الاطلاع 2025/02/07م. / ميثاق تطوير واستخدام الذكاء الاصطناعي في دولة الإمارات، متوفر على الرابط: تشريعات الإمارات العربية المتحدة تاريخ الاطلاع 2025/02/07م. / موقع منظمة التعاون والتنمية، توصية المجلس بشأن الذكاء الاصطناعي، متوفر على الرابط: الصكوك القانونية لمنظمة التعاون والتنمية في الميدان الاقتصادي تاريخ الاطلاع 2025/02/08م. / جامعة لوسيل في دولة قطر نظمت مؤتمراً خاصاً بالذكاء الصناعي وهو (مؤتمر القانون والذكاء الاصطناعي) وذلك في يوم الأربعاء 13 سبتمبر 2023م، وهو أول مؤتمر دولي تنظمه الجامعة عن القانون والذكاء الاصطناعي، والذي يتزامن مع الاحتفال باليوم العالمي للقانون، انظر: موقع جامعة لوسيل متوفر على الرابط:

هذه التقنيات تحتاج لتنظيم قانوني يوازن بين الاستفادة من هذه التقنيات وبين الحماية من مخاطرها.

الفرع الثاني

التطور التقني السريع في مقابل التطور القانوني البطيء

يعتبر الفارق الزمني بين التطورات التقنية المتسارعة والقدرة القانونية على مواكبتها أحد أبرز التحديات القانونية الوطنية في حماية الخصوصية والبيانات الشخصية؛ إذ يعد هذا الفارق فرصة للشركات الانتهازية وللمجرمين في انتهاك الخصوصية واستغلال البيانات الشخصية مع الإفلات من العقاب بسبب مبدأ قانونية الجرائم والعقوبات وأنه لا جريمة ولا عقوبة إلا بنص سابق على الفعل،⁽⁴⁴⁾ وهذا المبدأ نص عليه الدستور القطري صراحة في المادة 40.

ومع أننا مع هذا المبدأ، وهو أحد المبادئ الأساسية التي تحمي الحقوق والحريات؛ إلا أنه يشكل تحدياً في مواجهة الجرائم التي تستغل التقنيات الحديثة بوتيرة متسارعة قبل الوصول القانوني لها. كما أن تعدد الجهات الفاعلة، مثل: شركات التقنية، والحكومات، والمستخدمون، والجهات التنظيمية يعقد عملية سن القوانين الفعالة.

الفرع الثالث

عدم وجود تنظيم قانوني لمراكز البيانات الوطنية

رغم الجهود المبذولة إلا أنه لا يوجد في القانون القطري - حسب اطلاعنا - قانون خاص ينص بشكل صريح على تنظيم إلزام المؤسسات الوطنية بتوطين البيانات وتخزينها داخل

مؤتمر القانون والذكاء الاصطناعي - جامعة لوسيل تاريخ الاطلاع 2025/02/07م. / قرار مجلس الوزراء رقم 10 لسنة 2021 بإنشاء لجنة الذكاء الاصطناعي، دولة قطر.

44 - انظر: علي حسين الخلف وسلطان عبد القادر الشاوي، مرجع سابق، ص 30.

الدولة؛ مما يسمح لبعض الشركات والجهات بنقل بيانات الأفراد إلى دول أخرى، فهذه المسألة تثير إشكالات حول مدى السيطرة القانونية والسيادة الرقمية على البيانات، وحماية المواطنين والمقيمين من تسريب معلوماتهم أو استغلالها خارج نطاق الولاية القضائية القطرية.

إن البنية التحتية الرقمية تعتبر الأساس الذي تعتمد عليه حماية الخصوصية، كما أنها من الأهداف الرئيسة للمجرمين لما تحتويه من أصول رقمية. فكلما كانت البنية التحتية ومراكز البيانات آمنة ومحكمة بصرامة، زادت قدرة الأفراد على الحفاظ على خصوصيتهم والتحكم في بياناتهم الشخصية من جهة، ومنع الاعتداء عليها من جهة أخرى. فالبنية التحتية وبما فيها من مراكز بيانات تعتبر مستودعا للخصوصية وحافطة للبيانات الشخصية، وتستحق التوطين والتنظيم القانوني الصارم؛ سواء في القطاع العام أم الخاص. فالاعتداء على البنية التحتية الرقمية الحرجة وبالذات مراكز البيانات فيها هو اعتداء على السيادة الوطنية الرقمية.

الفرع الرابع

إشكالية حماية البيانات الشخصية

في الشركات الكبرى متعددة الجنسيات

إن عدم وجود إطار قانوني وطني واضح وفعال لحماية البيانات الشخصية في الشركات الكبرى متعددة الجنسيات التي تعالج البيانات الشخصية وتنقلها خارج الحدود الوطنية يؤدي إلى صعوبة مراقبة تلك الشركات للتأكد من التزامها بالقوانين الوطنية، وفي هذا السياق تقوم بعض الدول، مثل: دولة قطر، بالتنسيق المباشر مع بعض الشركات العالمية التي تجمع البيانات الشخصية، مثل: شركة سناب شات، لتعزيز سبل التعاون ودعم التحول الرقمي وضمان الامتثال لمعايير حماية البيانات الشخصية.⁽⁴⁵⁾

45 - انظر: الموقع الرسمي لمكتب الاتصال الحكومي في دولة قطر متوفر على الرابط: شركة سناب تعتزم افتتاح مكتب في قطر وتوقع مذكرة تفاهم مع مكتب الاتصال الحكومي، وقعت شركة سناب شات (Snap Inc) مذكرة تفاهم مع مكتب الاتصال الحكومي في قطر لافتتاح مكتب في الدوحة. تاريخ الاطلاع: 2025/02/08م.

بالإضافة إلى ما سبق؛ فهناك العديد من التحديات القانونية الوطنية الأخرى فيما يخص حماية الخصوصية والبيانات الشخصية، مثل: إشكاليات حق النسيان، والاحتفاظ لمدة زمنية طويلة بالبيانات الشخصية؛ مما يعرضها للتسرب والخطر، بالإضافة إلى الصعوبات التي تواجه الجهات المعالجة في تنفيذ القوانين الرقمية داخل الدولة، مثل: ضعف ونقص الكوادر المتخصصة، وضعف التعاون بين الجهات المختصة؛ مما يؤدي إلى عدم التزام بعض الجهات بالمعالجة بالقوانين الأمر الذي يسمح للمجرمين باستغلال هذه الإشكاليات كثغرات لارتكاب جرائمهم الرقمية وذلك على المستوى الوطني؛ فضلا عن أن هناك تحديات أخرى على الصعيد الدولي.

المطلب الثاني

تحديات التعاون الدولي في حماية البيانات الشخصية

أصبحت حماية البيانات الشخصية قضية ذات بعد عالمي يتجاوز الحدود الوطنية، وذلك نظرا لطبيعة الشبكة العالمية والتقنيات الحديثة التي تتجاوز الحدود الجغرافية للدول؛ مما يخلق تحديات قانونية وتنظيمية كبيرة في فرض الحماية الفاعلة على الخصوصية والبيانات الشخصية في الفضاء الرقمي. وفي هذا السياق، تواجه الدول تحديات متعددة عند التعامل مع الجرائم الرقمية العابرة للحدود التي تستهدف البيانات الشخصية. ومن أبرز التحديات القانونية الدولية في حماية البيانات الشخصية من الجرائم والتهديدات الرقمية العابرة للحدود:⁽⁴⁶⁾

46 - انظر: الأمم المتحدة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، سلسلة الوحدات الجامعية: الجرائم الإلكترونية، الوحدة التعليمية 7: التعاون الدولي على مكافحة الجريمة الإلكترونية، متوفر على الرابط: Cybercrime Module 7 Key Issues تاريخ الاطلاع: 2025/02/09م. / سامي جاد واصل، مرجع سابق، ص 84-87. / أيمن سيد محمد مصطفى العسقلاني، «دور مجلس التعاون الخليجي القانوني والتعاوني في مكافحة الجرائم الإلكترونية: دراسة تحليلية واستراتيجية مقترحة»، مجلة الدراسات الدولية، معهد الأمير سعود الفيصل للدراسات الدبلوماسية، ع32، شعبان 1443هـ / 2022م، 107-155، ص130-134.

الفرع الأول

غياب الأساس القانوني الموحد لحماية الخصوصية والبيانات الشخصية

رغم تعدد المبادرات والوثائق الدولية التي تناولت حماية الخصوصية والبيانات الشخصية كاتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لعام 2025؛ فإنه لا تزال المنظومة الدولية تفتقر إلى وجود معاهدة دولية عامة وموحدة تلزم جميع الدول بتبني معايير شاملة ومتكاملة لمعالجة البيانات الشخصية وضمان حمايتها، على نحو مماثل لما قرره بعض الأطر الإقليمية وعلى رأسها اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، وذلك في ظل الطبيعة العالمية للفضاء الرقمي وأهمية البيانات الشخصية كمورد استراتيجي في الاقتصاد الرقمي.

علاوة على ذلك، يفتقر المجتمع الدولي إلى قانون إجرائي موحد ينظم التحقيقات والتحريات المتعلقة بالجرائم التي تستهدف البيانات؛ مما يؤدي إلى إشكاليات قانونية وإجرائية. إذ لا توجد قواعد دولية متفق عليها تضمن حماية البيانات الشخصية خلال عمليات الرقابة والتفتيش الرقمي، أو تحدد السبل القانونية للحصول على الأدلة الرقمية وآليات حفظها بشكل يضمن عدم انتهاك الخصوصية. هذا الفراغ القانوني يعقد التعاون الدولي، ويضعف فاعلية الجهود المشتركة في مواجهة الجرائم الرقمية العابرة للحدود التي تستهدف البيانات الشخصية.

الفرع الثاني

إشكاليات السيادة الوطنية

تمثل إشكالية السيادة الوطنية أحد التحديات الكبرى في حماية البيانات الشخصية على المستوى الدولي، حيث ترتبط السيادة ارتباطاً وثيقاً بقدرة الدول على فرض قوانينها داخل

حدودها الإقليمية. ومع تزايد الجرائم والانتهاكات الرقمية العابرة للحدود، تظهر تعقيدات قانونية تتمثل في التضارب بين حق الدولة في حماية سيادتها، بما يشمل بيانات مواطنيها، وبين الحاجة إلى التعاون الدولي لمكافحة الجرائم والانتهاكات الرقمية التي تستهدف تلك البيانات.

الفرع الثالث

تنازع الاختصاص القضائي الدولي

تتداخل سلطات الدول في تحديد الجهة القضائية المختصة بالتحقيق والمحاكمة، وتنشأ هذه الإشكالية عندما تكون الجريمة الرقمية قد حدثت في دولة، ولكن وقعت آثارها في دولة أخرى، أو إذا كان المجرم والضحية ومزود الخدمة يتبعون أنظمة قانونية مختلفة بحيث تقع أجزاء الجريمة المكونة لركنها المادي في مجموعة دول.

الفرع الرابع

إشكالية التجريم المزدوج

تنشأ هذه الإشكالية عندما لا يكون الفعل المجرم في دولة معينة مصنفاً كجريمة في الدولة الأخرى المعنية بالقضية؛ مما يعيق تنفيذ طلبات التعاون القانوني، مثل: تسليم المجرمين أو تبادل الأدلة.

فبدون ازدواجية التجريم والقوانين المنسقة، يتم إنشاء ملاذات آمنة للجرائم الرقمية بحيث لا يمكن مقاضاة مرتكبي هذه الجرائم. وقد لوحظ هذا في قضية فيروس (Love Bug) سيئ السمعة لعام 2000م، والتي لا يمكن مقاضاة مبتكرها وموزعها؛ لأن أفعالها لم تكن تعتبر جريمة في بلده الفلبين وقت وقوع الحادث.

الفرع الخامس

رفض طلبات المساعدة

تعتمد الدول على مبدأ السيادة الوطنية لحماية مصالحها؛ مما يجعلها ترفض تقديم المساعدة إذا رأت أن الطلب يتعارض مع سيادتها أو أمنها أو نظامها العام، أو يتعارض مع قوانينها الداخلية.

الفرع السادس

عدم وجود قنوات اتصال فاعلة بين الدول ومزودي الخدمة العالميين

على الرغم من وجود اتفاقيات دولية، مثل: اتفاقية بودابست، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وحتى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية؛ إلا أن آليات التعاون القانوني المتبادل، مثل: طلبات المساعدة القانونية، وتبادل المعلومات، أو تسليم المجرمين غالباً ما تعاني من تأخيرات زمنية طويلة قد تمتد لأشهر. هذا التأخير يضعف من فاعلية التحقيقات، حيث يؤدي إلى تدهور جودة الأدلة الرقمية أو فقدانها، بالإضافة إلى صعوبة تعقب المجرمين الذين يستغلون الطبيعة السريعة للتقنيات الحديثة للإفلات من العدالة.

بالإضافة إلى ذلك، تعتمد العديد من التحقيقات على الحصول على معلومات حيوية من شركات التقنية الكبرى ومزودي الخدمات الرقمية، مثل: منصات التواصل الاجتماعي ومحركات البحث. ومع ذلك؛ فإن هذه الشركات قد لا تكون ملزمة قانوناً بالاستجابة الفورية لطلبات الدول الأجنبية، خاصة في ظل غياب التزامات دولية واضحة تلزمها بالتعاون العاجل. هذا البطء في الاستجابة يؤدي إلى فجوات زمنية تعيق سير التحقيقات، ما يسمح للمجرمين بإخفاء آثارهم أو مواصلة جرائمهم دون رادع.

الفرع السابع

إشكاليات تسليم المجرمين

إن تسليم المجرمين هو في الأصل من وسائل تجاوز حدود مبدأ الإقليمية والصلاحيات المكانية للولاية القانونية؛ فالدولة التي وقعت فيها الجريمة لا تملك سلطة القبض على المجرم إذا فر إلى دولة أخرى؛ لأنها لا تملك الولاية المكانية لقوانينها خارج حدودها، ولذلك يقتضي الأمر إبرام اتفاقيات بين الدول لتسليم المجرمين من أجل مد أثر قوانينها الجنائية بصورة قانونية من خلال التعاون الدولي؛ لتفعيل العدالة الجنائية في الجرائم العابرة للحدود.

ومع ذلك؛ فإن هذا التعاون يصطدم باختلاف القوانين والإجراءات بين الدول، حيث ترفض دولة طلب تسليم مجرم لدولة أخرى إذا كان الفعل المجرم غير معاقب عليه في قانونها، أو إذا اعتبرت الجريمة سياسية أو مرتبطة بها أو عسكرية، أو كان الطلب مبني على أسباب طائفية أو دينية. وبالإضافة إلى ذلك، يرفض التسليم في الحالات التي قد يتعرض فيها الشخص المطلوب لعقوبة أو معاملة لا إنسانية أو مهينة، أو كان سجل الدولة طالبة في مجال حقوق الإنسان محل انتقاد دولي.

كما تشمل الأسباب الأخرى لرفض التسليم عدم كفاية الأدلة لتبرير التسليم أو كون الشخص المطلوب مواطناً في الدولة التي يقيم فيها، حيث يعد مبدأ عدم تسليم المواطنين مكرساً في العديد من الدساتير والقوانين الوطنية والاتفاقيات الإقليمية والدولية، كما نص القانون القطري على ذلك.⁽⁴⁷⁾

47 - قانون مكافحة الجرائم الإلكترونية الصادر بالقانون رقم 14 لسنة 2014، مادة 40 بند 5، دولة قطر.

الفرع الثامن

اختلاف القوانين بين الدول وتعارضها مع التعاون الدولي

تعتمد كل دولة إطارا قانونيا خاصا بها؛ مما يؤدي إلى تباين كبير بينها في الإجراءات والمعايير القانونية والقضائية⁽⁴⁸⁾. ففي اليابان على سبيل المثال، لا يسمح بطلبات الحصول على المعلومات من خلال قنوات التعاون الدولي إلا عندما لا ينوي البلد الطالب استخدام المعلومات كدليل. وبالإضافة إلى ذلك؛ قد يعتبر الدليل الرقمي الذي تم الحصول عليه من قنوات التعاون الدولي غير الرسمية كشكل من أشكال المساعدة التقنية غير مقبولة كدليل أمام المحاكم الوطنية للدولة طالبة إذا لم يتم الاحتفاظ بسلسلة العهدة أو سلسلة متابعة الأدلة،⁽⁴⁹⁾ وسلسلة العهدة للأدلة الرقمية هي عملية تتبع لدورة حياة الأدلة الرقمية؛ فهي عملية توثيق دقيقة تظهر كيفية جمع الأدلة الرقمية، والهدف منها هو ضمان سلامة الأدلة وعدم التلاعب بها حتى تصل إلى المحكمة؛ فإذا لم يتم الحفاظ على هذه السلسلة أو إذا كانت غير موثقة بشكل صحيح؛ فإن الدليل الرقمي قد يفقد مصداقيته، وبالتالي قد ترفضه المحكمة.

الفرع التاسع

إشكاليات تدفق البيانات عبر الحدود

تعد إشكاليات تدفق البيانات عبر الحدود عائقا أمام التعاون الدولي، فعلى الرغم من أن هذه العملية تعد من أساسيات الاقتصاد الرقمي العالمي؛ إلا أن اختلاف القوانين، وسياسات الخصوصية، وتحديات أمن البيانات، والصعوبات التقنية للامتثال، قد يعرقل هذا الأمر ويؤثر على الملاحقة الجنائية.

48 - Arum Widiastuti and Yasmirah Mandasari Saragih, "Transnational Cyber Crime: Challenges of International Cooperation in Combating Cybercrime," International Journal of Contemporary Sciences, Vol. 3, No. 7, 2025, pp. 109-122: 116

49 - عبد الرزاق المرجان وآخرون، الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية، دار جامعة نايف للنشر، الرياض: د ط، 2024م، ص 12.

الفرع العاشر

الفجوة التقنية بين الدول

يعتمد نجاح التعاون الدولي في التصدي للجرائم والانتهاكات الرقمية على قدرة الدول على الملاحقة التقنية، ومعالجة طلبات الأدلة الرقمية بطريقة تضمن مقبوليتها أمام المحاكم، وهو ما يتطلب بنية تحتية تقنية متقدمة وفرقا مختصة ومدربة على التعامل مع هذا النوع من الجرائم.

فالكثير من الدول لا تمتلك بنية تحتية رقمية متقدمة؛ لأنها قد تعاني من نقص حاد في الموارد البشرية المؤهلة للتعامل مع التقنيات الحديثة ومكافحة الجرائم وحماية البيانات، وكذلك قد تعاني هذه الدول من نقص في الموارد التقنية، وكذلك نقص في القدرة المالية؛ مما ينعكس سلبا على قدرة هذه الدول على جمع الأدلة الرقمية، وتحليلها، وتقديمها للمحاكم؛ فضلا عن القدرة على مكافحة الاستباقية أو حتى اللاحقة للجريمة الرقمية، بل إن بعض هذه الدول قد لا يكون مؤهلا لحماية البيانات الشخصية في البيئة الرقمية.

وفي هذا السياق نرى ضرورة إنشاء صندوق إقليمي عربي تحت مظلة الجامعة العربية يختص بسد الفجوة التقنية بين الدول العربية الغنية والمتقدمة تقنيا من جهة، وبين الدول العربية الفقيرة والضعيفة تقنيا من جهة أخرى.

الفرع الحادي عشر

عدم وجود نموذج موحد للنشاط الرقمي الإجرامي ولمعايير التعامل

إن غياب نموذج موحد للنشاط الرقمي الإجرامي يعد من التحديات البارزة التي تعيق التعاون الدولي في مكافحة الجرائم الرقمية العابرة للحدود، ويتمثل هذا التحدي في افتقار

الدول إلى تعريفات ومعايير موحدة لما يعد نشاطا رقميا إجراميا، بالإضافة إلى تطور وتغير الأساليب الإجرامية الرقمية بوتيرة متسارعة.

الفرع الثاني عشر

تنوع اللغات والثقافات بين الدول

يتجلى هذا التحدي في صعوبة ترجمة القوانين والمصطلحات القانونية التقنية بشكل دقيق بين الدول؛ مما يؤدي إلى سوء الفهم أو تأخير تنفيذ طلبات المساعدة القانونية المتبادلة. كما أن الاختلافات الثقافية تؤثر على تفسير بعض الأفعال الرقمية، حيث قد ينظر إلى بعض السلوكيات على أنها طبيعية أو قانونية في دولة معينة، بينما تعتبر انتهاكا للخصوصية أو جريمة في دولة أخرى، مثل: تصوير النساء في المناسبات الخاصة، أو الصالونات النسائية قد يعتبر جريمة في الدول المحافظة، ولا ينظر إليه كذلك في الدول غير المحافظة.

علاوة على ذلك، ينعكس هذا التنوع في التواصل بين السلطات المعنية، حيث تواجه الدول التي تعتمد على لغات مختلفة صعوبات في صياغة طلبات المساعدة القانونية أو ترجمة الأدلة الرقمية؛ خاصة إذا كانت هذه الأدلة تحتوي على محتوى تقني أو قانوني معقد. كما يؤدي الاختلاف في القيم الثقافية إلى تباين الأولويات في حماية البيانات الشخصية؛ مما يعيق التواصل إلى فهم مشترك حول سبل التعامل مع الجرائم الرقمية والبيانات الشخصية. ويتضح من ذلك أن التحديات الدولية في حماية البيانات الشخصية من الجرائم والانتهاكات الرقمية تشكل عائقا كبيرا أمام تحقيق تعاون دولي فعال.

مما لا شك فيه أن هذه التحديات القانونية الوطنية أو الدولية تحتاج للكثير من الجهود القانونية والتقنية والتعاون الدولي للتصدي لها؛ مما ينعكس إيجابا على مواجهة التهديدات الرقمية للخصوصية والبيانات الشخصية والتعزيز من مستوى حمايتها.

الخاتمة

وفي الختام خلص البحث إلى مجموعة من النتائج التي تساهم في تسليط الضوء على ما يحمله موضوع الحماية الجنائية للبيانات الشخصية في ظل تزايد التهديدات الرقمية من استنتاجات مهمة، وصولاً إلى تقديم توصيات وحلول عملية يستفاد منها في مواجهة التحديات القانونية ومكافحة التهديدات الرقمية بفاعلية، وتأمين الحماية الجنائية اللازمة للبيانات الشخصية، الأمر الذي يساهم في تعزيز مسيرة الحضارة الإنسانية في العصر الرقمي.

أولاً: أهم النتائج

يمكن تلخيص أبرز النتائج التي توصل إليها البحث فيما يلي:

- 1 - يشكل الدستور القطري وقانون مكافحة الجرائم الإلكترونية وقانون حماية خصوصية البيانات الشخصية أساساً قانونياً لإضفاء الحماية على البيانات الشخصية في دولة قطر.
- 2 - القوانين الوطنية رغم أهميتها قد تكون غير كافية للتعامل مع الانتهاكات العابرة للحدود، وهو ما يجعل الأطر القانونية الإقليمية والدولية ركيزة أساسية لتعزيز حماية الخصوصية والبيانات الشخصية من جهة، ولمواكبة التقنيات الحديثة والتطورات الإجرامية من جهة أخرى.
- 3 - لا تزال العديد من الدول، ومنها دولة قطر، بحاجة إلى إطار قانوني وطني شامل ومتكامل وقوي ينظم استخدام التقنيات الحديثة، مثل: الذكاء الصناعي، وشبكة الأشياء أو إنترنت الأشياء (IoT)، ومعالجة البيانات الضخمة (Big Data)، الحوسبة السحابية، والأجهزة القابلة للارتداء، وتقنيات المدن الذكية.

- 4 - غياب إطار قانوني دولي موحد لحماية البيانات الشخصية ولتنظيم تدفقها عبر الحدود، وتحديات السيادة الوطنية وتنازع الاختصاص القضائي ورفض طلبات المساعدة، كل ذلك يعرقل التعاون بين الدول لمكافحة الجرائم والتهديدات الرقمية وحماية البيانات الشخصية.
- 5 - البنية التحتية وبما فيها من مراكز بيانات تعتبر مستودع للخصوصية وحافطة للبيانات الشخصية.

ثانياً: أهم التوصيات

بناء على النتائج التي تم التوصل إليها، يقدم البحث مجموعة من التوصيات التي يمكن الاستفادة منها في تعزيز الحماية الجنائية للبيانات الشخصية ومواجهة التحديات القانونية ومكافحة التهديدات الرقمية، وهي على النحو الآتي:

1 - التوصية باستكمال تطوير القوانين والإجراءات الرقمية القطرية؛ بما يواكب توقيع دولة قطر على اتفاقية الأمم المتحدة لمكافحة الجريمة الرقمية 2025م، بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، وبما يضمن مواءمة أحكامها مع القوانين الوطنية؛ لا سيما معايير التعامل مع البيانات الشخصية، وبما يراعي السيادة الوطنية واحترام دين الدولة والعادات والتقاليد، تعزيزاً للتعاون الدولي في مواجهة التهديدات الرقمية والتنسيق العابر للحدود.

2 - نتمنى على المشرع القطري مراجعة القوانين التقنية، أو القوانين واللوائح والمواد القانونية المتصلة بالفضاء الرقمي بشكل عام مرة كل خمس سنوات على الأقل، أو عند ظهور تقنية جديدة، وبشكل استباقي.

3 - بخصوص إثبات الركن المعنوي للجريمة الرقمية، نوصي باعتبار أن القصد الجنائي متوفر

في أي جريمة رقمية تستهدف أي بيانات شخصية ما دامت هذه البيانات محمية بنظام أو إجراءات حماية على غرار حماية الأسرار التجارية؛ فوجود نظام أو إجراء من شأنه أن يحمي البيانات الشخصية وقت وقوع الجريمة يدل على قرينة نية الجاني العمدية، وأنه تجاوز هذه الحماية، وذلك يتماشى مع المادة الثانية من اتفاقية بودابست، والتي أجازت للدول الأعضاء باعتبار خرق نظام الحماية جزءاً من الركن المادي للجريمة.

4 - التوصية بتبني سياسات عقابية رقمية جديدة، مثل: سلب الحرية الرقمية كنوع من العقوبات البديلة أو التبعية التي يمكن تطبيقها على مرتكب الجريمة الرقمية، بحيث لا يمكنه من الدخول إلى الشبكة العالمية، كما لا يمكنه الاستفادة من الخدمات الرقمية.

5 - نوصي بضرورة تعزيز حماية البنية التحتية الحيوية الحرجة بأن يشملها مبدأ الاختصاص العيني للقانون الجنائي، وذلك بأن تكون أي جريمة تمس أي قطاع من قطاعات البنية التحتية الحيوية الحرجة كمراكز البيانات من الجرائم التي تمتد إليها ولاية القانون الجنائي القطري، بغض النظر عن جنسية فاعلها أو مكانه، أو مكان وقوع الجريمة، وكذلك بغض النظر عن رأي الدولة التي ارتكبت الجريمة على إقليمها ولا عبءة لازدواجية التجريم، وذلك ما دامت تلك الجريمة تستهدف أحد القطاعات للبنية التحتية الحيوية الحرجة القطرية؛ سواء كان أحد أجزاء هذا القطاع داخل الدولة أم خارجها، فالمساس بالبنية التحتية الحيوية الحرجة هو مساس بالمصالح العليا للبلاد.

قائمة المصادر والمراجع

أولاً: المراجع باللغة العربية:

1 - الكتب

- 1 - تاج الدين عبد الوهاب بن علي بن عبد الكافي السبكي (المتوفى ٧٧١ هـ)، الأشباه والنظائر، تحقيق: عادل أحمد عبد الموجود وعلي محمد معوض، ط1، دار الكتب العلمية، بيروت، 1411 هـ/1991 م.
- 2 - عبد الرزاق المرجان وآخرون، الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية، دار جامعة نايف للنشر، د ط، 2024 م.
- 3 - علي حسين الخلف وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، د ط، 1982 م.

2 - الدوريات والمجلات العلمية

- 1 - أحمد محمد عبد الغفار، «مبدأ السيادة الرقمية الفردية على البيانات»، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون، ع43، أكتوبر 2023 م، 767-862.
- 2 - أيمن سيد محمد مصطفى العسقلاني، «دور مجلس التعاون الخليجي القانوني والتعاوني في مكافحة الجرائم الإلكترونية: دراسة تحليلية واستراتيجية مقترحة»، مجلة الدراسات الدولية، معهد الأمير سعود الفيصل للدراسات الدبلوماسية، ع32، شعبان 1443 هـ/ 2022 م، 107-155.
- 3 - سامي جاد واصل، «التعاون الدولي في مكافحة الجريمة الإلكترونية»، مجلة القانون والتكنولوجيا، كلية القانون بالجامعة البريطانية في مصر، مج3، ع1، أبريل 2023 م، 13-99.
- 4 - سلطان بن عبد الرحمن بن عبد القادر العبيدان، «التأصيل الفقهي لنظام حماية البيانات الشخصية السعودي»، مجلة أبحاث، اليمن: كلية التربية بجامعة الحديدة، مج11، ع2، يونيو 2024 م، 460-541.
- 5 - طارق جمعة السيد راشد، «الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والمقارن»، المجلة القانونية والقضائية، دولة قطر: وزارة العدل - مركز الدراسات القانونية والقضائية، مج11، ع2، 2017 م، 75-138.
- 6 - طارق جمعة السيد راشد، «الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي دراسة مقارنة»، مجلة القانون والاقتصاد، جامعة القاهرة، كلية الحقوق، مج92، ع3، أغسطس 2019 م، 190-314.
- 7 - عبد الكريم صالح عبد الكريم وأند صلاح الدين تمر، «الحق في النسيان الرقمي والمسؤولية التقصيرية الناجمة عن انتهاكه - دراسة تحليلية مقارنة»، مجلة الحقوق، جامعة الكويت، مج48، ع3، سبتمبر 2024 م، 367-412.

8 - ياسر أحمد بدر محمد، «الإطار النظامي لحماية حق الأفراد في مواجهة مخاطر معالجة بياناتهم ذات الطابع الشخصي: دراسة مقارنة بين نظام حماية البيانات الشخصية السعودي واللائحة العامة الأوروبية لحماية البيانات»، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، مركز الدراسات والبحوث، مج31، ع83، يوليو 2022م، 69-128.

3 - الأطروحات العلمية

1 - عمر محمد منيب إدلبي، المسؤولية الجنائية الناتجة عن أعمال الذكاء الاصطناعي، رسالة ماجستير، كلية القانون، جامعة قطر، يناير 2023م.

ثانياً: المراجع باللغة الأجنبية

- 1 - Arum Widiastuti and Yasmirah Mandasari Saragih, "Transnational Cyber Crime: Challenges of International Cooperation in Combating Cybercrime," International Journal of Contemporary Sciences, Vol. 3, No. 7, 2025, pp. 109-122
- 2 - Davit Marikyan, Savvas Papagiannidis, Omer F. Rana, and Rajiv Ranjan, "General Data Protection Regulation: A Study on Attitude and Emotional Empowerment," Behaviour & Information Technology, Taylor & Francis, Vol. 43, No. 14, 2024, pp. 3561-3577
- 3 - Samuel D. Warren; Louis D. Brandeis 'The Right to Privacy' Harvard Law Review, Vol. 4, No. 5. (December 15, 1890), pp. 193-220

ثالثاً: المراجع الرقمية (الإنترنت)

1 - الأمم المتحدة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، سلسلة الوحدات الجامعية: الجرائم الإلكترونية، الوحدة التعليمية 7: التعاون الدولي على مكافحة الجريمة الإلكترونية، متوفر على الرابط:

Cybercrime Module 7 Key Issues

تاريخ الاطلاع: 09/02/2025م.

2 - جامعة لوسيل في دولة قطر نظمت مؤتمر خاص بالذكاء الصناعي وهو (مؤتمر القانون والذكاء الاصطناعي) وذلك في يوم الأربعاء 13 سبتمبر 2023م، وهو أول مؤتمر دولي تنظمه الجامعة عن القانون والذكاء الاصطناعي، والذي يتزامن مع الاحتفال باليوم العالمي للقانون، انظر: موقع جامعة لوسيل متوفر على الرابط:
مؤتمر القانون والذكاء الاصطناعي - جامعة لوسيل - تاريخ الاطلاع 07/02/2025م.

3 - الموقع الرسمي لمكتب الاتصال الحكومي في دولة قطر متوفر على الرابط:

شركة سناب تعتزم افتتاح مكتب في قطر وتوقع مذكرة تفاهم مع مكتب الاتصال الحكومي، وقعت شركة سناب شات (Snap Inc) مذكرة تفاهم مع مكتب الاتصال الحكومي في قطر لافتتاح مكتب في الدوحة. تاريخ الاطلاع: 08/02/2025م.

4 - الموقع الرقمي الرسمي لوكالة الانباء القطرية (قنا)، خبر بعنوان: اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية.. خطوة محورية نحو التصدي للتهديدات الرقمية، تاريخ 13 نوفمبر 2025م، على الرابط التالي:

<https://tinyurl.com/ye26ye2s>

5 - الموقع الرقمي لمركز قطر للتطور المهني، استراتيجية قطر الوطنية في مجال الذكاء الاصطناعي، متوفر على الرابط: ثورة الذكاء الاصطناعي: قطر على المسار الصحيح | QCDC تاريخ الاطلاع 07/02/2025م.

6 - موقع منظمة التعاون الاقتصادي والتنمية، توصية المجلس بشأن الذكاء الاصطناعي، متوفر على الرابط: الصكوك القانونية لمنظمة التعاون والتنمية في الميدان الاقتصادي تاريخ الاطلاع 08/02/2025م.

7 - ميثاق تطوير واستخدام الذكاء الاصطناعي في دولة الإمارات، متوفر على الرابط: تشريعات الإمارات العربية المتحدة - تاريخ الاطلاع 07/02/2025م.

رابعاً: القوانين والاتفاقيات والأحكام القضائية

1 - القوانين الوطنية

1 - الدستور الدائم 2004، دولة قطر.

2 - قانون تكنولوجيا المعلومات والملفات والحريات المدنية الفرنسي رقم 78-17 لسنة 1978م المؤرخ في 6 يناير 1978م والمعدل بالقانون رقم 801 لسنة 2004م، والمعدل بالقانون رقم 1125 لسنة 2018م، الجمهورية الفرنسية.

3 - قانون رقم 11 لسنة 2004 بإصدار قانون العقوبات، دولة قطر.

4 - قانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، دولة قطر.

5 - قانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، وتعديلاته انتهاء بالتعديل رقم 11 لسنة 2025م، دولة قطر.

6 - قانون رقم 17 لسنة 2025 بشأن البصمة الحيوية، دولة قطر.

- 7 - قانون رقم 2 لسنة 2011 بشأن الإحصاءات الرسمية، دولة قطر.
- 8 - قانون رقم 23 لسنة 2004 بإصدار قانون الإجراءات الجنائية، دولة قطر.
- 9 - قانون رقم 27 لسنة 2019 بإصدار قانون مكافحة الإرهاب، دولة قطر.
- 10 - قانون رقم 9 لسنة 2013 بشأن البصمة الوراثية، دولة قطر.
- 11 - قرار مجلس الوزراء رقم 10 لسنة 2021 بإنشاء لجنة الذكاء الاصطناعي، دولة قطر.
- 12 - مرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، دولة الإمارات العربية المتحدة.
- 13 - مرسوم رقم 40 لسنة 2018 بالموافقة على انضمام دولة قطر إلى العهد الدولي الخاص بالحقوق المدنية والسياسية، دولة قطر.

2 - الاتفاقيات والإعلانات الدولية

- 1 - الاتحاد الأوروبي، البرلمان الأوروبي والمفوضية الأوروبية، اللائحة العامة لحماية البيانات (GDPR)، قانون رقم 679 / 2016م والذي تم اعتماده بتاريخ 27 أبريل 2016م، وإلغاء القانون 95 / 46.EC.
- 2 - اتفاقية الاتحاد الأفريقي رقم XXV / 846 (EX.CL) بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، التي تم اعتمادها في مدينة مالابو عاصمة جمهورية غينيا الاستوائية، في الدورة العادية الثالثة والعشرين لقمة رؤساء دول وحكومات الاتحاد الأفريقي، بتاريخ 27 يونيو 2014م.
- 3 - الاتفاقية الأمريكية لحقوق الإنسان المعروفة باسم ميثاق سان خوسيه 1969م.
- 4 - الاتفاقية الأوروبية لحقوق الإنسان 1950م.
- 5 - الإعلان العالمي لحقوق الإنسان 1948م.
- 6 - إعلان القاهرة حول حقوق الإنسان في الإسلام، القاهرة 1990م.
- 7 - جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010م.
- 8 - الجمعية العامة للأمم المتحدة، الدورة التاسعة والسبعون، البند 108 من جدول الأعمال، قرار رقم 243/79، اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية. تاريخ 24 ديسمبر 2024م.
- 9 - العهد الدولي الخاص بالحقوق المدنية والسياسية 1966م.
- 10 - مجلس أوروبا، اللجنة الوزارية، مجموعة المعاهدات الأوروبية رقم 185، الاتفاقية المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست)، تم التوقيع على هذه الاتفاقية في العاصمة المجرية بودابست بتاريخ 8 نوفمبر 2001م.
- 11 - الميثاق العربي لحقوق الإنسان، تونس 2004م.

3 - الأحكام القضائية

- 1 - جمهورية مصر العربية، حكم المحكمة الدستورية العليا، قضية رقم 56 لسنة 18 القضائية، الجلسة العلنية المنعقدة في تاريخ 15 رجب 1418 هـ الموافق 15 نوفمبر 1997م، الجريدة الرسمية العدد 48 في 27 نوفمبر 1997 صفحة 2925.
- 2 - جمهورية مصر العربية، محكمة النقض، الدائرة الجنائية، الطعن رقم 22830 لسنة 88 القضائية، جلسة السبت الموافق 11 من سبتمبر سنة 2021م، برئاسة المستشار: أحمد الخولي نائب رئيس المحكمة.