

الإطار القانوني لحماية البيانات الشخصية في فلسطين في ضوء المعايير الدولية The Legal Framework for Personal Data Protection in Palestine in Light of International Standards

رمزي عوني محمود إبراهيم *

جامعة كوتاهيا دولوبينار، كوتاهيا، تركيا
dr.ramzi.ibrahim@gmail.com

أ.م.د. نظام الدين أيدن

جامعة كوتاهيا دولوبينار، كوتاهيا، تركيا
nizamettin.aydin@dpu.edu.tr

تاريخ الارسال: 2025/10/19

تاريخ القبول: 2025/11/14

تاريخ النشر: 2025/12/30

ملخص:

يهدف هذا البحث إلى دراسة الإطار القانوني لحماية البيانات الشخصية في فلسطين في ضوء المعايير الدولية، وذلك من خلال تحليل النصوص القانونية الوطنية ذات الصلة ومقارنتها بالتجارب الدولية. تكمن أهمية البحث في تناوله لموضوع حديث ومعقد يتصل بالحقوق في الخصوصية الرقمية، وفي إبراز مدى توافق التشريعات الفلسطينية مع الالتزامات الدولية ذات الصلة بحماية البيانات الشخصية، خصوصاً في ظل غياب قانون وطني شامل ينظم هذا المجال. اعتمدت هذه الدراسة على المنهج الوصفي التحليلي في تناول وتحليل النصوص القانونية الفلسطينية ذات الصلة بحماية الخصوصية والبيانات الرقمية. توصلت الدراسة إلى أن الإطار القانوني الفلسطيني ما يزال جزئياً وغير متكامل، إذ تقتصر الحماية الحالية على النصوص الدستورية العامة وبعض التشريعات القطاعية كقانون الجرائم الإلكترونية لسنة 2018، دون وجود منظومة موحدة تُعنى بحماية البيانات ومعالجتها. وانتهت الدراسة إلى التوصية بضرورة سن قانون فلسطيني خاص بحماية البيانات الشخصية، يستند إلى المبادئ الدولية، ويؤسس لهيئة رقابية مستقلة، بما يعزز الثقة في البيئة الرقمية ويحمي الحقوق الأساسية للأفراد.

كلمات مفتاحية: حماية البيانات الشخصية، الإطار القانوني الفلسطيني، الخصوصية الرقمية، المعايير

الدولية

Abstract:

This study examines the legal framework for personal data protection in Palestine in light of international standards, through an analytical review of national legal provisions and a comparative assessment of international experiences. The importance of the study lies in addressing a contemporary and complex issue related to the right to digital privacy, and in assessing the extent to which Palestinian legislation aligns with global obligations in the absence of a comprehensive national data protection law. Using the descriptive-analytical method, the study analyzes Palestinian legal texts related to privacy and digital data. The findings indicate that the current framework remains partial and fragmented, limited to constitutional guarantees and sectoral laws such as the 2018 Cybercrime Law, without a unified regulatory system. The study recommends enacting a specific Palestinian data protection law based on international principles and establishing an independent supervisory authority to strengthen trust in the digital environment and protect fundamental rights.

Keywords: Personal Data Protection, Palestinian Legal Framework, Digital Privacy, International Standards

*المؤلف المرسل

مقدمة

يشكل الحق في الخصوصية وحماية البيانات الشخصية أحد المرتكزات الجوهرية لحقوق الإنسان في العصر الرقمي، حيث أصبحت المعلومات الشخصية أداة ذات قيمة عالية في مختلف المجالات الاقتصادية والأمنية والسياسية. ومع التطور المتسارع لتقنيات الاتصال والمعلومات، تزايدت التحديات المتعلقة بكيفية جمع البيانات الشخصية ومعالجتها وتخزينها واستخدامها، الأمر الذي استدعى تدخل المنظومات القانونية الدولية والإقليمية لوضع معايير تضمن التوازن بين متطلبات التطور التكنولوجي وصون الكرامة الإنسانية.

وقد برز الاهتمام الدولي بحماية البيانات الشخصية منذ منتصف القرن العشرين، بدءاً من النصوص التأسيسية لحقوق الإنسان، كالإعلان العالمي لحقوق الإنسان لعام 1948، والعهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966، وصولاً إلى التشريعات الإقليمية الرائدة كالاتحاد الأوروبي الذي أرسى إطاراً قانونياً متكاملاً من خلال اللائحة العامة لحماية البيانات (GDPR) لعام 2016، فضلاً عن مبادرات منظمات دولية أخرى مثل منظمة التعاون الاقتصادي والتنمية والأمم المتحدة.

أما في السياق الفلسطيني، فإن مسألة حماية البيانات الشخصية تكتسب خصوصية مضاعفة بالنظر إلى الواقع القانوني والسياسي المعقد، وارتباطه بمرحلتين تاريخيتين الأولى، ما قبل تأسيس السلطة الوطنية الفلسطينية، حيث غابت التنظيمات الخاصة بالخصوصية الرقمية؛ والثانية، ما بعد عام 1994، حيث سعت التشريعات الوطنية إلى مواكبة التحولات الرقمية، دون أن تتبلور بعد منظومة قانونية شاملة لحماية البيانات الشخصية. تتجلى إشكالية الدراسة في التساؤل الرئيس الآتي:

ما مدى كفاية الإطار القانوني الفلسطيني في حماية البيانات الشخصية في ضوء المعايير الدولية؟
وتتفرع عن هذه الإشكالية مجموعة من الأسئلة الفرعية، من أبرزها:

- ما هو الأساس المفاهيمي والقانوني للحق في الخصوصية وحماية البيانات الشخصية؟
- كيف تطورت الأطر القانونية الدولية والإقليمية في هذا المجال؟
- إلى أي مدى تنسجم النصوص القانونية الفلسطينية مع المعايير الدولية ذات الصلة؟

تهدف هذه الدراسة إلى تحليل الإطار القانوني لحماية البيانات الشخصية في فلسطين، ومقارنته بالمعايير الدولية والإقليمية، بما يتيح تقييم مدى توافق التشريعات الوطنية مع التزامات الدولة الفلسطينية في مجال حقوق الإنسان. كما تسعى إلى تحديد مكامن القوة والقصور في التنظيم القانوني القائم دون أن تدّعي سدّ الفراغ القانوني، بل تسعى إلى المساهمة العلمية في فهم وتحليل الواقع القانوني وتطوره.

تتجلى أهمية الدراسة في كونها تجمع بين التحليل النظري للنصوص القانونية والمقاربة المقارنة مع التجارب الدولية، بما يتيح إثراء النقاش حول بناء منظومة وطنية فعالة لحماية البيانات الشخصية في فلسطين وفقاً للمعايير الدولية المعاصرة.

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي في تناول وتحليل النصوص القانونية الفلسطينية ذات الصلة بحماية الخصوصية والبيانات الرقمية، وذلك من خلال استقراء القوانين والقرارات بقوانين الصادرة، وتفسير مضامينها بهدف تحديد أوجه القوة والقصور فيها. وبناءً على ما تقدم، تنقسم الدراسة إلى قسمين رئيسيين: أولاً: الإطار الدولي لحماية الحق في الخصوصية وحماية البيانات الشخصية، ويتضمن ثلاثة فصول رئيسية تتناول المفاهيم، والتطور التاريخي، والتنظيمات القانونية الدولية والإقليمية.

ثانياً: الحماية القانونية للبيانات الشخصية في فلسطين، ويتناول الإطار الدستوري والجزائي والتنظيمي في التشريعات الفلسطينية، مع تحليل مستوى انسجامها مع المعايير الدولية.

أولاً: الإطار الدولي لحماية الحق في الخصوصية وحماية البيانات الشخصية

1. الحق في الخصوصية: المفهوم والنطاق

تُعد الخصوصية حقاً يمتلكه الإنسان منذ ولادته، وهي محمية بموجب المعايير الدولية لحقوق الإنسان. كما أن العديد من الدساتير الوطنية والقوانين في مختلف الدول تكفل حماية هذا الحق. ولا يُنظر إلى الحق في الخصوصية بوصفه حقاً مستقلاً فحسب، بل يُعتبر أيضاً أساساً مهماً لضمان باقي الحقوق الأساسية للإنسان، ويُعد من الركائز الأساسية للمجتمعات الديمقراطية¹. ووفقاً للأمم المتحدة، فإن الحق في الخصوصية لا يُصنف فقط ضمن حقوق الإنسان، بل يرتبط أيضاً ارتباطاً وثيقاً بحقوق أخرى أساسية، مثل حرية التعبير، وحق التجمع السلمي، وحرية تكوين الجمعيات، والحق في الصحة، والحق في الأمن الجسدي².

لم تقدّم أغلب الوثائق الرسمية سواء على المستوى الدولي أو الإقليمي أو الوطني تعريفاً شاملاً ودقيقاً للحق في الخصوصية، ولم تُوضح جميع عناصر هذا الحق بشكل مفصل. ومع ذلك، فإن غياب مثل هذا التعريف لا يقلل بأي حال من الأهمية الجوهرية للخصوصية كحق أساسي من حقوق الإنسان³. ونظراً لأن مفهوم الخصوصية يتمتع بطبيعة ديناميكية، فإن تطور الوسائل التي قد تهدد هذا المفهوم بمرور الوقت جعل من الصعب تحديده بدقة. فعلى سبيل المثال، كانت الخصوصية في الماضي تقتصر فقط على المراسلات البريدية التقليدية، ثم شملت لاحقاً رسائل البرق، وفي الوقت الحاضر أصبحت وسائل الاتصال الرقمية مثل البريد الإلكتروني من بين التهديدات التي تواجه الخصوصية⁴.

بشكل عام، فإن الاختلافات في تعريف مفهوم الخصوصية وعناصره لا تُعيق جمع هذا المفهوم تحت تعريف واحد شامل. بل إن هذا التنوع يُساهم في توفير حماية أوسع لحق الخصوصية، لأنه يُوسّع نطاق المفهوم ويُعزز ضمان حرية الأفراد. ومع ذلك، لا تزال هناك تعريفات عامة متعددة للخصوصية، ورغم استنادها إلى مقاربات فلسفية مختلفة، إلا أنها تتضمن العناصر الأساسية لهذا الحق. فعلى سبيل المثال، يُعرّف "معهد القانون الأمريكي" الخصوصية على أنها حق الفرد في عدم الكشف عن شؤونه وظروفه الشخصية للآخرين. وبالمثل، عبّر مؤتمر القانونيين الذي عُقد في ستوكهولم عام 1967 عن الخصوصية بأنها حق الفرد في اتخاذ القرار بشأن شؤونه الخاصة ومن يمكنه الوصول إلى تلك المعلومات⁵.

وبشكل عام، يمكن تعريف الخصوصية على أنها حق الفرد في السيطرة على جسده ومجاله الشخصي ومعلوماته وبياناته وعلاقاته الخاصة. وهذا الحق يمنع الأفراد أو الدولة من الوصول إلى هذه المعلومات أو استخدامها بدون موافقة الشخص المعني، ما لم يكن ذلك من أجل حماية حقوق الآخرين أو لتحقيق مصلحة عامة مشروعة وفي حدود ما يُقبله المجتمع الديمقراطي. وفي هذا السياق، تشمل الخصوصية خصوصية المعلومات، وخصوصية الجسد، وخصوصية الاتصالات والمراسلات، وكذلك الخصوصية المكانية⁶.

2. النشأة والتطور الدولي لحماية البيانات الشخصية

قبل تناول الوضع القانوني المتعلق بحماية البيانات الشخصية، من المهم تحديد الاتفاقيات الدولية التي تتناول هذه البيانات، ومعرفة متى تم الاعتراف بها لأول مرة كمفهوم قانوني. لقد تم تضمين المبادئ المتعلقة بحماية البيانات الشخصية لأول مرة على المستوى الدولي في الإعلان العالمي لحقوق الإنسان الذي اعتمدته الأمم المتحدة في 10 ديسمبر 1948⁷. كما تناول الاتفاق الأوروبي لحقوق الإنسان، الذي تم اعتماده في 4 نوفمبر 1950، قضايا تتعلق بحماية البيانات الشخصية. فقد نصت المادة الثامنة من الاتفاقية، التي تهدف إلى حماية الحريات الأساسية، على "ضمان حماية الحياة الخاصة والحياة الأسرية والمسكن والمراسلات". وقد مهدت هذه الاتفاقيات الطريق للتشريعات القانونية اللاحقة المتعلقة بحماية البيانات الشخصية، وشكلت الأساس للتنظيمات الوطنية والدولية في هذا المجال⁸.

منذ ستينيات القرن الماضي، سهلت التطورات السريعة في تقنيات المعلومات والاتصالات جمع البيانات الشخصية ومعالجتها، مما زاد من الحاجة إلى حماية خصوصية الأفراد. وقد بدأت الحاجة إلى تقييم البيانات الشخصية في سياق الخصوصية وحمايتها قانونياً تُناقش منذ سبعينيات القرن الماضي. وعلى الرغم من أن هذه المناقشات ظهرت أولاً في الولايات المتحدة الأمريكية، إلا أن أول تنظيم قانوني في هذا المجال تم في ألمانيا. ففي عام 1970، أقرت ولاية هيسن "قانون حماية البيانات"، مما سلط الضوء على أهمية حماية البيانات الشخصية⁹.

وبعد هذا التنظيم، تسارعت الجهود المبذولة في جميع أنحاء العالم لحماية البيانات الشخصية. وفي عام 1973، أصبحت السويد أول دولة تُصدر قانوناً وطنياً لحماية البيانات الشخصية، لتأخذ زمام المبادرة في هذا المجال. وفي عام 1980¹⁰، أصدرت دول منظمة التعاون الاقتصادي والتنمية (OECD) أول تقرير دولي حول حماية البيانات¹¹، مما أعطى لهذه المبادرات بُعداً عالمياً¹⁴.

3. الإطار الدولي والإقليمي لحماية البيانات الشخصية

مع تزايد الاعتماد على التقنيات الرقمية وتوسع استخدام البيانات في شتى مجالات الحياة، برزت الحاجة الماسة إلى وضع أطر قانونية تنظم عملية جمع ومعالجة وتخزين البيانات الشخصية، وتضمن احترام خصوصية الأفراد. ولم تعد حماية البيانات مسألة وطنية فحسب، بل أصبحت قضية دولية تتطلب تعاوناً عابراً للحدود، نظراً للطبيعة العالمية لتدفق المعلومات عبر الإنترنت.

في هذا السياق، تبنت العديد من المنظمات الدولية والإقليمية تشريعات واتفاقيات تهدف إلى وضع معايير موحدة لحماية البيانات الشخصية، وضمان التوازن بين حرية تداول المعلومات وحقوق الأفراد في الخصوصية. وقد تميز الاتحاد الأوروبي بوضع أكثر الأطر القانونية شمولاً وتطوراً، بينما ساهم كل من مجلس أوروبا، والأمم المتحدة، والولايات المتحدة الأمريكية، ومنظمة التعاون الاقتصادي والتنمية (OECD) في تطوير سياسات ومبادئ أساسية شكلت الأساس القانوني العالمي في هذا المجال.

ومن خلال دراسة هذه الأطر، يمكن فهم الاتجاهات القانونية الدولية في حماية البيانات الشخصية، واستخلاص الدروس التي يمكن الاستفادة منها في تطوير التشريعات الوطنية.

1.3. تطور الإطار القانوني لحماية البيانات الشخصية في الاتحاد الأوروبي

تأسس الاتحاد الأوروبي في عام 1951 مع إنشاء الجماعة الأوروبية للفحم والصلب من قبل ست دول. وقد تجاوز هذا المسار نطاق التكامل الاقتصادي، ليتناول أيضاً مسألة حماية حقوق الأفراد.

تم تنظيم حماية البيانات الشخصية بموجب التوجيه رقم EC/46/95 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 24 أكتوبر 1995. يتضمن هذا التنظيم أحكاماً تتعلق "بحماية الأفراد فيما يخص معالجة البيانات الشخصية والتنقل الحر لهذه البيانات"¹². وبالاستناد إلى معاهدة إنشاء الجماعة الأوروبية، ولا سيما المادة 100(أ) منها، واستناداً إلى اقتراح المفوضية الأوروبية، ورأي اللجنة الاقتصادية والاجتماعية، ووفقاً للإجراءات المنصوص عليها في المادة 189(ب) من المعاهدة، تُعد حماية البيانات الشخصية حقاً أساسياً في العالم الرقمي المعاصر. وفي هذا السياق، تُعتبر سياسات وتطورات الاتحاد الأوروبي بشأن حماية البيانات الشخصية ذات أهمية كبيرة. وفيما يلي بعض المبادئ والممارسات المهمة المتعلقة بحماية البيانات الشخصية في الاتحاد الأوروبي¹³. بالإشارة إلى معاهدة إنشاء الجماعة الأوروبية، ولا سيما المادة 100(أ) منها، وإلى اقتراح المفوضية الأوروبية، ورأي اللجنة الاقتصادية والاجتماعية، ووفقاً للإجراءات المنصوص عليها في المادة 189(ب) من المعاهدة، تُعد حماية البيانات الشخصية حقاً أساسياً في العالم الرقمي المعاصر. وفي هذا السياق، تحظى سياسات وتطورات الاتحاد الأوروبي المتعلقة بحماية البيانات الشخصية بأهمية كبيرة. وفيما يلي بعض المبادئ والممارسات المهمة المتعلقة بحماية البيانات الشخصية في الاتحاد الأوروبي¹⁴.

تمتلك الدول الأعضاء السلطة لتعريف حالات المعالجة بشكل أكثر دقة من خلال التشريعات التي تعتمد عليها بموجب هذه التوجيهات. كما تمتلك الدول الأعضاء السلطة لضمان حماية الأفراد من خلال قانون عام يتعلق بمعالجة البيانات الشخصية. تعكس مبادئ الحماية، من ناحية، التزامات مثل جودة البيانات، والأمن الفني، وإبلاغ السلطة الرقابية؛ ومن ناحية أخرى، يجب منح الأفراد الذين تتم معالجة بياناتهم حقوقاً في الاطلاع على البيانات، وطلب التصحيح، وفي بعض الحالات الاعتراض على المعالجة¹⁵.

يجب أن تتم معالجة البيانات الشخصية بموافقة صاحب البيانات أو في إطار مهمة تُنفذ لصالح المصلحة العامة؛ وفي هذه الحالة، يجب ألا تُفقد حقوق وحريات صاحب البيانات التوازن¹⁶. تم تطوير سياسات

الاتحاد الأوروبي المتعلقة بحماية البيانات الشخصية لضمان حقوق الأفراد وتحقيق الأمن في البيئة الرقمية. تهدف القوانين المتعلقة بمعالجة البيانات الشخصية إلى حماية خصوصية الأفراد وضمان الأمن العام. وتلعب هذه التوازنات دوراً حاسماً في مستقبل أوروبا الرقمي.

2.3. الإطار الأممي لحماية البيانات الشخصية

يُعَدُّ الإطار الأممي لحماية البيانات الشخصية أحد الركائز الأساسية في تطور القانون الدولي لحقوق الإنسان، إذ يهدف إلى ضمان التوازن بين حرية تداول المعلومات وحماية الخصوصية الفردية. وقد بدأ الاهتمام العالمي بهذا المجال منذ منتصف القرن العشرين، حينما تم إدراج مبادئ حماية الحياة الخاصة ضمن الإعلان العالمي لحقوق الإنسان الذي اعتمدته الجمعية العامة للأمم المتحدة بتاريخ 10 ديسمبر 1948، حيث نصّت المادة (12) منه على أنه: "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته..."، وهو ما يُعَدُّ أول اعتراف أممي بحق الأفراد في حماية بياناتهم الشخصية¹⁷.

وفي ذات السياق، جاء الاتفاق الأوروبي لحقوق الإنسان لعام 1950 ليُكرِّس هذا المبدأ من خلال المادة (8)، التي تضمن لكل إنسان الحق في احترام حياته الخاصة والعائلية، وتضع قيوداً صارمة على تدخل السلطات العامة في هذا الحق إلا في الحالات التي تقتضيها المصلحة العامة وبما يتفق مع القانون¹⁸.

وفي تطور لاحق، اعتمدت العديد من الدول تشريعات وطنية في ضوء المبادئ الأممية، مثل قانون حماية البيانات في ولاية هسن الألمانية لعام 1970، الذي يُعتبر أول قانون وطني في العالم ينظّم معالجة البيانات الشخصية ضمن إطار قانوني محدد، مما شكّل نقطة انطلاق نحو تقنين شامل لحماية الخصوصية الرقمية¹⁹.

وقد تعزز هذا التوجه من خلال توجيه الاتحاد الأوروبي رقم 46/95 /EC الصادر سنة 1995، الذي هدف إلى توحيد قواعد حماية البيانات الشخصية وضمان حرية انتقالها داخل السوق الأوروبية المشتركة، تمهيداً لاعتماد اللائحة العامة لحماية البيانات (GDPR) رقم 679/2016²¹، الصادرة عن الاتحاد الأوروبي عام 2016، والتي أصبحت النموذج الأكثر تطوراً وشمولية في مجال حماية البيانات على المستوى الدولي²².

ويُستخلص من هذا التطور أن الإطار الأممي لحماية البيانات الشخصية لا يقوم فقط على النصوص القانونية، بل يركز كذلك على مجموعة من المبادئ القانونية العالمية، مثل الشرعية، والشفافية، والمسؤولية، وتقيد الغرض، وهي المبادئ التي أصبحت تشكل أساس التشريعات الحديثة في هذا المجال.

3.3. التنظيمات القانونية الأمريكية لحماية البيانات الشخصية

تتبنّى الولايات المتحدة الأمريكية مقاربةً تنظيميةً متميزة في مجال حماية البيانات الشخصية، تختلف عن النماذج المعتمدة في كلّ من الاتحاد الأوروبي أو منظومة الأمم المتحدة. فحتى اليوم، لا يوجد تشريع اتحاديّ شاملٌ وموحّدٌ ينظّم بصورةٍ عامةٍ معالجة البيانات الشخصية وحمايتها في جميع القطاعات والمجالات. وبدلاً من

ذلك، تتكوّن البنية القانونية الأمريكية من مجموعة من التشريعات الفيدرالية المتخصصة إلى جانب قوانين الولايات المختلفة، التي تُعنى بتنظيم أنواع معيّنة من البيانات أو قطاعات محددة، الأمر الذي يُنتج نظاماً متشعباً ومتعدد المستويات في حماية الخصوصية²³.

يُعدّ التعديل الرابع للدستور الأمريكي أحد المرتكزات الدستورية الأولى التي أسهمت في ترسيخ مفهوم الحق في الخصوصية، إذ يحمي الأفراد من عمليات التفتيش والمصادرة غير المبرّرة من قبل السلطات. وقد تطوّر هذا المفهوم تدريجياً ليشمل لاحقاً حماية البيانات الشخصية في البيئة الرقمية²⁴.

كما يُعتبر قانون حماية بيانات الائتمان الصادر سنة 1970 أول تشريع فيدراليّ يُعنى بتنظيم جمع ومعالجة بيانات الأفراد، بما في ذلك ضمان دقّتها وحدود استخدامها، مما مهّد لظهور الإطار القانوني اللاحق لحماية الخصوصية في الولايات المتحدة²⁵.

نظراً لغياب تشريع اتحادي شامل، بادرت العديد من الولايات الأمريكية إلى سنّ قوانين خاصة بحماية خصوصية المستهلكين. ويُعد قانون حماية خصوصية المستهلك في كاليفورنيا من أبرز هذه القوانين، إذ يمنح الأفراد حقوقاً موسّعة في الوصول إلى بياناتهم الشخصية، ومعرفة الجهات التي تستخدمها، ومنع بيعها دون موافقتهم الصريحة. كما سنت بعض الولايات الأخرى تشريعات تتعلق بأمن البيانات وواجبات الإخطار في حالة حدوث خروقات أو تسريبات، بحيث تجاوز عدد الولايات التي تبنت تشريعاتٍ من هذا النوع خمساً وعشرين ولاية، في مسعى لتعزيز الحماية القانونية للبيانات ضمن الأطر المحلية رغم غياب الإطار الاتحادي العام²⁶.

4.3. الإطار التنظيمي لحماية البيانات الشخصية في منظمة التعاون الاقتصادي والتنمية

تأسست منظمة التعاون الاقتصادي والتنمية في عام 1960 بواسطة عشرين دولة مؤسّسة بهدف دعم التنمية الاقتصادية والتعاون. فيما يتعلق بحماية البيانات الشخصية، اتخذت المنظمة أول خطوة مهمة على الصعيد الدولي في عام 1980 بإصدار "المبادئ التوجيهية لحماية الحياة الخاصة وتدفق البيانات الشخصية عبر الحدود". يهدف هذا الوثيقة إلى تحديد المبادئ الأساسية لحماية البيانات الشخصية وضمان أمن تدفق البيانات على المستوى الدولي²⁷.

تتضمن المبادئ الثمانية التوجيهية التي حددتها منظمة التعاون الاقتصادي والتنمية ما يلي، مبدأ النقل من البيانات، ومبدأ جودة البيانات، ومبدأ تحديد الأغراض، ومبدأ تقييد الاستخدام، ومبدأ أمان البيانات، ومبدأ الشفافية، ومبدأ مشاركة الأفراد، ومبدأ المساءلة²⁸.

لم تكن هذه المبادئ مقتصرة على دول منظمة التعاون الاقتصادي والتنمية فقط، بل شكلت الأساس لكثير من التشريعات الوطنية والدولية المتعلقة بحماية البيانات الشخصية حول العالم. ومع تزايد الاحتياجات، قامت المنظمة بإصدار تنظيمات أكثر شمولاً مثل "الإعلان بشأن نقل البيانات عبر الحدود" و"إعلان الوزراء بشأن

حماية الخصوصية في الشبكة العالمية". وتُعد هذه الوثائق من الأدلة الدولية المهمة التي تهدف إلى مراقبة تدفق البيانات على نطاق عالمي وحماية خصوصية الأفراد²⁹.

لقد اتبعت اتحادات اقتصادية كبيرة مثل الاتحاد الأوروبي مبادئ منظمة التعاون الاقتصادي والتنمية فيما يخص حماية البيانات الشخصية، ووضعت تنظيمات تهدف إلى ضمان أمن البيانات الشخصية في إطار التعاون بين الدول. وفي هذا السياق، لم تقتصر مبادئ منظمة التعاون الاقتصادي والتنمية على دولها الأعضاء فحسب، بل شكّلت الأساس لتنظيمات دولية ملزمة أسهمت في تطوير معايير عالمية لحماية البيانات³⁰.

ثانياً: الحماية القانونية للبيانات الشخصية في فلسطين

1. الإطار القانوني لحماية البيانات الشخصية في فلسطين

إن الإطار القانوني الفلسطيني لحماية البيانات الشخصية يمثل نتاجاً لتطور تدريجي، بدأ بالحماية التقليدية المنصوص عليها في التشريعات الموروثة، وتدرج إلى ترسيخ الحماية الدستورية، ليختتم بالتشريعات المتخصصة التي تهدف إلى معالجة الفضاء الرقمي المتنامي. يعود تاريخ هذه الحماية إلى ما قبل تأسيس السلطة الوطنية، مروراً بالقانون الأساسي، والذي يُعتبر المرجعية العليا لكافة التشريعات اللاحقة.

1.1. الإطار القانوني التقليدي قبل تأسيس السلطة الوطنية الفلسطينية وحماية الخصوصية الرقمية

قبل قدوم السلطة الوطنية الفلسطينية عام 1994، كان الإطار القانوني السائد، وخاصة في الضفة الغربية، يعتمد بشكل كبير على القوانين الأردنية النافذة قبل عام 1967، وعلى رأسها قانون العقوبات الأردني رقم 16 لسنة 1960. هذا القانون تضمن نصوصاً تجرم انتهاك الخصوصية في سياقاتها التقليدية، مثل حرمة المسكن. على سبيل المثال، تناولت المادة 348 من قانون العقوبات الأردني جريمة التسلل إلى أماكن تخص الغير ليست مباحة للجمهور، وعاقبت عليها بالحبس أو بالغرامة³¹.

كانت هذه الحماية التقليدية قاصرة بطبيعتها عن توفير حماية فعالة وشاملة للبيانات الرقمية والمراسلات الإلكترونية. فالتجريم المتعلق بالتسلل المادي إلى الأماكن الخاصة لا يمكن أن يمتد ليشمل بشكل مباشر وواضح التسلل إلى الأنظمة المعلوماتية أو انتهاك سرية البيانات المخزنة إلكترونياً، مما أدى إلى وجود فراغ تشريعي واسع في المجال الرقمي استمر لعدة سنوات.

2.1. الإطار الدستوري لحماية الخصوصية والبيانات الشخصية في القانون الأساسي الفلسطيني

2003

يُعد القانون الأساسي الفلسطيني المعدل لسنة 2003 حجر الزاوية الذي وفر الأساس الدستوري لحماية الحريات العامة، بما في ذلك الحق في الخصوصية. وعلى الرغم من أن القانون لم يتناول مصطلح "حماية البيانات الشخصية" بشكل مباشر عند صدوره، إلا أنه رسخ مبادئ أساسية تم الاستناد إليها لاحقاً في مختلف التشريعات الفلسطينية الحديثة المتعلقة بالخصوصية وحماية البيانات. وقد أرسى هذا القانون ضمانات دستورية

عامة تحد من تدخل السلطات في حياة الأفراد، وهو ما يشكل الأساس لمفهوم حماية البيانات في العصر الرقمي.

تتمثل المواد الدستورية الأساسية لحماية الخصوصية في القانون الأساسي الفلسطيني في ثلاثة مواد رئيسية: المادة 11، والمادة 17، والمادة 32³².

تنص المادة 11 على أن "الحرية الشخصية حق طبيعي وهي مكفولة لا تمس"، كما تحدد أنه "لا يجوز القبض على أحد أو تفتيشه أو حبسه أو تقييد حريته بأي قيد أو منعه من التنقل إلا بأمر قضائي وفقاً لأحكام القانون". وتكمن أهمية هذه المادة في تقييد صلاحيات السلطة التنفيذية عند ممارسة أي إجراءات قد تؤثر على حرية المواطنين، بما في ذلك الإجراءات المتعلقة بالوصول إلى بياناتهم الشخصية أثناء عمليات التفتيش أو التحقيق. وبذلك، تمثل المادة 11 ضماناً أساسياً لحرية الأفراد في مواجهة تدخل الدولة في حياتهم الخاصة.

أما المادة 17 فتتعلق بحرمة المساكن، حيث تنص على أن "للمساكن حرمة، فلا تجوز مراقبتها أو دخولها أو تفتيشها إلا بأمر قضائي مسبب ووفقاً لأحكام القانون". وتضيف هذه المادة ركيزة قانونية مهمة للتعويض عن الانتهاكات، إذ تكفل للمواطنين المتضررين الحصول على تعويض عادل في حال خرق حرمة مساكنهم، وهو ما يعزز من حماية الحياة الخاصة ويحد من التجاوزات على حقوق الأفراد في أماكنهم الشخصية.

وتعتبر المادة 32 النص الدستوري الأقوى والأكثر مباشرة في مجال حماية الخصوصية وحماية البيانات ضمن الإطار الفلسطيني، حيث تنص على أن "كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع عليه الضرر".

تعكس صياغة المادة 32 إدراكاً عميقاً لأهمية حماية الحقوق الأساسية، خصوصاً حرمة الحياة الخاصة، إذ لم تقتصر الحماية على ضمان التعويض العادل فقط، بل ربطت هذه الحماية بضمانة قانونية استثنائية، وهي عدم سقوط الدعوى الجنائية والمدنية بالتقادم. وتمثل هذه الميزة رادعاً قانونياً قوياً، يضمن مساءلة الجهات المخالفة عن أي انتهاك لحرمة الحياة الخاصة، بما يشمل ضمناً حماية البيانات الرقمية، حتى بعد مرور فترة زمنية طويلة قد تصل إلى عقود، وهو ما يوفر قاعدة صلبة لملاحقة أي اعتداء على الخصوصية الرقمية وفقاً للقانون الفلسطيني.

3.1. الإطار الجزائي لحماية البيانات الشخصية في فلسطين

في ظل غياب قانون شامل ومحدد لحماية البيانات الشخصية لفترة طويلة، حاول المشرع الفلسطيني معالجة الفجوة التشريعية من خلال إصدار قرارات بقوانين متخصصة شملت المجالات الجنائية، والتجارية، وتنظيم قطاع الاتصالات. مثلت هذه التشريعات جسراً وصل بين الحماية الدستورية العامة وحماية البيانات الرقمية المنظمة في القوانين اللاحقة، لتوفير حد أدنى من الضمانات القانونية لحماية حقوق الأفراد الرقمية.

في هذا الإطار، جاء قرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية ليشكل الركيزة الأساسية للحماية الجزائية للبيانات المخزنة والمعالجة إلكترونياً. وقد قدم هذا القرار تعريفات قانونية حاسمة لمصطلحات مثل "البيانات"، و"الدخول غير المشروع"، و"الشبكة المعلوماتية"، مؤسساً لتجريم الأفعال التي تمس سلامة البيانات وسريتها.

وتضمنت نصوص العقوبات في المادة 3 من القرار بقانون رقم 10 لسنة 2018³³ ما يلي:
أولاً، تجريم إفشاء ونقل البيانات بعد الدخول غير المشروع، حيث نصت الفقرة 3 من المادة 3 على أنه:
"إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو حذفها أو إضافتها أو إفشاؤها أو إتلافها أو تغييرها أو نقلها أو التقاطها أو نسخها أو نشرها أو إعادة نشرها، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلا العقوبتين."

ثانياً، تجريم الإفشاء بقصد الحصول على منافع، حيث نصت الفقرة 4 من المادة 3 على أنه: "إذا تم ارتكاب الأفعال المنصوص عليها في أحكام هذه المادة بقصد الحصول على أموال أو بيانات غيره أو ما يتيح من خدمات، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلا العقوبتين."

كما نصت المادة 8 على تجريم فك البيانات المشفرة أو استخدام أدوات التشفير أو التوقيع الإلكتروني الخاصة بالغير بطريقة غير قانونية، بعقوبات تصل إلى الحبس لمدة سنة والغرامة التي تصل إلى ثلاثة آلاف دينار أردني.

ورغم الدور المهم الذي لعبه القانون في توفير الحماية الجزائية للبيانات، فقد واجه انتقادات حقوقية، إذ أشارت التقارير إلى أن القرار منح صلاحيات واسعة للنسابة العامة ومأموري الضبط القضائي لضبط وتفتيش الأجهزة والرسائل الإلكترونية لفترات غير محددة. وقد يشكل استغلال هذه الصلاحيات بشكل واسع انتهاكاً للخصوصية والحقوق الدستورية للأفراد، لا سيما النشاط والمحتجين، ما يثير تساؤلات جدية حول التوازن بين حماية البيانات الرقمية وسلطة الدولة في الوصول إليها³⁴.

4.1. الإطار التنظيمي لحماية البيانات التجارية والقطاعية في فلسطين

يمثل قرار مجلس الوزراء رقم 3 لسنة 2019³⁵م نقطة تحول مهمة في الإطار القانوني لحماية البيانات الشخصية، إذ ركز على الجوانب التجارية المباشرة، مسلطاً الضوء على ضرورة حماية بيانات المواطنين من الاستغلال التجاري غير المصرح به من قبل الشركات والمؤسسات الخاصة. ويعكس هذا القرار الوعي المتزايد بأهمية حماية الخصوصية في المجال التجاري، مع وضع أسس قانونية واضحة للالتزام بالموافقة المسبقة.

تنص المادة الأولى من القرار على حظر الاستغلال التجاري للبيانات الشخصية للمواطنين دون إذن مسبق، سواء كانت البيانات مباشرة أو غير مباشرة، مؤكداً على المسؤولية القانونية للجهات المخالفة. يُظهر هذا

التنظيم التطور التشريعي من الردع الجنائي في القرارات السابقة إلى الحوكمة والتنظيم الوقائي الذي يضمن حماية الحقوق الفردية ويحدد شروط الاستخدام القانوني للبيانات.

فيما يتعلق بالحماية القطاعية، جاء قرار بقانون رقم 37 لسنة 2021 بشأن الاتصالات وتكنولوجيا المعلومات ليضع إطاراً مؤسسياً وتنظيماً للقطاع، مع التركيز على التزامات المرخص لهم تجاه المستهلك وحماية بياناته. يعرف القانون "بيانات المشتركين" بأنها المعلومات التي تحدد هويتهم بشكل مباشر أو غير مباشر، ويشير إلى بيانات الحركة التي تُعالج لغرض توصيل الاتصالات مع استثناء محتوى الاتصالات نفسه، ما يعزز حماية خصوصية المستخدمين ضمن قطاع الاتصالات.

تنص المادة 52 على التزامات المرخص لهم بتوفير خدمات الاتصالات العامة بما يضمن حماية المستهلك، وذلك عبر إبرام عقود اشتراك واضحة ومفهومة تتضمن جميع شروط الخدمة، مع اعتماد هذه العقود من الهيئة المختصة. هذا الإجراء يعكس حرص التشريع على أن تكون حماية البيانات جزءاً لا يتجزأ من تنظيم القطاع.

علاوة على ذلك، يؤكد القانون على تأسيس "هيئة تنظيم قطاع الاتصالات" كجهة رقابية وتنظيمية مستقلة، تتولى مسؤولية الإشراف على التزام الشركات بتقديم خدمات بمعايير عالمية، وضمان حقوق المستخدمين وحماية بياناتهم، بما يرسخ دور الدولة في تنظيم القطاع وفرض الالتزام بالقوانين وحماية الخصوصية.

الخاتمة

يتضح من خلال الدراسة أن حماية البيانات الشخصية تمثل عنصراً جوهرياً في الحفاظ على الحريات الفردية وضمان أمن المعلومات في البيئة الرقمية. ويظهر القانون الأساسي الفلسطيني المعدل لسنة 2003 كقاعدة دستورية مهمة لحماية الحق في الخصوصية، من خلال المواد 11 و17 و32، التي كرست مبدأ حرمة الحياة الخاصة والحقوق الفردية العامة، وضمنت حماية المواطنين من أي اعتداء على حرياتهم أو ممتلكاتهم الشخصية.

ومع ذلك، فإن حماية البيانات الرقمية في فلسطين لم تتضج بعد لتصبح شاملة وموحدة، بل اعتمدت على مجموعة من القرارات بقوانين والتشريعات التنظيمية القطاعية. من أبرزها قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، الذي أسس للحماية الجزائية للبيانات المخزنة والمعالجة إلكترونياً، وقرار مجلس الوزراء رقم 3 لسنة 2019 المتعلق بحماية البيانات التجارية، إضافة إلى قانون تنظيم قطاع الاتصالات رقم 37 لسنة 2021، الذي وضع إطاراً لتنظيم البيانات في قطاع الاتصالات.

عند مقارنة الإطار الفلسطيني بالإطارات الدولية، يظهر عدد من النقاط الجوهرية التي تبرز الفروقات والتحديات. يعتمد الاتحاد الأوروبي على تشريعات شاملة، مثل التوجيه EC/46/95 واللائحة العامة لحماية البيانات (GDPR)، التي توفر حماية قوية للحقوق الفردية وتحدد بوضوح واجبات المعالجين ومسؤوليات الدول

الأعضاء. كما تضمن هذه التشريعات حماية الحقوق الفردية مثل الوصول إلى البيانات والتصحيح والاعتراض، مع وجود آليات رقابية فعالة لتحقيق التوازن بين حماية الأفراد ومتطلبات المصلحة العامة. تعتمد الولايات المتحدة على مقاربة قطاعية ومتعددة المستويات، إذ لا يوجد قانون اتحادي شامل، ويتم تنظيم البيانات من خلال قوانين فدرالية متخصصة مثل قانون حماية بيانات الائتمان، بالإضافة إلى قوانين الولايات مثل CCPA. ويعزز التعديل الرابع للحماية الدستورية ضد التفتيش والمصادرة غير المبررة حماية البيانات الرقمية ضمن كل ولاية، مع تفاوت مستوى الحماية بين الولايات. قدمت منظمة التعاون الاقتصادي والتنمية إطارًا إرشاديًا دوليًا عبر المبادئ التوجيهية لحماية البيانات الشخصية لعام 1980، والتي تضمنت ثمانية مبادئ أساسية: النقل من البيانات، جودة البيانات، تحديد الأغراض، تقييد الاستخدام، أمان البيانات، الشفافية، مشاركة الأفراد، والمساءلة. وقد ساعدت هذه المبادئ في توجيه التشريعات الوطنية والإقليمية، بما في ذلك الاتحاد الأوروبي، لتعزيز حماية البيانات وتدفقها بشكل آمن عبر الحدود.

عليه، يظهر جليًا أن الفجوة بين الإطار الفلسطيني والمعايير الدولية تتمثل في محدودية التشريعات الشاملة، غياب تنظيم تدفق البيانات عبر الحدود، تفاوت آليات الرقابة والمساءلة، وصلاحيات واسعة للسلطة التنفيذية قد تؤثر على حماية الحقوق الفردية الرقمية.

النتائج

أظهرت الدراسة أن القانون الأساسي الفلسطيني المعدل لسنة 2003 قد وفر حماية عامة للحق في الخصوصية، من خلال المواد الدستورية الأساسية مثل المواد 11 و17 و32، التي تضمنت الحرية الشخصية وحماية المساكن والحق في التعويض عن الانتهاكات، إلا أن هذا الإطار الدستوري لم يتناول حماية البيانات الرقمية بشكل محدد عند صدوره، مما ترك فجوة واضحة في مواجهة التحديات الحديثة المرتبطة بالتحول الرقمي واستخدام البيانات الشخصية.

كما بينت التحليلات أن القرارات بقوانين الوطنية والتنظيمات القطاعية، مثل قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، وقرار مجلس الوزراء رقم 3 لسنة 2019 بشأن البيانات الشخصية، وقرار بقانون رقم 37 لسنة 2021 المتعلق بالاتصالات وتكنولوجيا المعلومات، شكلت بداية مهمة لتوفير حماية قانونية للبيانات الرقمية، لكنها بقيت حماية جزئية ومحدودة، وغير موحدة، حيث اعتمدت على تشريعات متفرقة لم تكن تغطي جميع القطاعات والجهات العامة والخاصة، ولم توفر آليات رقابية وإشرافية مستقلة وموحدة لضمان الالتزام.

وعند المقارنة مع الإطار الأوروبي، يتضح أن فلسطين ما زالت تعاني من ضعف في الحماية الشاملة للبيانات الشخصية، إذ تتميز دول الاتحاد الأوروبي، خاصة بعد اعتماد اللائحة العامة لحماية البيانات (GDPR) (2016/679)، بشمولية القانون وتكامل الحقوق، مثل حق الاطلاع على البيانات وتصحيحها والاعتراض على

معالجتها، مع آليات رقابية قوية، وفرض عقوبات مالية صارمة على المخالفين، وهو ما لم يكن متوفرًا بشكل متكامل في النظام الفلسطيني قبل صدور قانون حماية البيانات الشخصية لسنة 2023. أما بالمقارنة مع الولايات المتحدة الأمريكية، فيلاحظ أن النموذج الأمريكي يعتمد على تشريعات فيدرالية متخصصة وقوانين ولاية قوية، مثل قانون حماية خصوصية المستهلك في كاليفورنيا، الذي يوفر حقوقًا موسعة للأفراد، بما في ذلك منع بيع البيانات الشخصية دون موافقة صريحة، بينما في فلسطين كانت الحماية موزعة بين قوانين متفرقة وغير متكاملة، مع تفاوت في مستوى الحماية بين القطاعات المختلفة، مما أثر على فعالية الإطار القانوني في حماية البيانات الرقمية.

وعند النظر إلى المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية (OECD)، يتبين أن فلسطين لم تتبنَّ بشكل كامل تنظيم تدفق البيانات عبر الحدود، ولم تحدد بعد معايير واضحة للشفافية والمساءلة المؤسسية، وهي المبادئ التي تعتبر أساسية لضمان حماية البيانات الشخصية على مستوى دولي، وتعزيز الثقة في البيئة الرقمية، خاصة فيما يتعلق بالمعالجة بين القطاعين العام والخاص.

بشكل عام، تُظهر النتائج أن الإطار القانوني الفلسطيني قبل عام 2023 كان محدودًا ومتدرجًا، واعتمد على حماية دستورية عامة ومجموعة من التشريعات الجزئية، وأن صدور قانون حماية البيانات الشخصية لسنة 2023 يمثل نقطة تحول نوعية، إذ أسس لإطار شامل وموحد يغطي جميع الجهات، ويوفر حقوق الأفراد والتزامات المعالجين، ويضع آليات رقابية وعقوبات واضحة، بما يتماشى مع المعايير الدولية وأفضل الممارسات العالمية.

التوصيات

بناءً على النتائج المستخلصة من دراسة الإطار القانوني لحماية البيانات الشخصية في فلسطين مقارنة بالمعايير الدولية، يُوصى بما يلي:

- **تطوير إطار تشريعي شامل:** ينبغي صياغة قوانين متكاملة للبيانات الشخصية تشمل جميع القطاعات العامة والخاصة، وتحدد بوضوح حقوق الأفراد وواجبات الجهات المعالجة، بما يضمن حماية فعالة للخصوصية الرقمية وتوفير أسس قانونية راسخة للتعامل مع المعالجات الرقمية.
- **تأسيس هيئة إشرافية مستقلة:** يُعد إنشاء هيئة مستقلة لحماية البيانات أمرًا ضروريًا لضمان الرقابة الفعالة والإشراف على التزام المؤسسات بالقوانين، بما في ذلك متابعة الانتهاكات وتطبيق العقوبات بشكل عادل وشفاف، مما يعزز ثقة المواطنين في حماية بياناتهم الشخصية.
- **تعزيز الشفافية والمساءلة:** يجب أن تتضمن التشريعات آليات واضحة تتيح للأفراد الاطلاع على بياناتهم الشخصية وتصحيحها والاعتراض على معالجتها، مع وضع نظم للمساءلة المؤسسية لضمان الالتزام، ما يعزز حماية الحقوق الفردية ويحد من المخاطر المرتبطة باستخدام البيانات بطريقة غير قانونية.

- الاستفادة من المعايير الدولية: ينبغي مراعاة المبادئ والتجارب الدولية، خاصة تجربة الاتحاد الأوروبي ولائحة GDPR، ومبادئ منظمة التعاون الاقتصادي والتنمية (OECD)، لضمان توافق التشريعات الفلسطينية مع المعايير العالمية، وتحقيق حماية شاملة ومرنة تتكيف مع التطورات الرقمية الحديثة.
- تدريب الجهات المختصة والقضاء على التجاوزات: يتطلب الإطار القانوني تدريب الجهات التنفيذية والقضائية على تطبيق التشريعات بشكل مسؤول، مع وضع ضوابط تمنع الاستخدام التعسفي لصلاحيات الوصول إلى البيانات، بحيث يُحافظ على التوازن بين حماية الحقوق الرقمية للأفراد ومتطلبات الأمن والمصلحة العامة للدولة.
- تنظيم تدفق البيانات عبر الحدود: في ظل التوسع الرقمي والتجارة الإلكترونية العابرة للحدود، يُوصى بوضع قواعد وإجراءات واضحة لتنظيم تبادل البيانات الشخصية خارج فلسطين، بما يضمن توافقها مع المعايير الدولية ويعزز حماية الخصوصية ويحد من المخاطر المرتبطة بالمعالجة العابرة للحدود.

الهوامش:

¹ Diggelmann, Oliver, and Cleis, Maria Nicole, "How the Right to Privacy Became a Human Right," *Human Rights Law Review*, Oxford University Press, Vol. 14, No. 3, 2014, p. 444.

² غريفيث، ج.، *الحق الإنساني في الخصوصية*، مجلة سان دييغو للقانون، تصدر عن جامعة سان دييغو، المجلد 44، 2007، ص. 697.

³ شيلز، إ.، *الخصوصية: دستورنا وتقليداتها*، مجلة القانون والمشكلات المعاصرة، تصدر عن جامعة ديوك، المجلد 31، العدد 2، 1966، ص. 283.

⁴ المرجع نفسه، ص. 290.

⁵ United Nations General Assembly, Resolution 68/167: The Right to Privacy in the Digital Age, United Nations, 2013, Official Gazette, September 1980 / March 2003, retrieved from <https://www.kisa.link/qzhQa>, Accessed on 8 October 2025.

⁶ دولغر، م. ف.، "حماية البيانات الشخصية في سياق حقوق الإنسان والحريات الأساسية"، مجلة كلية الحقوق بجامعة إسطنبول ميديبول، جامعة إسطنبول ميديبول، المجلد 5، العدد 1، 2018، ص. 74.

⁷ United Nations, Universal Declaration of Human Rights (G.A. Res. 217 A (III), U.N. Doc. A/810), adopted on 10 December 1948, Official Gazette, September 1980 / March 2003, retrieved from <https://www.kisa.link/PHBOK>, Accessed on 15 October 2025.

⁸ Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 15, adopted in Rome on 4 November 1950, entry into force on 1 August 2021, Official Gazette, September 1980 / March 2003, retrieved from <https://www.kisa.link/IvIAF>, Accessed on 10 October 2025.

⁹ Land Hessen, Hessisches Datenschutzgesetz (Data Protection Law of the Land of Hesse, 1970), <https://www.kisa.link/StyEn>, accessed on November 2, 2025

¹⁰ Fuster, G. G., *The emergence of personal data protection as a fundamental right of the EU*, Vol. 16, Springer Science & Business Media, Berlin, 2014, p. 23.

¹¹ United Nations Economic and Social Affairs, *The Economic and Social Impact of Open Government (Arabic version): Policy Recommendations for the Arab Countries*, 1st ed., OECD Publishing, Paris, 2022, p. 50.

¹² European Union, General Data Protection Regulation (GDPR) No. 2016/679, Official Journal of the European Union, April 27, 2016, retrieved from <https://www.kisa.link/rbyHj>. Accessed on 2 October 2025.

¹³ فوستر، ج. ج.، "الأمن ومستقبل حماية البيانات الشخصية في الاتحاد الأوروبي"، مجلة الأمن وحقوق الإنسان، المجلد 23، 2012، ص. 331.

¹⁴ European Union, Op.

¹⁵ Martínez-Martínez, D. F., *Unification of personal data protection in the European Union : Challenges and implications*, *Profesional de la Informacion*, 27(1), 2018, pp. 188.

¹⁶ Ibid., p190

¹⁷ الأمم المتحدة، الإعلان العالمي لحقوق الإنسان، تم اعتماده من قبل الجمعية العامة للأمم المتحدة في 10 ديسمبر 1948 .
<https://www.kisa.link/geRrf>

¹⁸ Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)*, adopted in Rome on 4 November 1950, entered into force on 3 September 1953, available at: <https://www.kisa.link/ggoIp> , consulted on 1 November 2025.

¹⁹ González Fuster, Gloria, *The Surfacing of National Norms on Data Processing in Europe*, in *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham : Springer International Publishing, 2014, pp. 58.

²⁰ يُعد هذا التوجيه أول إطار قانوني شامل في الاتحاد الأوروبي يهدف إلى تنظيم معالجة البيانات الشخصية داخل الدول الأعضاء. وقد نصّ على مبادئ أساسية مثل الشفافية، والشرعية، والغرض المحدد لجمع البيانات، وحقوق الأفراد في الوصول إلى بياناتهم وتصحيحها. كما سعى إلى توحيد القواعد بين الدول الأعضاء وضمان حرية انتقال البيانات داخل السوق الأوروبية المشتركة.

²¹ جاءت هذه اللائحة لتحلّ محلّ التوجيه السابق (EC/46/95)، ولتعزيز الإطار القانوني الأوروبي بما يتناسب مع العصر الرقمي الحديث. وقد دخلت حيز التنفيذ في 25 مايو 2018. تتميز الـ GDPR بأنها ملزمة مباشرة في جميع دول الاتحاد دون الحاجة إلى تشريعات وطنية إضافية، وتهدف إلى تعزيز حقوق الأفراد في حماية خصوصيتهم وفرض التزامات صارمة على المؤسسات التي تعالج البيانات الشخصية، مع عقوبات مالية كبيرة في حال مخالفة أحكامها.

²² European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR)*, *Official Journal of the European Union*, L 119, 1–88, 2016, available at: <https://www.kisa.link/fonbZ>, accessed November 2, 2025.

²³ Osano Staff, *Data Privacy Laws: What You Need to Know in 2025*, updated September 26, 2025, published August 12, 2024, available at: <https://www.kisa.link/oYypz>, accessed November 8, 2025.

²⁴ Robin Andrus, *A Brief History of Data Privacy, and What Lies Ahead*, Skyflow, published June 27, 2022, available at : <https://www.kisa.link/ilMJA>, accessed November 6, 2025.

²⁵ Robin Andrus, 2022

²⁶ U.S. Department of Justice, *Overview of the Privacy Act: 2020 Edition*, available at : <https://www.kisa.link/GhOBu>, accessed November 7, 2025.

²⁷ منظمة التعاون الاقتصادي والتنمية، المبادئ التوجيهية لحماية الحياة الخاصة وتدفق البيانات الشخصية عبر الحدود، اعتمدت بتاريخ 23 سبتمبر 1980، الرابط المختصر: <https://www.kisa.link/qiZHJ>، تاريخ التصفح: 3 نوفمبر 2025.

²⁸ منظمة التعاون الاقتصادي والتنمية، مرجع سبق ذكره.

²⁹ نايل محمود المعاينة، استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الالكترونية في البلديات، مجلة العلوم الإنسانية والطبيعية، المجلد 5، العدد 4، 2024، ص. 365.

³⁰ نايل محمود المعاينة، مرجع سبق ذكره، ص. 374

³¹ قانون العقوبات رقم (16) لسنة 1960م، تاريخ الإصدار: 1960، مضمون القانون: القانون الجنائي، عدد الجريدة الرسمية: غير محدد، تاريخ النشر: غير محدد، الصفحة: غير محددة، الرابط الإلكتروني المختصر: <https://www.kisa.link/RXfhq>، تاريخ التصفح: 2 نوفمبر 2025.

- ³² السلطة الوطنية الفلسطينية. (2003). القانون الأساسي المعدل لسنة 2003م. رئيس السلطة الوطنية الفلسطينية، الرائد الرسمي رقم 2، 19 مارس 2003. <https://www.kisa.link/JNFdl> تاريخ التصفح: 5 نوفمبر 2025.
- ³³ رئيس السلطة الوطنية الفلسطينية. (2018). قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية. الرائد الرسمي رقم 16، 3 مايو 2018. <https://www.kisa.link/UvVsZ>، تاريخ التصفح : 6 نوفمبر 2025.
- ³⁴ فراس الطويل، بثينة سفحمة. (2022). ملف الخصوصية والبيانات الشخصية في فلسطين: انتهاكات مزدوجة وقانون غائب. المركز العربي لتطوير الإعلام الاجتماعي، 5 يوليو 2022. الرابط الإلكتروني: <https://www.kisa.link/qPTya> ، تاريخ التصفح: 7 نوفمبر 2025.
- ³⁵ قرار مجلس الوزراء رقم (3) لسنة 2019م بشأن البيانات الشخصية الخاصة بالمواطنين. الصادر بتاريخ 19 آذار/مارس 2003، المنشور في الرائد الرسمي الفلسطيني، العدد الخاص بشهر أيلول/سبتمبر 1980، ساري النفاذ في الضفة الغربية وقطاع غزة. موقع التشريعات الفلسطيني الرسمي: <https://www.kisa.link/zgRCM> ، تاريخ التصفح: 5 نوفمبر 2025.