Journal of Al-Farabi for Humanity Sciences Volume (8), Issue (3) September(2025)

ISSN: 2957-3874 (Print)
Journal of Al-Farabi for Humanity Sciences (JFHS)
https://iasj.rdd.edu.iq/journals/journal/view/95
مجلة الفارابي للعلوم الإنسانية تصدرها جامعة الفارابي

الحماية الدولية للخصوصية الرقمية في إطار الذكاء الاصطناعي

نور ماهر موفق

أ.د. بشير جمعة عبد الجبار

الجامعة العراقية كلية القانون والعلوم السياسية

International protection of digital privacy in the framework of artificial intelligence

Noor Maher Muoafaq

Dr. Basheer Juma Abdul Jabbar

المستخلص

يواجه المجتمع الدولي تحديات متصاعدة في حماية الخصوصية الرقمية في ظل التطوّر المتسارع لتقنيات الذكاء الاصطناعي، التي باتت تعتمد بشكل متزايد على جمع وتحليل كميات هائلة من البيانات الشخصية؛ وبينما يُنظر إلى الذكاء الاصطناعي بوصفه أداة ثورية لتعزيز الكفاءة وتحقيق التنمية، فإنه يُثير في المقابل تساؤلات قانونية وأخلاقية معقّدة تتعلّق بحدود المشروعية، وسبل حماية خصوصية الأفراد في البيئة الرقمية العابرة للحدود؛ لذا نسعى إلى وضع سبل حامية للخصوصية الرقمية، مع التركيز على مدى كفايتها لمواجهة التحديات الناتجة عن استخدام الذكاء الاصطناعي؛ ويقترح مقاربات تشريعية بديلة توازن بين الابتكار التقني والحفاظ على الحقوق الرقمية.**الكلمات المفتاحية:** الجهود الدولية، جهود المنظمات الدولية المتخصصة، السبل التنظيمية، السبل التقنية.

Abstract

The international community is facing mounting challenges in protecting digital privacy in light of the accelerated development of artificial intelligence technologies, which increasingly rely on the collection and analysis of huge amounts of personal data; while artificial intelligence is seen as a revolutionary tool to enhance efficiency and achieve development, it raises complex legal and ethical questions related to the limits of legality, and ways to protect the privacy of individuals in the transnational digital environment; therefore, we are seeking to develop ways to protect digital privacy, focusing on its adequacy to meet the challenges resulting from the use of artificial intelligence; and proposes alternative legislative approaches that balance technical innovation and preserving Digital rights.**Keywords:** international efforts, efforts of specialized international organizations, organizational means, technical means.

المقدمة

في ظل التحوّلات الرقمية المتسارعة التي يشهدها العالم، بات الذكاء الاصطناعي يشكّل ركيزة رئيسية في بنية المجتمعات المعاصرة، متجاوزًا الأطر التقليدية للتكنولوجيا إلى فضاءات تتقاطع مع الحقوق والحريات الأساسية للأفراد. ومن أبرز الإشكاليات التي تثيرها هذه التحوّلات مسألة الخصوصية الرقمية، التي أصبحت في صلب النقاشات القانونية والأخلاقية على الصعيدين الوطني والدولي؛ إذ إن الخوارزميات التي تُمكّن الذكاء الاصطناعي من اتخاذ قرارات مبنية على تحليل البيانات الضخمة، غالبًا ما تستند إلى معلومات شخصية تُجمع وتُعالج بطرق قد تهدّد خصوصية الأفراد.فضلاً عن ذلك أن الإطار القانوني الدولي الحالي لا يزال غير كافٍ لمواكبة التحديات التي تفرضها تطبيقات الذكاء الاصطناعي على الحق في الخصوصية الرقمية؛ وتتفاقم هذه الإشكاليات في ظل غياب إطار قانوني دولي موحد يُنظّم حدود استخدام الذكاء الاصطناعي بما يضمن احترام الحق في الخصوصية، الذي يُعد أحد أبرز الحقوق الأساسية المحمية بموجب الاتفاقيات الدولية لحقوق الإنسان.

أهمية البحث

تتجسد أهمية البحث من التداخل المتزايد بين تطبيقات الذكاء الاصطناعي وحياة الأفراد، خاصة في ظل توسّع عمليات جمع البيانات وتحليلها دون وجود إطار قانوني موحد ومُلزم دوليًا يضمن احترام الخصوصية الرقمية، كما يكتسب البحث أهمية من كونه يساهم في سد الفجوة بين التقدم التكنولوجي السريع والمعايير الحقوقية الراسخة، ويضع تصوّرًا لتعزيز الحماية القانونية في مواجهة الانتهاكات الرقمية العابرة للحدود.

مشكلة البحث

تكمن الإشكالية الرئيسة في أن تطوّر تقنيات الذكاء الاصطناعي يقابله قصور في الإطار القانوني الدولي القادر على حماية الخصوصية الرقمية، مما يثير تساؤلات حول فعالية القوانين الحالية، وقدرتها على حماية الأفراد من انتهاكات غير مرئية أو معقّدة تقنيًا، وخاصة في ظل غياب توافق دولي حول المعايير القانونية المُنظِّمة لهذا المجال.

فرضية البحث

يفترض البحث أن الإطار القانوني الدولي الراهن غير كافٍ ولا يواكب التحديات التي تفرضها تطبيقات الذكاء الاصطناعي على خصوصية الأفراد الرقمية، الأمر الذي يستوجب إعادة النظر في الاتفاقيات الدولية، وإعداد مقاربة تشريعية عالمية تُراعي اعتبارات الحقوق الرقمية وتوازن بينها وبين متطلبات التطور التكنولوجي.

منهجية البحث

يعتمد هذا البحث على منهجية متعددة المحاور تجمع بين الجانب النظري والتحليل العملي، منها المنهج الوصفي التحليلي لرصد الجهود المبذولة لحماية الخصوصية الرقمية في ظل استخدام الذكاء الاصطناعي، سواء على المستوى الوطني أو الدولي، مع التركيز على الثغرات والقصور التشريعي مع الاستعانة بالمنهج المقارن في ثناء الدراسة .

خطة البحث

إذ سيتم تقسيم البحث الى مبحثيين: حيث سنبين في المبحث الاول الجهود العالمية لحماية الخصوصية الرقمية، اما المبحث الثاني فسوف نتطرق الى الآليات الدولية لحماية الخصوصية الرقمية.

المبحث الأول الجهود العالمية لحماية الخصوصية الرقمية

ففي ظل العولمة الرقمية؛ أصبح تعزيز الجهود العالمية المشتركة بين الدول والمنظمات ضروري للمساهمة في حماية الخصوصية والحفاظ على حقوق الأفراد، وبناءً عليه سوف نبين هذه الجهود أدناه.

المطلب الاول الجهود الدولية

تكمن المشكلة المتبادلة بين حاجة المجتمع الدولي لمواجهة التهديدات لخصوصية الافراد وبين حماية حقوق الانسان التي يجري تجاهلها جراء المخاطر المعلوماتية[1]، ومن هذه الجهود وكالآتي: _

أولاً: على مستوى الاتفاقيات والقرارات الدولية

١.فعلى صعيد الاتفاقيات الدولية قررت الجمعية العامة للأمم المتحدة بتقرير "اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية" التي تم اعتمادها في ٢٤ أيلول ٢٠٢٤ من قبل الدول بعد اختتام عملية التفاوض التي استمرت خمس سنوات؛ والهادفة الى منع الجرائم الإلكترونية بفعالية وكفاءة أكبر عن طريق تعزيز التعاون الدولي وتقديم كافة المساعدات الفنية والمعنوية في بناء القدرات وبالأخص للدول النامية، كما سيتم فتح الاتفاقية لتوقيع في حفل توقيع رسمي في فيتنام ٢٠٢٥ ومن ثم تدخل الاتفاقية حيز النفاذ بعد ٤٠ يوم من التصديق عليها من قبل الدول الموقعة عليها[2]اما في ما يخص نطاقها حددته المادة (٣) من الاتفاقية المذكورة؛ أذ اوضحت المادة المذكورة على انطباق الاتفاقية على الجرائم السيبرانية التي تقع من قبل نظم المعلومات او المستهدفة لها او المستغلة لارتكاب جرائم أخرى، كما تشمل الجرائم العابرة للحدود والتي تتطلب تعاون دولي مشترك من اجل جمع الادلة في شكل إلكتروني وتبادلها لأغراض التحقيق[3]؛ اما فيما يتعلق بمضمونها أشارت الاتفاقية على تحديد الافعال الاجرامية في النطاق المعلوماتي وضرورة التعاون الدولي المتبادل لمكافحتها[4]؛ كذلك اشتملت الاتفاقية على مبادئ منها: الشفافية في نظم التكنولوجيا المعلومات والتعاون الدولي المشترك لمكافحة الجريمة وحماية البيانات من خلال احترام حقوق الانسان من خلال فرض تدابير وقائية تعزز من الوعي الذاتي والأمني واحاطة المعرفة بالمخاطر الإلكترونية[5].

٢. اما على صعيد القرارات الدولية

أ.قرار مجلس حقوق الإنسان الذي اعتمده في ١٢ تشرين الاول ٢٠٢٣ بعنوان "الحق في الخصوصية في العصر الرقمي"؛ حيث أشار القرار على أن الحقوق التي يتمتع بها الافراد خارج الأنترنت ومنها الحق في الخصوصية يجب حمايتها ايضاً على الأنترنت لاسيما في الوقت الذي تشهدهُ زيادة سرعة وتيرة التطور التكنولوجي؛ لذا تشجع الأفراد على استخدام نظام تكنولوجيا المعلومات، وفي نفس الوقت يزيد من فرصة الدول والأفراد والمؤسسات التجارية للقيام بالاختراق والمرقبة وجمع البيانات التي من شأنها تشكل انعكاس سلبي من خلال انتهاك او تجاوز لحقوق الإنسان ومنها الحق في الخصوصية الرقمية[6].وعليه يشدد على ضرورة أخذ العناية الواجبة لحقوق الانسان وعند تصميم التكنولوجيا الجديدة ومنها الذكاء الاصطناعي التي تؤثر على حقوق الانسان؛ كما من الضرورة تجنب او تخفيف هذه المخاطر عن طريق تدابير وقائية مشروطة بشفافيتها وأمانها بالإضافة لذلك عن توفير سبل قضائية وآليات لجبر الضرر وأنشاء رقابة ذاتية، لاسيما قيام استخراج البيانات من خلال التقنيات الخفية او ملفات الارتباط والتي من الممكن استنادها الى بيانات مغلوطة او بيانات مضللة وخطاب الكراهية من خلال منصات التواصل الاجتماعي؛ كذلك الاثار الناجمة عن المراقبة وتزايد استخدام الخوارزميات المنطوية على تطبيقات الذكاء الاصطناعي عن طريق انظمة التعرف على الوجه التي تؤدي الى التمييز في بعض الاحيان وبالأخص عند ما يتم برمجة الخوارزميات على بيانات غير دقيقة[7].

ب. قرار المفوض السامي لحقوق الانسان (فولكر تورك) في حدث جانبي رفيع المستوى في الدورة ٥٣ بعنوان "ما هي الحدود التي يجب فرضها؟ المرحلة التالية للذكاء الاصطناعي والتكنولوجيات الجديدة والناشئة من منظور حقوق الإنسان"، والذي أشار على الرغم من الفوائد العائدة من الذكاء الاصطناعي للخدمة البشرية عن طريق التنبؤ والاستشراف الاستراتيجي؛ فمن من اجل التمتع بهذه الفوائد علينا أن نتأكد من تفوقه على المخاطر وما نعنيه عند الحديث عن الحدود هو التنظيم، وآلية التنظيم يكون من خلال تقييم المخاطر من قبل مطوري الذكاء الاصطناعي ودمج حقوق الانسان طوال فترة حياة الذكاء الاصطناعي بأكملها سواء في فترة التصميم ام بعدها (الافتراضية)؛ كذلك يقترن التقييم بشفافيته والرقابة الذاتية مع سبل انتصاف فعالة لاسيما عندما تكون الدولة تستخدم تكنولوجيا الذكاء الاصطناعي موقفاً استخدامها لحظر التقنيات التي لا تتماشى مع القانون الدولي لحقوق الانسان؛ تطبيق القوانين واللوائح المعنية بحماية البيانات الشخصية؛ وإضافة لذلك أنشاء هيئات دولية استشارية معنية بالتكنولوجيات الخطيرة أذ من خلالها تقديم وجهات نظر متباينة حول كيفية مواءمة المعايير التنظيمية مع الأطرة القانونية لحقوق الانسان وسيادة القانون[8]ختاماً، نجد الجهود الدولية كانت مواكبة للحداثة التكنولوجية من خلال الوثائق التي ذكرناها سلفاً وهذا بدوره يؤكد مدى اهتمام المجتمع الدولي في المحافظة على الحق في الخصوصية في العصر الرقمي؛ وتأكيداً لذلك كانت هذه الجهود عابرة للحدود كون التحديات الحالية لا تكرس في دولة معينة.

المطلب الثاني جهود المنظمات الدولية المتخصصة

سعت المنظمات المتخصصة بجدية لحماية الخصوصية في الفضاء الرقمي؛ وسوف نبين جهودها وفق الآتي:

أولاً: الجمعية العالمية للخصوصية (GPA)اعلنت الجمعية في قرارها بعنوان "حماية المراقبة وحماية الافراد في الخصوصية" في ٢٠٢٤؛ ألذي أشار ومع التقدم التكنولوجيا المرافق لعصرنا وعلى وجه الخصوص لتقنيات المراقبة وانظمة تحديد المواقع مما يستلزم اهمية بالغة لحماية البيانات الشخصية والخصوصية على اعتبارها حقاً من حقوق الانسان المشكلة شرطاً اساسي لمجتمع ديمقراطي فعال[9]. وعليه قررت المنظمة في قرارها بأنشاء مجموعة فرعية معنية بتقيات المراقبة ضمن مجموعة عمل الاقتصاد الرقمي والمجتمع التابعة للجمعية العالمية للخصوصية لتقديم رؤية واضحة ذات الصلة من خلال اجراء البحوث وتطوير الاوراق البحثية الموضوعية بهذا الشأن، كما سعت الجمعية الى عقد مؤتمرات دولية معنية بحماية الخصوصية ومنها هذه المؤتمرات: المؤتمر الدولي لمفوضي حماية البيانات والخصوصية (ICDPPC) في تيرانا ٢٠١٩؛ أذ تضمن المؤتمر وضع استراتيجية سياسية لهذه المنظمة للعامين القادمين المعتمدة على اعلان مدريد الصادر من مفوضي حماية البيانات والخصوصية (ICDPPC) وترتكز الاستراتيجية على ثلاث ركائز اساسية منها: تطوير الاطر والمعايير العالمية لحماية الخصوصية؛ وتعزيز التعاون الدولي للخصوصية في العصر الرقمي؛ وبناء القدرات الداعمة في تبادل الخبرات للأعضاء[10].

ثانياً: منظمة أمن نظم المعلومات (ISSA)تعد من المنظمات غير ربحية تقع في الولايات المتحدة الامريكية وتختص بحماية تكنولوجيا المعلومات والاتصالات ومواجهة التحديات الناشئة والمحتملة[11]، ومن ابرز جهودها في هذا الشأن تحتوي على لجنة الاخلاقيات الدولية التي تصدر توجيهات حول السلوك الاخلاقي لمتخصصي أمن المعلومات وتطوير والمحافظة على المبادئ التوجيهية المتعلقة بأمن المعلومات[12]، كذلك توفر منتديات تعليمية من اجل التعزيز بأمن المعلومات والتفاعل بين الخبراء والمهنين من خلال المؤتمرات الدولية والحلقات النقاشية ودورات تدريبية ومنها: دورة آمن وحماية نظم المعلومات في المؤسسات ودورة التشفير وآمن الشبكات[13].

ثالثاً: منظمة توحيد المعايير الدولية (ISO) كان لمنظمة توحيد المعايير دوراً كبيراً في حماية البيانات الشخصية عن طريق معايير التي ساهمت في تحقيق التوازن للاستخدام الامثل للتقنيات الذكية وحماية خصوصية الافراد ومنها: معيار آمن المعلومات (ISO/IEC 27002) الذي يعد هاماً للشركات والمؤسسات حيث يعمل على توفير لها توجيه لتحسين وتطوير نظام امن المعلومات باستمرار ومن فوائده التصدي للهجمات السيبرانية وحماية البيانات الشخصية والحماية على مستوى المؤسسة او الشركة لاسيما في نسخته المحدثة لعام ٢٠١٣ ركز على تقييم المخاطر وكيفية التعامل معها[14]، ومعيار حماية البيانات الشخصية في السحابة 27018 (ISO/IEC)؛ أذ يهدف الى توفير تدابير رقابية من خلال مساعدة مزودي خدمة السحابة العامة على الامتثال عند معالجة البيانات الشخصية وتمكين الشفافية للعملاء التي من خلالها يمكن اختيار خدمات السحابة المتضمنة حماية عالية عند معالجة البيانات والمساعدة في الاتفاقيات التعاقدية بين مزودي خدمات السحابة العامة والعملاء[15]، ومعيار إدارة خصوصية المعلومات27701 (ISO/IEC) الذي يعد امتداد لمعيار آمن المعلومات(ISO/IEC 27001) ومعيار إدارة آمن المعلومات(ISO/IEC 27002)؛ لذا يساهم في الدعم لأنشاء نظام لإدارة خصوصية المعلومات ويوفر فيها إرشادات توضح كيفية الامتثال للمعايير الدولية للمنظمات التي تتعامل مع البيانات الشخصية من خلال التحكم بها او معالجتها[16]،ومعيار إطار عمل الخصوصية (ISO/IEC 29100) حيث يساهم في تعزيز الخصوصية من خلال الإرشادات التي يقدمها حول كيفية حماية البيانات الشخصية من المخاطر ويتضمن مبادئ منها الشفافية وحدية البيانات والمساءلة وكذلك يحدد مسؤولية الجهات المتحكمة او المعالجة للبيانات الشخصية[17]؛ وعلى ضوء ما تقدم ساهمت منظمة المعايير بحماية كافة ضد المخاطر المعلوماتية سواء كانت قبل ظهور التقنيات الذكية او بعدلها وخاصة يتبين لنا كان لها دور فعال في تنمية الوعي التكنولوجي وحماية الحق في الخصوصية كونه حق من حقوق الانسان وعليه ظهرت معايير اخرى ذات الصلةختاماً، وجدنا لما سبق ذكره بأن المنظمات الدولية بذلت جهود واسعة في حماية الحق في الخصوصية في ادوار متنوعة حيث كانت منها بمثابة دور توجيهي وفعلي والاخرى دور توعي فد كانت سباقة في توفير إطار لحمايتها فضلاً عن ذلك تبين ان الجهود التي كانت مبذولة لم تكرس على وقت السلم وانما في حالات الاستثنائية.

المبحث الثاني الآليات الدولية لحماية الخصوصية الرقمية

ونتيجة لجهود الدولية لحماية الخصوصية الرقمية التي أصبحت من اهم القضايا تتلقى اهتمام في ظل الفضاء الرقمي؛ لذا فأن حمايتها تتطلب آليات دولية ولما تشكله هذه من أهمية خاصة بالنسبة للمجتمعات الحاضرة والقادمة لذا سوف نبين أبرز آليات واثرها على التنمية المستدامة وفق الآتي:

المطلب الاول السبل التنظيمية

أن مواجهة تحديات البيئة الرقمية تتجسد في السبل التنظيمية المواكبة للمستجدات الحديثة سواء كانت على الصعيد الإقليمي او الدولي؛ ويكون من خلال:

أولاً: تطور التشريعات المعنية بالحمايةلضمان حماية الأفراد من التدخل غير القانوني والتعسفي الناتج عن التقنيات الذكية؛ لابد من وجود أطر قانونية سواء كانت إقليمية او دولية فعالة؛ لاسيما أن بعض الدول تشريعاتها تكون غامضة او مفتقرة او قديمة وغير كافية لحماية من المخاطر الناتجة في الفضاء الرقمي[18]، فعلى سبيل المثال في اوكرانيا حيث طورت تشريعاتها المعنية بحماية البيانات الشخصية نتيجة التأثير الدولي لاعتمادها معايير الحماية المتضمنة الاعلان العالمي لحقوق الانسان والعهد الدولي الخاص بالحقوق السياسية والمدنية كأساس الزامي لتطوير تشريعاتها؛ وعليه يبرز التطور في الدستور الاوكراني الذي وضع أساس مبدا الحماية لحقوق الانسان ومنها الحق في الخصوصية وبموجبه شرع قانون خاص لحمايتها وهو "قانون حماية البيانات الشخصية"؛ مضيفاً لذلك تم توقيع على اتفاقية الاوروبية المحدثة رقم (+١٠٨) المشجعة على انضمامها مع دول الاعضاء في الاتفاقية ونتيجة تطور التكنولوجيا التي من خلالها برزت الحاجة الملحة لتطوير التشريعات الاوكرانية لحماية البيانات[19]، كما في بريطانيا لا يعد الحق في الخصوصية حقاً مستقلاً وانما يرتبط بحقوق شخصية اخرى مثل حق الصورة والسمعة معتقدين ان له قيمة ثانوية او خارج القانون؛ وعليه فمثل هكذا تشريعات لابد من تحسين القوانين واللوائح ذات الصلة من خلال النص التشريعي والحال مماثل بالنسبة لأمريكا المفتقرة لتشريع شامل مستقل[20]، اما في سنغافورة فقد اصبحت عضواً في نظام قواعد الخصوصية عبر الحدود التابع لمنتدى التعاون الاقتصادي لدول آسيا والمحيط الهادي(APEC) ونظام معالجة البيانات الشخصية التابع له ايضاً؛ ومن ثم فأن انضمام سنغافورة يعزز من الحاجة لتطوير التشريعات الحالية او وضع جديدة لضمان حماية البيانات الشخصية لاسيما في التجارة الالكترونية لحل النزاعات الحاصلة في تحديد القوانين والاختصاص القضائي لذا لابد من إيلاء اهتمام خاص في هذا الشأن[21]، كما في القارة الافريقية شهدت تغيرات ملحوظة من قبل

بعض الدول منها مصر وكينيا وجنوب إفريقيا تشريعات لحماية البيانات ومنها قانون جالبون بشان حماية البيانات الشخصية رقم (٠٢٥) لسنة (٢٠٢٣) المعدل الذي يتضمن إشارة صريحة لذكاء الاصطناعي والتنميط ومعالجة اللغة الطبيعية وهذا غير وارد في باقي مناطق ولاسيما في جنوب إفريقيا[22].

ثانياً: أنشاء الهياكل الادارية المعنية بحماية البيانات الشخصيةتعتبر الخصوصية قضية عالمية بالغة الأهمية؛ لذلك نجد اغلب الدول تقريباً تسعى في العديد من قوانينها وقراراتها واحكامها القضائية الى حمايتها[23]، أذ أن الدعم القانوني من خلال استحداث وتطوير قواعد قانونية معنية بحماية هذا الشأن لم يكن كافي مالم يكن مشروط بالدعم الاداري المتضمن الآليات واجراءات فعالة وإنفاذ الحقوق والمسؤولية عن انتهاكها[24]، فأن الدعم الاداري متمثل في أنشاء سلطة مستقلة من خلال نص تشريعي يكون دورها إشرافي ورقابي بشكل يؤمن الامتثال للقوانين الدولية والإقليمية المعنية بحماية البيانات الشخصية؛ على الرغم من وجود اختلاف في التسميات المطلق عليها مع التشريعات المقارنة فالبعض منهم اعتبرها "لجنة" و البعض الاخر "هيئة" او "مكتب مفوض" كما ان الصلاحيات المخولة لها مختلفة من دولة لأخرى[25]؛ وعليه فأن السبل التنظيمية تتجسد في وجود تشريعات حديثة مواكبة للمستجدات ومرفقة بوجود سلطات معنية بحماية البيانات الشخصية؛ حيث ان اختلاف احدهم يخل في آمن البيئة الرقمية وخير المثال عقدت سلسلة جهود إفريقية كندية وكان الغرض منها مناقشة المعايير القارية لحماية البينات الشخصية في إطار القارتين؛ ومن هذه الجهود كانت تشريعات منها لجنوب إفريقيا قانون المجموعة الانمائية (SADC) لعام (٢٠١٢) وايضاً الاطار القانوني لقوانين الانترنت لمجموعة شرق إفريقيا (EAC) لعام (٢٠٠٨) التي لم يتم التصديق عليها من قبل اغلبية الدول منهم لغاية الان وكان القانون الوطني هو المحور المبذول فقط على الرغم من وجود هيئة معنية بحماية البيانات الشخصية في جنوب وشرق إفريقيا[26]؛ وكذلك في امريكا حيث أن الدستور الامريكية لا يشير الى الخصوصية وكذلك الحال بالنسبة للتشريعات الفرعية فلا يوجد تشريع شامل منظم لها من كافة الجوانب ولكن وجود تشريعات تنظم على مستوى فيدرالي لقطاعات محددة؛ غير أن هذه القوانين لا تغطي باقي القطاعات وعليه سعت الحكومة الامريكية بسنن تشريعات اخرى لسد الفراغ القانوني[27]؛ كما قامت وزارة العدل الامريكية بأنشاء مكتب حماية الخصوصية والحريات المدنية والذي يتراسها مدير الخصوصية من خلال تقديم تقارير الى إدارة تتبع وزارة العدل؛ وايضاً هناك بعض المؤسسات تحمي جزء من الحق في الخصوصية منها لجنة التجارة الاتحادية(FTC) من خلال إشرافها على الامتثال لتنفيذ القوانين الفيدرالية[28]، أذ نجد على مستوى الاتحاد الاوروبي وجود هيئات معنية منها: هيئة الاشراف على حماية البيانات الأوروبية (EDPS) فهي مستقلة تابعة للاتحاد تحمي وتراقب البيانات داخل مؤسساته[29]، والنهج مماثل تم استحداث في العديد من الدول الاوروبية لهذه السلطات منها في فرنسا أنشاء لجنة الحقوق والحريات بموجب القانون رقم (١٧_٧٨) المعدل لسنة (٢٠١١) رقم (٣٣٤) ومن مهامها حماية حقوق الأفراد من خلال اثبات مشروعة معالجة بياناتهم ومنحهم رخصة ولاسيما البيانات الحساسة وإعلامها في حالة الانتهاك؛ وفرض عقوبات في حالة مخالفة الاجراءات من قبل المتحكمين؛ واقتراح تدابير تشريعية او تنظيمية على الحكومة ليتماشى مع البيئة التكنولوجية المتطورة؛ وتقديم تقرير سنوي يتضمن مهام اعمالها الى السلطة التنفيذية والتشريعية[30]؛ وايضاً في المانيا حيث تعتمد على نظام المفوض الفيدرالي لحماية البيانات وحرية المعلومات بعد صدور قانون حرية المعلومات (٢٠٠٦) الذي يقوم بمهمة مراقبة حماية البيانات في القطاعات الحكومية والشركات الاتصالات والخدمات البريدية مرفق بتقرير نصف سنوي عن نشاطاته في هذا المجال؛ ويعد المفوض جزءاً من وزارة العدل ويتح له تقديم المشورة والمساعدة للحكومة ضد المعالجات غير المشروعية للوزراء والمسؤولين[31]؛ كذلك على مستوى إفريقيا ففي نيجريا شكلت هيئة تنمية تكنولوجيا المعلومات والاتصالات بموجب قانون حماية البيانات الشخصية كهيئة إدارية مستقلة مخول لها صلاحيات إدارية وقضائية[32].ختاما، وجود السبل التنظيمية بكلا عنصريها تشكل إطاراً هاماً لحماية الخصوصية حيث لا يمكن انفراد احدهم عن الاخر سواء في تطور التشريعات او انشاء الهياكل الادارية.

المطلب الثاني السبل التقنية

مع إمكانية التطبيق الواسع لأنظمة تكنولوجيا المعلومات والاتصالات؛ لابد من وجود تدابير تقنية لاسيما اذا لم يكن هناك تطبيق سليم وفعال لسبل التنظيمية ويتبع ذلك تصبح عديمة الفائدة ومعدومة الأثر[33]؛ ولبيان الحماية التقنية سوف نوضحها وفق الآتي:_

أولاً: التشفيرأصبحت الخصوصية تتلقى صدى للأفراد وذات معنى جديد لدول؛ لذا حظيت باهتمام كبير من قبل المحاكم والهيئات التشريعية منذ القدم؛ لكن مع التقنيات الرقمية التي خلقت فرصاً جديدة لتواصل والتعبير مرفقة بجميع وتخزين ونشر كميات كبيرة من البيانات الشخصية المتعلقة بالأفراد وتفاصيل حياتهم، وعلى ضوء ذلك نشر المقرر الخاص المعني بالمدافعين عن حقوق الانسان في عام (٢٠١٣) تقريراً حول مراقبة الدولة للاتصالات والخصوصية ولخص فيه آمن المعلومات عنصراً اساسياً لحماية الحق في الخصوصية لاسيما هناك تشريعات تمنع من استخدام ادوات لتعزيز الخصوصية ومنها التشفير[34]؛ وعليه يعرف التشفير "هو الانضباط الذي يتجسد في مبادئ و وسائل واساليب لتحويل البيانات من اجل

إخفاء محتوى المعلومات الخاص بها والتأكد من صحتها ومنع تعديلها دون اكتشافها ورفض او منع استخدام غير مصرح بها"[35].ولتشفير أنواع منها المماثل الذي يشمل المستلم والمرسل يستخدمان نفس مفتاح التشفير وكذلك مفتاح فك التشفير؛ أذ يشبه هذا النوع قفلاً ميكانيكياً يمكن قفله وفتحه كما لا يمكن معرفة البيانات المتضمنة من قبل شركات الاتصال[36]؛ ومن أمثله هذا النوع تطبيقات (Messenger,Signa,WhatsApp) ومن مزايا هذا النوع سريع وفعال ومفيد لاسيما عندما يقوم نفس الطرف بالتشفير وفكه دون الحجة الى مفتاحين مختلفين[37]؛ اما التشفير غير المماثل وهو استخدام مفتاحين مختلفين لتشفير البيانات المتضمن مفتاح عام والخاص؛ أذ يعد أكثر اماناً من التشفير المماثل ولكن ابطئ في معالجة المعلومات[38]؛ ولطالما حماية البيانات الشخصية هي حقاً مستقلاً فالتشفير كذلك الحال لكن لا يمنح هذا الحق بشكل مطلق وفق لما تبين من خلال تقرير أشارت اليه منظمة العفو الدولية في وجود بعض دول تفرض قيود على مستخدمين التشفير ومنها كوبا وباكستان والهند والبعض منهم حظرته تماماً منها المغرب وروسيا وباكستان وكازاخستان[39]؛ كما قامت شركة (Virtru) المختصة بآمن المعلومات والتشفير باستخدام معيار تنسيق البيانات الموثوق (TDF)[40] الذي يأمن البيانات التي يتم ارسالها عبر البريد الالكتروني حيث يقوم بتشفير الرسائل والمرفقات اثناء النقل والتخزين ولا يسمح بفتح البيانات الا لشخص المرسل اي الشخص الذي تمت مشاركته بها[41].

ثانياً: البصمة الإلكترونيةتلعب خوارزميات التدريب الآلي دوراً مهماً في أنظمة المصادقة البيومترية؛ أذ تستخدم تقنيات الدعم (SVM) والشبكات العصبية في التعرف على الانماط والتصنيف من اجل تحليل البيانات البيومترية وتحديد الميزات الفريدة[42]؛ ومن ابرز مزاياها تحليل الصفات البيولوجية لصاحب الشأن والتي من الاستحالة مشاركته بها مع الاخرين؛ وتشكل حلاً لنسيان كلمة السر التي يترتب عليها الكثير من الخسائر؛ وتوفير خصوصية أمنية وسرية مقارنة بغيرها من الوسائل التقنية؛ والقدرة الفائقة للتعرف على الاشخاص والتحقق من هوياتهم ولاسيما ما يعرف " Face ID "[43].فعلى سبيل المثال استخدمت الحكومة الامريكية برنامج الهجرة(US–VISIT) الذي يعمل من خلال جمع البصمات الرقمية وصور فوتوغرافية لتحقق اذا كان الزائر بحاجة الى تأشيرة عن طريق وزارة الخارجية أثناء عملية طلب التأشيرة بعد جمع بياناته البيومترية وعند وصوله للولايات المتحدة الامريكية تستخدم وزارة الامن الداخلي اجراءات التحقق اذا كان الزائر هو الذي طلب التأشيرة؛ وعليه فأن البرنامج يهدف الى تعزيز الامن وحماية البيانات الشخصية باستخدام تقنيات بيومترية محدثة[44].

ثالثاً: جدران الحمايةفي إطار تسهيل تبادل المعلومات بين المؤسسات المالية؛ أذ تقوم الاخيرة بربط فروعها المتعددة بشبكة واحدة من اجل تسهيل العملية بين الفروع الاخرى وتسمى "بالشبكة الداخلية الخاصة" ويمكن للمؤسسات أن تقوم بإنشاء شبكة افتراضية خاصة المتضمنة قناة اتصال مشفرة تقام من قبل شبكات غير آمنة مثل الانترنت وتربط بين شبكتين او موقعين لتشفير جميع المعلومات المتبادلة بينهم[45]؛ وعليه فيمكن أن نعرف جدران الحماية بأنها "حاجز تقني يهدف الى منع المستخدمين غير المصرح بهم من الوصول للشبكة وخدماتها من الشبكات الخارجية الاخرى؛ وبالعادة يتم بين شبكة موثوقة وشبكة غير موثوقة غالباً ما تكون الأنترنت" [46]؛ وتكون الآلية عمل الجدار عن طريق مراحل منها: المرحلة الاولى هي القاعدة الاساسية باستقبال البيانات وفحصها بفصل الشبكة المحمية والأنترنت؛ اما المرحلة الثانية بعد فحص البيانات يسمح بمرورها اذا كانت موثوقة ومطابقة للقواعد او رفضها اذا كانت خلاف ذلك؛ وعلى سبيل المثال شركة (Sophos) المتخصصة في مجال الأمن السيبراني حيث استخدمت هذه التقنية للحماية من التهديدات السيبرانية[47].

رابعاً: اخفاء الهويةيعُد الاخفاء "عملية ازالة البيانات او تغيرها للمعلومات القابلة للاستبدال بحيث لا يمكن التعرف على الافراد بسهولة"؛ كما أن الهدف منه حماية الخصوصية ومن ثم الاخفاء يحمي البيانات من الكشف مع الاحتفاظ بصيغتها الاساسية[48]؛ ومن انواعه: إخفاء البيانات اي استبدالها بقيم عشوائية او غير ذلت معنى على سبيل المثال استبدال اسم العميل بسلسلة عشوائية من الاحرف مع الاحتفاظ بصيغته الاصلية؛ وتجميع البيانات ودمج بيانات لأفراد عدة لتكوين رؤية واسعة على مستوى مجموعة وعليه يصعب التعرف على احد منهم مثال بدلاً من الكشف عن رواتب الافراد تظهر البيانات المجمعة متوسط رواتب المجموعة؛ وتعميم البيانات يتضمن التعميم تقليل لحماية الخصوصية من ما يجعلها اكثر دقة مثل تعميم العمر الدقيق البالغ ٢٩ على فئة عمرية من ٣٠–٢٠؛ حيث ان هذه الطريقة تحجب التفاصيل الدقيقة التي المؤدية الى تحديد الهوية؛ واخفاء البيانات فعلى الرغم من الجهود المبذولة في إخفاء البيانات الا أن ذلك لا يمنع من خطورة اعادة تحديد الهوية من خلال الدمج البيانات المخفية مع مصادر اخرى للبيانات المتاحة وبالتالي يزداد احتمالية لإعادة تحديد الهوية لاسيما اذا كانت البيانات المخفية مجهولة المصدر او نادرة او تفتقر الى التغطية الكافية وعليه تسمى هذه العملية "قابلية تحديد الهوية المتبقية" والتي تشكل تحديداً كبيراً لضمان الخصوصية؛ وايضاً فقدان البيانات، حيث إخفاء البيانات يقلل من فائدتها وعليه تفقد البيانات البعض من تفاصيلها الاصلية فعلى سبيل المثال قد يحد من استخدام

البيانات على إجراء تحليل احصائي دقيق او قد تحدث اختلاف داخل المجموعة ويؤدي الى تحدياً في التطبيق الفعال لإخفاء الهوية فلا بد من إيجاد التوازن بين حماية الخصوصية وفائدة البيانات.

خامساً: برامج ضد الفيروساتيجب أن يحتوي الكومبيوتر على برامج لرصد الفيروسات لقياس مؤشرات الخطر والتي تصنف الى: الاصابة الذي يحدد اذا كان الجهاز مصاباً بالفيروسات الخبيثة ام لا؛ وتصنيف الخطر من (٠ الى ٣) حيث يشير الرقم الاعلى الى المستوى الاكثر تعرض للخطورة وفق التسلسل (ضعيف؛ منخفض، خطير جداً؛ عالي الخطورة)؛ واجمالي الاصابات يتضمن قائمة بالفيروسات الخبيثة المصيبة للبرمجيات مرفقة بمستوى الخطر بكل نوع من البرامج الضارة[49]؛ فعلى سبيل المثال في عام (٢٠١٧ و٢٠١٠) اندلعت فيروسات خبيثة منها (WannaCry؛ Stuxnet) اللذان شكلان هجوم الكترونياً وبموجبه سلط الضوء على ضرورة اعتماد نهج متعدد الطبقات لحماية الأمن السيبراني منها الحاجة لتصحيحات استباقية وتجزئة الشبكات واستراتيجيات النسخ الاحتياطي الفعال لتخفيف من أثر تفاشي البرامج الخبيثة من قبل المؤسسات وبين المؤسسات التي نجحت في الدفاع هي شركة (Maersk) في استعادة وإعادة بناء بنيتها التحتية بعد هجوم إلكتروني مدمر(NotPetya) منسوب الى قراصنة في كوريا الشمالية وكذلك الحال بالنسبة لشركة (Sony)[50].ختاماً؛ وجود السبل التنظيمية غير كافي لحماية البيانات الشخصية في الفضاء الرقمي نتيجة عدم اكتفاء التنظيم وسرعة التطور التكنولوجي ومرونة التهديدات وبالتالي لابد من حماية بيانات الافراد بشكل مباشر من خلال التدابير التقنية، وبناءً عليه السبل التنظيمية تضع القواعد لكن السبل التقنية هي الدرع الاساسي في الحماية الفعلية للبيانات.

الخاتمة

١. تبين لنا أن الجهود العالمية والمنظمات الدولية المتخصصة تضمنت حماية على كافة المستويات للحق في الخصوصية كما تبين أن نهج الحماية في ظل الرقمنة كان كافياً.

٢. عدم اكتفاء احد الآليات لحماية البيانات الشخصية سواء كانت تنظيمية او تقنية؛ أذ يشكلان علاقة تكاملية في تطبيق الحماية الفعالة للحق في الخصوصية الرقمية؛ وعليه نستطيع القول تشكيل السبل التنظيمية على إرساء الاطار القانوني، اما التقني فهو يحمي البيانات بشكل مباشر عن طريق الاداة التكنولوجية.

المقترحات

١. نقترح أن يكون هناك اتفاق دولي منظم للخصوصية على الصعيد العالمي إسوة بالإقليمي مواكب لتغيرات التقنية.

٢. نقترح لجميع الشركات التكنولوجية عندما تسعى لأطلاق تقنية جديدة ضرورة مراعاة تقيمها او على الاقل خصوصية التصميم فلا ينبغي اقتصار الامر على المنافسة مع الشركات الاخرى في كثرة اطلاق التقنيات دون توفير حماية مناسبة تلاءم السياق المعلوماتي.

٣. بإكمال السبل التنظيمية لدول التي تفتقر لاحد العنصرين او استحداث في حالة الافتقار او التطوير لاسيما وجودها يشكل ركيزة هامة لحماية السيادة الرقمية لدولة المعنية وبالأخص المشرع العراقي.

٤. نشر التوعية والثقافة التقنية في صفوف المجتمع فضلاً عن ذلك تنظيم ورش تدريبة للعاملين في الهيئات العامة والخاصة من اجل احاطة بالمعارف حول صور الثقافة التقنية والاستخدام الامثل لها في تنظيم الامور الحياتية وعدم استغلال كفاءتها في انتهاك حقوق الانسان.

المصادر والمراجع

أولا: المصادر باللغة العربية

الكتب

١. د. سعيداني نعيم، الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)، ط ١، المؤسسة الحديثة للكتاب، لبنان، ٢٠٢٣.

٢. د. وليد سليم النمر، حماية الخصوصية في الإنترنت، ط١، دار الفكر الجامعي، الاسكندرية، مصر، ٢٠١٧.

البحوث

١. أ. م. د أنسام عوني رشيد، الحماية التقنية للمصنفات الرقمية، مجلة الدراسات حول فعلية القاعدة القانونية، الجزائر، العدد ٥٨، د م ، ٢٠٢٢.

٢. فايق عوضين، البصمة الرقمية ودورها في الكشف عن الجريمة، المجلة الجنائية القومية، مصر، المجلد ٦٦، العدد ١، ٢٠٢٣.

٣. هداية بوعزة، الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الإلكتروني، مجلة الدراسات والبحوث القانونية، الجزائر، المجلد ٣، العدد ٤، ٢٠١٨.

الاتفاقيات والبروتوكولات والمواثيق الدولية

١. الاعلان العالمي لحقوق الانسان (١٩٤٨)

٢. العهد الدولي الخاص بالحقوق المدنية والسياسية (١٩٦٦)

٣. الاتفاقية الاوروبية المحدثة رقم (+١٠٨) لعام (١٩٨١)

القوانين الدولية

١. قانون حرية المعلومات الالماني (٢٠٠٦)

٢. القانون الفرنسي بشأن حماية البيانات الشخصية رقم (١٧_٧٨) المعدل لسنة (٢٠١١) رقم (٣٣٤)

٣. قانون المجموعة الانمائية (SADC) لعام (٢٠١٢)

٤. قانون جالبون بشان حماية البيانات الشخصية رقم (٠٢٥) لسنة (٢٠٢٣)

التقارير الدولية

١. تقرير الجمعية العامة للأمم المتحدة، الدورة التاسعة والسبعون، بعنوان "مكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض الإجرامية "، A/79/460، ٢٠٢٤.

٢. تقرير مجلس حقوق الانسان، الدورة الرابعة والخمسون، الحق في الخصوصية في العصر الرقمي، A/HRC/RES/54/21، ٢٠٢٣.

المصادر الإلكترونية

١. اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية عبر الرابط الآتي:

(https://news.un.org/ar/story/2024/12/1137776?form=MG0AV3) تاريخ الزيارة ٢٤|٢|٢٠٢٥.

٢. تقرير المفوض السامي لحقوق الانسان، ما هي الحدود التي يجب فرضها؟ المرحلة التالية للذكاء الاصطناعي والتكنولوجيات الجديدة والناشئة من منظور حقوق الإنسان"، ٢٠٢٣، متوفر عبر الرابط الآتي: (https://www.ohchr.org/ar/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner) الزيارة ٢٥|٢|٢٠٢٥.

ثانياً: المصادر باللغة الانكليزية

1. Books

1. Daniel Castro and others , Report about Unlocking Encryption: Information Security and the Rule of Law Information Technology and Innovation Foundation , USA, 2016.
2. Daniel J. Solove , Understanding Privacy , Harvard University Press , first publishing , Printed in the United States of America , 2020.
3. Muhammad Sarfraz , Biometric Systems , published by IntechOpen, London, United Kingdom , 2021.
4. Umesh Hodeghatta and others , The Infosec Handbook An Introduction to Information Security, Apress , United State America , 2014.

5. Theses

1. Adekunle Adewumi ,'Adequate protection': An analysis of Nigeria's data protection laws within an emerging global data protection framework , Master Thesis , Faculty of Law , University of Victoria , London, 2022.
2. Giovanni De Meo , Personal Data Privacy and Protective Federal Legislation:: An Exploration of Constituent Position on the Need for Legislation to Control Data Reliant Organizations Collecting and Monetizing Internet-Obtained Personal Data Thesis of PhD , School of Leadership and Education Sciences , University of San Diego ,USA, 2021.

3. Research

1. Alvaro Arenas and others , How to keep your information secure? Toward a better understanding of users security behaviour , Technological Forecasting & Social Change , Volume 198 , 2024.
2. Ashley Dix , The International Legal Dynamics of Encryption , Lawfare Institute collaboration with the Brookings Institution , series Paper no 1609 , 2016.
3. Dino C Joseph, The Role of Biometrics in Enhancing Cyber security , International Journal of Research Publication and Reviews , Volume 5 , Issue 3 , 2024.
4. Dino C Joseph, The Role of Biometrics in Enhancing Cyber security , International Journal of Research Publication and Reviews , Volume 5 , Issue 3 , 2024.

5. Echegu Darlington Arinze and others , Advancements in Computer Virus Protection: From Origins to Future Trends , Eurasian Journal of Scientific and Applied Research , Volume 6 , Issue 1 , 2024.
6. Guide about Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders , publication by Global Partners Digital , London , 2017.
7. Gulyamov Said Saidakhrarovich and others ,The role and importance of encryption in modern legal systems , Law and Artificial Intelligence Journal ,Volume: 2, Issue 1 , 2023.
8. Justin Bryant , Africa in the Information Age: Challenges , Opportunities and Strategies for Data Protection and Digital Rights , Stanford Technology Law Review , Volume 24 , Issue 389, 2021.
9. Laura Grava , Personal Data Protection in the EU – Cooperation and Competences of EU and National Data Protection Institutions and Bodies ,Riga Graduate School of Law Research Papers ,Issue 18 , 2017.
10. Man YIP , Protecting consumers' personal data in the digital world: Protecting consumers' personal data in the digital world: Challenges and changes , Singapore Personal Data Protection Commission, 2018, P.115.
11. Måns Svensson and others , Digitalization and Privacy A systematic literature review , first Publishing , Lund University Internet Institute, Sweden , 2016.
12. Pashynskyi Volodymyr and others , Administrative-Legal Support for the Protection of Citizens' Personal Data: Contemporary Theoretical Approaches , Visegrad Journal on Human Rights , Issue 4 , 2023.
13. Petro Melnyk and others , Experiencing Personal Data Protection on the Internet and Its Possibilities of Recognition and Enforcement in Ukraine , Ius Humani: Law Journal , Volume 10 , Issue 2 , 2021.
14. Radi P. Romansky and others , Challenges of the digital age for privacy and personal data protection , Mathematical Biosciences and Engineering , Volume 17 , Issue 5 , 2020 .
15. Tim Jiam and others ,The Role of Data Anonymization in Protecting Customer Data: Examining the techniques and benefits of data anonymization in ensuring compliance with data protection regulations , 2024.
16. Yekini Nureni and others , Firewall Approach to Computer Network Security: Functional Viewpoint , International Journal of Advanced Networking and Applications , Volume 13 , Issue 3 , 2022.

4. International Reports

1. Report Resolution on surveillance technologies and protecting individuals' rights to privacy , 46th Closed Session of the Global Privacy Assembly, October 2024.
2. The Right to Privacy in the Digital Age: Meeting Report , Office of the United Nations High Commissioner for Human Rights , 2021.
3. Report about Encryption: A Matter of Human Rights , Amnesty International , 2016.
4. Wolfgang Schulz and others , Human Rights and Encryption , UNESCO, 2016.
5. Report about Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses , APEC Policy Support Unit , 2019.

6. Official Documents

1. Privacy Report in Africa 2023/2024 A Review of Policy Trends and Digital Outlook in Africa's Data Protection Landscape , first publishing, publication by the Lawyers' Hub.

2. Electronic Resources

1. 41st International Conference of Data Protection and Privacy Commissioners for more information visit this link:(https://globalprivacyassembly.org/41st-icdppc-closed-session-summary/) data of visit 3/2/2025.
2. For more information about International Ethics Committee visit this link:(https://www.members.issa.org/page/ISSAInternationalCommittees) data of visit 4/1/2025.
3. For more information About (ISSA) visit this link: (https://www.issa.org/) data of visit 4/1/2025.
4. For more information about ISO/IEC 27002 visit this link: (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en) data of visit 22/4/2025.
5. For more information about ISO/IEC 27018 visit this link: (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27018:ed-2:v1:en) data of visit 22/4/2025.
6. For more information about ISO/IEC 27701 visit this link: (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27701:ed-1:v1:en) data of visit 22/4/2025.
7. For more information about ISO/IEC 29100 visit this link: (https://www.iso.org/standard/85938.htmI) data of visit 22/4/2025.
8. Zhiheng Yi and others , Personal Privacy Protection Problems in the Digital Age , published on (https://arxiv.org/?form=MG0AV3) , 2022.

(1)Måns Svensson and others , Digitalization and Privacy A systematic literature review , first Publishing , Lund University Internet Institute, Sweden , 2016 , P. 63.

(2): لمزيد من المعلومات حول اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية عبر الرابط الآتي

(https://news.un.org/ar/story/2024/12/1137776?form=MG0AV3 تاريخ الزيارة ٢٤|٢|٢٠٢٥، وقت الزيارة ١:٠٦ صباحاً)

(3) تقرير الجمعية العامة للأمم المتحدة، الدورة التاسعة والسبعون، بعنوان "مكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض الإجرامية A/79/460.٢٠٢٤"، ص ١٠،

(4) المصدر نفسه، المادة ٦-٤.

(5) اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية، المواد ٢٥،٢٤،١٠،١٥،٢٠.

(6)A/ HRC/ RES/ 54/ 21 تقرير مجلس حقوق الانسان، الدورة الرابعة والخمسون، الحق في الخصوصية في العصر الرقمي، ص ٢، ٢٠٢٣.

(7) تقرير مجلس حقوق الانسان، مصدر سابق ص ٣-٢.

(8) تقرير المفوض السامي لحقوق الانسان، ما هي الحدود التي يجب فرضها؟ المرحلة التالية للذكاء الاصطناعي والتكنولوجيات الجديدة والناشئة من منظور حقوق الإنسان"، ٢٠٢٣، متوفر عبر الرابط الآتي: (https://www.ohchr.org/ar/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner وقت الزيارة ٤:٣٣ الزيارة ٢٥|٢|٢٠٢٥) صباحاً .

(9) Report Resolution on surveillance technologies and protecting individuals' rights to privacy , 46th Closed Session of the Global Privacy Assembly, October 2024, pp.1- 2.

(10) 41st International Conference of Data Protection and Privacy Commissioners for more information visit this link:(https://globalprivacyassembly.org/41st-icdppc-closed-session-summary/) data of visit 3/2/2025 , time of visit 4:00 pm.

(11) Radi P. Romansky and others , Challenges of the digital age for privacy and personal data protection , Mathematical Biosciences and Engineering , Volume 17 , Issue 5 , 2020 , P.5.

(12) For more information about International Ethics Committee visit this link:(https://www.members.issa.org/page/ISSAInternationalCommittees) data of visit 4/1/2025 , time of visit 7:00 pm.

(13) For more information About (ISSA) visit this link: (https://www.issa.org/) data of visit 4/1/2025 , time of visit 7:56 pm.

(14) For more information about ISO/IEC 27002 visit this link: (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en) data of visit 22/4/2025 time of visit 4:00 pm.

(15) For more information about ISO/IEC 27018 visit this link: (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27018:ed-2:v1:en) data of visit 22/4/2025 time of visit 5:00 pm.

(16) For more information about ISO/IEC 27701 visit this link: (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27701:ed-1:v1:en) data of visit 22/4/2025 time of visit 6:00 pm.

(17) For more information about ISO/IEC 29100 visit this link: (https://www.iso.org/standard/85938.htm l) data of visit 22/4/2025, time of visit 6:44 pm.

(18) The Right to Privacy in the Digital Age: Meeting Report , Office of the United Nations High Commissioner for Human Rights , 2021 , P.3.

(19) Petro Melnyk and others , Experiencing Personal Data Protection on the Internet and Its Possibilities of Recognition and Enforcement in Ukraine , Ius Humani: Law Journal , Volume 10 , Issue 2 , 2021 , P. 97.

(20) Zhiheng Yi and others , Personal Privacy Protection Problems in the Digital Age , published on (https://arxiv.org/?form=MG0AV3) , 2022 , pp. 7-8.

(21) Man YIP , Protecting consumers' personal data in the digital world: Protecting consumers' personal data in the digital world: Challenges and changes , Singapore Personal Data Protection Commission, 2018, P.115.

(22) Privacy Report in Africa 2023/2024 A Review of Policy Trends and Digital Outlook in Africa's Data Protection Landscape, first publishing, publication by the Lawyers' Hub, pp. 19_20.

(23) Daniel J. Solove , Understanding Privacy , Harvard University Press , first publishing , Printed in the United States of America , 2020 , P.2.

(24) Pashynskyi Volodymyr and others , Administrative-Legal Support for the Protection of Citizens' Personal Data: Contemporary Theoretical Approaches , Visegrad Journal on Human Rights , Issue 4 , 2023 , P. 57.

(25) د. سعيداني نعيم، الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)، ط ١، المؤسسة الحديثة للكتاب، لبنان، ص ٥٢٤، ٢٠٢٣.

(26) Justin Bryant , Africa in the Information Age: Challenges , Opportunities and Strategies for Data Protection and Digital Rights , Stanford Technology Law Review , Volume 24 , Issue 389, 2021 , P. 396.

(27) Giovanni De Meo , Personal Data Privacy and Protective Federal Legislation:: An Exploration of Constituent Position on the Need for Legislation to Control Data Reliant Organizations Collecting and Monetizing Internet-Obtained Personal Data Thesis of PhD , School of Leadership and Education Sciences , University of San Diego ,USA, 2021 , P.35.

(28) د. وليد سليم النمر، حماية الخصوصية في الإنترنت، ط١، دار الفكر الجامعي، الاسكندرية، مصر، ص٦٠٤ -٦١٠، ٢٠١٧.

(29) Laura Grava , Personal Data Protection in the EU – Cooperation and Competences of EU and National Data Protection Institutions and Bodies ,Riga Graduate School of Law Research Papers ,Issue 18 , 2017 , P.35.

(30) د. وليد سليم النمر، حماية الخصوصية في الإنترنت، مصدر سابق، ص ٥٦٢ وبعدها.

(31) د. وليد سليم النمر، المصدر نفسه، ص ٦٣١.

(32) Adekunle Adewumi ,'Adequate protection': An analysis of Nigeria's data protection laws within an emerging global data protection framework , Master Thesis , Faculty of Law , University of Victoria, 2022 , P. 72.

(33) أ. م. د أنسام عوني رشيد، الحماية التقنية للمصنفات الرقمية، مجلة الدراسات حول فعلية القاعدة القانونية، الجزائر، العدد ٥٨، د م ، ص ٨٥، ٢٠٢٢.

(34) Report about Encryption: A Matter of Human Rights , Amnesty International , 2016 , P.14.

(35) Wolfgang Schulz and others , Human Rights and Encryption , UNESCO , 2016 , P.4.

(36) Daniel Castro and others , Report about Unlocking Encryption: Information Security and the Rule of Law Information Technology and Innovation Foundation , USA, 2016 , P.4.

(37) Guide about Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders , publication by Global Partners Digital , London , 2017 , P.15.

(38) Gulyamov Said Saidakhrarovich and others ,The role and importance of encryption in modern legal systems , Law and Artificial Intelligence Journal ,Volume: 2, Issue 1 , 2023 , P. 2.

(39) Ashley Dix , The International Legal Dynamics of Encryption , Lawfare Institute collaboration with the Brookings Institution , series Paper no 1609 , 2016 , P. 6.

(40) اختصار الاحرف الاولى ل Trusted Data Format.

(41) Report about Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses , APEC Policy Support Unit , 2019 , P. 2.

(42) Dino C Joseph, The Role of Biometrics in Enhancing Cyber security , International Journal of Research Publication and Reviews , Volume 5 , Issue 3 , 2024 , P.3.

(43) فايق عوضين، البصمة الرقمية ودورها في الكشف عن الجريمة، المجلة الجنائية القومية، مصر، المجلد ٦٦، العدد ١، ص ١٧، ٢٠٢٣.

(44) Muhammad Sarfraz , Biometric Systems , published by IntechOpen, London, United Kingdom , 2021 , P.105.

(45) هداية بوعزة، الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الإلكتروني، مجلة الدراسات والبحوث القانونية، الجزائر، المجلد ٣، العدد ٤، ص ٣٥، ٢٠١٨.

(46) Umesh Hodeghatta and others , The Infosec Handbook An Introduction to Information Security, Apress , United State America , 2014 , P.223.

(47) Yekini Nureni and others , Firewall Approach to Computer Network Security: Functional Viewpoint , International Journal of Advanced Networking and Applications , Volume 13 , Issue 3 , 2022 , pp. 4996 – 4999.

(48) Tim Jiam and others ,The Role of Data Anonymization in Protecting Customer Data: Examining the techniques and benefits of data anonymization in ensuring compliance with data protection regulations , 2024 ,pp.3-4.

(49) Alvaro Arenas and others , How to keep your information secure? Toward a better understanding of users security behaviour , Technological Forecasting & Social Change , Volume 198 , 2024 , P. 3.

(50) Echegu Darlington Arinze and others , Advancements in Computer Virus Protection: From Origins to Future Trends , Eurasian Journal of Scientific and Applied Research , Volume 6 , Issue 1 , 2024 , pp. 14-15.