HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

التحديات التي تواجه القانون الدولي في مجال حماية البيانات الشخصية

وليد فرمان عبود[1]، أ.د. موسى إبراهيم[2]

[1] باحث، الجامعة الإسلامية في لبنان. لبنان.

[2] تدريسي بالجامعة الإسلامية في لبنان.

HNSJ, 2026, 7(1); https://doi.org/10.53796/hnsj71/71

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/71/71

تاريخ الاستقبال: 2025/12/10م تاريخ القبول: 2025/12/17م تاريخ النشر: 2026/01/01م

المستخلص

يتناول هذا البحث التحديات التي تواجه القانون الدولي في مجال حماية البيانات الشخصية في ظل التحول الرقمي المتسارع والطبيعة العابرة للحدود لتدفقات البيانات. ويُبرز البحث أن الإطار القانوني الدولي الراهن يعاني من التجزئة وغياب تعريف وتشريع دوليين موحدين وملزمين للبيانات الشخصية، بما ينعكس على تباين مستويات الحماية بين الدول واتساع الفجوات التنظيمية التي تستغلها الجهات الفاعلة العابرة للحدود. كما يوضح أن التطور التقني—وخاصة الذكاء الاصطناعي وتحليل البيانات الضخمة والحوسبة السحابية وإنترنت الأشياء—فاقم المخاطر المرتبطة بجمع البيانات ومعالجتها ونقلها، وعمّق الفجوة بين الواقع العملي وقدرة القواعد الدولية التقليدية على المواكبة. ويركز البحث كذلك على التحديات القانونية والمؤسساتية، وفي مقدمتها ضعف المواءمة بين التشريعات الوطنية والمعايير الدولية، وتعقيدات التعاون القضائي وتبادل الأدلة الرقمية عبر الحدود، فضلًا عن قصور آليات الإنفاذ والرقابة الدولية وغياب سلطة إلزامية فعّالة لمساءلة الدول والفاعلين من غير الدول، ولا سيما الشركات الرقمية الكبرى. ويخلص البحث إلى ضرورة تعزيز التعاون الدولي وبناء قدرات الدول النامية، والعمل نحو اتفاقية دولية شاملة وملزمة تتضمن معايير موحدة وآليات تنفيذ ورقابة مرنة وقابلة للتحديث، بما يحقق توازناً بين متطلبات الابتكار الرقمي وصون الحق في الخصوصية وحماية البيانات.

الكلمات المفتاحية: حماية البيانات الشخصية؛ القانون الدولي؛ الخصوصية الرقمية؛ الأمن السيبراني؛ الذكاء الاصطناعي؛ إنفاذ القواعد.

RESEARCH TITLE

Challenges Facing International Law in the Field of Personal Data Protection

Walid Farman Aboud[1], Prof. Dr. Musa Ibrahim[2]

[1] Researcher, Islamic University of Lebanon, Lebanon.
[2] Lecturer at the Islamic University of Lebanon.

HNSJ, 2026, 7(1); https://doi.org/10.53796/hnsj71/71
Arabic Scientific Research Identifier: https://arsri.org/10000/71/71

Received at 10/12/2025 Accepted at 17/12/2025 Published at 01/01/2026

Abstract

This study examines the challenges facing international law in protecting personal data amid rapid digital transformation and the cross-border nature of data flows. It highlights that the current international legal framework remains fragmented and lacks a unified, binding definition and comprehensive global regulation of personal data, resulting in uneven levels of protection and widening regulatory gaps that can be exploited by cross-border actors. The study also shows that fast-paced technological developments—particularly artificial intelligence, big data analytics, cloud computing, and the Internet of Things—have intensified risks related to data collection, processing, and transfer, thereby widening the gap between practical realities and the capacity of traditional international legal rules to keep pace. In addition, the study addresses legal and institutional challenges, most notably the lack of harmonization between national laws and international standards, the complexities of cross-border judicial cooperation and digital evidence sharing, and the shortcomings of international enforcement and oversight mechanisms. This is further compounded by the absence of an effective, binding accountability system for both states and non-state actors, especially major digital companies. The study concludes by emphasizing the need to strengthen international cooperation, build capacity in developing countries, and work toward a comprehensive and binding international agreement that establishes unified standards and flexible, updatable enforcement and monitoring mechanisms—balancing digital innovation with the protection of privacy and personal data.

Key Words: Personal data protection; International law; Digital privacy; Cybersecurity; Artificial intelligence; Enforcement mechanisms.

المقدمة

أصبحت البيانات الشخصية في العصر الرقمي مورداً استراتيجيا لا يقل أهمية عن الموارد الاقتصادية التقليدية لما تمثله من قيمة معلوماتية هائلة في مجالات الإدارة والاقتصاد والأمن والتكنولوجيا، ومع التوسع غير المسبوق في استخدام الإنترنت، ومنصات التواصل الاجتماعي، والتقنيات الحديثة كالذكاء الاصطناعي والحوسبة السحابية، باتت البيانات الشخصية عرضة لجملة متزايدة من المخاطر، سواء من حيث الجمع غير المشروع، أو المعالجة غير المشروعة، أو الاستغلال التجاري والسياسي غير المنضبط.

وفي هذا السياق، يواجه القانون الدولي تحدياً حقيقياً في توفير حماية فعالة للبيانات الشخصية، لاسيما في ظل الطبيعة العابرة للحدود لتدفقات البيانات، وتباين النظم القانونية الوطنية واختلاف مستوى الالتزام الدولي بمعايير الخصوصية، فبينما تسعى بعض الدول إلى تكريس حماية صارمة للبيانات، تتبنى دول أخرى مقاربات أقل تشدداً، الأمر الذي يفرز فجوة تنظيمية تضعف من فاعلية الحماية الدولية.

كما أن التطور التقني المتسارع يفوق في كثير من الأحيان قدرة القواعد القانونية الدولية على المواكبة، مما يخلق حالة من عدم التوازن بين الابتكار التكنولوجي ومتطلبات حماية الحقوق الأساسية للأفراد وعلى رأسها الحق في الخصوصية وحماية البيانات، ومن هنا تبرز أهمية دراسة التحديات التي تواجه القانون الدولي في هذا المجال، وتحليل أبعادها القانونية والتنظيمية، وصولاً إلى استجلاء مدى قدرة النظام القانوني الدولي على الاستجابة لهذه التحولات.

أولاً_ أهمية الدراسة

تنبع أهمية هذا الموضوع من كونه يتصل اتصالًا مباشرًا بحماية أحد الحقوق الأساسية للإنسان، وهو الحق في الخصوصية، الذي يشكل ركيزة جوهرية من ركائز الكرامة الإنسانية في المجتمعات المعاصرة. كما تتجلى أهميته في كونه يعالج إشكالية قانونية دولية حديثة ومتجددة، تتقاطع فيها اعتبارات السيادة الوطنية مع متطلبات التعاون الدولي.

وتزداد أهمية البحث بالنظر إلى تصاعد الانتهاكات المرتبطة بالبيانات الشخصية، سواء من قبل شركات عابرة للحدود أو جهات حكومية، في ظل ضعف آليات الرقابة والمساءلة الدولية. كما يكتسب الموضوع بعدًا عمليًا، لارتباطه الوثيق بالتجارة الإلكترونية، والاقتصاد الرقمي، والأمن السيبراني، الأمر الذي يجعل من حماية البيانات مسألة تتجاوز الإطار القانوني البحت إلى أبعاد اقتصادية وسياسية وأمنية.

ثانياً_ أهداف الدراسة

يهدف هذا البحث إلى تحقيق جملة من الأهداف العلمية، من أبرزها:

1. بيان الإطار المفاهيمي والقانوني لحماية البيانات الشخصية في القانون الدولي.
2. تحليل أبرز التحديات القانونية والتقنية التي تواجه حماية البيانات على المستوى الدولي.
3. إبراز أوجه القصور في القواعد والاتفاقيات الدولية القائمة ذات الصلة بحماية البيانات.
4. تقييم مدى فاعلية التعاون الدولي في مجال حماية البيانات الشخصية.

ثالثاً_ اشكالية الدراسة

تتمحور إشكالية البحث حول مدى قدرة القانون الدولي، بصوره التقليدية والحديثة على توفير حماية فعّالة وشاملة للبيانات الشخصية في بيئة رقمية عابرة للحدود، في ظل غياب إطار دولي موحد وملزم وتباين التشريعات الوطنية، وتفاوت مستويات التطور التكنولوجي بين الدول.

ويتفرع عن هذه الإشكالية تساؤل جوهري مفاده: هل يشكل النظام القانوني الدولي القائم أداة كافية لمواجهة التحديات التقنية والتنظيمية المرتبطة بحماية البيانات، أم أن هذا النظام لا يزال قاصرا عن مواكبة التحولات الرقمية المتسارعة؟

رابعاً_ منهج الدراسة

يعتمد البحث على المنهج التحليلي من خلال تحليل النصوص والاتفاقيات الدولية ذات الصلة بحماية البيانات، وبيان مضمونها وحدود فاعليتهان كما يوظف المنهج الوصفي لعرض واقع حماية البيانات في البيئة الرقمية، ورصد أبرز التحديات العملية التي تواجه القانون الدولي في هذا المجال

ويُستعان كذلك بالمنهج المقارن عند الاقتضاء، من خلال مقارنة بعض التجارب الدولية والإقليمية في تنظيم حماية البيانات، بهدف استخلاص النتائج وتحديد أفضل الممارسات التي يمكن أن تسهم في تعزيز الإطار القانوني الدولي.

خامساً_ خطة الدراسة

المطلب الأول: التحديات التقنية والهيكلية لحماية البيانات.

الفرع الأول: ضعف البنية أمام التطور التكنولوجي السريع.

الفرع الثاني: غياب التكييف القانوني والتشريعي الموحد للبيانات الشخصية في الاتفاقيات الدولية.

المطلب الثاني: التحديات القانونية والمؤسساتية لحماية البيانات.

الفرع الأول غياب المواءمة بين التشريعات الوطنية والمعايير الدولية.

الفرع الثاني قصور آليات الإنفاذ الدولية.

المطلب الأول

التحديات التقنية والهيكلية لحماية البيانات

تواجه حماية البيانات الشخصية في العصر الرقمي جملة من التحديات التقنية والهيكلية التي تعقد جهود الدول والمنظمات في تأمين الخصوصية الرقمية، فالتطور التكنولوجي المتسارع، وتعدد أدوات المعالجة والتخزين، وانتشار الذكاء الاصطناعي، قد جعل من البيانات هدفاً ثميناً يسهل اختراقه أو إساءة استخدامه، كما أن غياب بنى تحتية رقمية متكاملة، وتفاوت مستويات الأمن السيبراني بين الدول يزيد من هشاشة منظومات الحماية القائمة، ومن هنا يطرح هذا المطلب لبحث أبرز التحديات التقنية التي تواجه حماية البيانات إلى جانب الإشكاليات الهيكلية التي تحد من فعالية الأطر القانونية والمؤسسية في التصدي للانتهاكات الرقمية. **بناء على ذلك سوف نقوم بتقسيم المطلب إلى فرعين، سوف نتحدث في الفرع الأول عن ضعف البنية أمام التطور التكنولوجي السريع، أما في الفرع الثاني سوف نتحدث عن غياب التكييف القانوني والتشريعي الموحد للبيانات الشخصية في الاتفاقيات الدولية.**

الفرع الأول

ضعف البنية التقنية أمام التطور التكنولوجي السريع

يعد التطور التكنولوجي المتسارع أحد أبرز السمات المميزة للعصر الرقمي، إذ بات يشكل محوراً رئيسياً في حياة الأفراد والدول على حد سواء غير أن هذا التطور على الرغم مما يحمله من فرص للنمو والابتكار قد خلق تحديات قانونية هائلة

تتعلق بحماية البيانات الشخصية، وبخاصة في ظل ضعف الإطار القانوني الدولي القادر على مواكبة هذا التغير التقني الهائل، فالفضاء السيبراني يتطور بسرعة تفوق قدرة الأنظمة القانونية التقليدية على التكيف معه ما أوجد فجوة زمنية وتشريعية بين الواقع التقني والمقتضيات القانونية، وأضعف فعالية الحماية الدولية للبيانات الشخصية[1]، وعليه يمكننا بيان أبرز أسباب ضعف البنية التقنية وانتشار الاعتداء على البيانات بوجه خاص وعلى النحو الآتي:

أولاً_ تمويل أفعال الاعتداء السيبراني

إن الباعث على ارتكاب أغلب الجرائم يكون مالياً محضاً بالدرجة الأساس، لذلك تتطلب عملية مكافحة الاعتداء على الأمن السيبراني بشكل خاص منع المنظمات الاجرامية من امتلاك الوسائل اللازمة لتنفيذ عملياتها، وكذلك منعها من الحصول على مكان آمن لتنظيم عناصرها والتخطيط لعملياتها واتخاذ إجراءات إدارية وقانونية لمنعها من الحصول على التمويل اللازم، علاوة على عدم تمكنها من امتلاك الوسائل والأدوات والأسلحة التي تستخدمها في عملياتها ضد المدنيين الأمنين والمؤسسات الوطنية ويحصل المجرمون على الدعم المالي بطرائق مختلفة سواءً بطريقة مباشرة أو غير مباشر عن طريق منظمات ذات أهداف خيرية أو اجتماعية أو ثقافية أو تدعي ذلك أو عن طريق العمل في انشطة غير مشروعة، كالإتجار بالمخدرات أو السلاح أو ابتزاز الأموال[2].

في الحقيقة أن أسباب انتشار الاعتداء على الأمن السيبراني في العالم كثيرة ومتعددة، إلا أن العامل الرئيس الذي يقف وراء ارتكاب هذه الجرائم ويسهم في تجنيد الإرهابين وكذلك في عمليات شراء وتوزيع الأسلحة التي تستعمل في الجرائم الإرهابية وإيواء الإرهابين فإن كل ذلك يستند إلى عملية التمويل الذي تحصل عليه الجماعات الاجرامية، ولاسيما وان المنظمات الإرهابية اصبحت تدرك أن تكنولوجيا المعلومات والاتصالات تستطيع أن تؤدى دوراً في التمويل والتجنيد وتعكف الكثير من هذه المنظمات على توسيع نطاق الاستفادة القصوى من هذه التكنولوجيا الأمر الذي يؤكد أن القضاء على التمويل وحرمان الجماعات الاجرامية من الحصول عليه، يؤدي في نهاية المطاف إلى القضاء على الجرائم السيبرانية أو في أقل تقدير الحد منها بشكل كبير جداً، إذ إن ذلك قد دفع الكثير من الدول التي تحارب هذه الاعتداءات باتخاذ قرارات بشأن تجفيف منابع تمويله، وإذا كان هذا الأمر سهلاً لتجفيف منابع الاعتداء على الأمن السيبراني الظاهرة، إلا إن الأمر يبدو صعباً بالنسبة لتمويل الجريمة السيبرانية عن طريق مصادر التمويل غير الظاهرة، إذ أن التمويل يتم بواسطة غسيل الأموال القذرة بشكل مصدراً خفياً للتمويل لتلك الجرائم.

ثانياً_ ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق

التطور التكنولوجي ذاته يفرز باستمرار أدوات وأساليب جديدة لمعالجة البيانات تفوق ما يمكن أن تتنبأ به التشريعات القائمة، فظهور تقنيات الذكاء الاصطناعي، والتعلم الآلي، وإنترنت الأشياء، والتعرف البيومتري، أدى إلى بروز أنواع جديدة من المخاطر على الخصوصية الفردية، مثل التتبع الذكي والمراقبة المستمرة وتحليل السلوك البشري عبر البيانات الضخمة، هذه الظواهر التقنية جعلت النصوص القانونية التقليدية التي صيغت في عصر مختلف عاجزة عن مواجهة التحديات المستحدثة أو تنظيمها تنظيماً فعالاً، إذ غالباً ما تركز القوانين على جمع البيانات ومعالجتها من قبل جهات محددة في حين أن التقنيات الحديثة تجعل عملية جمع البيانات عملية لامركزية ومتداخلة الأطراف بشكل معقد، وإن شبكة المعلومات مصممة في الأصل بشكل مفتوح من دون قيود أو حواجز أمنية عليها رغبة في التوسع وتسهيل دخول

[1] أسماء الحسين، أسباب الإرهاب والعنف والتطرف، دون دار نشر، الرياض، 2014، ص64.

[2] أمير فرج يوسف، جريمة مكافحة الإرهاب الالكتروني، دار الكتب والدراسات العربية، مصر، 2016، ص285.

المستخدمين وتحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على شفرات معلوماتية ويمكن للمنظمات الإجرامية استغلال هذه الثغرات في التسلل إلى البنى المعلوماتية التحتية وممارسة العمليات التخريبية[3].

ثالثاً_ غياب الحدود الجغرافية وتدني مستوى المخاطرة:

إن السمة العالمية لشبكات المعلوماتية فضلاً عن عدم وضوح الهوية الرقمية للمستخدم وأنها مفتوحة وتعد فرصة مناسبة للمجرمين السيبرانيين، حيث يستطيع محترف الحاسوب أن يقدم نفسه بالهوية والصفة التي يرغب بها أو يتخفى تحت شخصية وهمية، ويطلق على نفسه ألقاباً أو أسماء مستعارة ويؤيدها بأدلة ملموسة كالصور أو بعض المعلومات الصحيحة ليثبت جديته، ومن ثم يشن هجومه الإلكتروني وهو في منزله من دون مخاطرة مباشرة وبعيداً عن أعين الناظرين[4]، وتأسيساً على ما تقدم نستطيع القول إن غياب الحدود المكانية في الشبكة المعلوماتية وعدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته غير المقفلة والمفتوحة كل هذا يشكل فرصة كبيرة ومناسبة للمجرمين لتحقيق مأربهم.

رابعاً_ سهولة الاستخدام وقلة التكاليف

إن السمة العالمية لشبكات المعلومات تتمثل في كونها وسيلة سهلة الاستعمال طيعة للانقياد قليلة الكلفة لا تستغرق وقتاً وجهداً كبيراً، مما هيا لمرتكبي الاعتداء على الأمن السيبراني فهي فرصة ثمينة للوصول إلى أهدافهم غير المشروعة ومن دون الحاجة إلى مصادر تمويل ضخمة فالقيام بشن اعتداء سيبراني لايتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة[5].

خامساً_ صعوبة اكتشاف وإثبات الاعتداء على الأمن السيبراني

في كثير من أنواع الجرائم المعلوماتية لايعلم بوقوع الجريمة أصلاً ولاسيما في مجال جرائم الاختراق، وهذا يساعد مرتكبها على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته، كما أن صعوبة الإثبات تعد من اقوى الدوافع المساعدة على ارتكاب الاعتداء على الأمن السيبراني، لأنها تعطي المجرم أملاً في الإفلات من العقوبة[6].

سادساً_ الفراغ التنظيمي والقانوني وغياب جهة السيطرة والمراقبة على الشبكات المعلوماتية:

كما إن التفاوت الكبير بين الدول في القدرات التقنية والتنظيمية يعمق من هذا الضعف البنيوي فبينما تمتلك الدول المتقدمة أطر حماية قوية مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، تعاني غالبية الدول النامية من غياب تشريعات متخصصة، أو من ضعف في تطبيقها الفعلي بسبب نقص الكوادر الفنية والقضائية القادرة على فهم القضايا التقنية المعقدة وهذا التباين يخلق بيئة غير متكافئة تتيح للشركات العابرة للحدود أن تستغل الثغرات القانونية في بعض الدول لنقل البيانات إلى مناطق ذات حماية ضعيفة، بما يعرف بظاهرة "الملاذات الرقمية"، الأمر الذي يقوض فعالية أي جهود دولية لتحقيق حماية متجانسة.

سابعاً: أسباب أخرى تمثلت بالاتي:

1- غياب دور البيت والمدرسة في الرقابة على عموم أفراد العائلة ما يفسح المجال أمامهم في استعمال هذه التكنولوجيا استعمالاً خاطئاً، أو تمادي الطالب في استعمال التقنية استخداماً سيئاً.

---

[3] عفيفي كامل عفيفي، بدائل الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار الثقافة، عمان، 1999، ص83.

[4] علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، بيروت، 2011، ص72.

[5] مرعي علي الرميحي، الحرب السيبرانية ومتطلبات الأمن القومي الجديدة، هاتريك للنشر والتوزيع، اربيل، 2025، ص 30.

[6] علي عدنان الفيل، الإجرام الالكتروني، مرجع سابق، ص73.

2 – الغلو والتشدد في بعض أمور الدين فالبعض ومن الشباب الذين يستعملون الشبكة العالمية للمعلومات من الشباب يرون أنهم أعلم من غيرهم وإن بعض العلماء على ضلالة، ما يتطلب محاربة آرائهم تقنياً[7].

3 – الفراغ الذي يشكل سبباً رئيساً يدفع الشباب للجوء إلى استعمال هذه التكنولوجيا، ما يجعله عرضة للوقوع في مصائد الجماعات الإجرامية بسبب مواقع التواصل الاجتماعي.

الفرع الثاني

غياب التكييف القانوني والتشريعي الموحد للبيانات الشخصية

لابد من الإقرار بأن النقاش حول التكييف القانوني والتشريعي للبيانات الشخصية على مستوى الاتفاقيات الدولية يعكس صراعاً بين رؤى قانونية وفلسفات سيادية واقتصادية متباينة، وهو في جوهره صراع بين سرعة تحول الواقع التقني وبطء تراكم الإرادة القانونية الدولية، وإن غياب تكييف موحد لايقتصر على فروق تعريفية مجردة بل يمتد إلى أطر القيم والمبادئ التي تنطلق منها الأنظمة القانونية: هل تعامل البيانات كامتداد للخصوصية والكرامة الإنسانية أم كمورد اقتصادي يخضع لمنطق السوق؟ هل تعتبرها الدولة عنصراً من عناصر سيادتها التي يجب حمايتها أو عائداً تجارياً قابلاً للتداول؟ هذه الخلافات الجوهرية تنتج عنها نتائج عملية حاسمة على مستوى صياغة النصوص، وتحديد الاختصاصات، ووضع آليات إنفاذ فعالة، كما تؤثر على قدرة الأفراد على نيل الحماية الواجبة لحقوقهم الرقمية، في ضوء ذلك يكتسب هذا الفرع أهمية مزدوجة: فهو لايهدف فقط إلى رصد الفجوات المعيارية بل إلى تحليل الجذور الفكرية والسياسية لتلك الفجوات وتبيان انعكاسها العملي على الاتفاقيات الدولية وفاعلية تطبيقها.

أولاً_ غياب التكييف القانوني الموحد للبيانات الشخصية

يعد غياب التكييف القانوني الموحد للبيانات الشخصية أحد أبرز مظاهر الاضطراب المعياري في النظام القانوني الدولي، وأحد أهم العوامل التي تضعف فعالية الحماية المقررة لهذا الحق في مواجهة التهديدات السيبرانية المتزايدة، فبينما باتت البيانات الشخصية تمثل جوهر الوجود الرقمي للفرد في العصر الحديث، لا يزال المجتمع الدولي يفتقر إلى تعريف جامع وملزم يحدد طبيعتها القانونية، وما إذا كانت تعد حقاً من حقوق الإنسان أم مصلحة اقتصادية أم موردًا سيادياً، هذا الغموض المفاهيمي أفرز تبايناً واسعاً في التوجهات الدولية، وأدى إلى تضارب التشريعات الوطنية والإقليمية، وإلى هشاشة البنية القانونية التي يفترض أن تحمي الخصوصية الرقمية على المستوى العالمي[8].

وقد أدى هذا الاختلاف في المنطلقات إلى تباين كبير في التكييف القانوني للبيانات عبر الاتفاقيات الدولية والإقليمية، فالاتحاد الأوروبي على سبيل المثال من خلال لائحته العامة لحماية البيانات (GDPR) يعامل البيانات الشخصية باعتبارها حقاً أساسياً غير قابل للتصرف يقتضي موافقة صريحة من الفرد على معالجتها، ويضع قيوداً صارمة على نقلها إلى دول لاتوفر حماية كافية، في المقابل تتبنى الولايات المتحدة نهجاً قطاعياً يعتمد على تنظيم خصوصية البيانات في مجالات محددة (كالصحة أو الاتصالات أو الخدمات المالية)، دون وجود تشريع شامل أو مبدأ عام لحماية البيانات، وهو ما يعكس اختلاف التكييف القانوني من حق إنساني إلى مصلحة تنظيمية[9].

أما على المستوى الدولي فإن معظم الاتفاقيات المتعددة الأطراف لم تدرج مفهوماً موحداً للبيانات الشخصية، فعلى سبيل

---

[7] بهاء عدنان السعبري، أليات ومسارات التمدد الجيو– استراتيجي للإرهاب العابر للحدود، مجلة السياسة الدولة، العدد214، مؤسسة الاهرام، القاهرة، 2018، ص 46.

[8] لبنى خميس مهدي وتغريد صفاء، اثر السيبرانية في تطور القوة، مجلة حمورابي، العدد 34، مركز حمورابي للبحوث والدراسات الاستراتيجية، بغداد، 2020، ص150.

[9] أحمد علو، الحروب السيبرانية والعنف الرقمي واقع عالمي جديد، مجلة الجيش، العدد402، قيادة الجيش اللبناني، بيروت، 2018، ص185–186.

المثال لم تتضمن اتفاقية بودابست لمكافحة الجريمة السيبرانية لعام 2001 تعريفاً واضحاً للبيانات الشخصية أو لحدود حمايتها بل ركزت على تجريم الأفعال السيبرانية كاختراق النظم أو إساءة استخدام الأجهزة، مما جعلها غير كافية لتأسيس التزامات إيجابية بحماية الخصوصية الرقمية، كذلك لم تتضمن اتفاقيات منظمة التجارة العالمية المتعلقة بالتجارة الإلكترونية إطاراً واضحاً لحماية البيانات، بل تركت الأمر لاتفاقات لاحقة أو لمبادئ توجيهية طوعية صادرة عن منظمة التعاون الاقتصادي والتنمية (OECD) وهي مبادئ غير ملزمة من الناحية القانونية[10].

ويضاف إلى ذلك أن التكييف القانوني للبيانات يتأثر بتباين فلسفات الدول حول السيادة الرقمية، فبعض الدول لاسيما في آسيا وروسيا والصين تعتبر البيانات الشخصية جزءاً من السيادة المعلوماتية للدولة، وتفرض قيوداً على خروجها إلى الخارج باعتبارها مورداً استراتيجياً يجب الحفاظ عليه داخل الإقليم الوطني، بينما تنظر دول أخرى إلى البيانات على أنها عنصر من عناصر التدفق الحر للمعلومات الذي يجب ألا يقيد لأن تقييده يمس حرية الإنترنت والتجارة الدولية، هذا التضارب في الرؤى يؤدي إلى تعارض بين القوانين الوطنية وإلى صعوبات في إنفاذ الأحكام القضائية أو في تنفيذ قرارات الحماية عبر الحدود[11].

ومن زاوية فقهية يظهر هذا التشتت القانوني غياب مقاربة دولية متكاملة تربط بين البعد الإنساني والاقتصادي للبيانات الشخصية، فالتعامل مع البيانات كحق إنساني بحت يجعلها خاضعة لمعايير حقوق الإنسان التقليدية التي تركز على الدولة كفاعل رئيسي في حين أن أغلب الانتهاكات المعاصرة ترتكبها شركات خاصة أو منصات رقمية عملاقة تتجاوز سيطرة الدول، وفي المقابل فإن التعامل مع البيانات كسلعة اقتصادية بحتة يفرغها من مضمونها الحقوقي ويحول الإنسان إلى مجرد مستهلك رقمي دون ضمانات حقيقية، ومن هنا تبرز الحاجة إلى صياغة تكييف قانوني جديد للبيانات الشخصية يقوم على مفهوم الحق في السيطرة على البيانات أي الجمع بين الملكية القانونية والخصوصية الإنسانية ضمن إطار واحد متكامل[12].

ثانياً_ غياب التكييف التشريعي الموحد للبيانات الشخصية

إن غياب تشريع دولي موحد لحماية البيانات الشخصية يعد من أبرز مظاهر الضعف في النظام القانوني الدولي المعاصر في مواجهة التحديات الرقمية المتصاعدة، فبرغم الأهمية الجوهرية التي باتت تكتسبها البيانات في العصر الحديث سواء على المستوى الاقتصادي أو الأمني أو الاجتماعي، فإن المجتمع الدولي لم يتمكن حتى الآن من صياغة اتفاقية عالمية ملزمة تنظم بصورة شاملة ومتكاملة عمليات جمع البيانات الشخصية ومعالجتها ونقلها واستخدامها، هذا الفراغ التشريعي الدولي ترك الباب مفتوحاً أمام الدول لتبني مقاربات تشريعية متباينة، تتأرجح بين الحماية الصارمة والانفتاح اللامحدود، مما أدى إلى تضارب في المعايير، وإلى تقويض فعالية الجهود الرامية إلى حماية الحق في الخصوصية الرقمية على المستوى الكوني.

ورغم تعدد المبادرات الدولية فإنها لاترقى إلى مستوى الالتزام القانوني الملزم، فمبادئ منظمة التعاون الاقتصادي والتنمية بشأن حماية الخصوصية الصادرة في عام 1980 والمحدثة في 2013 وإن كانت تمثل مرجعاً دولياً مهماً إلا أنها ذات

---

[10] Nikola Brzica ،Understanding Contemporary Asymmetric Threats ،Croatian International Relations Review ،Vol)24 ، (NO (83) ،Institute for Development and International Relations (IRMO) ،Zagreb ،2018 ،pp 40-43

[11] ادمام شهرزاد، الطبيعة اللاتماثلية للتهديدات الأمنية الجديدة، مجلة الندوة للدراسات القانونية، العدد1، الجزائر، 2013، ص53.

[12] غادة محمد عامر، تطور الصراع الدولي وفق التقدم التكنولوجي وظهور الحروب اللاتماثلية (الحروب الغير نمطية)، مجلة الدراسات الاستراتيجية والعسكرية، العدد8، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ص40.

طابع إرشادي، ترك تطبيقها لتقدير الدول الأعضاء وكذلك اتفاقية مجلس أوروبا رقم (108) لعام 1981 الخاصة بحماية الأفراد تجاه المعالجة الآلية للبيانات الشخصية، رغم أنها تعد أول صك دولي في هذا المجال فإن نطاقها الإقليمي ومرونتها المفرطة جعلاها غير كافية لمواكبة التطور التكنولوجي السريع أو لتغطية الطابع العابر للحدود الذي يميز الفضاء السيبراني[13].

وفي مقابل ذلك لايوجد تحت مظلة الأمم المتحدة حتى الآن أي اتفاق شامل أو معاهدة دولية خاصة بحماية البيانات الشخصية على الرغم من أن الجمعية العامة أقرت في قراراتها المتعددة أهمية الحق في الخصوصية في العصر الرقمي، فالمبادرات التي أطلقتها مؤسسات الأمم المتحدة بقيت في مستوى البيانات التوجيهية والتوصيات غير الملزمة دون أن تتحول إلى قواعد قانونية ذات قوة تنفيذية ويرجع هذا الفشل في جانب كبير منه إلى تباين الرؤى بين الكتل الجيوسياسية المختلفة: فالاتحاد الأوروبي يدفع باتجاه نهج قائم على حماية الحقوق الأساسية، بينما تميل الولايات المتحدة إلى نموذج يعتمد على التنظيم الذاتي للشركات في حين تركز الصين وروسيا على مبدأ السيادة الرقمية وسيطرة الدولة على تدفق البيانات داخل حدودها، وهذه التباينات الجوهرية جعلت من المستحيل حتى الآن إيجاد أرضية مشتركة يمكن أن تؤسس لمعاهدة دولية موحدة[14].

وتبرز خطورة هذا الغياب في كونه يخلق بيئة قانونية مضطربة وغير متكافئة، إذ تخضع البيانات التي ينتجها الأفراد لأنظمة حماية متفاوتة تبعاً لمكان تواجدهم أو لطبيعة الدولة التي تستضيف الخوادم التي تخزن فيها تلك البيانات. فعلى سبيل المثال، قد يتمتع المواطن الأوروبي بحماية قانونية واسعة بموجب لائحة حماية البيانات العامة (GDPR)، بينما يفتقر المواطن في كثير من دول العالم النامي إلى أي حماية قانونية فعالة من المراقبة أو الاستغلال التجاري لمعلوماته الشخصية هذا التفاوت لا يخل فقط بمبدأ المساواة بين الأفراد في التمتع بالحقوق الرقمية، بل يؤدي أيضاً إلى نشوء ما يعرف بالاستعمار الرقمي، حيث تصبح الدول الضعيفة تابعة رقمياً لتلك التي تملك التشريعات الأكثر نفوذاً والأدوات التقنية الأقوى[15].

كما أن غياب التشريع الدولي الموحد يجعل من الصعب تحديد المسؤولية القانونية في حالة انتهاك البيانات عبر الحدود، إذ تتعدد الاختصاصات القضائية وتتنازع القوانين الوطنية، مما يفتح المجال أمام الإفلات من المساءلة، فالشركات العابرة للحدود تستغل هذا الفراغ لتفادي المحاسبة عبر تسجيل مقارها في دول ذات تشريعات متساهلة أو غير مفعلة هذا الواقع يقوض أسس العدالة الرقمية ويجعل الأفراد الطرف الأضعف في معادلة تتحكم فيها القوى الاقتصادية الكبرى[16].

ولا يمكن إغفال البعد التكنولوجي في تفسير هذا الضعف التشريعي الدولي، إذ أن وتيرة الابتكار التقني تتجاوز قدرة المشرعين على مواكبتها، فكلما حاول المجتمع الدولي وضع قواعد تنظم جمع البيانات واستخدامها ظهرت تقنيات جديدة مثل الذكاء الاصطناعي التحويلي أو تقنيات تحليل البيانات الضخمة، أو تطبيقات التعرف على الوجه تجعل الأطر القانونية المقترحة غير كافية أو متقادمة بسرعة، هذه السرعة الهائلة في التحول الرقمي تجعل من التشريع الدولي عملية معقدة تحتاج إلى مرونة عالية وتوافق سياسي عميق، وهو ما لا يتوفر حتى الآن[17].

---

[13] بلال وليد مجيد السامرائي، الامن السيبراني – دراسة مقارنة بين القانون والشريعة القانونية، دار هاتريك للنشر والتوزيع، اربيل، 2025، ص90.

[14] ايهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة الى مراجعة جديدة، بقلم خبير، العدد (23)، مركز المعلومات واتخاذ القرار، القاهرة،2021، ص7-9.

[15] صباح نوري علوان وصلاح حسن الربيعي، إستراتيجية حروب التحرير الوطنية، مركز الكتاب الأكاديمي، عمان، 2015، ص 177.

[16] مصطفى موسى محمد، أثر بناء الدولة على التهديدات الأمنية اللاتماثلية في منطقة الساحل والصحراء، مجلة دفاتر السياسة والقانون، المجلد(12)، العدد(1)، الجزائر، 2020، ص4-5.

[17] كريمة عباسي، التفكير الاستراتيجي الإيراني في ظل التهديدات اللامتماثلة لفترة ما بعد احداث الحادي عشر من سبتمبر 2001، أطروحة دكتوراه، جامعة لحاج لخضر، الجزائر، 2019، ص97.

من ثم فإن غياب تشريع دولي موحد لحماية البيانات الشخصية لايمثل مجرد قصور قانوني، بل هو انعكاس لفشل النظام الدولي في إعادة تعريف مسؤولياته في العصر الرقمي، فالبيانات لم تعد مجرد معلومات تقنية، بل أصبحت عنصراً من عناصر السيادة ووسيلة من وسائل السيطرة والتأثير لذا فإن الحاجة إلى معاهدة دولية شاملة باتت ضرورة وليست ترفاً، بحيث تضع مبادئ واضحة تنظم جمع البيانات ومعالجتها، وتلزم الدول والشركات باحترام معايير موحدة للحماية، وتنشئ آلية دولية للمساءلة والرقابة، فبدون مثل هذا الإطار، سيظل العالم يعيش حالة من اللايقين القانوني التي تهدد استقرار النظام الدولي الرقمي، وتترك الأفراد عرضة لانتهاكات مستمرة في فضاء سيبراني بلا حدود ولا ضوابط.

المطلب الثاني

التحديات القانونية والمؤسساتية لحماية البيانات

رغم الجهود المتزايدة على المستويين الوطني والدولي لوضع أطر قانونية لحماية البيانات الشخصية لا تزال هناك فجوات تشريعية ومؤسساتية تحول دون تحقيق حماية فعالة وشاملة فالقوانين القائمة غالبًا ما تعجز عن مواكبة التطورات التكنولوجية السريعة، كما أن غياب التنسيق بين التشريعات الوطنية والمعايير الدولية يؤدي إلى تضارب في التطبيق ويضعف فعالية الإنفاذ، إضافة إلى ذلك تعاني العديد من الدول من ضعف المؤسسات المختصة بمراقبة تطبيق قواعد حماية البيانات وغياب آليات رقابة مستقلة قادرة على المساءلة، **لذا سوف نقوم بتقسيم المطلب إلى فرعين، سوف نتحدث في الفرع الأول عن غياب المواءمة بين التشريعات الوطنية والمعايير الدولية، أما في الفرع الثاني سوف نتحدث عن قصور آليات الإنفاذ الدولية.**

الفرع الأول

غياب المواءمة بين التشريعات الوطنية والمعايير الدولية

لتمكين أجهزة إنفاذ القانون من جمع الأدلة على الصعيد العالمي تعتبر المواءمة بين القوانين الإجرائية متطلبا ثانياً ضرورياً للتعاون الدولي الفعال ومن المهم التمييز بين المبادئ والإجراءات في مناسبة مناقشة تحديث التشريعات الإجرائية، فقاموس ويبستر يعرف المبدأ بأنه: شامل وقانون أساسي أو النظرية أو الافتراض أو القاعد»، أما الإجراء فهو طريقه خاصة لإنجازه ومن هنا يمكن فهم الفرق بأن المبدأ هو حقيقة أساسية تحكم مسعى محدد والإجراء هو طريقة لإنجاز شيء ما[18].

وتعد إشكالية التعاون القضائي العابر للحدود في الجرائم السيبرانية من أكثر التحديات القانونية تعقيداً في العصر الرقمي، إذ تمثل العقبة الجوهرية أمام تحقيق العدالة في بيئة تتسم باللاحدود، وبقدرة الفاعلين على ارتكاب أفعال غير مشروعة تمتد آثارها عبر دول متعددة في لحظات معدودة إن الجرائم السيبرانية وفي مقدمتها انتهاكات البيانات الشخصية لا تعترف بالمكان ولا بالزمن، فهي تنفذ من خلال شبكات دولية متداخلة، وتدار أحياناً من مناطق لا تخضع لأي رقابة قانونية فعالة، مما يجعل التعاون القضائي بين الدول أمراً ضرورياً ولكنه في الوقت ذاته بالغ الصعوبة من الناحية العملية والقانونية[19].

تكمن جوهر الإشكالية في الطبيعة العابرة للحدود للجريمة السيبرانية، التي تجعل تحديد الدولة المختصة بالتحقيق أو بالملاحقة أو بتنفيذ العقوبة مسألة معقدة، ففي الكثير من الحالات، يكون الفاعل في دولة، والخوادم التي نفذت عبرها الجريمة في دولة ثانية، بينما توجد الضحية في دولة ثالثة، هذا التوزع الجغرافي للركن المادي للجريمة يجعل القواعد

[18] كيفن كاردويل وآخرون، الجرائم الإلكترونية والطب الشرعي الرقمي، نشرته سبرينغر، نيويورك، 2007، ص 54.

[19] عواطف محمد عثمان عبد الحليم، "جرائم المعلوماتية، تعريفها، صورها، جهود مكافحتها دولياً، وإقليمياً، ووطنياً"، مجلة العدل، العدد الرابع والعشرون، السنة العاشرة، 2011، ص69.

التقليدية للاختصاص القضائي القائم على مبدأ الإقليمية عاجزة عن الإحاطة بهذه الوقائع، كما أن مبدأ الشخصية سواء الإيجابي أو السلبي لايكفي وحده لتغطية الأبعاد التقنية المتشابكة لهذه الجرائم التي تتم أحياناً عبر وسطاء أو برمجيات ذاتية التنفيذ يصعب تتبع مصدرها الحقيقي[20].

ومن ناحية أخرى فإن التعاون القضائي الدولي في هذا المجال يصطدم بعوائق سياسية وتشريعية عديدة، أبرزها اختلاف النظم القانونية بين الدول وتباين تعريفات الجريمة السيبرانية ذاتها، فما يعد انتهاكاً للبيانات الشخصية في دولة ما قد لا يعتبر كذلك في دولة أخرى تختلف في فلسفة الحماية أو في حدود الحرية المعلوماتية التي تعترف بها، هذا التباين يعرقل تنفيذ طلبات تسليم المجرمين أو تبادل الأدلة الرقمية، إذ تتردد الدول في الاستجابة لطلبات المساعدة القضائية التي تتعلق بأفعال غير مجرمة في تشريعاتها الداخلية، تطبيقاً لمبدأ "ازدواج التجريم"[21].

إن التفاوت في المقاربات التشريعية بين الدول يعزى في جوهره إلى اختلاف الأولويات السياسية والاقتصادية والثقافية، فبينما تتجه بعض الدول، مثل دول الاتحاد الأوروبي نحو إقرار معايير صارمة لحماية البيانات الشخصية استناداً إلى فلسفة تعتبر الخصوصية حقاً أساسياً من حقوق الإنسان تميل دول أخرى إلى تفضيل حرية تدفق البيانات وتعزيز الابتكار التكنولوجي ولو على حساب مستوى الحماية الممنوح للأفراد، وهذا التباين ينتج شبكة غير متجانسة من القواعد القانونية، تجعل من الصعب تحديد القانون الواجب التطبيق في حال وقوع انتهاك سيبراني عابر للحدود، أو عند نقل البيانات من دولة إلى أخرى ذات مستوى حماية مختلف[22].

وقد أدى هذا الانقسام إلى نشوء ما يمكن وصفه بتعدد أنظمة السيادة الرقمية، حيث تسعى كل دولة إلى فرض رؤيتها الخاصة حول تنظيم البيانات، مما يعرقل مساعي التعاون الدولي. فعلى سبيل المثال، تشترط اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) أن تلتزم الدول أو الكيانات التي تتلقى بيانات من الاتحاد الأوروبي بمعايير حماية تعادل مستواها، بينما تفتقر الكثير من الدول النامية إلى تشريعات مماثلة أو إلى القدرات المؤسسية اللازمة لتطبيقها ونتيجة لذلك يصبح نقل البيانات إلى تلك الدول مقيداً، مما يخلق فجوة رقمية جديدة بين الشمال والجنوب العالمي، ويجعل من حماية البيانات أداةً للهيمنة القانونية بدلاً من أن تكون وسيلة لحماية الحقوق الفردية، وتتجلى الصعوبة كذلك في الجانب الإجرائي، إذ إن الأدلة في الجرائم السيبرانية ذات طبيعة رقمية متغيرة، يمكن محوها أو تعديلها بسهولة، ما يستدعي سرعة في التعاون القضائي لا تتناسب مع بطء الإجراءات التقليدية المعتمدة في تبادل المساعدة بين الدول، كما أن العديد من الدول تضع قيوداً على نقل البيانات الشخصية إلى الخارج لأسباب تتعلق بالسيادة أو بحماية الخصوصية الوطنية، وهو ما يتعارض مع متطلبات التحقيقات المشتركة التي تحتاج إلى الاطلاع على تلك البيانات لتحديد الجناة وإثبات التهمة[23].

كما أن غياب المواءمة بين التشريعات الوطنية والمعايير الدولية يفرز إشكاليات عملية في تنفيذ الالتزامات الدولية ذات الصلة بحقوق الإنسان، فالدول التي صادقت على العهد الدولي الخاص بالحقوق المدنية والسياسية، مثلاً، تلتزم بحماية الحياة الخاصة، لكن دون وجود آليات داخلية فعالة أو قوانين وطنية منسجمة مع المعايير الدولية، تبقى هذه الالتزامات حبراً على ورق، إضافةً إلى ذلك فإن ضعف التنسيق بين الأجهزة الوطنية المسؤولة عن حماية البيانات يؤدي إلى تضارب في القرارات وتكرار في الإجراءات، مما يقلل من فعالية أنظمة الرقابة والمساءلة[24].

---

[20] محمود علي أحمد مدني، دور المحكمة الدستورية العليا في استجلاء المفاهيم الأساسية التي يقوم عليها النظام القانوني، أطروحة دكتورة، حقوق حلوان، 2015، ص349.

[21] محمود رجب فتح الله، الوسيط في الجرائم المعلوماتية، ط1، دار الجامعة الجديدة، الإسكندرية، 2019، ص187.

[22] راشد بن حمد البلوشي، التوقيع الالكتروني–الحماية الجزائية المقررة له، منشورات الحلبي الحقوقية، بيروت، 2018، ص35.

[23] محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص360.

[24] نصيف صفاء، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد الخامس، العدد الثاني، جامعة ديالى، العراق، 2016، ص23.

وتتجلى خطورة هذا الوضع في المجال السيبراني حيث تتجاوز الهجمات والاختراقات الإلكترونية الحدود الجغرافية بسهولة، بينما تظل الأطر القانونية حبيسة الإقليمية، فحين تخترق بيانات مواطن في دولة ما من خلال خوادم تقع في دولة أخرى، يصبح من الصعب تحديد الجهة المختصة بالتحقيق والمساءلة، خاصة إذا كانت تشريعات الدولتين مختلفة أو متعارضة في تعريف الانتهاك أو في شروط المسؤولية، وهذا التنازع التشريعي يخلق بيئة خصبة للإفلات من العقاب، ويفتح المجال أمام الشركات متعددة الجنسيات لاستغلال الفجوات القانونية من خلال تسجيل مقارها في الدول ذات القوانين الأقل صرامة[25].

إن غياب المواءمة لا يقتصر على الفجوة بين الدول، بل يمتد أيضاً إلى الداخل الوطني ذاته، حيث غالباً ما تتعارض التشريعات المتعلقة بحماية البيانات مع قوانين الأمن القومي أو مكافحة الإرهاب أو تنظيم الإعلام، ففي كثير من الحالات، تمنح السلطات التنفيذية صلاحيات واسعة لجمع البيانات ومراقبة الاتصالات بذريعة حماية الأمن، دون ضوابط واضحة توازن بين متطلبات الأمن واحترام الخصوصية. هذا التناقض الداخلي يعكس غياب رؤية شاملة تدمج المعايير الدولية ضمن المنظومة التشريعية الوطنية على نحو متسق ومتوازن[26].

وتعد مسألة الثقة المتبادلة بين الأنظمة القضائية عاملاً حاسماً في هذه الإشكالية ففي غياب آليات واضحة لتبادل المعلومات وضمانات كافية لاحترام حقوق الإنسان في أثناء التحقيق والملاحقة، تخشى بعض الدول من أن يستخدم التعاون القضائي في أغراض سياسية أو في انتهاك حقوق الخصوصية لمواطنيها، هذا الحذر المتبادل يؤدي إلى تردد في توقيع اتفاقيات التعاون أو إلى الاقتصار على التنسيق في أضيق الحدود، مما يضعف من فعالية الجهود الدولية في مكافحة الجرائم السيبرانية، ومن زاوية أخرى فإن المؤسسات الدولية نفسها لم تنجح بعد في إرساء آلية فعالة لمتابعة مدى التزام الدول بتلك المعايير، فالمبادئ التوجيهية الصادرة عن الأمم المتحدة أو منظمة التعاون الاقتصادي والتنمية تبقى ذات طابع غير ملزم، وتفتقر إلى آليات للرصد أو الجزاء، مما يجعل الدول حرة في تبني ما يناسبها من تلك المبادئ دون الالتزام الكامل بها، كما أن الانقسام السياسي بين الدول الكبرى حول قضايا الأمن السيبراني والبيانات الاستراتيجية يعوق التوصل إلى معاهدة دولية ملزمة في هذا المجال[27].

وعلى الرغم من وجود بعض الأطر الدولية التي سعت لمعالجة هذه المسألة، مثل اتفاقية بودابست لعام 2001 بشأن الجريمة السيبرانية، فإنها لا تزال محدودة من حيث العضوية والالتزامات، إذ لم تنضم إليها عدد من الدول الكبرى المؤثرة في المجال الرقمي كروسيا والصين، بسبب خلافات حول بنود تتعلق بالسيادة وتبادل المعلومات، وبالتالي بقيت الاتفاقية إطاراً إقليمياً أكثر منها آلية عالمية للتعاون القضائي مع ما يرافق ذلك من ثغرات في الممارسة العملية لاسيما في القضايا التي تشمل أطرافاً من خارج نطاق الدول الأطراف فيها، وتتسع الإشكالية أيضاً إلى المجال المؤسسي، إذ تفتقر المنظومة الدولية إلى هيئة قضائية أو تحقيقية متخصصة في الجرائم السيبرانية يمكنها التنسيق بين الدول وإدارة الأدلة العابرة للحدود، كذلك، فإن بطء البيروقراطية الدولية وتعدد الجهات المسؤولة في الدول المختلفة يعرقل الاستجابة السريعة للهجمات التي تتطلب معالجة فورية لتتبع مسارات البيانات وحفظ الأدلة قبل زوالها[28].

وتنعكس هذه التحديات على حق الأفراد في الحماية القانونية، إذ يؤدي ضعف التعاون القضائي إلى إفلات مرتكبي الجرائم من العقاب وإلى بقاء ضحايا الانتهاكات وخاصة انتهاكات البيانات الشخصية دون إنصاف فعلي، فحتى في الحالات التي

---

[25] زين العابدين عواد الكردي، جرائم الإرهاب المعلوماتي، ط1، منشورات الحلبي الحقوقية، بيروت، 2018، ص70.

[26] ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية الالكترونية، عدد2، الجزائر، 2017، ص495.

[27] إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مرجع سابق، ص100.

[28] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت دار المطبوعات الجامعية، مصر، 2018، ص237.

تتمكن فيها السلطات الوطنية من تحديد هوية الفاعل، قد تعيق المسائل الإجرائية أو السياسية عملية تسليمه أو محاكمته، مما يضعف الثقة العامة في قدرة القانون الدولي على حماية الحقوق الرقمية، وإن معالجة هذه الإشكالية تتطلب تجاوز النموذج التقليدي للتعاون القضائي القائم على الطلبات الثنائية والإجراءات الورقية البطيئة، نحو نموذج جديد يقوم على المساعدة الفورية والتبادل الآمن للبيانات الرقمية ضمن أطر قانونية تضمن احترام الخصوصية وسيادة القانون في آنٍ واحد، كما أن الحاجة باتت ماسة إلى تطوير اتفاقية دولية خاصة بالتعاون القضائي في الجرائم السيبرانية، تتضمن آليات فنية متقدمة لتبادل الأدلة، وتنشئ قواعد موحدة لتحديد الاختصاص القضائي، وتضمن الموازنة بين مقتضيات الأمن وحماية الخصوصية[29]. وبناءً على ما تقدم فإن غياب المواءمة بين التشريعات الوطنية والمعايير الدولية لايمثل مجرد خلل قانوني، بل هو تعبير عن أزمة بنيوية أعمق في النظام القانوني الدولي الذي لم يستطع حتى الآن أن يواكب واقع التحول الرقمي العابر للحدود، وهذا الغياب يضعف من الحماية الممنوحة للأفراد، ويجعل الخصوصية الرقمية خاضعة لمعادلات القوة والسيادة بدلاً من أن تكون حقاً عالمياً مضموناً لذا بات من الضروري الدفع نحو بناء إطار قانوني دولي موحد أو على الأقل متقارب يحقق الانسجام بين النظم الوطنية، ويرسخ مبدأ المساواة في الحماية القانونية للبيانات الشخصية، بوصفها حقاً إنسانياً لا يقل أهمية عن أي من الحقوق التقليدية الأخرى.

الفرع الثاني

قصور آليات الإنفاذ

يعد ضعف آليات الإنفاذ الدولية أحد أبرز العوائق التي تحول دون تحقيق حماية فعالة وشاملة للبيانات الشخصية في النظام القانوني الدولي المعاصر. فحتى مع وجود بعض المبادئ أو الاتفاقيات التي تقر بحق الأفراد في حماية بياناتهم، يبقى التحدي الأكبر متمثلاً في غياب أدوات عملية لإلزام الدول أو حتى الفاعلين غير الحكوميين، باحترام تلك الالتزامات وتنفيذها، ويكشف هذا القصور عن فجوة خطيرة بين الإطار المعياري النظري وبين التطبيق الفعلي على أرض الواقع، حيث لاتوجد آليات رقابية أو قضائية دولية تمتلك سلطة إلزامية أو صلاحية محاسبة الأطراف المقصرة أو المنتهكة[30].

إن نظام حماية البيانات على المستوى الدولي ما زال يتسم بالطابع اللامركزي، إذ يعتمد بدرجة كبيرة على المبادرات الوطنية أو الإقليمية، بينما تظل الجهود الأممية ذات طبيعة استرشادية أو توصيات غير ملزمة، فعلى سبيل المثال تعد اتفاقية مجلس أوروبا رقم (108) لعام 1981 أول وثيقة دولية تنظم حماية الأفراد تجاه المعالجة الآلية للبيانات الشخصية، لكنها اقتصرت على الدول الأوروبية في المقام الأول، ولم تنشئ جهازاً قضائياً أو رقابياً دولياً يتولى مراقبة التنفيذ أو الفصل في النزاعات، ومع أن البروتوكول المعدل للاتفاقية لعام 2018 (المعروف بالاتفاقية 108+) حاول توسيع نطاقها ليشمل أطرافاً من خارج أوروبا، إلا أنه أبقى على الطبيعة الطوعية للالتزامات، دون فرض جزاءات أو آليات إنفاذ ملزمة[31].

ويضاف إلى ذلك أن المؤسسات الأممية مثل مجلس حقوق الإنسان أو المقررين الخاصين المعنيين بالخصوصية، تفتقر إلى الصلاحيات القضائية أو التنفيذية التي تمكنها من مساءلة الدول عن انتهاكات البيانات، فعملها يقتصر على إصدار تقارير أو توصيات عامة تفتقد في كثير من الأحيان إلى الطابع الإلزامي أو إلى آلية متابعة فعالة. وحتى المنظمات

[29] محمد عزت فاضل، ونواف علي الصفو، جرائم تقنية المعلومات المخلة بالأخلاق العامة (دراسة مقارنة)، دار السنهوري، بغداد، 2017، ص 14.

[30] روني حداد، الإرهاب الإلكتروني وتحديات مواجهته، مجلة الجيش، العدد394، بيروت، 2018، ص2.

[31] طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي والمعاصر، بحث منشور في مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد التاسع عشر، العدد الأول، الأردن، 2019، ص84.

المتخصصة مثل الاتحاد الدولي للاتصالات (ITU) أو منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)، فإن دورها يظل تقنياً واستشارياً أكثر منه قانونياً أو رقابياً الأمر الذي يجعل الحماية الدولية للبيانات أقرب إلى التوجيه الأخلاقي منها إلى الالتزام القانوني[32].

أما على صعيد القضاء الدولي فإن المحاكم والهيئات التحكيمية لم تطور بعد نظاماً مستقلاً لمعالجة الانتهاكات المتعلقة بالبيانات الشخصية، فمحكمة العدل الدولية لا تختص إلا بالنزاعات بين الدول، وغالباً ما تعرض عليها قضايا تتعلق بتجاوزات سيادية أو انتهاكات لحقوق الإنسان بالمعنى التقليدي دون تناول مباشر لمسألة البيانات الرقمية. كما أن المحكمة الأوروبية لحقوق الإنسان على الرغم من ريادتها في حماية الحق في الخصوصية بموجب المادة (8) من الاتفاقية الأوروبية لحقوق الإنسان، فإن أحكامها تبقى إقليمية ولا تمتد إلى باقي دول العالم، إضافة إلى أن معالجتها للبيانات الشخصية تظل ضمن إطار الخصوصية العامة، دون تأسيس نظام قانوني خاص بها[33].

ولا يمكن تجاهل أن القوى الاقتصادية والتقنية الكبرى، التي تهيمن على سوق التكنولوجيا العالمية، تلعب دوراً مؤثراً في إضعاف أي توجه نحو إنشاء آلية إنفاذ دولية فعالة. فالشركات العملاقة العابرة للحدود مثل منصات التواصل الاجتماعي ومحركات البحث وشركات الذكاء الاصطناعي تمتلك من القوة الاقتصادية والتقنية ما يجعلها قادرة على التأثير في السياسات الدولية، بل وأحياناً على مقاومة محاولات إخضاعها للقواعد القانونية الصارمة، ويؤدي هذا الواقع إلى بروز نوع جديد من السلطة الرقمية الخاصة التي تعمل في فضاء شبه مستقل عن إرادة الدول، مما يجعل أدوات الإنفاذ القانونية التقليدية عاجزة عن مواجهتها[34].

الخاتمة

إن حماية البيانات الشخصية لم تعد مسألة قانونية هامشية بل أضحت من القضايا الجوهرية التي تواجه القانون الدولي في ظل التحول الرقمي المتسارع وتزايد الاعتماد على التقنيات الحديثة. فقد أفرزت الطبيعة العابرة للحدود لتدفقات البيانات واقعاً قانونياً معقداً، تتداخل فيه اعتبارات السيادة الوطنية مع متطلبات التعاون الدولي، الأمر الذي أضعف من فاعلية القواعد الدولية التقليدية في توفير حماية شاملة وموحدة للبيانات.

كما إن الإطار القانوني الدولي الحالي لا يزال يعاني من التجزئة وعدم الانسجام، نتيجة غياب اتفاقية دولية جامعة وملزمة تنظم حماية البيانات الشخصية بصورة واضحة. ويضاف إلى ذلك القصور في آليات الرقابة والتنفيذ، فضلاً عن الفجوة المتنامية بين التطور التقني السريع وقدرة القواعد القانونية الدولية على مواكبته.

وعليه فإن تعزيز حماية البيانات على المستوى الدولي يتطلب إعادة النظر في البنية القانونية القائمة وتكثيف الجهود الدولية من أجل تطوير قواعد مرنة وقابلة للتكيف مع المستجدات التقنية، بما يحقق التوازن بين متطلبات الابتكار الرقمي وضمان الحقوق الأساسية للأفراد.

وفي نهاية الدراسة توصلنا الى العديد من الاستنتاجات والمقترحات التالية:

---

[32] وفاء لطفى، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 23، العدد 1، مصر، 2022، ص165.

[33] ايهاب خليفة، الحرب السيبرانية مراجعة العقيدة العسكرية استعداداً للمعركة القادمة، مقال منشور في مجلة السياسة الدولية، العدد 211، مصر، 2018، ص 20.

[34] سعد عاطف عبد المطلب، دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي–دراسة مقارنة، بحث منشور في مجلة كلية الآداب، مصر، 2019، ص 526.

أولاً_ الاستنتاجات

1.إن غياب إطار دولي موحد وملزم لحماية البيانات الشخصية يشكل أحد أبرز التحديات التي تعيق فاعلية القانون الدولي في هذا المجال، ويؤدي إلى تفاوت مستويات الحماية بين الدول.

2. أن التطور التقني المتسارع ولاسيما في مجالات الذكاء الاصطناعي وتحليل البيانات الضخمة، يفوق قدرة القواعد القانونية الدولية الحالية على التنظيم والمواكبة، مما يخلق فراغاً تشريعياً واضحاً.

3.إن ضعف آليات التنفيذ والرقابة الدولية واعتماد القانون الدولي بدرجة كبيرة على الالتزام الطوعي للدول يقلل من فعالية حماية البيانات ويحد من ضمان احترام الحق في الخصوصية على المستوى الدولي.

ثانياً_ المقترحات

1.الدعوة إلى إبرام اتفاقية دولية شاملة وملزمة لحماية البيانات الشخصية، تتضمن معايير موحدة لجمع البيانات ومعالجتها ونقلها عبر الحدود، مع مراعاة خصوصيات النظم القانونية الوطنية.

2.تعزيز التعاون الدولي والإقليمي في مجال حماية البيانات، من خلال إنشاء آليات تنسيق وتبادل للمعلومات بين الدول، ودعم بناء القدرات التقنية والقانونية للدول النامية.

3.العمل على تطوير قواعد قانونية دولية مرنة وقابلة للتحديث المستمر، بما يسمح بمواكبة التطورات التقنية المتسارعة، ولاسيما تلك المرتبطة بالذكاء الاصطناعي والأمن السيبراني.

قائمة المصادر والمراجع

أولاً_ الكتب

1.أسماء الحسين، أسباب الإرهاب والعنف والتطرف، دون دار نشر، الرياض، 2014.

2.أمير فرج يوسف، جريمة مكافحة الإرهاب الالكتروني، دار الكتب والدراسات العربية، مصر، 2016.

3.عفيفي كامل عفيفي، بدائل الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار الثقافة للطباعة والنشر، عمان، 1999.

4.علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، بيروت، 2011.

5.مرعي علي الرميحي، الحرب السيبرانية ومتطلبات الأمن القومي الجديدة، هاتريك للنشر والتوزيع، اربيل، 2025.

6.صباح نوري علوان وصلاح حسن الربيعي، إستراتيجية حروب التحرير الوطنية، مركز الكتاب الأكاديمي، عمان، 2015.

7.محمود رجب فتح الله، الوسيط في الجرائم المعلوماتية، ط1، دار الجامعة الجديدة، الإسكندرية، 2019.

8.راشد بن حمد البلوشي، التوقيع الالكتروني–الحماية الجزائية المقررة له، منشورات الحلبي الحقوقية، بيروت، 2018.

9.زين العابدين عواد الكردي، جرائم الإرهاب المعلوماتي، ط1، منشورات الحلبي الحقوقية، بيروت، 2018.

10.محمد أمين الرومي، جرائم الكمبيوتر والإنترنت دار المطبوعات الجامعية، مصر، 2018.

11.محمد عزت فاضل، ونواف علي الصفو، جرائم تقنية المعلومات المخلة بالأخلاق العامة (دراسة مقارنة)، دار السنهوري، بغداد، 2017.

ثانياً_ المجلات

1. أحمد علو، الحروب السيبرانية والعنف الرقمي واقع عالمي جديد، مجلة الجيش، العدد402، قيادة الجيش اللبناني، بيروت، 2018.
2. ادمام شهرزاد، الطبيعة اللاتماثلية للتهديدات الأمنية الجديدة، مجلة الندوة للدراسات القانونية، العدد1، الجزائر، 2013.
3. ايهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة الى مراجعة جديدة، بقلم خبير، العدد (23)، مركز المعلومات واتخاذ القرار، القاهرة،2021.
4. ايهاب خليفة، الحرب السيبرانية مراجعة العقيدة العسكرية استعداداً للمعركة القادمة، مقال منشور في مجلة السياسة الدولية، العدد 211، مصر، 2018.
5. بهاء عدنان السعبري، أليات ومسارات التمدد الجيو– استراتيجي للإرهاب العابر للحدود، مجلة السياسة الدولة، العدد214، مؤسسة الاهرام، القاهرة، 2018.
6. روني حداد، الإرهاب الإلكتروني وتحديات مواجهته، مجلة الجيش، العدد394، بيروت، 2018.
7. سعد عاطف عبد المطلب، دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي–دراسة مقارنة، بحث منشور في مجلة كلية الآداب، مصر، 2019.
8. طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي والمعاصر، بحث منشور في مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد التاسع عشر، العدد الأول، الأردن، 2019.
9. عواطف محمد عثمان عبد الحليم، "جرائم المعلوماتية، تعريفها، صورها، جهود مكافحتها دولياً، وإقليمياً، ووطنياً"، مجلة العدل، العدد الرابع والعشرون، السنة العاشرة، 2011.
10. غادة محمد عامر، تطور الصراع الدولي وفق التقدم التكنولوجي وظهور الحروب اللاتماثلية (الحروب الغير نمطية)، مجلة الدراسات الاستراتيجية والعسكرية، العدد8، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين.
11. كيفن كاردويل وآخرون، الجرائم الإلكترونية والطب الشرعي الرقمي، نشرته سبرينغر، نيويورك، 2007.
12. لبنى خميس مهدي وتغريد صفاء، اثر السيبرانية في تطور القوة، مجلة حمورابي، العدد 34، مركز حمورابي للبحوث والدراسات الاستراتيجية، بغداد، 2020.
13. ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية الالكترونية، عدد2، الجزائر، 2017.
14. مصطفى موسى محمد، أثر بناء الدولة على التهديدات الأمنية اللاتماثلية في منطقة الساحل والصحراء، مجلة دفاتر السياسة والقانون، المجلد(12)، العدد(1)، الجزائر، 2020.

15. نصيف صفاء، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد الخامس، العدد الثاني، جامعة ديالى، العراق، 2016.

16. وفاء لطفى، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 23، العدد 1، مصر، 2022.

ثالثاً_ الاطاريح

1. كريمة عباسي، التفكير الاستراتيجي الإيراني في ظل التهديدات اللامتماثلة لفترة ما بعد احداث الحادي عشر من سبتمبر 2001، أطروحة دكتوراه، جامعة لحاج لخضر، الجزائر، 2019.

2. محمود علي أحمد مدني، دور المحكمة الدستورية العليا في استجلاء المفاهيم الأساسية التي يقوم عليها النظام القانوني، أطروحة دكتورة، حقوق حلوان، 2015.

رابعاً_ المصادر الجنبية

1. Nikola Brzica ،Understanding Contemporary Asymmetric Threats ،Croatian International Relations Review ،Vol)24 ،(NO (83) ،Institute for Development and International Relations (IRMO) ،Zagreb. ،2018