مجـــلـة الحـــق للعلوم الشرعية والقانونية
Al-haq Journal for Sharia and Legal Sciences
تصدر عن كلية القانون – جامعة بني وليد – ليبيا
Website: https://www.al-haqjournal.ly/index.php/alhaq/index
المجلد الثالث عشر ــ العدد الأول 2026 ــ الصفحات (594-607)
ISSN 3005 – 3919 معامل التأثير العربي 1.72 لسنة 2025 2.113 (ISI) لسنة 2025

Constitutional and legal protection of personal data: A comparative study between the European General Data Protection Regulation (GDPR) and some comparative legislation

Aisha Ali Elnaas *
Department of Public Law, Faculty of Law, Misuratau University, Misrata, Libya
a.alnaa@law.misuratau.edu.ly

الحماية الدستورية والقانونية للبيانات الشخصية "دراسة مقارنة بين اللائحة الأوروبية لحماية البيانات الشخصية (GDPR) وبعض التشريعات المقارنة"

د. عائشة علي فتح الله النعاس*
قسم القانون العام، كلية القانون، جامعة مصراته، مصراتة، ليبيا

Received: 22-03-2026	Accepted: 29-04-2026	Published: 04-05-2026

الملخص:
تناول البحث الأطر الدستورية والقانونية التي تكفل حماية الخصوصية الرقمية، مع التركيز على الموازنة بين الحق في الخصوصية وحرية تدفق المعلومات، واستعرضت الدراسة الفلسفة التشريعية للائحة الأوروبية العامة لحماية البيانات *(GDPR)* باعتبارها المعيار العالمي الأسمى، وقارنتها بتشريعات عربية وأجنبية مختارة لبيان مدى مواءمتها للتطورات التقنية المتسارعة، وركز التحليل على آليات الرقابة وحقوق الأفراد كالحق في النسيان والوصول، والالتزامات الواقعة على عاتق معالجي البيانات، وخلصت الدراسة إلى أن الحماية الدستورية تظل الضمانة الأساسية، لكنها تتطلب نصوصاً قانونية إجرائية صارمة لردع الانتهاكات السيبرانية. كما شدد البحث على ضرورة توحيد المعايير التشريعية لمواجهة الطابع العابر للحدود للبيانات الشخصية في العصر الرقمي.

الكلمات الدالة: الحماية الدستورية، البيانات الشخصية، اللائحة الأوروبية (GDPR)، الخصوصية الرقمية ، معالجة البيانات.

Abstract:
The research examined the constitutional and legal frameworks that guarantee the protection of digital privacy, focusing on balancing the right to privacy with the free flow of information. The study reviewed the legislative philosophy of the European Union's General Data Protection Regulation (GDPR) as the supreme global standard, and compared it with selected Arab and foreign legislation to demonstrate its compatibility with rapid technological advancements. The analysis focused on oversight mechanisms, individual rights such as the right to be forgotten and the right of access, and the obligations of data processors. The study concluded that constitutional

protection remains the primary guarantee, but it requires strict procedural legal texts to deter cyber violations. The research also emphasized the need to unify legislative standards to address the transnational nature of personal data in the digital age.

Keywords: Constitutional protection, personal data, European Regulation (GDPR), digital privacy, data processing.

المُقَدِّمَة:

يشهد العالم حالياً، وبشكلٍ كبيرٍ، تطوراتٍ متلاحقةً في نظمِ المعلوماتِ، والتي واكبتها تطوراتٌ أخرى في مجالِ نظمِ الاتصالاتِ؛ وقد نجمَ عن الاقترانِ بين المجالين ظهورُ ثورةِ الاتصالاتِ والمعلوماتِ (لطفي، 1994، ص7).

ولقد اتجهت غالبيةُ الدولِ أمامَ سرعةِ التطورِ التكنولوجيّ في مواجهةِ اتساعِ دائرةِ الأعمالِ والخدماتِ وتعددِ التخصصاتِ، إلى تبني آلياتِ الإدارةِ الإلكترونيةِ كأحدِ أهمِّ المداخلِ الحديثةِ في الإصلاحِ الإداريّ (مرعي، 2017).

وأرى أنه ينبثقُ عن الإدارةِ الإلكترونيةِ أمرٌ هامٌّ، وهو حمايةُ الخصوصيةِ المعلوماتيةِ؛ حيث تكونُ بياناتُ الأفرادِ الشخصيةُ تحت بصرِ وسمعِ جهاتِ الإدارةِ.

ثانياً – أهمية البحث:

يشهدُ العصرُ الحديثُ تحولاً كبيراً في استفادةِ القانونِ الإداريّ من منجزاتِ الثورةِ الرقميةِ في تقديمِ الخدماتِ العامةِ وإدارةِ المرفقِ العامِ؛ وصاحبَ هذا التقدمَ التقنيَّ، في ظلِّ الإدارةِ الإلكترونيةِ، تطورٌ سريعٌ في الاعتداءِ على خصوصيةِ البياناتِ الشخصيةِ لمستخدمي شبكةِ الإنترنتِ، في ظلِّ ما أحدثته الثورةُ الرقميةُ من انتهاكاتٍ لخصوصياتِ الأشخاصِ في ظلِّ الإدارةِ الإلكترونيةِ.

ثالثاً – إشكالية البحث:

تتمثلُ إشكاليةُ البحثِ حول الحمايةِ التي أوردها المشرعُ الدستوريُّ أو القانونيُّ: هل هي حمايةٌ كافيةٌ لحمايةِ هذا الحقّ؟ أم أنَّ هذه الحمايةَ التي نصّ عليها الدستورُ والقانونُ غيرُ كافيةٍ كذلك في الموازنةِ بين الحقّ في الخصوصيةِ وحمايةِ الكرامةِ الإنسانيةِ، وبين التطورِ التكنولوجيّ ومعالجةِ البياناتِ الرقميةِ؟

لذلك، تواجهُ هذه الحمايةُ تحدياتٍ تتمثلُ في خطرِ الاعتداءِ والابتزازِ الإلكترونيّ؛ مما يستلزمُ نصوصاً دستوريةً وقوانينَ خاصةً لضمانِ سريةِ وسلامةِ هذه البياناتِ.

رابعاً – منهج البحث:

اعتمدتُ في هذه الدراسةِ على المنهجِ التحليليّ المقارنِ؛ من خلالِ تحليلِ النصوصِ القانونيةِ المتعلقةِ بموضوعِ الدراسةِ، من أجلِ الوصولِ إلى حلولٍ بشأنِ الإشكالياتِ التي يثيرها البحثُ.

كذلك التعرض للتشريعاتِ المقارنةِ في موضوعِ البحثِ للتمييزِ فيما بينها، والوقوفِ على التشريعِ الذي يواكبُ التطورَ التكنولوجيَّ للبياناتِ الرقميةِ.

خامساً – خطة البحث:

- **المبحث الأول: الإطار المفاهيمي والقانوني للبيانات الشخصية:**
  - المطلب الأول: مفهوم البيانات الشخصية.
  - المطلب الثاني: الإطار القانوني والتنظيمي لحماية البيانات.
- **المبحث الثاني: الحماية الدستورية للبيانات الشخصية في التشريعات المقارنة:**
  - المطلب الأول: ضوابط جمع ومعالجة البيانات الشخصية.
  - المطلب الثاني: المسؤولية القانونية عن انتهاك البيانات الشخصية.

المبحث الأول
الإطار المفاهيمي والقانوني للبيانات الشخصية

من أجلِ ضمانِ مستوىً عالٍ من الحمايةِ القانونيةِ والتقنيةِ للبياناتِ الشخصيةِ المعالجةِ إلكترونياً، وضعت التشريعاتُ آلياتٍ كفيلةً للتصدي للأخطارِ الناجمةِ عن استخدامِ البياناتِ الشخصيةِ للمواطنين، ومكافحةِ انتهاكِ خصوصياتِهم وحرياتِهم بصورةٍ غيرِ مشروعةٍ.

وكذلك صياغة الالتزاماتِ على كلٍّ من المعالجِ والمتحكمِ ومسؤولِ حمايةِ البياناتِ، أو معالجِ هذه البياناتِ؛ باعتبارهما من العناصرِ الفاعلةِ في مجالاتِ التعاملِ مع البياناتِ الشخصيةِ، سواءٌ عن طريقِ الجمعِ، أو النقلِ، أو التبادلِ، أو التخزينِ، أو التحليلِ، أو المعالجةِ بأيّ صورةٍ من الصورِ.

وإلزام المؤسساتِ أو الجهاتِ أو الأفرادِ المتحكمين في البياناتِ الشخصيةِ والمعالجين لها بتعيينِ مسؤولٍ لحمايةِ هذه البياناتِ داخلَ مؤسساتِهم أو جهاتِهم؛ بما يسمحُ لضمانِ خصوصيةِ بياناتِ الأفرادِ واقتضاءِ حقوقِهم المنصوصِ عليها في هذا القانونِ، وتنظيمِ عملياتِ المعالجةِ الإلكترونيةِ للبياناتِ الشخصيةِ، وإصدارِ تراخيصَ لمن يقومُ بها، وعلى الأخصّ فيما يتعلقُ بالبياناتِ الشخصيةِ الحساسةِ، بالإضافةِ إلى تقريرِ مسؤوليةٍ مدنيةٍ وجنائيةٍ من أجلِ حمايةِ البياناتِ الشخصيةِ (الإطار القانوني للمعالجة الإلكترونية للبيانات الشخصية، 2024).

المطلب الأول: مفهوم البيانات الشخصية:

في التشريع الليبي تُعرف البياناتُ الشخصيةُ بأنها: "كلُّ بيانٍ من شأنه أن يؤديَ إلى معرفةِ الفردِ على وجهِ التحديدِ، أو يجعلَ التعرفَ عليه ممكناً بصفةٍ مباشرةٍ أو غيرِ مباشرةٍ؛ مثل: الاسمِ، الرقمِ الوطنيّ، رقمِ ورقةِ العائلةِ، رقمِ قيدِ العائلةِ، رقمِ الهاتفِ، العنوانِ، رقمِ الهويةِ الشخصيةِ، البريدِ الإلكترونيّ، وغيرِ ذلك من البياناتِ ذاتِ الطابعِ الشخصيّ" (المادة الأولى من المنشور رقم (18)، 2025).

وبالتالي، فإنَّ مشاركةَ هذه البياناتِ تؤدي إلى فوائدَ، وغالباً ما يكونُ من الضروريّ مشاركتُها للتفاعلِ مع الأشخاصِ الآخرين في مجتمعاتِنا اليومَ؛ لكنَّ هذا لا يخلو من المخاطرِ، فبياناتُنا الشخصيةُ يمكنُ أن تكشفَ الكثيرَ عنا، وعن أفكارِنا وحياتِنا، وبالتالي يكونُ من السهلِ استغلالُ هذه البياناتِ بسهولةٍ، وهذا ما يشكلُ خطراً على الأفرادِ والمجتمعاتِ المستهدفين، ولذلك وجبَ أن تكونَ هذه البياناتُ محميةً بشكلٍ صارمٍ.

وفي المجتمعِ الليبيّ، لا يوجدُ قانونٌ شاملٌ وموحدٌ لحمايةِ البياناتِ الشخصيةِ على غرارِ اللائحةِ الأوروبيةِ العامةِ (GDPR)، ولكن يتمُّ حمايةُ البياناتِ عبرَ نصوصٍ متفرقةٍ، أبرزُها: قانونُ الجرائمِ الإلكترونيةِ رقم (5) لعام 2022م، كذلك قانونُ النظامِ الوطنيّ للمعلوماتِ لعام 1990م، وموادُ قانونِ العقوباتِ التي تُجرمُ إفشاءَ الأسرارِ، وجميعُ هذه القوانينِ تركزُ على سريةِ المعلوماتِ الرقميةِ وخصوصيةِ البياناتِ.

أما مفهومُ البياناتِ الشخصيةِ في القانونِ المصريّ، فهي: "أيُّ بياناتٍ متعلقةٍ بشخصٍ طبيعيٍّ محددٍ، أو يمكنُ تحديدُه بشكلٍ مباشرٍ أو غيرِ مباشرٍ، عن طريقِ الربطِ بين هذه البياناتِ وأيّ بياناتٍ أخرى؛ كالاسمِ، أو الصوتِ، أو الصورةِ، أو أيّ رقمٍ تعريفيٍّ، أو محددٍ للهويةِ عبرَ الإنترنتِ، أو أيّ بياناتٍ تحددُ الهويةَ النفسيةَ، أو الصحيةَ، أو الاقتصاديةَ، أو الثقافيةَ، أو الاجتماعيةَ" (المادة رقم (1) من قانون البيانات الشخصية المصري رقم (151)، 2020).

ونصَّ القانونُ المصريُّ على أنَّ "الشخصَ المعنيَّ بالبياناتِ" هو: أيُّ شخصٍ طبيعيٍّ تُنسبُ إليه بياناتٌ شخصيةٌ معالجةٌ إلكترونياً تدلُّ عليه قانوناً أو فعلاً، وتُمكّنُ من تمييزِه عن غيرِه. وأكدَ المشرعُ في ذاتِ المادةِ الأولى من القانونِ المصريّ رقم (151) لسنة 2020م، أنَّ إتاحةَ البياناتِ الشخصيةِ تشملُ: الاطلاعَ، أو التداولَ، أو النشرَ، أو النقلَ، أو الاستخدامَ، أو العرضَ، أو الإرسالَ، أو الاستقبالَ، أو الإفصاحَ عنها؛ وأنَّ أمنَ البياناتِ هو: إجراءاتٌ وعملياتٌ تقنيةٌ وتنظيميةٌ من شأنِها الحفاظُ على خصوصيةِ البياناتِ الشخصيةِ وسريتِها وسلامتِها ووحدتِها وتكاملِها فيما بينها (عبد الرحمن، 1990، ص76).

أما مفهومُ البياناتِ الشخصيةِ في القانونِ الفرنسيّ، فقد عرفهُ المشرعُ الفرنسيُّ بأنه: "يُعتبرُ بياناً شخصياً أيُّ معلوماتٍ تتعلقُ بشخصٍ طبيعيٍّ معروفةٍ هويتُه، أو يمكنُ التعرفُ على هويتِه سواءٌ بشكلٍ مباشرٍ أو غيرِ مباشرٍ؛ أو يمكنُ تحديدُ هويتِه بالرجوعِ إلى الاسمِ، ورقمِ تعريفِه الشخصيّ، وبياناتِ الموقعِ، والمعرّفِ عبرَ الإنترنتِ، لواحدٍ أو أكثرَ من العناصرِ المحددةِ الخاصةِ بالهويةِ الشخصيةِ، أو الفسيولوجيةِ، والجنينية، أو النفسيةِ، أو الاقتصاديةِ، أو الثقافيةِ، أو الاجتماعيةِ" (المادة الثانية من القانون الفرنسي رقم (801)، 2004).

كذلك عرفتها اللائحةُ رقم (679) لسنة 2016م على أنها: "بياناتٌ شخصيةٌ ناشئةٌ عن معالجةٍ تقنيةٍ أو فنيةٍ خاصةٍ، تتعلقُ بالخصائصِ الجسديةِ أو الفسيولوجيةِ أو السلوكيةِ للشخصِ الطبيعيّ، والتي يمكنُ من خلالِها تحديدُ هويتِه، ومن خلالِ صورةِ الوجهِ أو البياناتِ الخاصةِ ببصماتِ الإصبع.

ويلزمُ توافرُ مجموعةٍ من الشروطِ حتى يمكنَ الاستعانةُ بهذه البياناتِ واستخدامُها؛ فيجبُ أن تكونَ هذه البياناتُ فرديةً، ودائمةً، وقابلةً للقياسِ" (Humaine, 2002, p481).

وبالتالي يتضحُ لنا بعدَ البحثِ في مفهومِ البياناتِ الشخصيةِ في كلٍّ من ليبيا ومصر وفرنسا، نرى أنَّ المشرعَ الفرنسيَّ كان أسبقَ في تحديدِ البياناتِ الشخصيةِ بل ووضعَ تعريفاً حديثاً، ثم تلاه المشرعُ المصريُّ في اهتمامِه بمواكبةِ التطورِ ووضعِ قانونِ البياناتِ الشخصيةِ، وبالتالي تُعتبرُ خطوةً على الطريقِ.

في حينِ أنَّ غيابَ قانونٍ شاملٍ ومستقلٍ لحمايةِ البياناتِ الشخصيةِ في ليبيا يُعدُّ قصوراً تشريعياً بارزاً، رغمَ وجودِ نصوصٍ متفرقةٍ في قانونِ الجرائمِ الإلكترونيةِ رقم (5) لسنة 2022م؛ هذا الفراغُ يؤدي إلى ضعفِ حمايةِ الخصوصيةِ، وتزايدِ انتهاكِ البياناتِ، وصعوبةِ ملاحقةِ الاستخدامِ غيرِ المشروعِ للبياناتِ أو المعلوماتِ الشخصيةِ.

المطلب الثاني: الإطار القانوني والتنظيمي لحماية البيانات الشخصية:

تعدُّ التشريعاتُ الركيزةَ الأساسيةَ التي تنظمُ عمليةَ حمايةِ البياناتِ، وتعدُّ اللائحةُ العامةُ لحمايةِ البياناتِ (GDPR)الإطارَ القانونيَّ الأقوى لحمايةِ البياناتِ الشخصيةِ في الاتحادِ الأوروبيّ منذ عام 2018م؛ حيث تمنحُ الأفرادَ حقوقاً واسعةً (الوصول، الحذف، النقل)، وتفرضُ على المنظماتِ شفافيةً، وموافقةً صريحةً، وتدابيرَ أمنيةً مشددةً. ويرتكزُ التنظيمُ اللائحيُّ على خمسةِ أسسٍ قانونيةٍ للمعالجةِ، مع عقوباتٍ ماليةٍ ضخمةٍ تصلُ إلى 4% من الإيراداتِ السنويةِ.

وتتمثلُ الركائزُ القانونيةُ والتنظيميةُ للائحة (GDPR) في الآتي:

1- **المبادئُ الأساسيةُ لمعالجةِ البياناتِ:** متمثلةً في المادةِ (5) من اللائحةِ، وهي تتضمنُ: (الشفافية والعدالة، تحديد الغرض من جمع البيانات، تقليل البيانات، الدقة في التحديث أو حذف البيانات غير الدقيقة، تقييد التخزين، النزاهة والسرية).
2- **الأسسُ القانونيةُ للمعالجةِ:** تتمثلُ في نصّ المادةِ (6)؛ بحيثُ إنه لا يجوزُ معالجةُ البياناتِ إلا بناءً على موافقةٍ صريحةٍ من صاحبِ البياناتِ، وتنفيذِ العقدِ (العقد طرفه صاحبُ البياناتِ) والامتثالِ للالتزامِ القانونيّ، وحمايةِ المصالحِ الحيويةِ، وتنفيذِ المهامِ للصالحِ العامّ).
3- **حقوقُ الأفرادِ (موضوع البيانات):** وتتمثلُ في: الحقّ في الإعلامِ، الحقّ في الوصولِ أو الاطلاعِ على البياناتِ، الحقّ في التصحيحِ، الحقّ في المحوِ (حذف البيانات)، الحقّ في نقلِ البياناتِ، الحقّ في الاعتراضِ (رفضِ المعالجة).
4- **التدابيرُ التنظيميةُ والأمنيةُ:** وتتمثلُ في:
   - تعيينِ مسؤولِ حمايةِ بياناتٍ (DPO).
   - تقييمِ الأثرِ (DPIA): والذي يتمُّ إجراؤُه عند وجودِ مخاطرَ عاليةٍ.
   - الالتزامِ بخصوصيةِ التصميمِ والتصميمِ الافتراضيّ: والمتمثلةِ في دمجِ الحمايةِ في النظمِ من البدايةِ، وكذلك الإبلاغِ عن الاختراقاتِ خلال 72 ساعةً من أيّ خرقٍ للبياناتِ.

5- **العقوباتُ:** تصلُ الغراماتُ إلى 20 مليون يورو، أو 4% من إجمالي الإيراداتِ السنويةِ العالميةِ (أيهما أعلى) (اللائحة العامة لحماية البيانات (GDPR)، 2018).

وبالتالي، تُعدُّ اللائحةُ العامةُ الأوروبيةُ لحمايةِ البياناتِ (GDPR) أقوى قانونٍ للخصوصيةِ في العالمِ، والتي تهدفُ بشكلٍ رئيسيٍّ إلى منحِ الأفرادِ سيطرةً أكبرَ على بياناتِهم الشخصيةِ، وتعزيزِ الشفافيةِ، وفرضِ حمايةٍ صارمةٍ للبياناتِ الرقميةِ. وتوفرُ هذه اللائحةُ فوائدَ جوهريةً تتمثلُ في حمايةِ الحقوقِ الرقميةِ، وزيادةِ ثقةِ العملاءِ، والحدِّ من اختراقاتِ البياناتِ وغراماتِها الباهظةِ.

أما في التشريعاتِ المقارنةِ، وتحديداً في السياقِ الليبيِّ، ورغمَ عدمِ وجودِ قانونٍ شاملٍ وموحدٍ على غرارِ اللائحةِ العامةِ لحمايةِ البياناتِ (GDPR) الأوروبيةِ حتى الآنَ، فإنَّ هناك بعضَ القوانينِ والنصوصِ المتفرقةِ التي يمكنُ الاستنادُ إليها لتوفيرِ مستوىً أساسيٍّ من الحمايةِ.

ومن أبرزِ القوانينِ واللوائحِ المنظمةِ في التشريعِ الليبيِّ:

1- **قانونُ المعاملاتِ الإلكترونيةِ رقم (6) لسنة 2022م:** والذي يُلزمُ الجهاتِ بإخطارِ المستخدمين بآلياتِ حمايةِ البياناتِ، ويمنحُ الأفرادَ الحقَّ في النفاذِ إلى بياناتِهم وتحديثِها، ويضعُ ضوابطَ لنقلِ البياناتِ خارجَ ليبيا.
2- **قانونُ الجرائمِ الإلكترونيةِ رقم (5) لسنة 2022م:** والذي يُجرمُ الدخولَ غيرَ المشروعِ للبياناتِ (الاختراقَ)، والاعتراضَ غيرَ القانونيِّ للمعلوماتِ.
3- **قانون رقم (4) لسنة 1990م بشأن النظام الوطني للمعلومات:** والذي ينظم حماية سرية البيانات الحكومية والشخصية، ويحدد مسؤوليات الهيئة العامة للمعلومات.
4- **لوائح مصرف ليبيا المركزي 2025م:** حيث أصدر المنشور رقم (18) لسنة 2025م لإلزام المؤسسات المالية بتعيين مسؤولي بيانات، وتطبيق تدابير أمنية وسيادة البيانات (تخزينها داخل ليبيا).
5- **العقوبات:** تتفاوت العقوبات في التشريع الليبي بين الحبس والغرامات المالية؛ حيث تصل في بعض اللوائح المالية إلى عقوبات رادعة لضمان الامتثال، كما يُجرم القانون حيازة البيانات دون إذن (الزوي، 2021).

أما في التشريع المصري، فقد نصت المادة (2) من اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020م على أنه: يلتزم مقدمو خدمات تقنيات المعلومات باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذاً للبندين (2، 3) من الفقرة أولاً من المادة رقم (2) من القانون:

أ. تشفير البيانات والمعلومات بما يحافظ على سريتها وعدم اختراقها، باستخدام نظام تشفير قياسي متماثل أو غير متماثل، بما لا يقل في تأمينه عن (Advanced Encryption Standard ASE - 128)، بمفتاحِ شفرةٍ لا يقلُّ عن 128 بت، مع مسؤوليتِه بالحفاظِ على سريةِ وأمانِ مفتاحِ التشفيرِ.
ب. تنصيب واستخدام نظم وبرامج ومعدات مكافحة البرمجيات والهجمات الخبيثة، والتأكد من صلاحيتها وتحديثها.
ج. استخدام بروتوكولات آمنة مثل: بروتوكول نقل النص التشعبي المؤمن (https).
د. وضع صلاحيات بالشبكات والملفات وقواعد البيانات وتحديدها؛ لضمان حماية الوصول المنطقي (Logical access) إلى الوصول المعلوماتية والتقنية، ولمنع الوصول غير المصرح به للمعلومات التي تُستبعدُ بناءً على اعتراض صاحب الشأن.

كما وتنصُّ قوانينُ المعلوماتيةِ على أنه يحقُّ للشخصِ أن يعترضَ على تخزينِ بعضِ المعلوماتِ الاسميةِ المتعلقةِ به إذا قدّم أسباباً مشروعةً ومبررةً لذلك.

ويظهرُ دورُ الضماناتِ القضائيةِ في عدمِ انتهاكِ الحقوقِ والحرياتِ العامةِ عن طريقِ تطبيقِ مبدأِ المشروعيةِ، وتحقيقِ التوازنِ بين السلطةِ والحريةِ؛ بما يستوجبُ إعطاءَ الدولةِ السلطةَ للقيامِ بمسؤولياتِها، وتحصينِ حرياتِ الأفرادِ وتوفيرِ الضماناتِ التي تحول دون إساءة استعمالها (حسين، 2014، ص198).

وتطبيقاً لذلك، قضت محكمة القضاء الإداري أنه: يتعيّن على الدولةِ أن تُنشئَ الأطراف القانونيةَ القويةَ التي تحمي حقَّ الأفرادِ في الوصولِ إلى المعلوماتِ وبما يضمنُ الحفاظَ على سريتِها، وبالتالي تؤدي إلى خلقِ مجتمعٍ نشطٍ.

وبالتالي، من أهم الوسائل التقنية التي اقتدى بها المشرع المصري لحماية البيانات الشخصية نظام التشفير؛ لذلك نؤيد الرأي الفقهي القائل بأنه: "تعتبر تقنيات التشفير من أهم الأدوات التي توفر أمن وسلامة المعلومات المتبادلة عبر شبكات الإنترنت".

والسبب في اعتبارها من أهم الأدوات أنها لا تقتصر على حماية البيانات وحسب، بل تشتمل وظيفتها على التحقق ومعرفة مرسل الرسائل، والمصادقة على مضمونها وعلى توقيع أصحابها إلكترونياً عليها، والتأكد من سلامتها؛ أي التثبت من عدم تعييبها (أنطونيوس وعبدالناصر، د.ت، ص259).

أما في التشريع الفرنسي، فيستند هذا التشريع بشكل أساسي إلى اللائحة العامة لحماية البيانات (GDPR) الأوروبية، معززة بقانون حماية البيانات الفرنسي (المعدل للقانون رقم 6 يناير 1978م)، وتتولى اللجنة الوطنية للمعلوماتية والحريات (CNIL) الإشراف والرقابة، ملزمةً المؤسسات بالحصول على موافقة صريحة وضمان حقوق الأفراد (الاطلاع، التصحيح، الحذف)، مع فرض عقوبات صارمة على المخالفين.

لذلك، من أهم الأسس القانونية والتنظيمية في التشريع الفرنسي:

1- **الإطار الأوروبي الشامل:** الذي يحكم جمع واستخدام البيانات الشخصية للمقيمين داخل الاتحاد الأوروبي بما في ذلك فرنسا.
2- **قانون حماية البيانات الفرنسي 1978م:** تم تعديله ليتوافق مع اللائحة الأوروبية، وهو يحدد كيفية تطبيق القواعد الأوروبية، ويُعرّف البيانات الشخصية بأنها: "أي معلومات تسمح بتحديد هوية الشخص بشكل مباشر أو غير مباشر.
3- **اللجنة الوطنية للمعلوماتية والحريات (CNIL):** هي السلطة الإدارية المستقلة المسؤولة عن مراقبة تنفيذ هذه القوانين، وتلقي الشكاوى، وتوقيع العقوبات. كما يضمن التشريع الفرنسي حقوقاً للأفراد، منها:
   - **حق الاطلاع:** الحصول على تأكيد حول معالجة البيانات.
   - **حق الوصول:** الوصول إلى البيانات ذاتها.
   - **حق التصحيح:** تعديل أو إكمال البيانات الشخصية غير الدقيقة.
   - **حق الحذف (النسيان):** طلب حذف البيانات الشخصية.
   - **حق الاعتراض:** الحق في رفض معالجة البيانات لأسباب مشروعة.
   - **حق النقل:** استعادة البيانات بصيغة منظمة وشائعة الاستخدام (التهامي، 2011).

المبحث الثاني
الحماية الدستورية للبيانات الشخصية في التشريعات المقارنة

تحتلُّ القواعدُ الدستوريةُ قمةَ الهرمِ القانونيِّ في الدولةِ؛ لذلك فإنها تعلو على كلِّ ما عداها من قواعدَ قانونيةٍ. وإنَّ من نتائجِ التعاملِ عبرَ الإنترنتِ ظهورَ وسائلِ غشٍّ واحتيالٍ تتجاوزُ حدودَ الدولةِ، تعرضُ الأطرافَ لمخاطرِ الاعتداءِ والاختراقِ من طرفِ القراصنةِ؛ الأمرُ الذي دفعَ روادَ التجارةِ الإلكترونيةِ لحمايةِ البياناتِ ذاتِ الطابعِ الشخصيِّ.

يُعرفُ "أمنُ البياناتِ" بأنه: حمايةٌ وتأمينٌ لكافةِ الموارِدِ المستخدمةِ في معالجةِ البياناتِ؛ حيث يتمُّ تأمينُ هذه الأخيرةِ عن طريقِ اتباعِ إجراءاتٍ ووسائلِ حمايةٍ تضمنُ في النهايةِ سلامةَ خصوصيةِ الأطرافِ المتعاملةِ عبرَ الشبكةِ (عبيد، 2001، ص44).

لذلك، سوف نتطرقُ في هذا المبحثِ إلى ضوابطِ جمعِ ومعالجةِ البياناتِ الشخصيةِ من خلالِ اللائحةِ العامةِ لحمايةِ البياناتِ (GDPR) ومقارنتها التشريعاتِ الوطنيةِ الحديثةِ؛ مثلَ نظامِ حمايةِ البياناتِ الشخصيةِ الفرنسيِّ، والقوانينِ العربيةِ كالقانونِ المصريِّ والقانونِ الليبيِّ في مطلبٍ أولٍ، وسنعرضُ في المطلبِ الثاني المسؤوليةَ القانونيةَ عن انتهاكِ تلك البياناتِ.

المطلب الأول: ضوابط جمع ومعالجة البيانات الشخصية:

يكونُ جمعُ البياناتِ الشخصيةِ، طبقاً للائحةِ العامةِ لحمايةِ البياناتِ (GDPR) في الاتحادِ الأوروبيِّ، قانونياً فقط إذا تمَّ بشكلٍ شفافٍ وعادلٍ ومبنيٍّ على أساسٍ قانونيٍّ صريحٍ.

ويجبُ جمعُ الحدِّ الأدنى الضروريِّ من البياناتِ لأغراضٍ محددةٍ ومشروعةٍ، مع إعلامِ الأفرادِ بهويةِ المراقبِ ومدى التخزينِ ومدةِ التخزينِ وحقوقِهم؛ وذلك لضمانِ أعلى درجاتِ الأمانِ.

القواعدُ الأساسيةُ لجمعِ البياناتِ وفقاً لـ (GDPR): (https://gdpr.eu، 2026)

1- الأساسُ القانونيُّ: يجبُ توفيرُ سببٍ قانونيٍّ قبلَ الجمعِ، مثلَ:

- الموافقة الصريحة: يجبُ أن تكونَ حرةً، محددةً، وواضحةً.
- تنفيذ العقد: البياناتُ ضروريةٌ لتقديمِ خدمةٍ أو منتجٍ للمستخدمِ.
- الالتزام القانوني: البياناتُ مطلوبةٌ للامتثالِ للقانونِ.
- المصالح المشروعة: الجمعُ ضروريٌّ لمصلحةِ الشركة دونَ الإضرارِ بحقوقِ الفردِ.

2- الشفافية والإعلام: يجبُ إبلاغُ الفردِ بوضوحٍ بمن يجمعُ البياناتِ، ولماذا، ومن سيطلعُ عليها.

3- تقليل البيانات: جمعُ أقلِّ كميةٍ ممكنةٍ من البياناتِ الضروريةِ للغرضِ المحددِ فقط.

4- دقة البيانات: اتخاذُ إجراءاتٍ لضمانِ صحةِ البياناتِ وتحديثِها.

5- حدود التخزين: حذفُ البياناتِ فورَ انتهاءِ الغرضِ من جمعِها.

6- الأمان والسرية: حمايةُ البياناتِ باستخدامِ تدابيرَ تقنيةٍ (مثلِ التشفير) لحمايتِها من الاختراقِ.

أما معالجةُ البياناتِ فتشترطُ اللائحةُ العامةُ لحمايةِ البياناتِ (عليه المادة رقم 40 من اللائحةِ العامةِ الأوروبيةِ)؛ حيث نصت على أنه: "لكي تكونَ معالجةُ البياناتِ الشخصيةِ قانونيةً، يجبُ أن تتمَّ بناءً على موافقةِ صاحبِ البياناتِ المعنيِّ أو أيِّ أساسٍ قانونيٍّ".

بعبارةٍ أخرى، تُعدُّ الموافقةُ أحدَ الأسسِ القانونيةِ التي يمكنُ استخدامُها لتبريرِ جمعِ البياناتِ الشخصيةِ ومعالجتِها وتخزينِها.

وهذه الموافقةُ يجبُ أن تكونَ موافقةً بحريةٍ - موافقةً واضحةً لا لبسَ فيها - موافقةً محددةً مستعيرةً. ومع ذلك، يحقُّ لصاحبِ البياناتِ سحبُ موافقتِه في أيِّ وقتٍ على بياناتِه الشخصيةِ.

أما في التشريعاتِ الفرنسيةِ، فقد نصَّ قانونُ حمايةِ المعلوماتِ والحرياتِ الصادرُ في 6 يناير 1978م المعدل بالقانون رقم (20) يونيو 2018م على أنه: حقُّ الشخصِ في عدمِ احتفاظِ المسؤولُ عن المعالجةِ ببياناتِه الشخصيةِ لمدةٍ تتجاوزُ الغرضَ أو الغايةَ الأصليةَ التي جُمعت من أجلِها. كما نصَّ أيضاً على أنه: يُفرضُ على المسؤولِ عند معالجةِ البيانات ذاتِ الطابعِ الشخصيِّ أن تكونَ المعلوماتُ قد جُمعت بطريقةٍ معلومةٍ ومشروعةٍ، وأن لا يُحتفظَ بها لمدةٍ تتجاوزُ الغرضَ الذي جُمعت من أجلِه.

كما نصت اتفاقية (108) والصادرة عن المجلس الأوروبي والمطبقة في فرنسا سنة 1995م، في المادة الخامسة على أن: "البيانات ذات الطابع الشخصي التي تكون محلاً لمعالجةٍ آليةٍ، يُحتفظ بها تحت شكلٍ يسمح بتحديد هوية الأشخاص المعنيين خلال مدة لا تتجاوز المدة الضرورية اللازمة للغاية التي من أجلها تم التسجيل" (حسبو، د.ت، ص125).

وبالتالي، بتحديثُ فرنسا للقانون رقم (78-17) الصادر في 6 يناير 1978م، بشأن تكنولوجيا المعلومات وملفات البيانات الشخصية، جاء متوافقاً مع اللائحة العامة الأوروبية للبيانات الشخصية

(GDPR)؛ من حيث فرض قواعد صارمة وشاملة لجمع ومعالجة البيانات الشخصية، حيث تضع الحق في الخصوصية كأولوية قصوى. وتشمل أبرز مميزاتها: إلزامية الموافقة الصريحة والشفافية المطلقة، وتقليل البيانات، وتحديد الغرض، وفرض عقوبات مالية ضخمة لضمان الامتثال.

أما في التشريعات المصرية، فقد حرص المشرع المصري في دستور 2014م (المادة (68) من دستور مصر، 2014)، على التأكيد على حماية البيانات والمعلومات؛ حيث نص المشرع الدستوري المصري على أن: "المعلومات، والبيانات، والإحصاءات، والوثائق الرسمية ملك للشعب، والإفصاح عنها من مصادرها المختلفة حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها وقواعد إيداعها وحفظها، والتظلم من رفض إعطائها، وعقوبة مخالفتها" (العاكوم، 2000، ص10).

ويعتبر جمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني هو ضابط جمع وتخزين البيانات الشخصية في ظل القانون المصري رقم (151) لسنة 2020م. وقد حرص المشرع المصري على ذلك حيث أكد على الآتي:

1- إجراء المعالجة الإلكترونية وتنفيذها طبقاً للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية (المادة رقم (5) من قانون حماية البيانات الشخصية المصري رقم (151)، 2020).
2- تطبيق إطار معياري يتواكب مع التشريعات الدولية لحماية البيانات الشخصية للأفراد وحرياتهم.
3- صياغة التزامات على كل من المتحكم في البيانات والمعالج؛ باعتبارهما من العناصر الفاعلة في مجال التعامل مع البيانات الشخصية، سواء عن طريق الجمع أو النقل أو التخزين أو المعالجة بأي صورة من الصور.
4- إلزام الجهات والأفراد المتحكمين في البيانات بتعيين مسؤول لحماية البيانات الشخصيةِ والمعالجين لها بتعيينِ مسؤولٍ لحمايةِ البياناتِ الشخصيةِ داخلَ مؤسساتِهم.
5- إنشاءِ مركزِ حمايةِ البياناتِ الشخصيةِ كهيئةٍ عامةٍ يكونُ مختصاً بتنظيمِ والإشرافِ على تنفيذِ أحكامِ القانونِ (تقرير اللجنة المشتركة حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية المصري، 2020، ص9-10).

وبالتالي، يُعدُّ القانونُ المصريُّ لعامِ 2020م بشأنِ حمايةِ البياناتِ الشخصيةِ إطاراً تشريعياً شاملاً لتعزيزِ خصوصيةِ الأفرادِ في البيئةِ الرقميةِ، ومتوافقاً مع المعاييرِ الدوليةِ (GDPR)؛ حيث يرتكزُ على موافقةِ المستخدمِ الصريحةِ، ويمنحُ حقوقاً كطلبِ حذفِ البياناتِ، ويُلزمُ الشركاتِ بتعيينِ مسؤولٍ عن حمايةِ البياناتِ (DPO)، مع فرضِ غراماتٍ صارمةٍ لضمانِ الامتثالِ والحدِّ من اختراقِ البياناتِ، والتي سنتعرضُ لها في المطلبِ الثاني.

أما في التشريعاتِ الليبيةِ، فتعتمدُ معالجةُ البياناتِ الشخصيةِ على نصوصٍ قانونيةٍ متفرقةٍ، أبرزُها: قانونُ النظامِ الوطنيِّ للمعلوماتِ رقم (4) لسنة 1990م، وقانونُ المعاملاتِ الإلكترونيةِ رقم (6) لسنة 2022م، مع إشرافِ الهيئةِ الوطنيةِ لأمنِ وسلامةِ المعلوماتِ؛ حيث تفرضُ التشريعاتُ ضرورةَ الموافقةِ المسبقةِ، وشفافيةَ الأغراضِ، وحمايةَ البياناتِ الحساسةِ، والحصولَ على إذنٍ قبلَ إنشاءِ مشاريعَ خدميةٍ تعتمدُ على بياناتِ المواطنين.

وبالنظرِ إلى مسودةِ مشروعِ قانونِ النظامِ الوطنيِّ للمعلوماتِ الليبيِّ الصادرِ في 8 أكتوبر 2022م، فإنه يهدفُ إلى تحديثِ المنظومةِ المعلوماتيةِ عبرَ استبدالِ القانونِ رقم (4) لسنة 1990م؛ لتعزيزِ حوكمةِ البياناتِ، وضمانِ سهولةِ تبادلِها بين المؤسساتِ، وحمايةِ الخصوصيةِ الشخصيةِ.

وقد تمَّ رفعُ هذه المسودةِ من قِبلِ الهيئةِ المكلفةِ من الهيئةِ العامةِ للمعلوماتِ لاتخاذِ الإجراءاتِ التشريعيةِ اللازمةِ، لكن لا يوجدُ ما يشيرُ إلى صدورِ قانونٍ نهائيٍّ ملزمٍ وتفعيلِه رسمياً حتى هذا الوقتِ.

ومن الأسسِ القانونيةِ لجمعِ ومعالجةِ البياناتِ في ليبيا:

1- **الموافقة المسبقة:** يجبُ الحصولُ على موافقةٍ كتابيةٍ وصريحةٍ من صاحبِ البياناتِ قبلَ جمعِها أو معالجتِها، ولا يجوزُ معالجتُها في غيرِ الأغراضِ التي جُمعت من أجلِها.
2- **القانون رقم (4) لسنة 1990م (النظام الوطني للمعلومات):** ينظمُ سريةَ البياناتِ الحكوميةِ والشخصيةِ، ويفرضُ آلياتٍ لحمايةِ الوصولِ إليها.
3- **قانون المعاملات الإلكترونية رقم (6) لسنة 2022م:** يحددُ التزاماتِ مقدمي خدماتِ التصديقِ الرقميِّ، ويحظرُ التزويرَ أو انتحالَ الشخصيةِ، ويعاقبُ على مخالفةِ القواعدِ الخاصةِ بحمايةِ البياناتِ الشخصية.
4- **إذن الجهة المختصة:** حيث تطلبُ الهيئةُ العامةُ للمعلوماتِ عدمَ بدءِ أيِّ مشاريعَ تعتمدُ على البياناتِ الشخصيةِ قبلَ أخذِ إذنٍ مسبقٍ.
5- **حماية البيانات الشخصية:** حيث يُحظرُ تبادلُ بياناتٍ شخصيةٍ مع جهاتٍ خارجيةٍ دون توافرِ ضماناتٍ قانونيةٍ مماثلةٍ (https://libya.rmg-sa.com).

وبالتالي، نستخلصُ إلى أنه لا يعدُّ جمعُ البياناتِ الشخصيةِ في ليبيا حالياً متوافقاً بشكلٍ كاملٍ وشاملٍ مع اللائحةِ العامةِ الأوروبيةِ (GDPR)؛ نظراً لغيابِ قانونٍ وطنيٍّ موحدٍ وشاملٍ لحمايةِ البياناتِ. ومع هذا، توجدُ جهودٌ تنظيميةٌ مثلَ اللوائحِ المصرفيةِ الحديثةِ لعام 2025م، التي تتبنى معاييرَ دوليةً لحمايةِ البياناتِ الماليةِ، بما في ذلك التخزينُ المحليُّ للبياناتِ.

المطلب الثاني: المسؤولية القانونية عن انتهاك البيانات الشخصية:

المسؤوليةُ عن انتهاكِ البياناتِ الشخصيةِ في اللائحةِ العامةِ الأوروبيةِ (GDPR) هو التزامُ (المتحكمِ) و(المعالجِ) قانوناً بتعويضِ الأفرادِ عن أيِّ أضرارٍ ماديةٍ أو معنويةٍ، وتحمُّلِ غراماتٍ باهظةٍ قد تصلُ إلى 20 مليون يورو أو 4% من الإيراداتِ السنويةِ.

وفيما يخصُّ الإبلاغَ عن هذه الانتهاكاتِ، فقد نصت عليه المادتان (33) و(34) من اللائحةِ العامةِ لحمايةِ البياناتِ، اللتان تُلزمانِ المتحكمَ بإبلاغِ السلطاتِ خلال 72 ساعةً.

كما تحددُ المواد (82 - 84) المسؤوليةَ المدنيةَ (التعويض) والغراماتِ الإداريةَ (حتى 4% من الإيرادات السنوية). وأهمُّ تفاصيلِ المسؤوليةِ القانونيةِ عن انتهاكِ البياناتِ الشخصيةِ في (GDPR) الآتي:

- المادة (33): تُلزمُ المتحكمَ بإبلاغِ سلطةِ الإشرافِ المختصةِ بخرقِ البياناتِ خلال 72 ساعةً من علمِه به.
- المادة (34): تُلزمُ بإبلاغِ الأفرادِ المتضررين مباشرةً إذا كان الخرقُ يشكلُ خطراً مرتفعاً على حقوقِهم وحرياتِهم.
- المادة (82): الخاصة بالمسؤولية والتعويض والتي تمنحُ أيَّ شخصٍ الحقَّ في التعويضِ من المتحكمِ أو المعالجِ عن الأضرارِ الماديةِ أو غيرِ الماديةِ الناجمةِ عن خرقِ اللائحةِ.
- المادة (83): والخاصة بالغرامات الإدارية، والتي تفرضُ غراماتٍ ماليةً ضخمةً تصلُ إلى 20 مليون يورو أو 4% من إجمالي الإيراداتِ العالميةِ السنويةِ للشركةِ.
- المادة (28): والخاصة بالمسؤولية المشتركة تنصُّ على أنَّ المسؤوليةَ تكونُ مشتركةً وتشملُ المعالجين أيضاً (الموردين) للبيانات في حالِ تقصيرهم (اللائحة العامة لحماية البيانات (GDPR)، 2026).

أما في التشريعاتِ الفرنسيةِ، فتستندُ المسؤوليةُ عن انتهاكِ البياناتِ الشخصيةِ إلى منظومةٍ صارمةٍ تجمعُ بين القانونِ المدنيِّ وقانونِ العقوباتِ، وتتوافقُ مع اللائحةِ العامةِ لحمايةِ البياناتِ (GDPR)؛ حيث يلتزمُ المسؤولُ عن المعالجةِ بضمانِ أمنِ البياناتِ. وتتراوحُ العقوباتُ بين تعويضاتٍ مدنيةٍ وجرائمَ جنائيةٍ قد تصلُ إلى حدِّ السجنِ لمدةِ خمسِ سنواتٍ وغراماتٍ باهظةٍ (حسبو، د.ت، ص170).

ومن أبرزِ ملامحِ المسؤوليةِ في القانونِ الفرنسيِّ:

- المسؤوليةُ الجنائيةُ: يعاقبُ القانونُ الفرنسيُّ (المادة 16-226 وما بعدها من قانونِ العقوباتِ) على انتهاكِ حرمةِ البياناتِ الشخصيةِ؛ حيث قد تصلُ العقوباتُ إلى السجنِ لمدةِ 5 سنواتٍ وغرامةٍ تقاربُ 30,000 يورو.
- المسؤوليةُ المدنيةُ: يحقُّ للأشخاصِ المتضررين المطالبةُ بالتعويضِ عن الأضرارِ الماديةِ والمعنويةِ الناتجةِ عن سوءِ استخدامِ بياناتِهم أو تسريبِها، وذلك بناءً على قواعدِ المسؤوليةِ التقصيريةِ.
- سلطةُ الرقابةِ (CNIL): تتولى "اللجنةُ الوطنيةُ للمعلوماتيةِ والحرياتِ" دورَ الرقيبِ، وتمتلكُ صلاحيةَ فرضِ عقوباتٍ إداريةٍ وماليةٍ كبيرةٍ على المؤسساتِ التي تخالفُ شروطَ معالجةِ البياناتِ.
- التزاماتُ المعالجِ: يجبُ الحصولُ على موافقةٍ صريحةٍ وواضحةٍ من أصحابِ البياناتِ قبلَ جمعِها، مع الالتزامِ بأمنِ البياناتِ ونقلِها الآمنِ.

وبالتالي، فإنَّ حمايةَ البياناتِ الشخصيةِ في التشريعاتِ الفرنسيةِ تُعدُّ جزءاً لا يتجزأُ من الحقِّ في الخصوصيةِ، ويتمُّ تطبيقُها بصرامةٍ على المعالجاتِ الإلكترونيةِ(العاكوم، 2000، ص74-75).

وبالتالي فإن التشريعات الفرنسية تطبق اللائحة العامة لحماية البيانات الشخصية (GDPR) حيث تعملُ الهيئةُ الوطنيةُ للمعلوماتيةِ والحرياتِ (CNIL) كسلطةٍ رقابيةٍ لضمانِ المعالجةِ القانونيةِ والشفافيةِ، مع منحِ الأفرادِ حقوقاً واسعةً وشاملةً كالتصحيحِ، والحذفِ، والاضافة وغيرها من الحقوق الأخرى بموجبِ القانونِ الفرنسيِّ.

أما عن التشريعِ المصريِّ، فقد حرصَ المشرعُ المصري في شأن مكافحةِ جرائمِ تقنيةِ المعلوماتِ على الآتي:

- للجنة التحقيقِ المختص بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين لمدة لا تزيد عن ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة يعاقب عليها بمقتضى أحكام هذا القانون (المادة (6) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175)، 2018) بواحد أو أكثر مما يأتي:
  أ. ضبطِ، أو سحبِ، أو جمعِ، أو التحفظِ على البياناتِ والمعلوماتِ وأنظمةِ المعلوماتِ، أو تتبعِها في أيِّ دعامةٍ إلكترونيةٍ أو حاسبٍ.
  ب. البحثِ، والتفتيشِ، والدخولِ، والنفاذِ إلى برامجِ الحاسبِ وقواعدِ البياناتِ والأجهزةِ تحقيقاً لغرضِ الضبطِ.

وأبرزِ عقوبات انتهاك البيانات الشخصية في التشريعِ المصريِّ رقم (175) لسنة 2020م كما يلي:

- الاعتداء على الخصوصية: حيث نصت عليها المادة (25) من القانون وتفرض عقوبة الحبس مدة لا تقل عن 6 أشهر وغرامة من 50,000 إلى 100,000 جنيه لكل من اعتدى على مبادئ القيم الأسرية أو حرمة الحياة الخاصة.
- معالجة البيانات الشخصية: حيث نصت عليها المادة (26) وفرضت عقوبة الحبس مدة لا تقل عن سنتين ولا تتجاوز 5 سنوات، وغرامة من 100,000 إلى 300,000 جنيه لمن تعمدَ استخدامَ تقنيةِ معلوماتٍ لمعالجةِ البياناتِ الشخصيةِ للغيرِ وربطِها بمحتوىً مخلٍّ بالآدابِ العامةِ.
- الدخول غير المشروع: نصت عليهما المادتان (14-15) من القانون المصري، حيث يعاقب بالحبس مدة لا تقل عن سنة، وغرامة من 50,000 إلى 100,000 جنيه لكل من دخل موقعاً أو حساباً خاصاً أو نظاماً معلوماتياً دون وجه حق.
- وغيرها من العقوبات الإضافية الأخرى والتي يترتب عليها إتلاف، أو تغيير، أو نسخ البيانات الشخصية، بحيث تزيد العقوبة لتصبح الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن 100,000 جنيه (قانون مكافحة جرائم تقنية المعلومات المصري رقم (175)، 2018).

وفرض هذه العقوبات في التشريع المصري جاء متوافقاً مع التطور السريع الذي لحق بوسائل تقنية المعلومات الحديثة كالتجسس الإلكتروني؛ إذ أن الوسائل الإلكترونية أتاحت وسائل رقابة عالية سمعية، ومرئية، ومقروءة، فأصبحت هناك قدرة عالية على جمع المعلومات ومعالجتها إلكترونياً (مغبغب، د.ت، ص161).

ونتفق مع الرأي الذي ينادي بأهمية توفير الحماية القانونية للبيانات الشخصية في وقتنا الحاضر، وخاصة بعد ظهور العلاقة القوية بين التقنيات الحديثة والحق في الخصوصية من خلال عمليتي تجميع المعلومات الشخصية ومشاركتها (سعيد، https://coeia.ksu.edu.sa).

أما في القوانين الليبية، وخاصة قانون الجرائم الإلكترونية رقم (5) لسنة 2022م، فيعاقب عن انتهاك البيانات الشخصية بالحبس والغرامة المالية، لتشمل هذه العقوبات الحبس مدة لا تقل عن سنة وغرامات تصل إلى 10,000 دينار ليبي عند الدخول غير المشروع أو إفشاء البيانات وتزيد هذه العقوبة في حال التشهير أو الابتزاز.

حيث تضمن هذا القانون مجموعة من المواد التي تهدف إلى تنظيم استخدام الانترنت ووسائل التقنية الحديثة، وحماية الأفراد من الانتهاكات والجرائم التي قد ترتكب عبرها.

ونعرض هنا بعضاً من المواد الأساسية التي تسلط الضوء على كيفية معالجة التشريع الليبي لهذه الجرائم الإلكترونية، أو ضمان حماية الخصوصية والنظام العام: (قانون الجرائم الإلكترونية رقم (5)، 2022)

- المادة (10) التأثير في النظام الإلكتروني: حيث تُجرّم هذه المادة الوصول غير المشروع إلى بيانات الأفراد الشخصية أو حساباتهم الإلكترونية.
- المادة (12) الدخول غير المشروع: كذلك تُجرّم هذه المادة الدخول إلى أجهزة الحاسب الآلي الخاصة بالأفراد دون إذنهم.
- المادة (22) مضايقة الغير: كذلك تُجرّم هذه المادة مضايقة الأفراد عبر الإنترنت أو بأي وسيلة إلكترونية أخرى بقصد إشباع رغبة جنسية.
- المادة (47) التصنت غير المشروع: حيث تُجرّم هذه المادة التجسس على اتصالات الأفراد عبر الإنترنت دون إذنهم.

كذلك من تطبيقات قانون العقوبات الليبي حول هذه المسألة نجد:

- المادة (49) من تطبيق قانون العقوبات والقوانين المكملة: والتي تهدف إلى ضمان عدم وجود فجوات في الحماية القانونية للأفراد من الجرائم التي تُرتكب باستخدام وسائل تقنية المعلومات.

ولكن بالنظر إلى واقع حماية البيانات الشخصية في ليبيا، نجد أن التشريع الليبي لا يوفر حماية كاملة وشاملة للبيانات الشخصية وفقاً للمعايير الدولية الحديثة؛ فرغم وجود نصوص متفرقة في قانون العقوبات، وقانون الجرائم الإلكترونية، وقانون النظام الوطني للمعلومات رقم (4) سنة 1990م، إلا أنه يفتقر لقانون موحد متخصص لحماية البيانات مثل (GDPR)، مما يجعل الحماية الحالية جزئية وتعتمد على قوانين عامة.

الخاتمة:

تعرضنا في هذا البحث الحماية الدستورية والقانونية للبيانات الشخصية دراسة تحليلية مقارنة في اللائحة العامة الأوروبية (GDPR) وبعض من التشريعات المقارنة كالتشريع الفرنسي والمصري والليبي، ثم عرجنا إلى الإطار القانوني والتنظيمي لحماية هذه البيانات في كلٍّ من التشريعات المقارنة.

ومن ثم تناولنا في المبحث الثاني الحماية الدستورية للبيانات الشخصية في التشريعات المقارنة، سواء في اللائحة العامة الأوروبية أو التشريعات الأخرى (الفرنسي والمصري والليبي)، وكيف كفلت الدساتير أو

القوانين حمايةً لهذه البيانات من حيث وضع ضوابط معينة لجمع هذه البيانات ومعالجتها، ومن ثم تقرير حمايةٍ لها من الانتهاكات الجسيمة التي تلحق بها، وفرض عقوبات وغرامات مالية على انتهاك هذه البيانات الشخصية؛ كونها تتعلق بحقوق الشخص المعنيّ بهذه البيانات.

النتائج:

1- تعتبر اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، والمعمول بها منذ عام 2018م، حجر الأساس لتشريعات الخصوصية الرقمية.
2- المشرع الفرنسي كان أسبق في تحديد البيانات الشخصية، بل وضع تعريفاً حديثاً للبيانات الشخصية.
3- أصدر المشرع المصري قانون حماية البيانات رقم (151) لسنة 2020م؛ لمواجهة تفاقم الاعتداءات على البيانات الشخصية بما استدعى تدخلاً من جانب المشرع، وكذلك شمولها بالحماية الدستورية.
4- اهتمام المشرع المصري بمواكبة التطور ووضع قانوناً للبيانات الشخصية، وإن أصابه بعض القصور في التشريعات، ولكنها خطوةٌ على الطريق.
5- يفتقر النظام القانوني الليبي إلى تشريعٍ عصريٍّ وحديث ينظم جمع ومعالجة وتخزين البيانات الشخصية، مشابهٍ للائحة العامة لحماية البيانات (GDPR).
6- تعتمد الحماية الحالية للبيانات الشخصية في التشريع الليبي على نصوصٍ مبعثرةٍ في قوانين مختلفة؛ مما يجعلها غير كافيةٍ لمواجهة التحديات الرقمية الحديثة.

التوصيات:

1- نوصي المشرع الليبي بضرورة وضع تشريعٍ مستقلٍ لحماية البيانات الشخصية، لا يقتصر فقط على قوانين الجرائم الإلكترونية، بل ينظم كيفية جمع، ومعالجة، وتخزين، وتداول البيانات الشخصية الإلكترونية.
2- فرض التزاماتٍ واضحةٍ على "المتحكم في البيانات" (الجهات التي تجمعها) بضمان أمن المعلومات، ووضع أدواتٍ لرسم خرائط البيانات وتقييم تأثير حماية البيانات.
3- تجريم الاعتداء على البيانات الشخصية؛ سواء كان ذلك عبر سرقتها، أو تعديلها غير المشروع، أو إفشائها.
4- على الجهات التي تتعامل مع البيانات الشخصية للمستخدمين أن يكون تعاملهم وفق غايةٍ محددةٍ ومشروعة، وألا يتم الاحتفاظ بها بعد انتهاء الغرض الذي جُمعت من أجله.
5- تدريس مواد المعلوماتية في جميع كليات الحقوق والمعاهد الإدارية.
6- ضرورة أن تكون علاقة المتحكم بالمعالج في القانون الليبي بناءً على تعليماتٍ تعاقدية واضحةٍ، أي أن تكون في صورة تعاقدية.

المراجع:

أولاً – الكتب والبحوث:

- أنطونيوس، بولين، وجمال عبد الناصر. (د.ت). الحماية الجنائية من أشكال المساس بحرمة الحياة الخاصة عبر المكالمات والصور: دراسة مقارنة. (د.ن).
- حسبو، عمرو أحمد. (د.ت). حماية الحريات في مواجهة نظم المعلومات: دراسة مقارنة. دار النهضة العربية.
- حسين، ياسر سيدج. (2014). الحق الدستوري في الحصول على البيانات: دراسة مقارنة [رسالة جامعية/بحث]. كلية الحقوق، جامعة القاهرة.
- الزوي، مشعل عثمان. (2021). الحماية الجنائية للبيانات الشخصية الإلكترونية: دراسة في القانون الليبي المقارن. مجلة العلوم الشرعية والقانونية، جامعة بنغازي.
- العاكوم، وليد. (2000). مفهوم وظاهرة الإجرام المعلوماتي [بحث مقدم]. مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة.
- عبد الرحمن، محمد محمود. (1990). نطاق الحق في الحياة الخاصة (ط1). دار النهضة العربية.

- عبيد، محمد كامل. (2001). مبدأ المشروعية. دار النهضة العربية.
- لطفي، حسام. (1994). عقود خدمات المعلومات: دراسة مقارنة. (د.ن).
- مغبغب، نعيم. (د.ت). مخاطر المعلوماتية والإنترنت: المخاطر على الحياة الخاصة وحمايتها: دراسة مقارنة. دار النهضة العربية.

ثانياً – المقالات العلمية والمواقع الإلكترونية:

- التهامي، سامح عبد الواحد. (2011). حماية القانون للبيانات الشخصية: دراسة في القانون الفرنسي (القسم الأول). مجلة الحقوق، https://www.researchgate.net/35.
- سعيد، فهد عبد العزيز. (د.ت). مفهوم الخصوصية وتاريخها. مركز التميز لأمن المعلومات https://coeia.ksu.edu.sa/.
- مجلة جامعة الإمارات للبحوث القانونية. (2024). الإطار القانوني للمعالجة الإلكترونية للبيانات الشخصية: دراسة تحليلية مقارنة 2022. مجلة جامعة الإمارات للبحوث القانونية.
- مرعي، إيمان. (2017، 15 يناير). الحكومة الإلكترونية كمدخل للإصلاح الإداري. مجلة رؤية مصرية. مركز الأهرام للدراسات التاريخية والاجتماعية /https://accronline.com .
- مؤسسة .RMG (د.ت). حماية البيانات في ليبيا: دليل شامل/https://libya.rmg-sa.com .
- Jacqueline, P. E. (2002). L'identité biologique en matière. In Pousson (Ed.), Bruylant, S1, 481.

ثالثاً – القوانين والوثائق الرسمية:

- دستور جمهورية مصر العربية. (2014). المادة (68).
- قانون رقم (151) لسنة 2020. قانون حماية البيانات الشخصية المصري. الوقائع المصرية.
- قانون رقم (175) لسنة 2018. قانون مكافحة جرائم تقنية المعلومات المصري ولائحته التنفيذية.
- قانون رقم (5) لسنة 2022. قانون الجرائم الإلكترونية (ليبيا).
- قانون رقم (801) لسنة 2004. القانون الفرنسي الخاص بحماية البيانات الشخصية.
- اللائحة العامة لحماية البيانات (GDPR) /https://gdpr-info.eu. (2018).
- مجلس النواب المصري. (2020). تقرير اللجنة المشتركة حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية.

References

First – Books and Research:

• Antonius, Pauline, and Gamal Abdel Nasser. (n.d.). Criminal Protection Against Forms of Infringement on Privacy Through Calls and Images: A Comparative Study. (n.p.).

• Hasabo, Amr Ahmed. (n.d.). Protecting Freedoms in the Face of Information Systems: A Comparative Study. Dar Al-Nahda Al-Arabiya.

• Hussein, Yasser Seidj. (2014). The Constitutional Right to Access Data: A Comparative Study [University Thesis/Research]. Faculty of Law, Cairo University.

• Al-Zawi, Meshaal Othman. (2021). Criminal Protection of Electronic Personal Data: A Study in Comparative Libyan Law. Journal of Sharia and Legal Sciences, University of Benghazi.

• Al-Akoum, Walid. (2000). The Concept and Phenomenon of Cybercrime [Research Paper]. Conference on Law, Computers, and the Internet, College of Sharia and Law, United Arab Emirates University.

• Abdel Rahman, Mohamed Mahmoud. (1990). The Scope of the Right to Privacy (1st ed.). Dar Al-Nahda Al-Arabiya.

• Obeid, Mohamed Kamel. (2001). The Principle of Legality. Dar Al-Nahda Al-Arabiya.

• Lotfi, Hossam. (1994). Information Service Contracts: A Comparative Study. (n.p.).

• Maghbagh, Naeem. (n.d.). Information Technology and Internet Risks: Risks to Privacy and its Protection: A Comparative Study. Dar Al-Nahda Al-Arabiya.

Second – Scientific Articles and Websites:
•Al-Tohamy, Sameh Abdel-Wahed. (2011). Legal Protection of Personal Data: A Study in French Law (Part One). Journal of Law, 35. https://www.researchgate.net/
• Saeed, Fahd Abdel-Aziz. (n.d.). The Concept of Privacy and its History. Center of Excellence for Information Security. https://coeia.ksu.edu.sa/
• Khalleefah, A. B., Abdalqadir, M. A., & Salem, A. A. (2025). Towards a New Theory of Civil Liability in the Context of Artificial Intelligence Systems and the Challenges of Reforming the Traditional Theory. *Al-haq Journal for Sharia and Legal Sciences*, 754-770.
• United Arab Emirates University Journal of Legal Research. (2024). The Legal Framework for Electronic Processing of Personal Data: A Comparative Analytical Study. 2022. United Arab Emirates University Journal of Legal Research.
• Dr.Hala mohamed imam mohamed. (2024). Legal challenges in the use of artificial intelligence techniques in editing and refereeing scientific research. Al-Haq Journal for Sharia and Legal Sciences, 86-109. https://doi.org/10.58916/alhaq.vi.238
• Hind aldawy mosbah. (2025). Inspection in electronic media. Al-Haq Journal for Sharia and Legal Sciences, 12(2), 326-339. https://doi.org/10.58916/alhaq.v12i2.361
• Marai, Iman. (2017, January 15). E-Government as an Approach to Administrative Reform. Egyptian Vision Magazine. Al-Ahram Center for Historical and Social Studies. https://accronline.com/ • RMG Foundation. (n.d.). Data Protection in Libya: A Comprehensive Guide. https://libya.rmg-sa.com/ • Jacqueline, P. E. (2002). L'identité biologique en matière. In Pousson (Ed.), Bruylant, S1, 481.

Third – Laws and Official Documents:
• Constitution of the Arab Republic of Egypt. (2014). Article (68).
• Law No. (175) of 2018. Egyptian Cybercrime Law and its Executive Regulations.
• Law No. (5) of 2022. Cybercrime Law (Libya).
• Law No. (801) of 2004. French Personal Data Protection Law.
• General Data Protection Regulation (GDPR) (2018). https://gdpr-info.eu/
• Egyptian House of Representatives (2020). Joint Committee Report on the Draft Law on Personal Data Protection.